

a TON of Grams

We initiate coverage of the Telegram Open Network (TON) project. We chose TON because of its size and importance for the blockchain industry development. The project has raised \$1.7bn in two private offerings – the largest in the crypto industry so far – while respected institutional investors participated in the placement, thus vindicating it. Telegram gave investors little time to analyze the offering and provided no additional updates after the sale was done. Nevertheless, the demand was so huge that the issuer increased the number of offered coins (Grams).

Conventional asset managers are being drawn to the blockchain industry, and the ICO has become a meaningful tool to raise funds. However, conventional investors usually lack an understanding of the underlying technology, while tech specialists, in turn, struggle to convey the concept to the financial community. We can bridge the gap thanks to having both blockchain development and investment expertise in our team, we believe.

Blockchain technology goes far beyond cryptocurrencies, which are just the gasoline in public blockchain systems. Just as the Internet – the Internet of Information – transformed our lives with the exchange of information, blockchain – the Internet of Value – can reshape the world by digitizing and making practically anything of value to humankind transferrable online. Decentralization is the breakthrough, the holy grail of blockchain technology, which has the potential to make many intermediaries and central authorities redundant.

However, regardless of how promising blockchain technology sounds, it remains far from mainstream adoption. Aside from obstacles such as legal restrictions and the volatility of cryptoassets, there are huge challenges on the technology side. Two main hurdles stand in the way of mass adoption and universality for contemporary blockchains: **Scalability** and **Interoperability**.

TON is among the breakthrough projects aiming to build a system that does not inherit those obstacles. Aware of the skepticism towards Telegram among crypto community, our technology counsel, an expert from QIWI Blockchain Technologies, has done a close reading of the White Papers of TON and its key competitors. While the TON document is poorly written, its concepts generally make sense and could be implemented. Due to the open source nature of the blockchain industry, other concurrently developing projects, such as Polkadot, Cosmos, or Dfinity, could be simultaneously competitive and supportive. However, unlike those projects, Telegram already has a critical mass of 200mn users to drive adoption.

An ambitious project in a nascent industry, TON will emerge in a competitive environment and faces many risks. Given the magnitude of proposed technological and engineering changes and their still-theoretical nature, successful, timely execution of the project will be extremely challenging. This internal risk is the highest for TON, in our view. At the same time, the project faces many external risks. The most important is competition, which comes from both contemporary messengers and blockchain projects, but legal risks are also considerable.

We introduce our in-house valuation method, attempting to solve one of the key unknowns for cryptoassets. The end-2019 Rational Value for Gram is \$5.90, according to our estimation¹. This represents a 4.4x potential upside for investors that participated in the second placement round. The TON Reserve, according to the pricing formula and additional statements made in the publicly available White Paper, should sell the next coin for at least \$3.62, which is 39% below the Rational Value.

¹ We provide details as to how we arrive at such an estimation and what assumptions we base it on in the valuation-dedicated (final) chapter of this report. No statement in this report is intended to be nor may be construed as a profit forecast and there can be no assurance that the assumptions described herein, the returns and targets indicated herein will be achieved.

Sandro Gorduladze
Head of Research
HASH CIB
s.gorduladze@hashcib.com

Rustam Botashev, CFA
Senior Analyst
HASH CIB
r.botashev@hashcib.com

Technology Counsel:

Peter Kalambet
System Architect
QIWI Blockchain Technologies
kalambet@qiwi.tech

LEGAL DISCLAIMER

THIS DOCUMENT MAY NOT BE DISTRIBUTED IN THE UNITED STATES, AUSTRALIA, CANADA OR JAPAN. THIS DOCUMENT HAS BEEN FURNISHED TO YOU SOLELY FOR YOUR INFORMATION AND MAY NOT BE REPRODUCED OR REDISTRIBUTED TO ANY OTHER PERSON.

This report is in each case disseminated solely to institutions and investment professionals as regulated in the respective jurisdiction, and solely to the extent such dissemination does not breach applicable laws and regulations. If this report is obtained by a person who is not considered to be an eligible investor under applicable local laws in the respective jurisdiction, or is obtained in a jurisdiction where dissemination of this report would be unlawful, this person should not review it, should disregard and/or immediately delete it and undertake their best effort to inform HASH CIB about having received this report by mistake.

THIS DOCUMENT IS PROVIDED SOLELY AS GENERAL INFORMATION ABOUT DEVELOPMENTS IN CRYPTOASSETS. THIS DOCUMENT AND ANY ATTACHMENTS THERETO SHOULD NOT BE CONSTRUED AS CONSTITUTING ANY FORM OF INVESTMENT ADVICE OR RECOMMENDATION, GUIDANCE OR PROPOSAL OF A FINANCIAL NATURE BY HASH CIB.

HASH CIB makes no representation or warranty, express or implied, as to the fairness, accuracy, completeness or correctness of information obtained from sources, nor does HASH CIB accept any liability arising from its use or for ensuring that the recipient complies with applicable laws and regulations. Furthermore, the information contained in this document has not been reviewed or independently verified by HASH CIB or any person acting on its behalf. Any opinions expressed herein are statements of HASH CIB's judgment as of this date and are subject to change without notice. Neither the information nor any opinion expressed constitutes a recommendation, an offer or an invitation to make an offer, to buy or sell any securities or other investment or any options, futures or any other financial instruments. This report does not take on your account and does not take into account any special or individual investment objectives, financial situations or particular needs of any particular person who may receive this report. The services, securities and investments discussed in this report may be neither available to nor suitable for all investors. Investors should seek financial advice regarding the appropriateness of investing in any security or other investment and the investment strategies discussed or recommended in this report and should understand that statements regarding future prospects may not be realized.

HASH CIB is not licensed to carry out any banking or broker services or similar activities in the Russian Federation or anywhere in the world, is not a regulated entity in any jurisdiction, and does not hold any licenses or other permits from any regulatory bodies of any jurisdiction.

HASH CIB and its affiliates assume no fiduciary responsibility or liability for any consequences, financial or otherwise, arising from an investment described herein or from the implementation of any investment strategy. Potential investors should be aware that any direct or indirect investment in any security or investment vehicle described herein is subject to significant risks, including total loss of capital, and there are significant restrictions on transferability and redemption of any such security.

No statement in this report is intended to be nor may be construed as a profit forecast and there can be no assurance that the assumptions described herein, the returns and targets indicated herein will be achieved. Some of the statements in this material may constitute forward-looking statements. Forward-looking statements relate to expectations, beliefs, projections, future plans and strategies, anticipated events or trends and similar expressions concerning matters that are not historical facts. Forward-looking statements in this material involve risks and uncertainty. Forward-looking statements are based on HASH CIB analysts' beliefs, assumptions and expectations of future performance, taking into account all information currently available to HASH CIB. These beliefs, assumptions and expectations can change as a result of many possible events or factors, not all of which are known to HASH CIB or are within HASH CIB's control.

Investors should note that income from such securities or other investments, if any, may fluctuate and that the price or value of such securities and investments may rise or fall. Accordingly, investors may receive back less than was originally invested. Past performance is not necessarily a guide to future performance, future returns are not guaranteed, and a loss of original capital may occur. HASH CIB accepts no liability whatsoever for any direct or indirect losses, damage, or other consequences of any kind that may arise out of the partial or full usage of the materials from its reports. Investors should conduct their own evaluation of risks and should not rely solely on the information presented in any reports provided by HASH CIB. Investors should obtain individual legal, tax, financial, accounting

or other professional advice based on their particular circumstances. Any information relating to the tax status of financial instruments discussed herein is not intended to provide tax advice or to be used by anyone to provide tax advice.

This report does not constitute or contain legal advice. Further, HASH CIB should not in any way be viewed as soliciting, facilitating, brokering or causing any persons within any country to invest in or otherwise engage in transactions that may be prohibited to those persons under relevant law. This report is provided in respect of entities or investments in both Russian domestic and international financial markets (as applicable in each case) and are intended for eligible investors in compliance with the legal and trading regulations of the relevant markets. HASH CIB's reports received by such eligible investors concerning entities or investments that may be sanctioned in other jurisdictions are not directed to, and should not be considered as investment advice in respect of, any transaction invoking such sanctions or involving persons within the jurisdiction of such sanctions, including but not limited to U.S., Canadian, Australian, Japanese, Swiss, European or EU investors. HASH CIB's reports are never to be used for unlawful activity, including activity that is contrary to or circumvents economic sanctions. After having read this report, investors should estimate the legality of their transactions in accordance with the legislation on economic sanctions or other legal acts regulating their investment activities or consult their legal advisers in respect of their own compliance with the applicable laws and trading rules.

THIS DOCUMENT IS STRICTLY CONFIDENTIAL. IT IS BEING SUPPLIED TO YOU SOLELY FOR YOUR INFORMATION AND MAY NOT BE REPRODUCED, REDISTRIBUTED OR PASSED ON, DIRECTLY OR INDIRECTLY, TO ANY OTHER PERSON OR PUBLISHED, IN WHOLE OR IN PART, FOR ANY PURPOSE. IN PARTICULAR, SUBJECT TO CERTAIN EXCEPTIONS, NEITHER THIS DOCUMENT NOR ANY COPY OF IT MAY BE TAKEN OR TRANSMITTED, DIRECTLY OR INDIRECTLY, INTO THE UNITED STATES, AUSTRALIA, CANADA OR JAPAN OR DISTRIBUTED, DIRECTLY OR INDIRECTLY, IN THE UNITED STATES, AUSTRALIA, CANADA OR JAPAN.

THE DISTRIBUTION OF THIS DOCUMENT IN OTHER JURISDICTIONS MAY BE RESTRICTED BY LAW, AND PERSONS INTO WHOSE POSSESSION THIS DOCUMENT COMES SHOULD INFORM THEMSELVES ABOUT, AND OBSERVE, ANY SUCH RESTRICTIONS. ANY FAILURE TO COMPLY WITH THESE RESTRICTIONS MAY CONSTITUTE A VIOLATION OF THE LAWS OF ANY SUCH OTHER JURISDICTIONS. BY ACCEPTING THIS REPORT YOU AGREE TO BE BOUND BY THE FOREGOING INSTRUCTIONS.

THIS DOCUMENT DOES NOT CONSTITUTE OR FORM PART OF, AND SHOULD NOT BE CONSTRUED AS, AN OFFER, SOLICITATION OR INVITATION TO SUBSCRIBE FOR OR PURCHASE ANY SECURITIES, AND NEITHER THIS DOCUMENT NOR ANYTHING CONTAINED HEREIN SHALL FORM THE BASIS OF OR BE RELIED ON IN CONNECTION WITH OR ACT AS AN INDUCEMENT TO ENTER INTO ANY CONTRACT OR COMMITMENT WHATSOEVER. THIS DOCUMENT HAS NOT BEEN PUBLISHED GENERALLY AND HAS ONLY BEEN MADE AVAILABLE TO INSTITUTIONAL INVESTORS. ANY DECISION TO PURCHASE OR SUBSCRIBE FOR SECURITIES MUST BE MADE SOLELY ON THE BASIS OF THE INFORMATION CONTAINED IN THE PROSPECTUS (AND ANY SUPPLEMENTS THERETO) OR OTHER OFFERING CIRCULAR ISSUED IN CONNECTION WITH SUCH OFFERING.

These materials are not for distribution, directly or indirectly, in or into the United States (including its territories and possessions, any State of the United States and the District of Columbia). These materials are not an offer or solicitation to purchase or subscribe for securities in the United States. Securities may not be offered or sold in the United States absent registration with the United States Securities and Exchange Commission or an exemption from registration under the U.S. Securities Act of 1933, as amended.

This document is being distributed to and is directed only at persons in member states of the European Economic Area ("EEA") who are "qualified investors" within the meaning of Article 2(1)(e) of the Prospectus Directive (Directive 2003/71/EC), as amended (and all relevant member states' implementing measures of such directive and such amendments) ("Qualified Investors"). Any person in the EEA who receives this document will be deemed to have represented and agreed that it is a Qualified Investor. Any such recipient will also be deemed to have represented and agreed that it has not received this document on behalf of persons in the EEA other than Qualified Investors or persons in the UK and other member states (where equivalent legislation exists) for whom the investor has authority to make decisions on a wholly discretionary basis. HASH CIB will rely upon the truth and accuracy of the foregoing representations and agreements. Any person in the EEA who is not a Qualified Investor should not act or rely on this document or any of its contents.

In the United Kingdom, this document is being distributed to and is directed only at Qualified Investors who are (I) persons who have professional experience in matters relating to investments falling within article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "Order"); (II) high net worth entities

falling within article 49(2)(a) to (d) of the Order; or (III) otherwise persons to whom it may lawfully be communicated (all such persons together being referred to as “Relevant Persons”). In the United Kingdom, this document is directed only at Relevant Persons, and other persons should not act or rely on this document or any of its contents. In the United Kingdom, any investment or investment activity to which this communication relates is available only to Relevant Persons and will be engaged in only with Relevant Persons.

HYPOTHETICAL PERFORMANCE RESULTS HAVE MANY INHERENT LIMITATIONS, SOME OF WHICH ARE DESCRIBED BELOW. NO REPRESENTATION IS BEING MADE THAT ANY ACCOUNT WILL OR IS LIKELY TO ACHIEVE PROFITS OR LOSSES SIMILAR TO THOSE SHOWN. IN FACT, THERE ARE FREQUENTLY SHARP DIFFERENCES BETWEEN HYPOTHETICAL PERFORMANCE RESULTS AND THE ACTUAL RESULTS SUBSEQUENTLY ACHIEVED BY ANY PARTICULAR TRADING PROGRAM.

ONE OF THE LIMITATIONS OF HYPOTHETICAL PERFORMANCE RESULTS IS THAT THEY ARE GENERALLY PREPARED WITH THE BENEFIT OF HINDSIGHT. IN ADDITION, HYPOTHETICAL TRADING DOES NOT INVOLVE FINANCIAL RISK, AND NO HYPOTHETICAL TRADING RECORD CAN COMPLETELY ACCOUNT FOR THE IMPACT OF FINANCIAL RISK IN ACTUAL TRADING. FOR EXAMPLE, THE ABILITY TO WITHSTAND LOSSES OR TO ADHERE TO A PARTICULAR TRADING PROGRAM IN SPITE OF TRADING LOSSES ARE MATERIAL POINTS WHICH CAN ALSO ADVERSELY AFFECT ACTUAL TRADING RESULTS. THERE ARE NUMEROUS OTHER FACTORS RELATED TO THE MARKETS IN GENERAL OR TO THE IMPLEMENTATION OF ANY SPECIFIC TRADING PROGRAM WHICH CANNOT BE FULLY ACCOUNTED FOR IN THE PREPARATION OF HYPOTHETICAL PERFORMANCE RESULTS AND ALL OF WHICH CAN ADVERSELY AFFECT ACTUAL TRADING RESULTS.

SEE LAST PAGES FOR DISCLOSURES.

INVESTMENT CASE 7

NEW DIGITAL ASSETS	7
THE ICO IS NO LONGER IN ITS INFANCY	7
INVESTORS' FOCUS – SHOW ME THE CODE	9
BLOCKCHAIN TECHNOLOGY CAN RESHAPE THE WORLD	9
TELEGRAM: A FAST AND SECURE MESSENGER	11
TELEGRAM OPEN NETWORK – A TECHNOLOGICAL BREAKTHROUGH	12
COMPETITIVE LANDSCAPE	14
HOW MUCH A GRAM WEIGHS	15
EXECUTION IS THE MAIN RISK	16

THE BLOCKCHAIN TECHNOLOGY REVOLUTION 18

NEW DIGITAL ASSETS	18
THE ICO IS NO LONGER IN ITS INFANCY	20
A BUBBLE IN THE MAKING	22
INVESTORS' FOCUS – SHOW ME THE CODE	23
BLOCKCHAIN TECHNOLOGY CAN RESHAPE THE WORLD	23
WHAT WE TALK ABOUT WHEN WE TALK ABOUT BLOCKCHAIN	23
LET'S DREAM IN COLOR: MOVING BEYOND THE BASICS	25
EVERYTHING COMES AT A COST	26
NO MASS ADOPTION WITHOUT SCALABILITY	27
THREE OBVIOUS BUT "FLAWED" APPROACHES TO SCALABILITY...	28
...LEAD US TO THE SCALABILITY TRILEMMA	29
SCALABILITY: THREE "FLAWLESS" APPROACHES	29
CONSENSUS ALGORITHMS: PROOF-OF-WORK VS. PROOF-OF-STAKE	29
FINALITY: PROBABILISTIC AND COMMERCIAL	30
STATE CHANNELS – A SECOND-LAYER, OFF-CHAIN SOLUTION TO SCALABILITY	32
MAINSTREAM STATE CHANNEL NETWORKS	34
SHARDING – AN ON-CHAIN APPROACH TO TACKLING SCALABILITY	35
INTEROPERABILITY – ANOTHER MUST FOR BLOCKCHAIN'S MAINSTREAM ADOPTION	36
CONCLUSION	39

TELEGRAM OPEN NETWORK – A TECHNOLOGICAL BREAKTHROUGH 40

A FAST AND SECURE MESSENGER	40
THE TELEGRAM OPEN NETWORK ECOSYSTEM	43
AN UNUSUAL BUT VERY SUCCESSFUL COIN OFFERING	43
TON PROJECT COMPONENTS	46
TECHNOLOGY ANALYSIS	49
TON PAYMENTS – THE KILLER APP	49
TON NETWORKING	51
TON SERVICES AND APPLICATIONS	53
Mixed TON Services: TON Storage and TON Proxy	53
On-chain TON Service: TON DNS	54
Off-chain TON applications	54
TON BLOCKCHAIN – AMONG THE MOST AMBITIOUS PROJECTS IN THE INDUSTRY	55

COMPETITIVE LANDSCAPE AND RISKS 58

INTERNAL RISKS	58
TECHNOLOGICAL CONCEPT	58
TON'S DEVELOPMENT AND LAUNCH	59
POST-LAUNCH RISKS	61
EXTERNAL RISKS – MESSAGING APP COMPETITORS	64
ONE OF A KIND IN A CROWDED COMPETITIVE LANDSCAPE	64
FACEBOOK APPEARS TO PLAN STRENGTHENING ITS P2P PAYMENTS	65
800MN PEOPLE USE WeCHAT PAY MONTHLY	66
VIBER, LINE, AND KIK – EVEN LESS OF A THREAT	66
EXTERNAL RISKS – BLOCKCHAIN PROJECT COMPETITORS	67
PAYMENT CHANNEL NETWORKS: BITCOIN LIGHTNING NETWORK	68
PAYMENT CHANNEL NETWORKS: RAIDEN	68
BLOCKCHAINS: EOS	69
BLOCKCHAINS: DFINITY	72
BLOCKCHAINS: POLKADOT	74
BLOCKCHAINS: COSMOS	75
BLOCKCHAINS: ETHEREUM	76
LEGAL RISKS	78

HOW MUCH A GRAM WEIGHS 81

VALUATION METHODS LAG, AS USUAL	81
THE EMERGING FIELD OF MULTIPLES	81
<i>NVT ratio</i>	82
<i>Network to Metcalfe ratio</i>	83
STORE OF VALUE	85
THE EQUATION OF EXCHANGE	86
GRAM PLACEMENT SETS UP THE MINIMAL PRICE FOR THE NEXT ISSUANCE	88
RATIONAL NETWORK VALUE GIVES 63% UPSIDE ON CONSERVATIVE ASSUMPTIONS	88

APPENDIX 92

GLOSSARY 97

Investment Case

The difference between a bad electronic cash system and well-developed digital cash will determine whether we will have a dictatorship or a real democracy.

David Chaum

Cryptoassets celebrate their tenth anniversary this year. The crypto boom gave birth to a new fundraising tool – ICO – and crypto-focused funds are mushrooming. Raising \$1.7bn from just 175 investors and registering the placements with US SEC, Telegram changed the ICO landscape. Blockchain technology goes far beyond cryptocurrencies – it can reshape the world by digitalizing and making practically anything valuable to humankind transferrable online. Decentralization is the holy grail of blockchain technology that jeopardizes the existence of intermediaries and the dominance of central authorities and governments. However, blockchain remains far from mainstream adoption, as scalability and interoperability hurdles stand in the way of universality. TON represents an ambitious attempt to build state-of-the-art network architectures with the ability to create blockchains for blockchains but without those inherited problems. With its 200mn monthly active users, Telegram already has the pre-existing critical mass necessary for its ecosystem to quickly expand and gain widespread adoption. We introduce our in-house valuation method attempting to solve one of the key unknowns for cryptoassets. The Rational Value for end-2019 Gram is \$5.90, according to our estimation. This represents a 4.4x upside to the investors that participated in the second placement round. TON will emerge in a very competitive environment and faces many risks both internally (execution) and externally (competition and legal).

New digital assets

The cryptocurrency era emerged on the heels of the collapse of financial markets in 2008 when a still-unknown person or a group using the alias Satoshi Nakamoto published *Bitcoin: A Peer-to-Peer Electronic Cash System*. On 3 January 2009 Satoshi mined block number zero, delivering a pre-mined one million bitcoins (BTC) to their Bitcoin address and thus launching what would become a multibillion-dollar industry and spurring the development of blockchain technology.

Ethereum, proposed in 2013 and going live in 2015, represented a quantum leap in the evolution of blockchain technology. Designed by a Russian-born Canadian, Vitalik Buterin, Ethereum is much more than Bitcoin's decentralized payment system. Built to become a "world computer", it is a blockchain platform for applications. Ethereum pioneered the smart contract² now used in most blockchains and created a Turing-complete³ virtual machine. These features paved the way for a subsequent avalanche of digital token issues. Some 79% of existing crypto token issues are based on Ethereum.

The full potential of blockchain technology is still to be realized. Public consciousness is focused on just one use case, pseudo-anonymous⁴ money transfer. And this is understandable given that governments worldwide are actively trying to squeeze money out of people to finance their ever-growing expenses. Seeing payments as the only utility function of blockchain is like seeing email as the only utility function of the Internet. But without the potential of payment systems, the industry would have not been able to attract so much funding, and research and development would have been left to a few academics and enthusiasts.

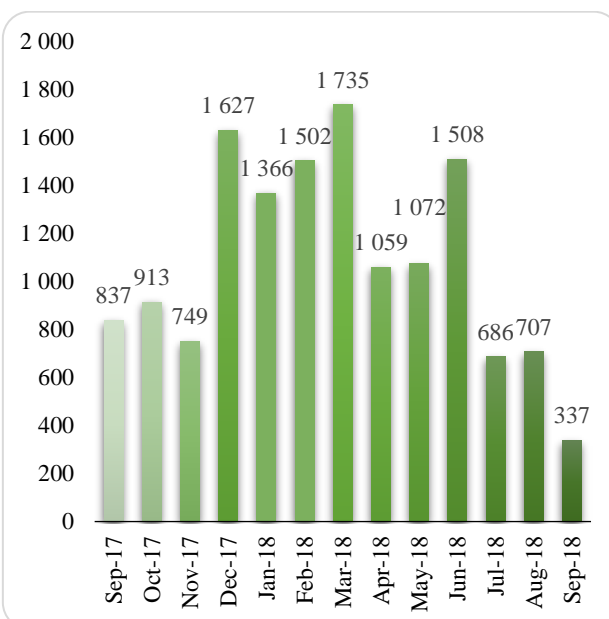
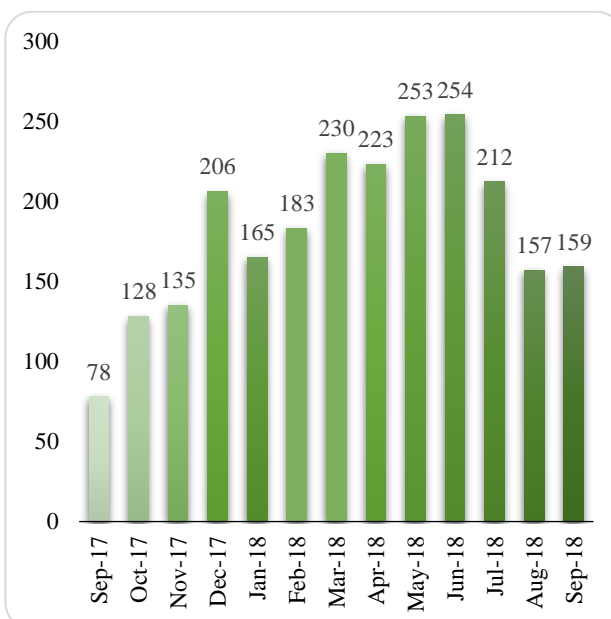
The ICO is no longer in its infancy

Crypto hype gave birth to a unique fundraising tool – the Initial Coin Offering. In 2017 total investments in ICOs reached over \$4bn. Yet the combination of just two of 2018's biggest fundraisers to date – EOS's year-long offering and concurrent secondary market, and Telegram's private placement, which raised \$4bn and \$1.7bn, respectively – were larger than the whole market the previous year. And even excluding those two, combined ICO volume YTD has hit the \$9.1bn mark, although the number of ICOs has fallen sharply since their June peak.

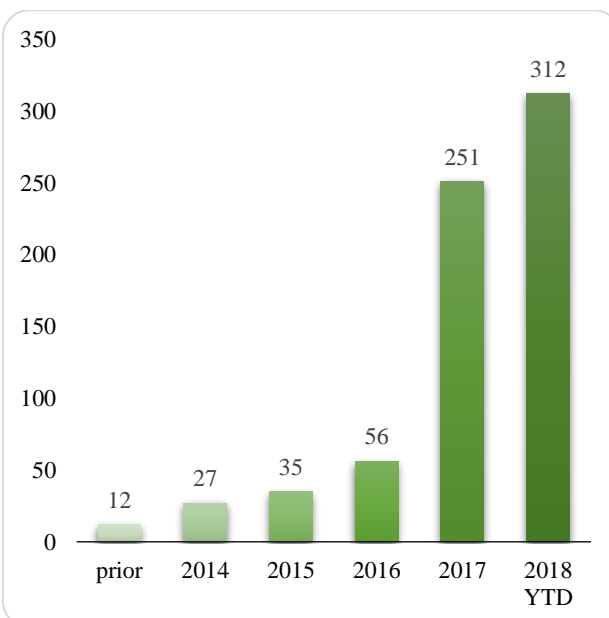
² A [smart contract](#) is a computer program intended to digitally facilitate, verify, or enforce the performance of a virtual contract. It has a predefined set of outputs (virtual actions) each responding to a certain type (or groups) of input(s), which thus automates the execution of virtual actions if conditions precedent for such actions are met. Smart contracts allow the performance of credible transactions without third parties; such transactions are trackable and irreversible.

³ A [Turing-complete](#) or computationally universal computer system is one that can process, store while using (multi-task), and long-term store data – like CPU, RAM and disk storage systems on a personal computer. A Turing-complete system is aware of its current and previous states and can run all types of computer programs.

⁴ "Anonymous" because initially we do not know who the account owner is, and "pseudo" as each transaction and the histories of its participants are traceable on most blockchain networks.

Funds raised on ICOs (\$mn), excluding EOS and TON**Number of ICOs**Source: [ICObench](#)

Traditional institutional investors are slowly joining in. Some 195 crypto funds were launched last year, compared to 56 in the five previous years. The total estimated number of funds is currently over 300 with overall AUM of \$7-10bn, according to [Autonomous Research](#). News of leading venture firms and top-tier traditional funds⁵ investing signal big money's interest in crypto despite the bear market. Telegram's placement has changed the ICO arena. It is likely to encourage other established companies to follow suit. Facebook, for example, is reportedly considering issuing its own cryptocurrency. The crypto boom is creating investment opportunities, simplifying fundraising, and facilitating business development.

Cumulative number of crypto funds**Assets under management (\$mn)**Source: [Autonomous Research](#), [Crypto Fund Research](#)

⁵ The main hurdle for the latter should be resolved by the proper licensing of crypto custody providers to financial institutions, an effort currently underway in the US, with EU/EFTA, Japan and other crypto-friendly jurisdictions following suit.

Investors' focus – show me the code

We divide blockchain projects into two broad categories – applied and breakthrough. Applied projects, which try to improve an existing business or facilitate processes, represent the first, massively crowded category. For example, such projects build platforms (predominately based on Ethereum) that directly connect producers to customers, eliminating intermediaries. Although such solutions do add real value, their blockchain-based distributed applications (DApps) can easily operate on the Ethereum coin, ether (ETH), and, as such, do not need native tokens. Therefore, we believe the majority of such tokens are likely to be short-lived.

The second category, breakthrough projects, is sparsely populated. Projects in this category attempt to offer solutions for the whole blockchain industry, invent new approaches, or develop unique technologies. Such projects tend to take into consideration the early build-out phase of blockchain infrastructure and cater to the needs of developers and early adopters, who will then build the products for end-users. Such projects will need to have both native blockchains and native coins. Provided the projects are successfully implemented, these cryptocurrencies are likely to be in high demand by end-users, and therefore attractive to investors. Although such projects can also fail, the risk-reward balance is very appealing, in our view.

Show me the code vs. show me the money. In conventional finance, to make an investment decision, analysts try to forecast the future cash flow generated by a company or project. Equipped with financials, they try to judge the current state of a business and make assumptions about its future development. Financials supplement, or sometimes substitute for, in-depth knowledge of the industries that an entity operates in. But crypto investors do not have such luxuries, as the majority of blockchain projects do not and will not have financials. **A diligent crypto investor needs to have a grasp of blockchain technology, an overview of the competitive landscape, and an understanding of the software engineering to identify the long-term winners.**

Blockchain technology can reshape the world

Blockchain technology goes far beyond cryptocurrencies, which are just the gasoline in public blockchain systems. Just as the Internet – the Internet of Information – transformed our lives with e-mail, e-commerce, and other exchange of information, blockchain – the Internet of Value – can reshape the world by digitizing and making practically anything of value to humankind transferrable online.

A **blockchain** is a form of a distributed ledger and a peer-to-peer (P2P) network of nodes that store data in blocks that are consecutively chained to each other⁶. The beauty of the technology is that blockchains are immutable and can be **decentralized** – without a single decision maker or governor, all governance is enforced through the consensus of participating nodes.

Decentralization is the breakthrough, the holy grail of blockchain technology; potentially, it can make many intermediaries and central authorities redundant. Decentralized blockchains are *trustless*: left to the consensus of participating nodes, they do not need trusted third parties to keep and run the ledgers. They are also censorship-resistant, as there is no authority to alter a record or to stop a transaction from going through. Such blockchains are also more robust in the face of malicious behavior. Participating nodes do not have to trust each other to reach consensus. Combined with immutability, these qualities should allow blockchain technology to reshape many economic sectors for the goodwill of society.

Over the long term, no business making money serving as a trusted third party will benefit from trustless blockchain development, we believe. Quite the opposite: this technology will dig the graves of such businesses, and therefore they are likely to resist its development. The most notable victims would be contemporary financial institutions, such as banks, exchanges, and payment systems. However, this threat will take a long time to materialize. In the meantime, some intermediaries will seek to benefit from the technology and build private blockchains to cut costs.

Trustless blockchains and cryptocurrencies could also jeopardize the dominance of governments. Blockchains could potentially substitute government agencies in keeping and updating trusted records, such as the registration of births, marriages, or property transfers. Blockchains could revolutionize current electoral voting processes by integrating identity management and cryptography to maintain the confidentiality, resilience, security, and integrity of an election. Furthermore, cryptocurrencies could theoretically complement official fiat money, drastically reducing states' control over the economy.

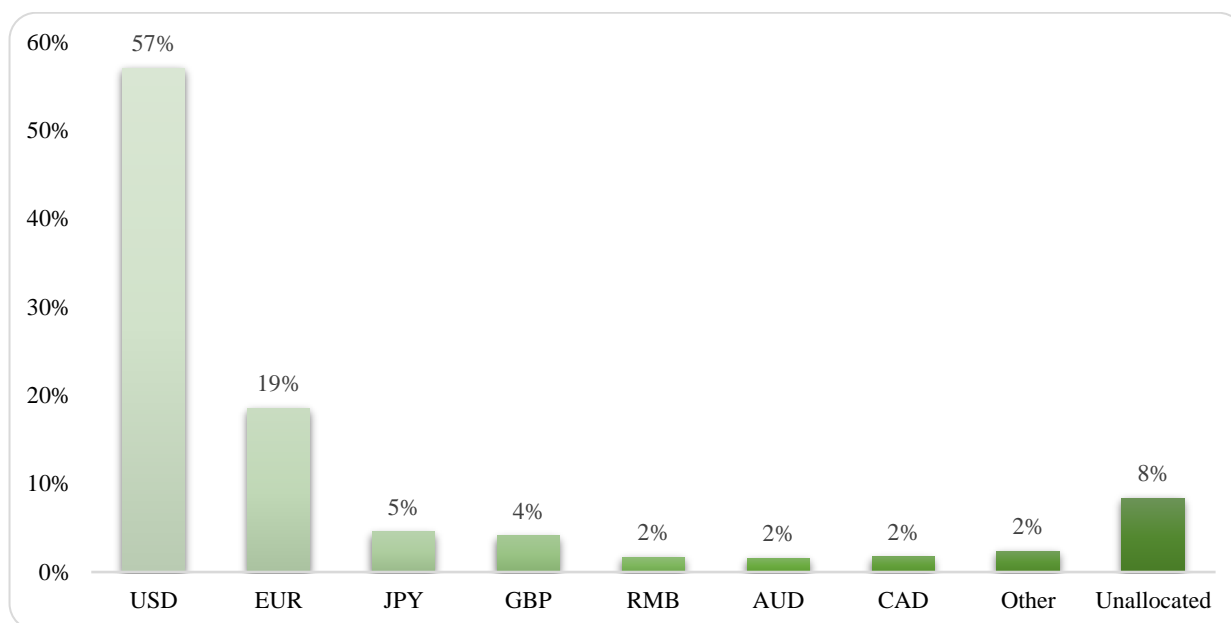
One of the main arguments against cryptocurrencies is that no government will accept them to pay taxes – the main purpose of a fiat currency. This argument does not exclude cryptos becoming accepted as a means of payment for international transactions, a role currently fulfilled primarily by USD. Many countries would likely welcome a

⁶ Please see [Glossary](#) if any of the terms presented herein are unfamiliar.

decentralized cryptocurrency for use in international trade (as an alternative to the greenback's current dominance), although the US government is likely to resist such a scenario.

Another contemporary consensus is that cryptocurrencies currently cannot serve as a means of payment or store of value due to their extreme volatility. However, high volatility is generally a function of speculation. When the cryptocurrency is at equilibrium, speculative short-term investors should disappear and volatility decline to the fiat level. What would then stop a decentralized cryptocurrency from becoming a widely adopted store of value? On one hand, governments dislike having anything uncontrolled. On the other hand, many countries keep most of their national reserves denominated in USD – a currency their governments have no control over – and they would like to diversify. The US seems to be the main loser in both of the above-mentioned cases, and therefore the US, along with financial institutions, should be among the strongest opponents of cryptocurrencies.

More than half of worldwide national reserves are kept in USD



Source: IMF

Regardless of how promising blockchain technology sounds, it is still far from mainstream adoption. Aside from obstacles such as legal restrictions and cryptoasset volatility, there are huge challenges faced on the technology side. There are two main hurdles for contemporary blockchains, standing in the way of mass adoption and universality:

- **Scalability** – The speed at which a blockchain can process transactions
- **Interoperability** – The ability to communicate between different blockchains

Resolving both these problems, in our opinion, is the key to winning the long-term race for blockchain supremacy. Backed by billions of dollars of investments, the best industry talents are focused on solving these engineering problems, and some promising outcomes should materialize soon. The future real-world application of blockchain relies on the technology's scalability. Established blockchains have limited speed given their current architecture. For Bitcoin this speed is around 10 minutes per block of transactions, while for Ethereum it is 12-15 seconds. This results in bottlenecks and high transaction costs, making the day-to-day usage of blockchains prohibitive.

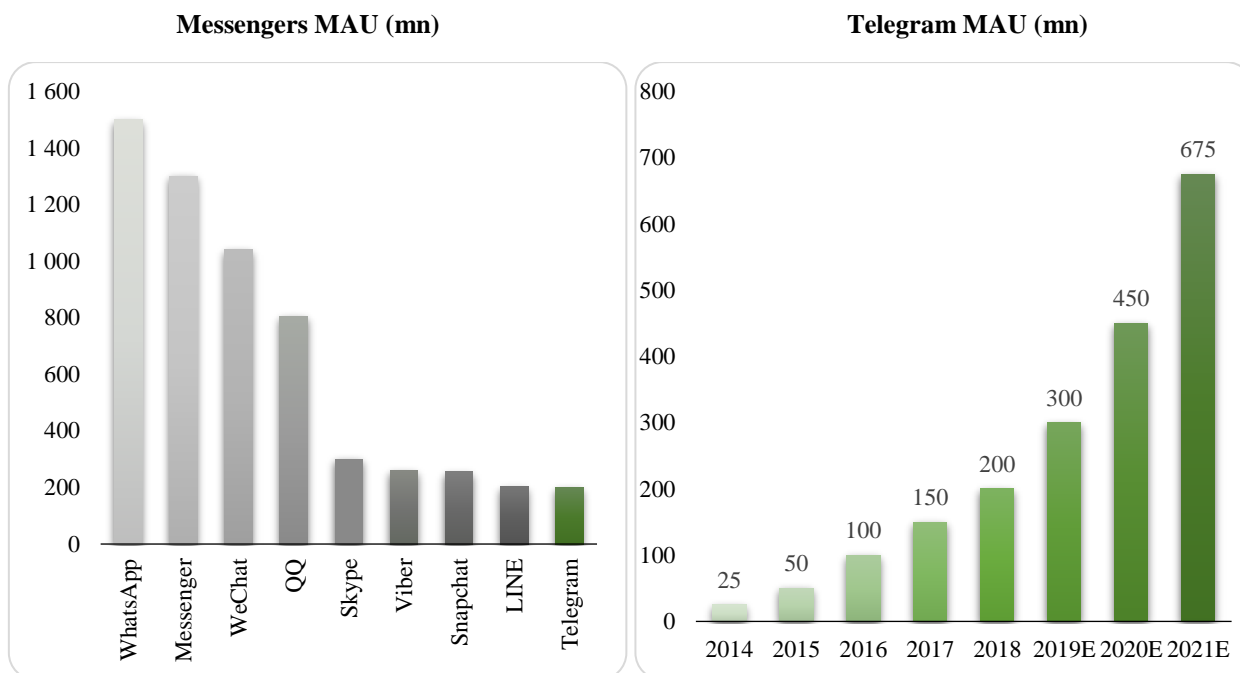
There are currently three mainstream approaches that should theoretically allow blockchains to massively scale: change of consensus algorithm, state channels, and sharding⁷. Different blockchains are trying to develop their own ways to tackle the scalability problem, but in fact, they use all variations or combinations of these three. However, as far as we know, any solution implemented so far has sacrificed decentralization or security or both.

TON is among the breakthrough projects aiming to build a system that does not inherit the scalability and interoperability problems. Aware of the skepticism towards Telegram among crypto community, our technology counsel, a QIWI Blockchain Technologies expert has done a close reading of both TON's and its competitors' White Papers. The conclusion is that while the TON document is poorly written, its concepts generally make sense and could be implemented. Due to the open source nature of the blockchain industry, other concurrently developing projects such as Polkadot, Cosmos or Dfinity could be competitive and supportive simultaneously. However, unlike those projects, Telegram already has a critical mass of users for its system's mass adoption.

⁷ All analyzed later in the report.

Telegram: a fast and secure messenger

Launched in 2013 by a team of Russian software developers, by spring 2018 Telegram messenger had gained 200mn monthly active users worldwide. Starting as a niche player, the messaging app has become one of the most widely used around the globe, with 500k new users reportedly joining daily. Telegram aims to have 675mn monthly active users (MAU) and one billion active users by end-2021, according to the TON Primer.



Source: TON Primer, Statista

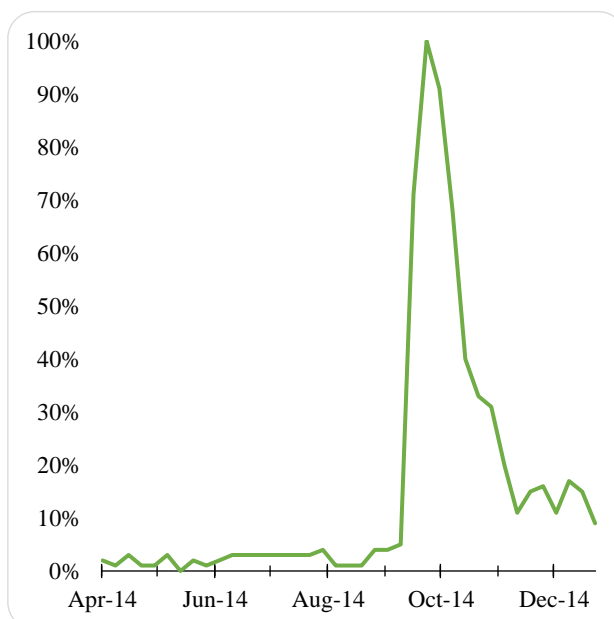
The technical advantages of any messaging app are unsustainable and unlikely to be the main reason for customer retention. For example, the value of encryption, which is now a prerequisite for any messaging app, is negligible if a messenger shares the encryption keys with third parties. Therefore, messaging platforms must have other properties to ensure loyalty. The way a messenger protects private information sheds light on the kind of security it provides. Telegram manages to maintain its image through multiple instances of proven ideological resistance to breaches of user privacy. Telegram founder Pavel Durov refused to give the protocol's encryption keys to Russian security agencies. In response, the Russian authorities have been trying (unsuccessfully) to block the messenger since April 2018.

The state-level attack was unprecedented, in our view, as no other Internet company had experienced one of such magnitude. In the first week, the number of Internet Protocol (IP) addresses banned in government attempts to block the messenger reached 18 million, according to [The Moscow Times](#). However, Telegram was able to resist efficiently by rapidly setting up new instances of the Telegram proxy on different cloud providers' infrastructure.

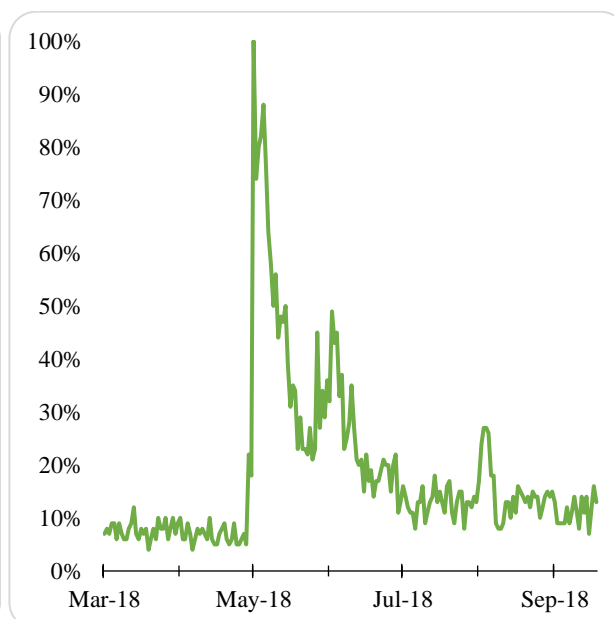
This confrontation, later called "Digital Resistance", earned the trust and won the hearts of additional users, even leading to [small protests in Russia](#). At almost the same time, a similar situation emerged in Iran, where Telegram has 40mn users – half of the country's population. [Telegram's popularity in Iran](#) has also been fueled by the company's refusal to submit to Iran's state censorship rules. "For many Iranians the Internet is Telegram, and Telegram is the Internet," [says Omid Memarian](#), deputy director of the Center for Human Rights in Iran.

Telegram has become the messenger of choice when other services are compromised. In 2014, Telegram saw [a massive increase in its user base in South Korea](#) – reporting 1.5mn new users signing up in just 7 days – after the country's president confirmed government surveillance of the region's biggest messenger app, KakaoTalk, spurring a user boycott.

Telegram's popularity spiked in Korea in 2014...



and in Iran in 2018



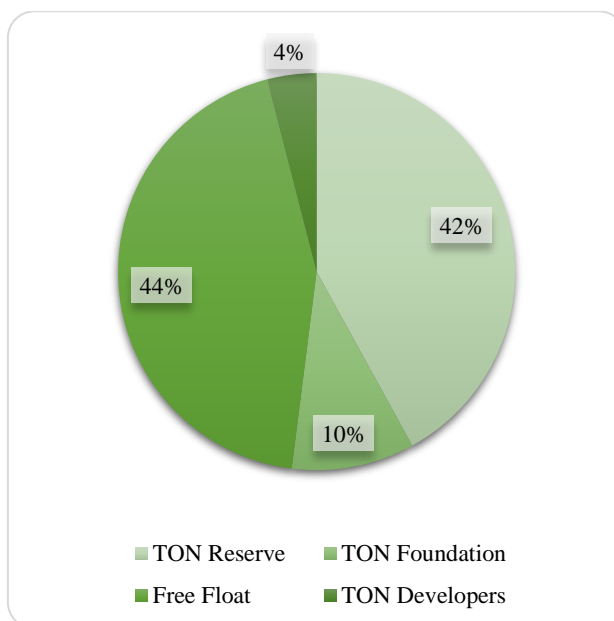
Source: [Google Trends](#)

Telegram Open Network – a technological breakthrough

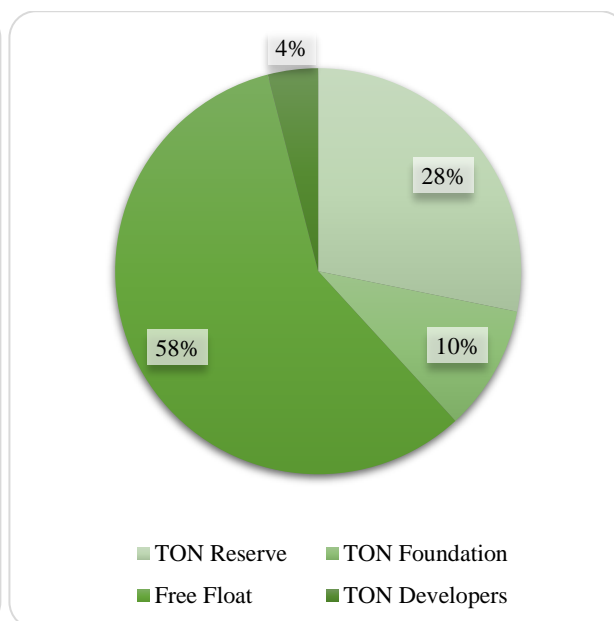
Telegram plans to launch its own, entirely new blockchain platform and native cryptocurrency. The company designed the Telegram Open Network as a fast and secure blockchain and wider peer-to-peer network project able to meet the speed and scalability requirements needed for mass adoption. The TON coins exchanged by Telegram users will be called Grams (GRM). Grams will serve as the principal currency for the in-app economy and will be available for external use.

Telegram raised \$1.7bn via two private placements and called off its expected ICO. Telegram sold 2.89bn Grams for \$1.7bn⁸ with no prior public announcements to communicate the concept and generate feedback, as is usually the norm in the public blockchain tech community. It gave investors little time to analyze the offering and provided no additional updates after the sale was done. Nevertheless, demand was so strong that the company increased the total number of coins it had planned to initially allocate.

Initially planned distribution of Grams



Grams distribution after placement



Source: TON Primer, TON White Paper, HASH CIB

⁸ See our Valuation chapter for a detailed calculation.

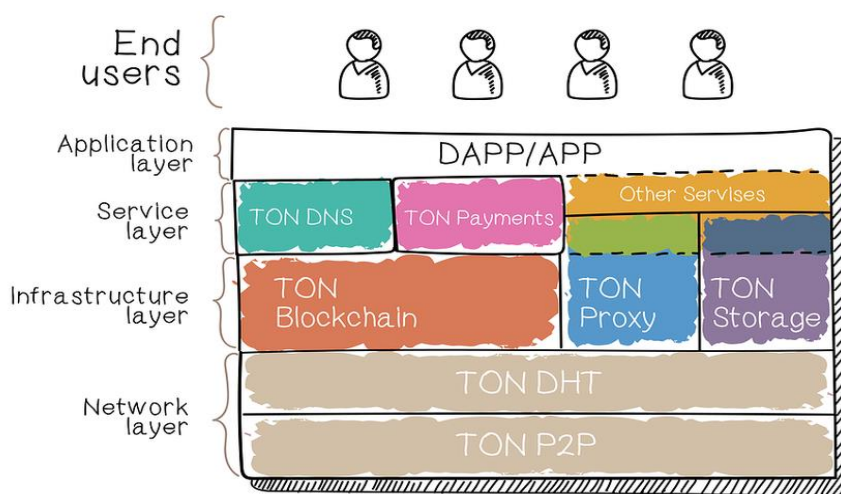
With 200mn monthly active users, Telegram already has the pre-existing critical mass necessary for the ecosystem to quickly expand and gain widespread adoption. Moreover, the messenger has become one of the main communication platforms for official ICO discussion groups. Most actors in the digital economy already have accounts with Telegram, and its popularity is rapidly expanding. Currently, 90% of blockchain-based projects have active communities in the messenger, compared to just 16% a year ago, according to ICObench.

Much more than just a blockchain or payment channels network, TON is an ambitious ecosystem that creates several parallel technologies on multiple levels⁹. TON is a stack of technologies to power a global community of users wishing to communicate, use applications, and buy and sell assets in a censorship-resistant and secure way. Telegram intends to build the infrastructure and basic features for such an *ecosystem of decentralized services over a distributed network* to thrive independently of the World Wide Web, while leveraging the global reach of its messenger's 200mn active user base.

Grams are the lifeblood needed for the ecosystem to exist, while smart contracts and decentralization are designed to protect it from abuse and censorship. TON not only plans to challenge VISA and Mastercard as an alternative for the new decentralized economy, but it also supports a wider array of functions needed for what is considered the Web 3.0 generation of applications and services.

A potentially widely adopted cryptocurrency is the cornerstone for the whole TON ecosystem. Although Gram is the first in the line of key ecosystem components to be delivered with the network launch, the team behind TON envisions a broader use for its blockchain than might initially appear. As soon as the peer-to-peer networking layer of the TON technological stack is laid down and the blockchain is running, the launch of the following protocols/features of the network should follow the distribution of Grams: *TON Storage*, *TON Domain Name System (DNS)*, *TON Proxy*, and *TON Payments*¹⁰ (an additional payment channel network built on top of the blockchain). Worth noting is that the P2P payment network – a key component in making the Gram currency truly widely adopted – is likely to be the last of these elements.

TON's stack of protocols and technologies



Source: TON White Paper, HASH CIB

Telegram plans to release a Wallet integration into its messenger before the TON Payments platform is developed, we believe. This means that Gram holders will initially be able to use their cryptocurrency not for "*instant money transfers and micropayments*" supported by TON Payments, but rather for more "regular" blockchain-based transactions, which implies higher fees to validators, longer confirmation times and less transaction throughput. Nevertheless, if working as promised, the blockchain's throughput should still be well above that of today's protocols.

⁹ e.g. the infrastructure level, the application development level, the user level, etc.

¹⁰ These protocols are discussed in detail later in the report.

Competitive landscape

The market typically views payments as the “killer app” for cryptocurrencies. Although TON Payments will not be the only service the blockchain offers and nor the first to appear, it is the most marketable and one of the most value-added, we believe. The service will be embedded into Telegram and will compete for users with other messaging apps in the already-crowded mobile payment industry. With the exception of Snapchat, all major messengers provide payment services in one way or another.

Largest Messaging Apps and Their Payment Services

Corporation	Messenger	MAU, mn	Payment Service
Facebook Inc.	Messenger	1 500	Messenger Pay
	WhatsApp	1 300	WhatsApp Pay
	Instagram	1 000	
Tencent Holding Inc.	WeChat / Weixin	1 040	WeChat Pay
	QQ	806	QQ Pay
	Snapchat (12% ownership)	255	<i>Discontinued Aug 2018</i>
			Tenpay
			WeBank
Rakuten Viber	Viber	260	Payments via Western Union
NAVER	LINE	203	LINE Pay
Telegram Inc.	Telegram	200	TON Payments
Kik	Kik	15	Kin cryptocurrency

Source: Statista, HASH CIB

Facebook appears to plan to strengthen its P2P payments offering, which has not seen wide adoption so far. The corporation is able and probably plans to build a blockchain, which could be used for payments on WhatsApp or Messenger. China’s largest messenger, Weixin (known as WeChat outside of its motherland), launched its payment service in 2014 and now has more than 800mn monthly users. LINE Pay invests heavily in the service and now has over 30mn accounts in Japan and 10mn in Taiwan. Moreover, LINE built its own blockchain and opened a captive crypto exchange, BITBOX, where its coins, LINK, are exclusively available.

TON’s blockchain-based competitors fall into three major categories, reflecting three core objectives for the TON project: scaling of payments, scaling of distributed computations, and inter-blockchain communication. However, from the software architecture standpoint they fall into two categories:

- **Layer 2** solutions on top of already existing blockchains – predominantly solving for *scalability* rather than *interoperability*. These projects are at development stages closer to production than projects in the other group. Key competitors include **Bitcoin Lightning Network** and **Raiden** (Ethereum payment channel network).
- **Layer 1** scalability and interoperability-enabling blockchain projects, which generally face longer development cycles. Effectively, new blockchain architectures that solve both two problems within their basic mainnet layer. Although all projects address both issues, we divide them into groups according to their focus:
 - Better performance of smart-contract execution and distributed computations (**EOS, Dfinity**)
 - Horizontal scaling and interoperability-enabling infrastructure projects – blockchains for other blockchains to be built on top of them (**Polkadot, Cosmos**).

Also, **Ethereum** is moving toward a series of major updates to also solve for general mainnet scalability (on layer 1) and payments/smart-contract execution scalability (on layer 2).

We see the blockchain projects rather than the messaging apps as the key competitors for TON as a whole. If one or several of them successfully solve the scalability and/or interoperability issues, the main thing missing for wide adoption (at least for the payment service) would be a user base. Then it becomes a matter of time what happens first: does TON solve the problems as well, or do the competitors attract users. We think that the former is more likely, given the open source nature of the blockchain industry. In other words, TON should be able to capitalize on any solutions already publicly available by then.

How much a Gram weighs

Equity markets had existed for four centuries and the New York Stock Exchange operated for 130 years before Discounted Cash Flow (DCF) methodology became the mainstream in equity valuation, spurred by the market crash of 1929. Unsurprisingly, with less than 10 years of history no one really knows how to value cryptoassets yet. Cryptocurrencies do not intend to deliver cash to their holders and cannot be valued as equities¹¹. Not only does cash flow to token holders not exist at the initial stages of the projects, it is never meant to appear¹². In other words, the classical DCF approach cannot be applied to cryptocurrencies.

The name itself suggests the right approach: cryptocurrencies should be valued as currencies. A cryptoasset serves as the currency within its native blockchain, fulfilling all three money functions – a store of value, means of exchange, and unit of account. Therefore, we can apply the equation of exchange to value cryptocurrencies. The equation of exchange addresses the relationship between money and price level, and between money and nominal GDP. The equation states that $M * V = P * Q$, where M is the size of the asset base, V is the velocity of the asset, P is the price of the digital resource being provisioned, and Q is the quantity of the digital resource being provisioned, as described by [Chris Burniske](#).

We introduce our in-house approach to value blockchains. Our approach is based on methodology proposed by both Burniske and [Brett Winton](#). We derive each period's blockchain current utility value (CUV), which at any given period t is forecast by the equation of exchange: $CUV_t = P_t Q_t / V$. The rational utility value of a network is not just the discounted future CUV of a particular year¹³, nor is it the sum of discounted CUVs of all projected years¹⁴, we believe. We think that blockchain's rational utility value is better modelled as **today's** utility value **plus** discounted **additional** current utility values (ACUV) for every year to infinity. $ACUV_t$ in a year t equals the difference between CUV_t in the year t and CUV_{t-1} in the year $t-1$.

$$ACUV_t = CUV_t - CUV_{t-1}$$

To account for infinity, we calculate the terminal value (TV) of ACUV at the period of network maturity. In this case, the model captures all the years. The approach is similar to the one used to value banks, for which traditional DCF is also not applicable. A financial institution is valued as a sum of its current shareholders' equity and the present value of future excess returns on equity (returns in excess of those required by the cost of equity).

The commonalities and differences of our approach are easier to explain with a simple example. Consider a network that matures in five years and subsequently grows with the annual rate g indefinitely. CUV_t is the network's utility value for the end of year t . The additional utility value $ACUV_t$ for the period t is equal to $CUV_t - CUV_{t-1}$. TV for the end of the year five equals $ACUV_6 / (r-g)$. This is a classic formula for terminal value, where r is the discount rate. We can simplify the formula for TV. Given that $ACUV_6 = CUV_6 - CUV_5$ and $CUV_6 = CUV_5 * (1+g)$, we arrive at $ACUV_6 = CUV_5 * g$, and $TV = CUV_5 * g / (r-g)$.

	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5	Terminal Value
CUV	CUV_0	CUV_1	CUV_2	CUV_3	CUV_4	CUV_5	
ACUV		$CUV_1 \text{ minus } CUV_0$	$CUV_2 \text{ minus } CUV_1$	$CUV_3 \text{ minus } CUV_2$	$CUV_4 \text{ minus } CUV_3$	$CUV_5 \text{ minus } CUV_4$	$CUV_5 * g / (r-g)$
Discount rate	1	$1+r$	$(1+r)^2$	$(1+r)^3$	$(1+r)^4$	$(1+r)^5$	$(1+r)^5$

Source: HASH CIB¹⁵

We would hesitate to call the number generated by this approach a “target” or “fair” price, given that the model only applies to coins with utility value and to developing blockchains. We would instead call it a **Rational Network Value (RNV)**. In the example above, the RNV would be as follows:

$RNV = CUV_5 / (1+r)^5$. Burniske model

$RNV = \sum CUV_t / (1+r)^t$, where $t = 0 \dots 5$. Multicoin Capital model

$RNV = CUV_0 + \sum ACUV_t / (1+r)^t + CUV_5 * g / (r-g) / (1+r)^5$, where $t = 1 \dots 5$. HASH CIB model

¹¹ While there are a few cryptoassets trading on the market that have equity-like features, the absolute majority serve as currencies or “internal” currencies for whatever the underlying network/distributed application provides.

¹² Again, we are generalizing for simplicity's sake: there are some cryptos designed specifically for capturing value for the projects' backers, but they represent a negligible fraction of the overall market at this point.

¹³ As in Burniske and Winton.

¹⁴ As in the [Multicoin Capital model](#).

¹⁵ Based on our own valuation model, described herein. Using this approach may not reflect actual results and is not a guarantee of future results.

We use a dynamic and increasing velocity to value cryptoassets in our in-house model. Only investors, not end-users, buy tokens during an ICO, and only investors hold tokens while the blockchain is under construction. Even if tokens trade, the average holding period is months rather than days, we believe. Thus, velocity is relatively low during the initial stages of the project. If and when the project is successful and the network is up and running, end-users come aboard and the tokens are used for their main purposes. As a result, end-users gradually substitute investors as token holders, and velocity grows. In our model we assume that a cryptoasset's velocity increases concurrently with blockchain adoption according to a logistic S-shaped curve.

To derive TON's Rational Value using our in-house model, we divide network development into three stages: current condition, the future, and terminal growth. Given the October 2019 target for the project's launch¹⁶, we consider the first stage to be the year 2019. The second period covers 2020-2028 and the last runs from 2028 to infinity.

First, we forecast TON's PQ for every period to calculate each year's current utility values (CUVs) using the equation of exchange. To predict TON's total PQ, we forecast and summarize the PQs for each of Gram's use cases: Payments, Storage, DNS, Proxy, Applications and Services (other than Storage, DNS and Proxy). TON Payments should create the largest demand for Grams – the main cryptocurrency used within the Telegram ecosystem.

Year	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	TV
Current Utility Value (CUV), \$bn		0	4	45	436	2 523	4 993	7 501	9 837	12 162	14 603	
Growth			1221%	1176%	864%	479%	98%	50%	31%	24%	20%	5%
Additional Current Utility Value (ACUV), \$bn		0	3	42	391	2 087	2 470	2 508	2 335	2 326	2 440	2 086
Velocity	0	0	1	6	42	183	281	335	356	363	365	365
Number of Grams, bn (average)	2.89	2.99	3.07	3.21	3.35	3.50	3.62	3.72	3.82	3.92	4.03	4.03
Discount Rate	40%											
Discount Factor	1	1	0.71	0.51	0.36	0.26	0.19	0.13	0.09	0.07	0.05	0.05
Discounted ECUV, \$bn	-	0	2	21	142	543	459	333	222	158	118	101
Value per Gram, \$		0.86	0.95	1.09	1.01	0.85	0.45	0.27	0.16	0.11	0.08	0.07
Rational Gram Value, \$	\$5.90											

Source: HASH CIB¹⁷

We estimate a Gram's Rational Value at \$5.90 as of end-2019. We summarize the transaction volume for each Gram utility line to arrive at aggregate CUVs and Additional CUVs for each period. Dividing ACUVs by the corresponding average number of coins in circulation and discounting the result to the end of 2019, we obtain \$5.90 per Gram. The result implies 63% upside to the \$3.62 minimal issuance price given by Gram's distribution formula (per White Paper) and 4.4x upside to our calculated second-round placement price of \$1.33.

Execution is the main risk

An ambitious project in a nascent industry, TON will emerge in a very competitive environment and faces many risks. We divide these risks into two broad categories, internal and external, which, in turn, are subdivided into a few other types. Given the magnitude of proposed technological and engineering changes and their still very theoretical nature, successful and timely execution of the project will be extremely challenging. This internal risk is the highest for TON, in our view. At the same time, the project faces many external risks beyond control of the Telegram team. The most important is competition, which comes from both contemporary messengers and blockchain projects, but legal risks are also considerable.

¹⁶ Our assumption based on the project's execution risk and [publicly available leaks](#) regarding the TON placement.

¹⁷ Based on our own valuation model, described herein. This table contains forward looking statements and actual results may differ, because such a statement is derived from mathematical modeling techniques of the economic or financial markets that may or may not reflect actual conditions or events.

The TON Project faces substantial risks, both internal and external

Internal				External		
Execution			Post-launch risk	Competition		Legal
Failure to hire enough talent	Theory doesn't meet practice	Failure to meet deadlines		Messaging Apps	Blockchain projects	Inability to trade Gram
Substantial	Very substantial	Very substantial	Substantial	Average	Substantial	Substantial (US only)

Source: HASH CIB

TON is envisioned as a complex system where multiple parties need to collaborate in order for it to thrive and expand. How third-party developers and service providers integrate with the TON ecosystem does not appear to pose a material risk for the project, given more than adequate funding to incentivize these third parties, at least for some time after launch. Of more concern are those potential risks related to the actual maintainers of TON – the nodes and parties providing their resources and services for blockchain validation and storage. These are risks that could materialize after the network is launched.

In terms of execution, there are two major risks related to project development, testing, and rollout: schedule and recruiting. The project is *already behind the schedule* presented in the offering Primer. Telegram Passport was scheduled for Q1 2018, but it was not announced until Q3 2018. This implies that other milestones, such as the Launch of the Minimal Viable Test Network of TON (scheduled for Q2 2018) and Testing and security audits of TON (scheduled for Q3 2018) have fallen behind the schedule.

As there has been no public indication of TON launching, testing or auditing the minimal viable version of its network, the technological challenges could be catching up with developers. Despite delays and a history of secrecy, we continue to believe the TON Blockchain protocol will be open source. An open source rollout ensures access to constant peer review and community-driven updates – almost mandatory for such complex technological systems as blockchains. Open source code would also drive the wider adoption of the platform by developers and service providers wishing to build on top of TON.

The inability to recruit developer talent could be another reason why TON appears behind schedule. Hiring in general entails a separate group of risks, as quality blockchain-focused developer talent is scarce. While TON's competitors are visibly hiring, our sources say there has been little talk of TON hiring among the blockchain developer communities that one would expect Telegram (predominantly EMEA-based, as we understand) to draw from: St. Petersburg, Berlin, or Switzerland. We are also unaware of TON-related hiring going on in other developer hubs of Eastern and Central Europe or in Silicon Valley.

Other blockchain projects represent substantial risk for TON. Ethereum (when updated), Cosmos, EOS, Polkadot and Dfinity are the main competitors in terms of scalability and interoperability solutions, and therefore, for the whole TON project. Bitcoin Lightning Network and Raiden are the strongest decentralized payment services competitors. Contemporary messaging apps, representing a competitive risk just for a single service – payments are likely to remain centralized, and therefore are far less of threat to TON, in our opinion.

We also highlight one legal issue possibly arising for TON and its investors, at least in terms of secondary market sales of the Gram cryptocurrency in the US or by the US residents. Telegram registered the placements with US SEC and at least two of the buyers are known to be US residents. Grams could therefore be considered US regulated securities, we believe. This could lead to substantial restrictions on a secondary market for Grams in the US. While there could be exemptions, legal issues clearly represent a separate area for specialized due diligence.

The Blockchain Technology Revolution

... initial Internet efforts have been very centralized. Blockchain technology, which implements data integrity via computer science rather than via “call the cops”, has so far made possible trust-minimized money —cryptocurrencies— and will let us make progress in other financial areas as well as other areas where transactions can be based primarily on data available online.

Nick Szabo

Cryptoassets celebrate their tenth anniversary this year. Initially purely an academic exercise, over the decade blockchain technology has turned into a multibillion-dollar industry, while cryptocurrencies – unheard of a few years ago – are now a must-cover topic in most mass media. The crypto boom gave birth to a new fundraising tool – the Initial Coin Offering (ICO) – and crypto-focused funds are mushrooming. Telegram’s 2018 placement has changed the ICO landscape. However, blockchain technology goes far beyond cryptocurrencies – it can reshape the world by digitalizing and making convertible practically anything valuable to humankind. Decentralization is the breakthrough, the holy grail of blockchain technology that jeopardizes the existence of intermediaries and the dominance of central authorities and governments. However, blockchain remains far from mainstream adoption, as scalability and interoperability hurdles stand in the way of universality. We divide industry projects into two broad categories: applied and breakthrough. Whereas applied projects focus primarily on improving specific existing businesses, breakthrough projects attempt to offer solutions for the whole blockchain industry. For such projects, native blockchains and native coins are a must. The Telegram Open Network (TON), Polkadot, and Cosmos all represent ambitious attempts to build state-of-the-art network architectures with the ability to create blockchains for blockchains but without those inherited problems.

New digital assets

The cryptocurrency era began on the heels of the collapse of financial markets in 2008 when a still-unknown person or a group using the alias Satoshi Nakamoto published *Bitcoin: A Peer-to-Peer Electronic Cash System*. On 3 January 2009 Satoshi mined block number zero (the so-called Genesis block), delivering a pre-mined one million bitcoins (BTC) to their Bitcoin address and receiving a 50-bitcoin mining reward, thus launching what would become a multibillion-dollar industry and spurring the development of blockchain technology. Several digital cash and related technologies had existed prior to the creation of the Bitcoin network¹⁸, but only the adoption of bitcoin cryptocurrency turned the academic subject and the idea of liberated digital money into a new asset class.

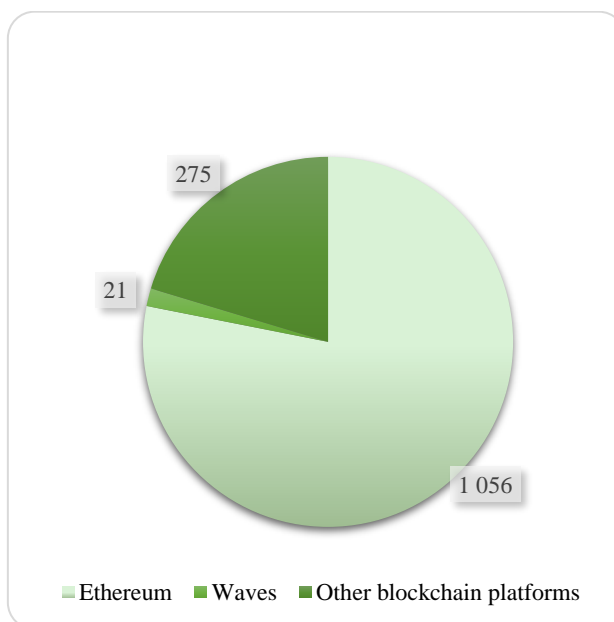
Ethereum, proposed in 2013 and going live in 2015, represented a quantum leap in the evolution of blockchain technology. Designed by a Russian-born Canadian, Vitalik Buterin, Ethereum is much more than Bitcoin’s decentralized payment system. Built to become a “world computer”, it is a blockchain platform for applications. Ethereum pioneered the smart contract¹⁹ now used in most blockchains and created a Turing-complete²⁰ virtual machine (the Ethereum Virtual Machine, or EVM). These features paved the way for a subsequent avalanche of digital token issues. Some 79% of existing crypto tokens by number are based on Ethereum. And its underlying cryptocurrency, ether (ETH), has become the first crypto commodity, as its actual utility function is to power the use of smart contracts on the Ethereum network, rather than being used as “programmable money” like bitcoins.

¹⁸ Notably *eCash* in the early 90s, which pioneered the use of cryptography to secure ownership of fungible digital assets; *Hashcash*, which introduced the minting of a proof-of-work-based token, *Reusable Proofs of Work*, that extended its use to token money; and *Karma*, which used the first implementation of a distributed proof-of-work minting algorithm – the latter three from the early-mid 2000s. Important theoretical projects – b-money (1998) and BitGold (2005) – also influenced the Bitcoin creator(s).

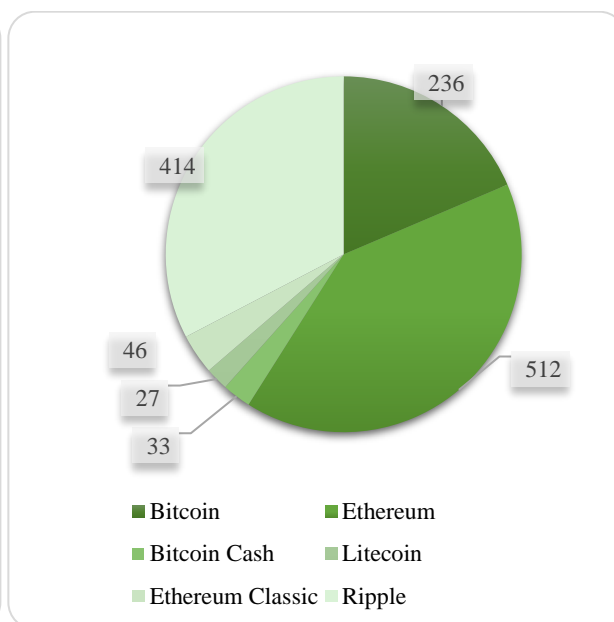
¹⁹ A *smart contract* is a computer program intended to digitally facilitate, verify, or enforce the performance of a virtual contract. It has a predefined set of outputs (virtual actions) each responding to a certain type (or groups) of input(s), which thus automates the execution of virtual actions if conditions precedent for such actions are met. Smart contracts allow the performance of credible transactions without third parties; such transactions are trackable and irreversible.

²⁰ A *Turing-complete* or computationally universal computer system is one that can process, store while using (multi-task), and long-term store data – like CPU, RAM and disk storage systems on a personal computer. A Turing-complete system is aware of its current and previous states and can run all types of computer programs.

Tokens on different blockchain platforms



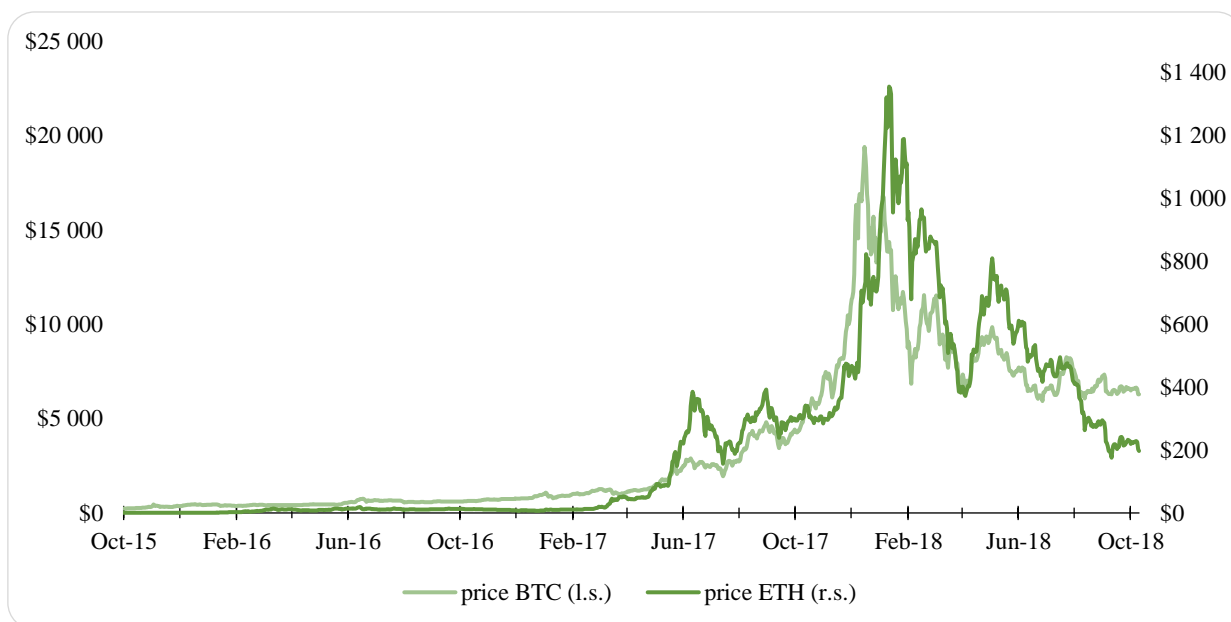
Number of daily blockchain transactions ('000)



Source: [TokenMarket](#), [BitInfoCharts](#)

The full potential of blockchain technology is still to be realized. Public consciousness is focused on just one use case, pseudo-anonymous²¹ money transfer. And this is well understood given that governments worldwide are active in their efforts to squeeze money out of people to finance their ever-growing expenses. However, seeing payments as the only utility function of blockchain is like seeing email as the only utility function of the Internet. But without the potential of payment systems, the industry would have not been able to attract so much funding, and research and development would have been left to a few academics and enthusiasts.

BTC and ETH price



Source: [CoinMarketCap](#)

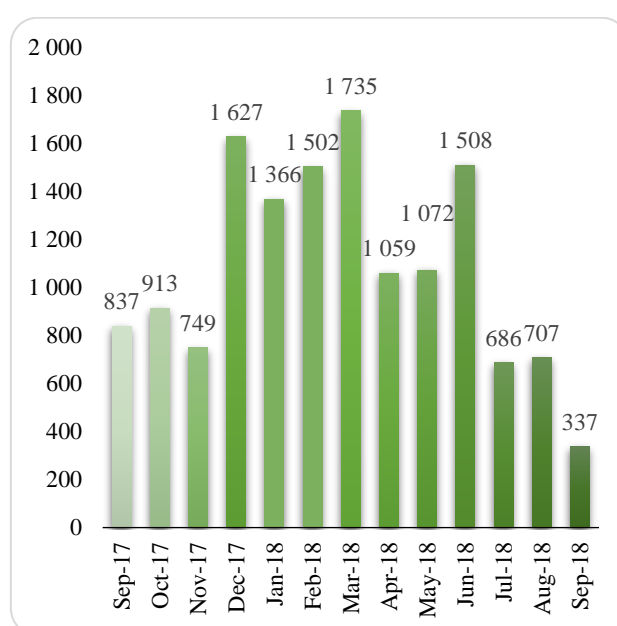
²¹ “Anonymous” because initially we do not know who the account owner is, and “pseudo” as each transaction and the histories of its participants are traceable on most blockchain networks.

The craze around cryptocurrencies led to skyrocketing prices for the two main coins, bitcoin (BTC) and ether (ETH), in 2017. BTC was initially priced at \$0.00076²² and first exchanged for a real asset – a Papa John’s pizza – at \$0.003²³; the coin’s value touched \$20,000 in December 2017. The price of ETH jumped 271-fold between inception and January 2018, peaking slightly later than BTC. However, this year has seen a substantial correction in both coins, which are now priced at around \$6,500 and \$200, respectively. But even c70% off last year’s peak, their combined market cap remains considerable at around \$130bn.

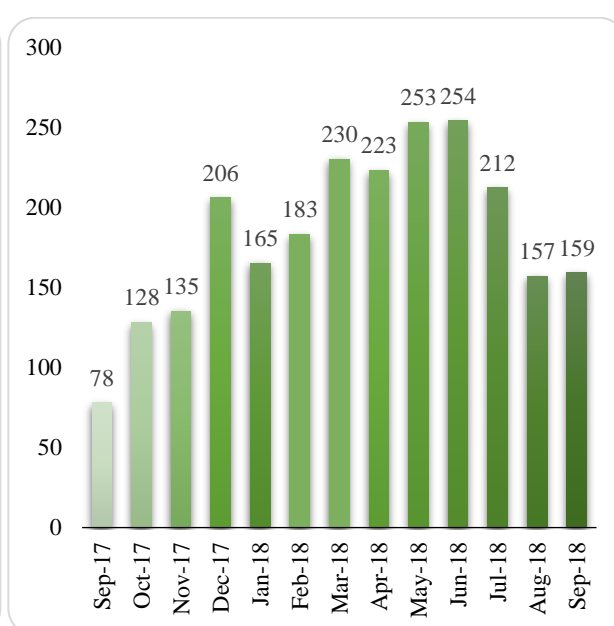
The ICO is no longer in its infancy

Crypto hype gave birth to a unique fundraising tool – the Initial Coin Offering. Between 2013, when a project called Mastercoin raised \$5mn in the very first ICO, and 2016, start-ups managed to raise around \$400mn altogether. In 2017 total investments in ICOs reached over \$4bn. Yet the combination of just two of 2018’s biggest fundraisers to date – EOS’s year-long offering and concurrent secondary market, and Telegram’s private placement, which raised \$4bn and \$1.7bn, respectively – were larger than the whole market the previous year. And even excluding those two, combined ICO volume YTD has hit the \$9.1bn mark, although the number of ICOs has fallen sharply since their June peak.

Funds raised on ICOs (\$mn)



Number of ICOs



Source: [ICObench](#)

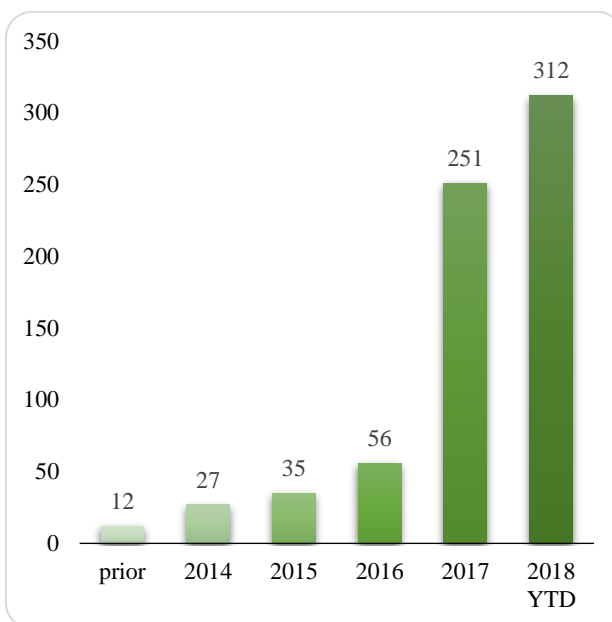
Unsurprisingly, blockchain firms favor ICOs over conventional funding given that coins or tokens (we will dwell on the distinction between the two terms later) do not provide any ownership rights or legal protection for their holders. Unlike in equity or debt placements, ICO investors do not become shareholders or lenders to companies. Unlike in venture funding, the issuers do not have an obligation to deliver or even attempt to deliver a product. Therefore, investors have no claim over the income or assets of the coin or token issuers, nor do such issuers usually have any responsibilities to deliver returns or product to the investors. Only if coins or tokens appreciate in value – on the expectation of future utility/network effects of the underlying blockchain project – can investors make a profit.

Nevertheless, conventional institutional investors seem to have accepted the rules of the new game and are slowly joining in. Some 195 crypto funds were launched last year, compared to 56 in the five previous years. Currently the total estimated number of funds is over 300 with overall AUM of \$7-10bn, according to [Autonomous Research](#). News of leading venture firms like Andreessen Horowitz [launching](#) a \$300mn crypto-dedicated fund, or a former Sequoia Capital partner leaving the highly successful organization for pure crypto investment [ventures](#), or one of the biggest over-the-counter crypto traders [seeing](#) a 30% spike in institutional clients in just one month – all of these are signs of big money’s interest in crypto, and they keep pouring in despite the bear market.

²² [New Liberty Standard](#) established the rate based on the amount of money it needed for electricity and rent to maintain the computer that mined bitcoin vs. the amount of bitcoin that had been reaped from so doing. On 5 October 2009 it priced BTC at 1,309 to the dollar, or 7/100 of a cent per bitcoin.

²³ ["May 22 is Bitcoin Pizza Day."](#) Business Insider.

Cumulative number of crypto funds



Assets under management (\$mn)

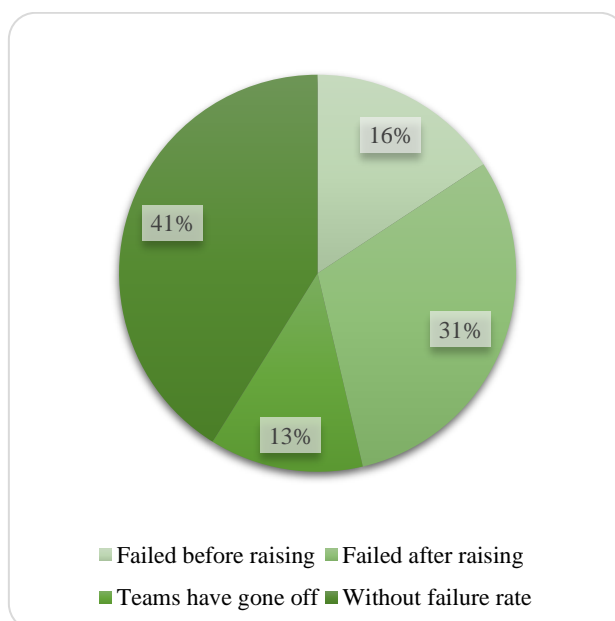


Source: [Autonomous Research](#), [Crypto Fund Research](#)

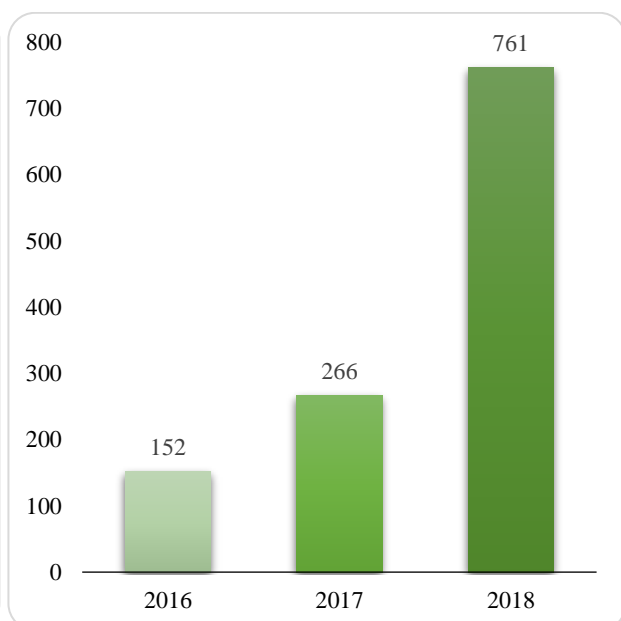
The ICO landscape is rapidly maturing, and attracting funds via ICOs is becoming increasingly difficult. The rising number of ICOs leaves investors with more choices and increases the competition for their money – hence the growing number of failing fundraisers. Institutional investors capable of conducting in-depth research and due diligence on issuers will weed out weak and/or questionable ICOs. Furthermore, concerned by fraud and rising coin placement volumes, financial regulators worldwide have launched efforts to control cryptocurrency issuance and trading. As a result, the recent ICO anarchy will likely end soon, with token offerings evolving into more conventional procedures. Start-ups hungry for investors' funds will be the main victims of such developments.

Crypto markets are fraught with fraud and price manipulation. Another trend that could trigger stiffening regulatory oversight is fraud and price manipulation on the secondary market, coming on top of initial offering fraud. There have been [allegations](#) of wash trading on some of the biggest exchanges, leading to [enforcement actions](#) and [criminal probes](#) by the Department of Justice with the help of CFTC in the U.S. As such, secondary market platforms for cryptoassets are finally realizing the necessity to either obey local security/commodity trading regulations or [find](#) regulatory regimes with “easier” oversight. All of this, in our understanding, will seriously affect crypto market secondary trading in the near future.

59% of all projects in 2017 did not succeed



\$761mn was stolen from crypto exchanges in 2018 YTD



Source: *Bloomberg, Fortune*

Telegram's placement has changed the ICO arena. First of all, its placement will encourage other established companies to follow suit. Facebook is reportedly considering issuing its own cryptocurrency, and we would not be surprised to hear about possible ICOs from major tech or financial players like Microsoft or Amex. Such developments would further tighten funding conditions for start-ups. Also, top-tier traditional funds will join the existing crowd of investors, bringing in long money and their own investment requirements²⁴. Finally, given the current consolidation, which has cooled but not killed off crypto speculators, this may be the beginning of a real bubble, one that might end up peaking well above either the near-trillion dollar crypto market size of late 2017/early 2018, or even the earlier \$4tr (adjusted for inflation) pinnacle of the dot-com bubble in March 2000.

A bubble in the making

Cryptocurrencies are a growing bubble, but not yet a threat to the financial markets, as digital currency capitalization is so far largely virtual. The near-halving of bitcoin's price in a month – wiping out \$160bn of market value – had no impact on the stock market or real economy. The reason is probably bitcoin's illiquidity, despite its reported peak market cap of \$325bn on 16 December 2017. On top of that 14% of the market's average trading volume for July 2018 was produced by crypto exchanges (predominantly aimed at Chinese/Southeastern Asian traders) with trading pairs consisting of mostly small-to-mid-cap crypto currencies without any legal tender (or even their virtual representation like the controversial dollar-pegged Tether).

Actual bubble risk is emerging as the crypto craze drives "real" capitalization. The simple announcement of blockchain-related activity excites the financial markets:

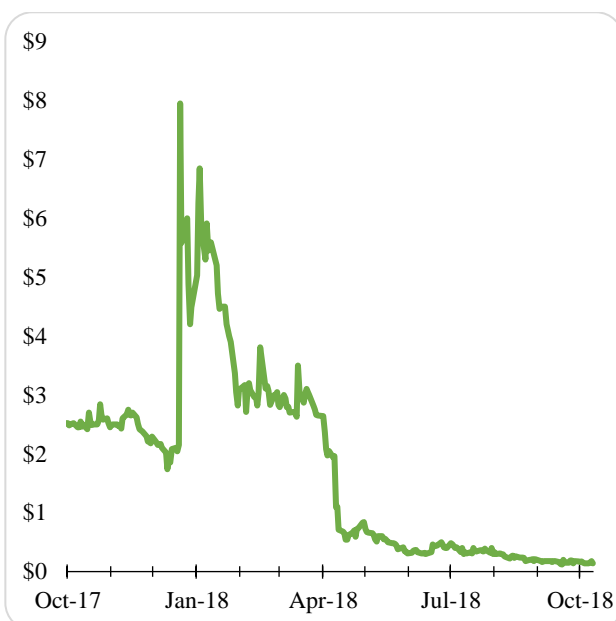
- When **Kodak** announced the launch of the KODAKOne image rights management platform and KODAKCoin, a photo-centric cryptocurrency, in January 2018, its NYSE-listed stock jumped from \$3.1 to \$11.4 in two weeks, boosting the company's market cap by \$352mn.
- **Long Island Iced Tea Corp.**, a US beverage producer, changed its name to Long Blockchain Corp. in December 2017 and announced a shift in its main corporate focus "towards the exploration of and investment in opportunities that leverage the benefits of blockchain technology". The share price jumped from \$2.44 to \$6.99.

Kodak is now trading below \$3, while Long Blockchain Corp. was delisted from NASDAQ in April 2018; the stock now trades over the counter at less than a tenth of its previous price.

Kodak



Long Blockchain Corp.



Source: [Yahoo! Finance](#)

History repeats itself. Having witnessed the high-tech bubble, we clearly see similar signs in the cryptocurrency boom. In the late 90s a company needed nothing more than to add ".com" to its name to become an "appealing" acquisition target or to send its share price through the roof. The consequences and end results are well known.

²⁴ The main hurdle for the latter should be resolved by the proper licensing of crypto custody providers to financial institutions, an effort currently underway in the US, with EU/EFTA, Japan and other crypto-friendly jurisdictions following suit.

Investors' focus – show me the code

Yet the crypto boom creates investment opportunities. One of the main reasons the dot-com bubble burst was the failure of most of companies to deliver profits. However, some firms and their shareholders did very well (e.g. Google and Amazon, to name just two). It is unlikely that such businesses would have appeared without easier access to funding. The current crypto euphoria simplifies fundraising and facilitates business development. But companies issuing coins or tokens will achieve Amazon-like success only if their digital assets are in high demand among end-users by the time they launch their products.

We suggest dividing blockchain projects into two broad categories – applied and breakthrough – rather than running the gamut of different cryptoassets. Applied projects, which try to improve some existing businesses or facilitate processes, represent the first, massively crowded category. For example, such projects build platforms (predominately based on Ethereum) that directly connect producers to customers, eliminating intermediaries. Although such solutions do add real value, their blockchain-based applications can easily operate on ethers and, as such, do not need native tokens. Therefore, we believe the majority of such tokens are likely to be short-lived. Another reason such projects may be unsuccessful in the longer run is that the blockchain infrastructure that is the basis for their DApps (distributed applications) remains immature. The current use of DApps is insignificant and disproportionate to the valuations of the tokens or blockchains they run on, in our opinion, due to the inefficiency and costliness of running such applications.

The second category, breakthrough projects, is sparsely populated. Projects in this category attempt to offer solutions for the whole blockchain industry, invent new approaches, or develop unique technologies. Such projects tend to take into consideration the early build-out phase of blockchain infrastructure and cater to the needs of developers and early adopters, who will then build the products for end-users. Such projects will need to have both native blockchains and native coins. Provided the projects are successfully implemented, these cryptocurrencies are likely to be in high demand by end-users, and therefore attractive to investors. Although such projects can also fail, the risk-reward balance is very appealing, in our view.

Show me the code vs. show me the money. In conventional finance, to make an investment decision, analysts try to forecast the future cash flow generated by a company or project. Equipped with financials, they try to judge the current state of a business and make assumptions about its future development. Financials supplement, or sometimes substitute for, in-depth knowledge of the industries that an entity operates in. But crypto investors do not have such luxuries. **A diligent crypto investor needs to have a grasp of blockchain technology, an overview of the competitive landscape, and an understanding of the software engineering to identify the long-term winners.**

Blockchain technology can reshape the world

What we talk about when we talk about blockchain

Blockchain technology goes far beyond cryptocurrencies, which are just the gasoline in public blockchain systems. Just as the Internet – the Internet of Information – transformed our lives with e-mail, e-commerce, and other exchange of information, blockchain – the Internet of Value – can reshape the world by digitizing and making convertible practically anything of value to humankind.

As often happens with new technologies, terminology is ill defined. This is the case even among blockchain technology experts, who continue to argue about terminology at times. Without attempting to resolve any debates, we recognize the need to clarify some terminology, presenting concepts in simple terms, as we understand them. We do not exclude that our understanding may be different from commonly used interpretations in some cases.

A **distributed ledger** is a digital database spread across multiple computing devices – separate entities in a network of such peer devices, called **nodes**. Ideally, each node mirrors and keeps an identical copy of the full ledger and **verifies** each transaction. However, partial storage and verification of the changes in the ledger are also possible if a so-called **light node** (a computing device of capacity lower than needed for full ledger storage and verification) uses a **light** software **client** to connect to some **full node** it trusts. To make an update to the ledger, the nodes have to reach an agreement, **consensus**. A distributed ledger can exist without a central authority or operator. Due to its distributed nature, such a ledger is much less susceptible to hacking attacks or internal failures, as the nodes affected by such attacks are backed up by those that are not affected. However, the protocols themselves (i.e. the software running on such nodes) are resilient to hacks, as they are protected by cryptographic algorithms.

A **blockchain** is a form of a distributed ledger and a peer-to-peer (P2P) network of nodes that store data in blocks that are consecutively chained to each other. Each block references the transactions of the previous block, with such references stored in a reliably unique fixed-size alphanumeric string, a **hash**. Altering or deleting a historical block requires both modifying all subsequent blocks and re-obtaining consensus among most nodes for every change.

Therefore, the longer a blockchain exists the more difficult it becomes to alter historical blocks (this is the reason why blockchains are considered immutable).

A **miner** creates blocks in the blockchain, consisting of different blockchain users' transactions (transfers of value in Bitcoin, computations in Ethereum), which all of the full nodes verify and store. Miners must have economic incentives to run and support the blockchain. The blockchain compensates them with units called **coins**, or **cryptocurrencies**. The title "miners" is misleading because it sounds like they mine (create) coins. In reality, they create (put together) blocks of user transactions, and an algorithm compensates them in the blockchain's native cryptocurrency for doing so.

A blockchain that supports **smart contracts** may also support **other units of account/value** – usually a special smart contract for accounting who owns how much of them at any given moment, which are called **tokens**. Ethereum, for example, supports multiple tokens of different smart contract specification – for fungible and non-fungible tokens. The distinction here is nominal, as the blockchain's underlying cryptocurrency can be considered a token as well, but it helps us distinguish an actual coin (i.e. digital currency/commodity universal within one network) from a special purpose unit of account or value in the system (i.e. token).

A blockchain can be **public** or **private**. **Public** (sometimes called **permissionless**) blockchains can be joined and left at any time. Everyone can participate in the core activities of a public blockchain network. **Private** or **permissioned** blockchains are closed systems in which each participant is well defined. Private blockchains do not need cryptocurrencies to run the network. These two predominant infrastructure schemes represent one of the key divisions in the blockchain industry currently; which group wins is likely to shape the future²⁵.

Confusion arises with the terms **centralized**, **decentralized** and **distributed** in relation to blockchain networks. The ambiguity comes from the fact that the same terms are often used for two absolutely different concepts. The first concept describes network *topology*: how the network keeps the data and conducts transactions. The second concept describes system *governance*: how the network is controlled, and decisions are made. A system can be distributed from the topology perspective but be absolutely centralized from the governance perspective – private blockchains or cloud services controlled by a single company are good examples of such a case. Or a system can be centralized from the topology perspective but decentralized from the governance perspective, i.e. a classical centralized system where a range of owners vote to resolve governance issues.

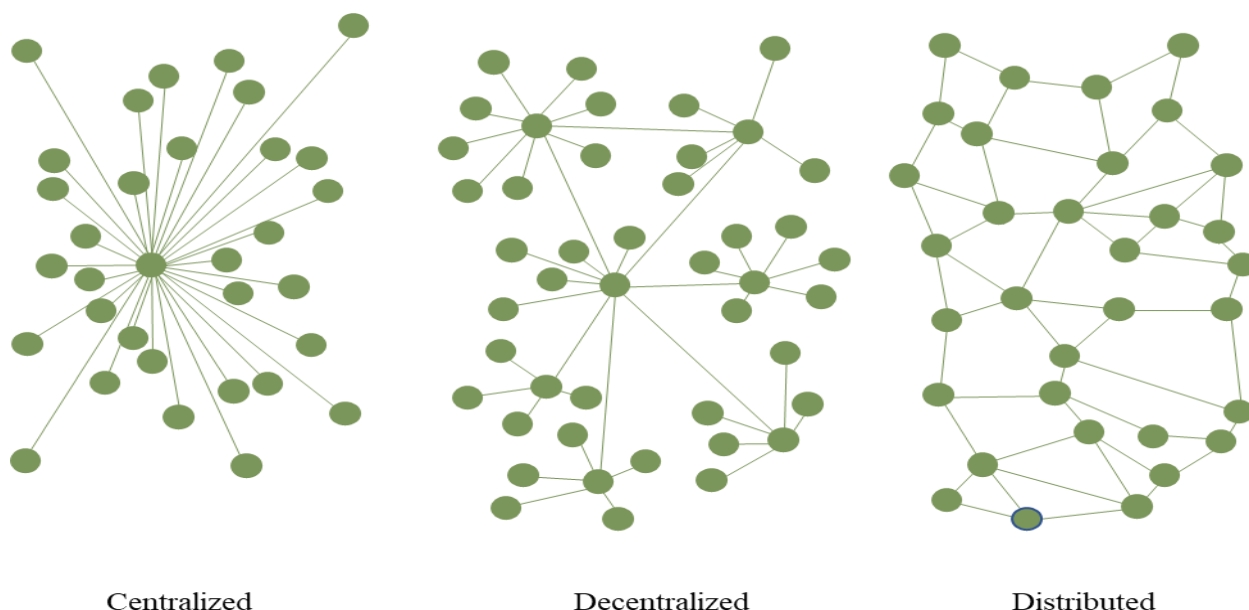
- **In terms of governance, there are two types of blockchains: centralized or decentralized.** A blockchain is *centralized* when it is controlled by a single authority or a consortium of authorities. A *decentralized* blockchain has no single decision maker or governor. All governance is enforced through consensus.
- **In terms of topology, there can be only one type of blockchain: distributed.** Distributed ledgers (and blockchains as a subset of such ledgers) are distributed by definition and cannot be topologically centralized as such. Going forward, to describe the governance of blockchains, we will use the terms *centralized* or *decentralized*, and to outline the topology (processing and data storage), we will use the term *distributed* for blockchains and other peer-to-peer systems, and the term *centrally processed* for systems other than distributed ledgers.

A diagram widely used to explain the difference between types of networks muddles the different concepts for **blockchains**, we believe. Without specifying from what angle to look at a blockchain – topology or governance – describing it makes little sense. The figure below depicts the origins²⁶ of the terminology often responsible for some confusion in relation to *distributed* and *decentralized* when discussing blockchain networks. However, the author was designing the command and control communication network for the US military in the midst of the US-USSR nuclear crisis. He never intended to depict a self-governing or *decentralized* system. In terms of governance *all* of the network nodes were still to be *centrally controlled* by the US government. Therefore, the figures should only be used to describe a network's topology, not its governance.

²⁵ Whether or not ownership and other rights to digitized or natively digital assets will be attested by all and everyone (public) or only a certain group (private) of actors may and will have enormous socio-economic impact on the way we create and distribute value in the future. The pendulum of industry sentiment continues to swing, usually following swings of the public blockchain market; however, we believe that in the upcoming years both blockchain architecture types will be developed, with private blockchains eventually getting "connected" to public chains as the latter group resolves scalability and interoperability problems.

²⁶ Paul Baran "On Distributed Communications: I. Introduction to Distributed Communications Networks", RAND Corporation (1964).

The original conceptual depiction of networks described only their topology, not their governance



Source: RAND Corporation

The *de*-centralized (to be more correct in the intended semantics) network depicted in the middle of the diagram would be less likely to withstand a Soviet nuclear strike if it happened to affect some of the more connected nodes, especially the one in the center (presumably a US military command post). The network depicted to the right, a distributed system where each node is connected to almost every neighboring node and without a single central node, would be more likely to maintain communication with the rest of the surviving nodes if disaster struck. The cited research formed the very basis of what became the Internet. Only almost half a century later did Bitcoin introduce the first *decentralized* distributed network in terms of governance.

Let's dream in color: moving beyond the basics

Decentralization is the breakthrough, the holy grail of blockchain technology; potentially, it can make many intermediaries and central authorities redundant. Decentralized blockchains are *trustless*: left to the consensus of participating nodes they do not need trusted third parties to keep and run the ledgers. They are also censorship-resistant, as there is no authority to alter a record or to stop a transaction from being conducted. Such blockchains are also more robust in the face of malicious behavior. Participating nodes do not have to trust each other to reach consensus. Combined with immutability, these qualities should allow blockchain technology to reshape many economic sectors for the goodwill of society.

Over the long term, no business making money serving as a trusted third party will benefit from trustless blockchain development, we believe. Quite the opposite: this technology will dig the graves of such businesses, and therefore they are likely to resist its development. The most notable victims would be contemporary financial institutions, such as banks, exchanges, and payment systems. However, this threat will take a long time to materialize. Meanwhile, some intermediaries will seek to benefit from the technology and to build private blockchains to cut costs.

Trustless blockchains and cryptocurrencies could also jeopardize the dominance of governments. Blockchains could potentially substitute government agencies in keeping and updating trusted records, such as the registration of births, marriages, or property transfers. Blockchains could revolutionize current electoral voting processes by integrating identity management and cryptography to maintain the confidentiality, resilience, security, and integrity of an election. Furthermore, cryptocurrencies could theoretically complement official fiat money, drastically reducing states' control over the economy. The much-anticipated tokenization of assets should enhance world trade by increasing the global turnover of goods, further breaking down barriers between markets and offline/digital economies.

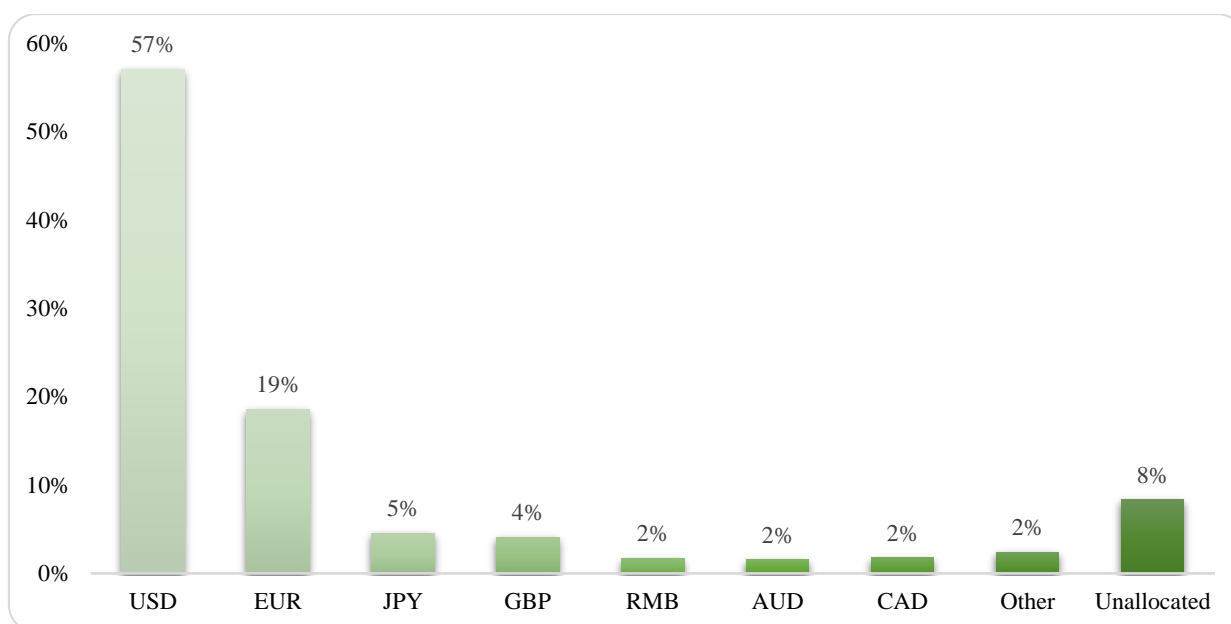
One of the main arguments against cryptocurrencies is that no government will accept them to pay taxes – the main purpose of a fiat currency. While this is likely to be the case for decentralized cryptocurrencies, governments could still issue their own cryptos and make them legal tender within their borders²⁷. There have been proposals (although not yet successful) to allow tax payments in crypto, as in the US [state of Arizona](#). In any case, this argument

²⁷ “China’s central bank is developing its own digital currency, even as it bans bitcoin and private cryptos”, South China Morning Post.

does not exclude cryptocurrencies becoming accepted as a means of payment for international transactions, a role currently fulfilled primarily by USD. Many countries would likely welcome a decentralized cryptocurrency for use in international trade (as an alternative to the greenback's current dominance), although the US government is likely to resist such a scenario.

Another contemporary consensus is that cryptocurrencies currently cannot serve as a means of payment due to their extreme volatility. However, high volatility is generally a function of speculation. When the cryptocurrency is at equilibrium, speculative short-term investors should disappear and volatility decline to the fiat level. What would then stop a decentralized cryptocurrency from becoming a widely adopted store of value? On one hand, governments dislike having anything uncontrolled. On the other hand, large economies such as Japan, China and Russia keep much of their national reserves denominated in USD – a currency that they have no control over – and they would like to diversify. The US seems to be the main loser in both of the above-mentioned cases, and therefore, logically, along with financial institutions, should be the strongest opponents of cryptocurrencies.

More than half of worldwide national reserves are kept in USD



Source: IMF

Countries' attitudes towards cryptocurrencies range from very friendly, as in Japan and Switzerland... [In April 2017, Japan became the only country in the world where bitcoin is legal tender.](#) Unsurprisingly, it has about 50% of all bitcoin trading volume. Switzerland, since becoming the home to Ethereum's ICO, has come up with the most predictable and clearly defined initial coin offering and secondary market regulation.

...to very hostile, as in Bangladesh, where using bitcoins can be punished with a 12-year prison term. China lies closer to this end of the spectrum. Both ICOs and crypto exchanges are illegal in the country, which makes trading cryptocurrencies technically illegal as well. And Chinese authorities [have been trying](#) to limit cryptocurrency mining operations, with the country still accommodating [the majority](#) of the global crypto mining power. At the same time, its government has long been believed to plan the launch of a state-backed cryptocurrency.

Although approaches differ, the general trend is to regulate the usage and adoption of cryptocurrencies rather than to try to eradicate them. Although it is banal, it must be said: it is impossible to stop progress. Given that the world's third-largest economy has accepted a cryptocurrency as a legal means of payment, others are likely to follow. Cryptocurrencies will eventually be adopted, albeit with some regulations.

Everything comes at a cost

The essential drawbacks are inherited. Distributed systems are less efficient and orders more expensive than centrally processed ones, simply because the former employ more hardware and store the data on multiple nodes across the globe, nodes that need to reach consensus before updating data. Supporting a decentralized blockchain is expensive and must offer economic incentives to the parties responsible for running and updating them to do so. To operate effectively, an active trustless chain also needs scale, in terms of both number of participants and operations processed.

Centrally processed systems are not distributed ledgers; distributed ledgers can be centralized or decentralized

	Centrally Processed (Single data storage place)	Distributed (Multiple data storage place)	
		Centralized (Single authority/group)	Decentralized (No single authority)
Private (Permissioned)	VISA, SWIFT	Ripple	Should not exist
Public (Permissionless)	WhatsApp	NEO, EOS	ETH, BTC

Source: HASH CIB

Therefore, we arrive at two important conclusions. First, to choose a blockchain structure over a centrally processed network, there must be a positive net economic effect from improved security and reduced cost of trust against a backdrop of substantial investment, reduced efficiency, reduced speed, and increased operating cost. This net impact is not always as clear-cut as it seems at first glance. Second, decentralized private blockchains should not exist. It makes no sense to build up and support a permissioned network to give up power afterwards. Centralized distributed systems tend to perform better and are easier to update and maintain, as there is little need to reach consensus on governance. An investor should bear both of these points in mind when analyzing a blockchain project.

Regardless of how promising blockchain technology sounds, it is still far from mainstream adoption. Aside from obstacles such as legal restrictions and the volatility of cryptoassets, there are huge challenges faced on the technology side. Contemporary blockchains face two main hurdles standing in the way of mass adoption and universality:

- **Scalability** – The speed at which a blockchain can process dozens of thousands of transactions in a distributed, spread out and trustless environment
- **Interoperability** – The ability to connect between different blockchains to execute smart contracts and/or transfer value

Backed by billions of dollars of investments, the best industry talents are focused on solving these engineering problems, and some promising outcomes should materialize soon. Resolving both these issues, in our opinion, is the key to winning the long-term race for blockchain supremacy.

No mass adoption without scalability

The future real-world application of blockchain relies on the technology's scalability. Unfortunately, established blockchains have limited speed in their current architecture. The number of transactions a blockchain can process is finite, since each node stores all states and processes all transactions. In other words, a blockchain cannot conduct more transactions than its least efficient node can. Although this provides tremendous security, it greatly restrains scalability.

A blockchain's throughput is restricted by the time needed to create a single block. For Bitcoin it takes around 10 minutes, while for Ethereum it is 12-15 seconds. This results in bottlenecks and high transaction costs – as only limited amount of transactions can fit into a block, which prohibits the day-to-day usage of blockchains. A common example of how these scalability issues limit blockchain's competitiveness vs. centrally processed systems is the comparison with VISA. The payment system regularly handles up to 2,000 transactions per second or more than 180mn daily, peaking at 56,000 tx/s during [testing](#) and a [reported](#) 11,000 tx/s load at Christmas years ago.

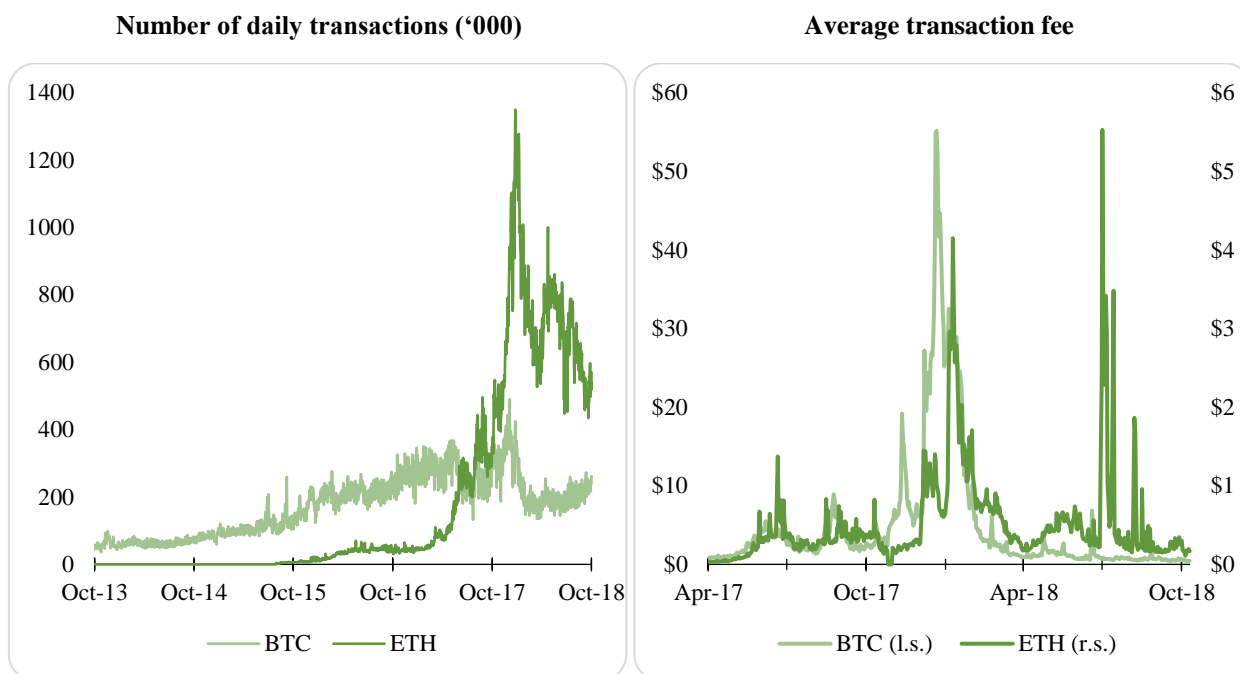
Centrally processed payment systems are likely to always be faster than decentralized blockchains. To handle more transactions and to increase scale, traditional database systems simply add computing power. Such an approach does not work for blockchains. Given that in a blockchain each node needs to process and verify every transaction, it would require adding same computing power to every single node in the network and enhancing bandwidth to reduce latency, as each new block needs to be propagated through the network. Taking this logic to an extreme, most nodes would ultimately be unable to keep up with growing requirements and have to drop out of the network, leaving it in the hand of just a few. The blockchain would lose its defining characteristic – decentralization.

Moreover, blockchains conduct transactions discreetly, while payment systems do so continuously. The maximum transaction speed of a blockchain is the speed at which it creates a block. A common belief that Bitcoin can conduct around 7 transactions per second comes from a misconception. A Bitcoin block, which is one megabyte in size²⁸, is formed in 10 minutes and can contain around 4,000 transactions (dependent on their byte size, which can vary, but approximately 250 bytes each). Therefore, rough throughput estimate equals 4,000 transactions per 600 seconds.

²⁸ Since 2017 Bitcoin can support blocks of up to 4Mb in size if all of the transactions contained in a block are using a major technological update to the protocol called [SegWit](#). However, at the time of writing most Bitcoin blocks are still [around 1Mb in size](#) and adoption of SegWit is far from being universal, while [steadily growing](#).

However, this does not mean that Bitcoin can process ~ 7 tx/s as some calculate (dividing 4,000 transactions by 600 seconds). A single transaction will still take 10 minutes to process, but Bitcoin is able to process 4,000 such transactions in each 10-minute interval.

The bottlenecks result in high transaction costs as users increase miner-rewarding fees for their transactions to be preferred. Average fees for Bitcoin peaked at \$55.16 on December 22, 2017, declining to around \$12 by the end of January 2018. The all-time high number of transactions with this cryptocurrency was 490K on December 14, 2017. For Ethereum the highest transaction fee was \$4.14 on January 19, and the largest number of transactions per day was 1.35mn on January 4²⁹. – a fraction of VISA’s peak.



Source: [BitInfoCharts](#)

However, this inherited comparative inefficiency should not matter much when the scalability issue is resolved. We doubt that it would bother anyone if VISA’s throughput were still higher than Bitcoin’s when the latter is able to conduct tens of millions of transactions in 10 minutes. Moreover, although VISA supports thousands of payments per second, settlement takes hours if not days, due to back-office and compliance procedures. This compares poorly to the minutes needed for effective finality in the Bitcoin network.

Traditional payment systems will have to dramatically reduce their charges. Being an oligopoly, these payment channels make extra economic profit, which is likely to evaporate due to emerging competition with blockchains. Although the cost of transactions via blockchains cannot be less than that through centrally controlled conventional systems (remember, running blockchains is more expensive), the former can charge much less than the latter. The reasons are a practical absence of both overhead and bureaucracy.

Three obvious but “flawed” approaches to scalability...

The first is to give up on scaling individual blockchains and instead assume that users will use many different alternative coins (altcoins³⁰). This greatly increases throughput but comes at a cost of security: an N-factor increase in throughput using this method necessarily comes with an N-factor decrease in security. Therefore, it is arguably non-viable for more than small values of N.

The second is to simply increase the block size limit, risking giving up on decentralization. This can work and has already been done with Bitcoin, when the chain split (**forked**) into two: traditional Bitcoin with 1 MB block size and Bitcoin Cash with 32 MB block size. However, such an approach has its restrictions: the higher the block size becomes, the more computing power each node needs to conduct processing and more storage to host a full ledger. As a result, as mentioned above, smaller nodes drop out and, left to a small number of supercomputers, the blockchain becomes centralized.

²⁹ According to [BitInfoCharts](#).

³⁰ By altcoins we mean cryptoassets that represent separate blockchain protocols “alternative” to Bitcoin (hence the name), and not tokens, released on platforms like Ethereum.

The third is “merge mining”, a technique where there are many chains, but all chains share the same mining power. Currently, Namecoin gets a large portion of its security from the Bitcoin blockchain by doing this. The same has been proposed for the RSK network – a Turing-complete protocol developed “on top” of the Bitcoin network. If all miners participate, this could theoretically increase throughput by a factor of N without compromising security. However, this also has a problem as it increases the computational, bandwidth and storage load on each miner by a factor of N , and so in fact this solution is simply a stealthy form of block size increase.

...lead us to the Scalability Trilemma

Vitalik Buterin, the initial proponent of the Ethereum protocol, formulated the Scalability Trilemma, which is a special case of the [CAP theorem](#) from theoretical computer science. At a fundamental level, blockchains are distributed data storage systems running “in the wild” - as different nodes with different hardware and bandwidth properties, located all around the world. This makes assuming so-called network partition (i.e. signal latency or the unavailability of a number of nodes at any particular time) a constant factor. Thus, according to the CAP theorem, if network partition is an issue present, one always has to choose between network consistency³¹ or availability³² since it is possible to only achieve two out of three of these traits at one time – at least at the current stage of technological development. Therefore, applying this to distributed ledger technology one can choose only two out of three following properties:

- **Decentralization** (defined as the system being able to run in a scenario where each participant only has access to $O(c)$ resources, e.g. a regular laptop)
- **Scalability** (defined as being able to process $O(n) > O(c)$ transactions)
- **Security** (defined as being secure against attackers with up to $O(n)$ resources),

where c refers to the size of computational resources (including computation, bandwidth and storage) available to each node, and n refers to the size of the ecosystem in some abstract sense, assuming that transaction load, state size, and the market cap of a crypto currency are all proportional to n .

Scalability: Three “flawless” approaches

Change of consensus algorithm, state channels, and sharding are the current mainstream approaches that should theoretically allow blockchains to massively scale. Different blockchains are trying to develop their own ways to tackle the problem, but in fact, they use all variations or combinations of these three. However, as far as we know, any solution implemented so far has sacrificed decentralization or security or both. Conventional wisdom holds that the first angle of attack on the scalability issue is changing the consensus algorithm from proof-of-work (PoW) to proof-of-stake (PoS).

Consensus algorithms: proof-of-work vs. proof-of-stake

The consensus algorithm is the cornerstone of any blockchain. It is the process used to reach agreement between a blockchain’s participants on a single data value, a block, or any transaction contained in that block. Algorithms are designed to achieve reliability in networks that consist of multiple unreliable nodes. Consensus algorithms must assume unstable communication and unavailability of some processes and participants. They must be also fault-tolerant to the participants’ malicious behavior – Byzantine Fault Tolerant³³ (BFT), to be precise, a concept explored in detail below.

Proof-of-work (PoW) is a consensus algorithm that requires a substantial but feasible effort to deter malicious behavior. A blockchain’s participants are concurrently trying to solve rather straightforward but computing power-consuming mathematical problems. This process is called **mining**. The miner that solves a given problem first is allowed to create a block. Then nodes check whether the solution is correct and validate the block. Consensus is achieved by nodes simply following the *longest chain* first made available to them. The blockchain rewards the winning miner with newly issued coins (this process also introduces **inflation** to the cryptocurrency supply). The miner is also allowed to choose which transactions to put in the block and therefore includes transactions ready to pay the highest fees. This way the system balances the transaction costs. To compensate for constantly improving computing productivity, the Bitcoin blockchain adjusts itself, so that it always takes around 10 minutes to solve the computational puzzles. This is called **difficulty adjustment** and happens roughly every two weeks in the Bitcoin network.

³¹ A network being able to update the database only with information guaranteed to be correct by last full network consensus, even if it means discarding the most recent update proposal.

³² A network updating with the most recent data at the risk of having to discard it in the future if the consensus deems it incorrect.

³³ The concept of Byzantine Fault Tolerance in distributed systems was introduced in 1982 by Lamport, Shostak and Pease in a theoretical computer science paper as “[The Byzantine Generals Problem](#)”.



PoW has served well so far in providing security and decentralization to trustless blockchains, particularly Bitcoin. At the same time, the algorithm is relatively slow and structurally unscalable. Moreover, takeover risk is growing as the concentration of mining capacity of some pools continues to rise. Bitcoin [experienced miner centralization](#) several times in its earlier days. Theoretically a miner obtaining more than 50% of all computational power (**hashrate**) of the network could rewrite the blockchain's history; such an action is called a **51% attack**. However, the longer the blockchain grows, the more expensive (and, in all unlikelihood, unprofitable) such an attack becomes. Although it runs against the commonly held view, we are not afraid of such a malicious attack on Bitcoin from widely known mining pools, as it would be against their interest. But the risks of centralization – where the dominant miner, for example, effectively increases transaction fees by not including transactions with fees below a certain threshold, or introduces other forms of transaction censorship³⁴ – could still materialize.

Estimated cost of a 51% attack on a blockchain (as of 11 October 2018)

Bitcoin	\$1 253 244 636
Ethereum	\$475 100 432
Zcash	\$123 780 268
Bitcoin Cash	\$91 814 070
Litecoin	\$85 152 199
Dogecoin	\$71 300 241
Ethereum Classic	\$28 593 817

Source: HASH CIB

Finality: probabilistic and commercial³⁵

The possibility of a long-lasting 51% attack from unknown pools is always there. Such an attack could revert all of a blockchain's history to the detriment of its users. According to MIT professor Silvio Micali, one should assume malicious behavior even without any economic benefit in mind, with such behavior illustrated in various large-scale (non-blockchain-related) hacker attacks in recent years. There are also [many examples](#) of short term profit-seeking attacks on less secure public blockchains. Given such a constant threat, PoW never provides *true* finality to any transaction on the blockchain, no matter how many blocks deep it lies. This phenomenon is called “probabilistic finality”.

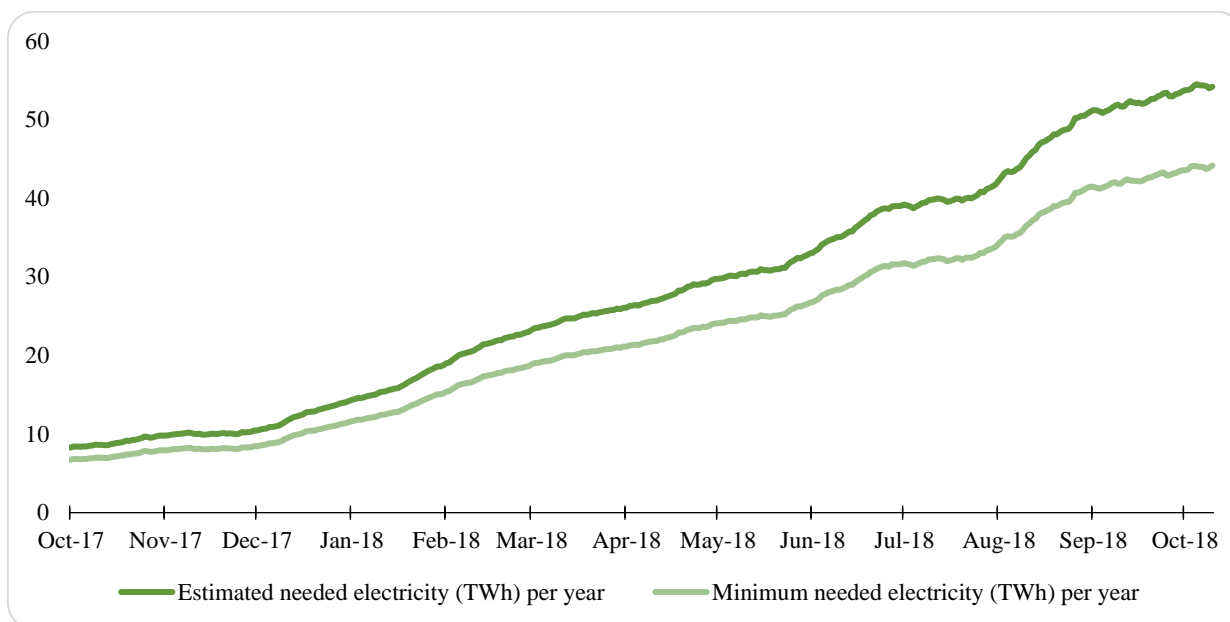
From the technical perspective, this means that we do not know whether someone is right now building a new chain of blocks that is longer than the current one and, as such, could successfully replace the latter. Generally speaking, it seems unlikely for now, but such behavior can be observed on smaller scale. This brings us to one important observation – probabilistic finality means full consistency may be achieved in a given period of time, but can never be guaranteed for all time. This is the sword of Damocles hanging over PoW blockchains.

PoW has been also widely criticized for wasting electric power on seemingly useless computations. The total amount of electricity annually used to mine bitcoins has already reached 44-54 TWh, what Singapore consumes in the same period of time. However, we would argue that the energy used for maintaining the Bitcoin network's security is not wasted, and on top of that Bitcoin mining drives global innovation in the energy sector.

³⁴ Again, such open behavior would be detrimental to the miner in the long run, as eventually no one would want to use such a chain. [Miners have historically reduced their hashrate](#) when approaching 51% of network's capacity for the same reason.

³⁵ **Finality** conditions are the rules that determine when a given block can be considered finalized.

Estimated Bitcoin energy consumption (as of 11 October 2018)



Source: HASH CIB

Proof-of-stake (PoS), which is much less energy consuming, offers a potential solution to the scalability problem.

A PoS blockchain delegates the right to create a block to one of its members, usually called a **validator**, selected through a certain algorithm accounting for such validator's coin ownership share **staked** to participate in such a selection. Then validators check whether the block is correct, vote on it, reach consensus with other nodes and thus, validate the block. As with PoW, the network compensates the validators for their work by issuing new coins. However, mining does not exist in PoS chains. Thus, there is no excessive electricity consumption and, much more importantly, no need to waste time or network computing power on work irrelevant to the actual processing of transactions. As a result, a blockchain can achieve consensus in a shorter time under PoS than under PoW, allowing higher throughput.

True finality does not exist in PoS either. The innovation of PoS is based on penalizing or slashing³⁶ the parties involved in block creation and validation³⁷ for malicious behavior. As with PoW, the probability that someone would spend funds buying hardware to attack a network just for the sake of a malicious action decreases as the blockchain grows longer, although it never reaches 0%. In PoS, to successfully attack a chain, the attacker would have to pay validators an amount exceeding what they have staked with the chain plus what they expect to earn from serving it. The likelihood of such an event declines with expanding networks, but never goes to 0%. Thus, in PoS one can speak of "commercial finality".

Decentralization and security are still at risk in PoS blockchains. The rich become richer and the poor become poorer under a simple version of PoS consensus: if the minimum stake to become a validator were high, only a limited number of nodes would be able to participate and earn rewards. Those above the minimal threshold would become richer proportionally to how rich they already are and those below the threshold would stay poor. The gap would grow over time, leaving the blockchain in the hands of just a few.

PoS algorithms are a research frontier, and their advantages over PoW are theoretical. Much work remains to be done to arrive at an optimal PoS consensus algorithm that would be adopted as best practice. **Chain-based PoS** and **BFT-based PoS** are the two main designs among the various ways to implement PoS. Chain-based PoS *pseudo-randomly* (hereinafter we'll just use "randomly", as true randomness is believed to be unachievable in artificial systems) chooses a validator to create the next block. In BFT PoS the acts of suggesting the next block and creating the next block are decoupled. First, BFT PoS randomly assigns a validator to propose a block. Then validating nodes determine which block gets added to the chain through a multi-round voting process. Most BFT-based PoS algorithms use, as a source of inspiration, an algorithm called Practical Byzantine Fault Tolerance (PBFT)³⁸. However, this algorithm requires synchronous communication between nodes (which is impossible "in the wild" of public

³⁶ **Slashing conditions** are rules that determine when a given validator can be deemed beyond a reasonable doubt to have misbehaved (i.e. voting for multiple conflicting blocks at the same time). If a validator triggers one of these rules, their entire stake (deposit) is deleted.

³⁷ In some PoS designs, block creation and validation are done by different parties, yet the incentive mechanism in both cases is based on involved parties "staking" their coins.

³⁸ Practical Byzantine Fault Tolerance was proposed as another theoretical solution to BFT in a 1999 [research paper](#) of the same name by M. Casto and B. Liskov.

blockchains), as well as multiple rounds of communication (which limits the number of nodes that could participate in validation without it losing speed). Thus, PBFT in its pure form could only apply to centrally controlled (permissioned) distributed systems.

Other BFT-based consensus approaches. It is worth noting that the term BFT is used for two different concepts: 1) the general category of algorithms resistant to Byzantine (malicious) behavior, and 2) different types of specific BFT-based algorithms (let us denote them *BFT). All consensus algorithms must be Byzantine Fault Tolerant – resistant to Byzantine behavior. In this sense, both PoW and all kinds of PoS (and many other distributed consensus protocols not discussed here) are BFT consensus algorithms (meaning their characteristic). At the same time, neither PoW nor chain-based PoS are *BFT algorithms (i.e. using BFT acronym as part of a name of a particular algorithm). To illustrate, we divided consensus algorithms into five types:

Base	Name	Example
Resources-Based	PoW, Po-Space etc.	Bitcoin, Bitcoin Cash, Litecoin, Monero, Zcash
Economic-Based	(chain-based) PoS, DPoS	Casper (CTFG), Ouroboros (Cardano), BitShares, Steem
Synchronous (*BFT)	Practical BFT, Simplified BFT	Hyperledger Fabric (v 0.6), Exonum
Asynchronous BFT (as *BFT extension)	Asynchronous BFT (as a name), BFT-based PoS	Hashgraph, Polkadot, Tendermint (Cosmos), Honey Badger BFT
Combination	Hybrid PoS+PoW, DPoS + Asynchronous BFT	Casper (CFFG), EOS

Source: HASH CIB

Choosing consensus architecture is vital for a blockchain, as it is extremely difficult to change it afterwards.

Ethereum has been building the so-called Casper protocol (effectively “PoS for Ethereum”) to switch from PoW to PoS since 2015. Two Casper solutions are being developed simultaneously. Casper The Friendly GHOST (CTFG) is an explicit chain-based PoS research and development project led by Vlad Zamfir³⁹. The more recently proposed Casper The Friendly Finality Gadget (CFFG) is an amalgamation of both PoW and BFT PoS consensus algorithms led by Vitalik Buterin. CFFG is intended as a hybrid, transition version of PoS and could be introduced to the Ethereum network by end-2018 – early 2019. The idea here is that PoW would be used to achieve consensus on the most recent blocks, while PoS validators finalize blocks older than a certain threshold (currently set at about 20-25 minutes).

Delegated proof-of-stake (DPoS) consensus gives up decentralization to improve scalability. In DPoS, users are rewarded for delegating their stakes to validators they trust rather than participating in validation themselves. As a result, with fewer validating nodes the network can reach consensus much faster. And because of this reduction in validator count, we can add some finality by bringing PBFT consensus to selected validators. Since there are just a few of them⁴⁰, the between-node-communication-heavy PBFT becomes possible without significant time delays. The tradeoff is again centralized control, since at the end of the day powerful validator nodes (nodes that convinced the network to vote for them) control the network.

Other pioneering consensus algorithms underlie the state-of-the-art blockchain architectures of Polkadot, Cosmos, and TON. Polkadot is developing a modern asynchronous BFT algorithm inspired by the simpler Tendermint (used by Cosmos protocol) and by the substantially more involved Honey Badger BFT. In doing so, it introduces additional participants in its consensus, essentially helping validators to create new blocks and ensure PoS blockchain finality. This approach has been adopted by TON and is discussed later in this report. While exciting and promising, these algorithms are at the forefront of blockchain technology research and still have to prove, through trial and error, their applicability and robustness.

State channels – a second-layer, off-chain solution to scalability

A state channel is a two-way communication channel between users, or between a user and a machine on a smart-contract capable network. The idea behind the state channels scalability solution is that only transactions needed to be kept forever are stored on the blockchain (or the first layer, for that matter), as it is too costly and too slow. Alternatively, two users of the same blockchain can open a two-way mutual communication channel. In this case, further transactions take place entirely off the main blockchain, exclusively between the participants, and only the initial and the final states (the opening and closing transactions) are written on-chain. Then a network of thousands

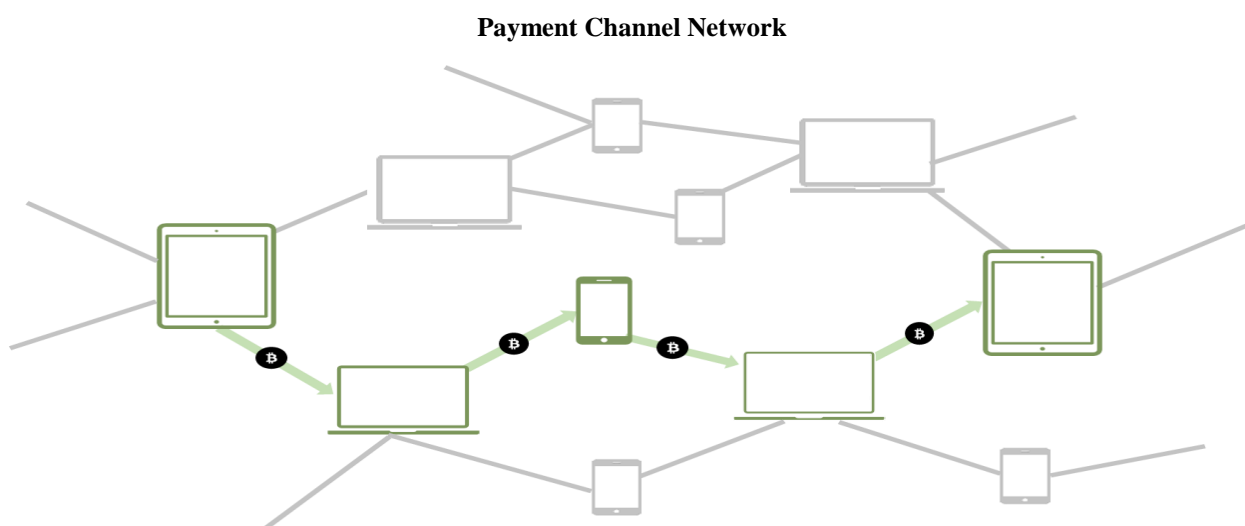
³⁹ It is built to emulate the Greedy Heaviest Observed Subtree (GHOST) protocol (currently used for PoW on Ethereum) for determining the chain that has most computation done on it – but in a “friendly” PoS way, hence the reference to a famous “friendly ghost” cartoon character Casper.

⁴⁰ EOS, for example, has 21, and uses its version of asynchronous BFT algorithm on top of DPoS.

of such two-party channels is created to enable a series of two-party nexuses, connecting participants that do not have a direct state channel between each other. In simple terms, state channels are off-chain networks that run parallel to the blockchains and can scale up to any number of participants. This should be a very cheap, fast and nearly limitless way to execute transactions.

The key value proposition of state channels is the ability to build trustless bidirectional communication channels. The concept of **payment channels** introduced the technology of off-chain transaction channels with Bitcoin Lightning Network (BLN) [White Paper](#)⁴¹. The idea of payment channels was adopted for stateful blockchains (like Turing-complete Ethereum) later, thus creating the concept of state channels. That is why below we refer to payment channels on Bitcoin in providing an overview of how state channels work in the simplest form. Other implementations might vary insignificantly from this overview, based on the underlying blockchain protocol's functionality.

To open a bidirectional payment channel, two users deposit on a blockchain the amount they want to trade. The parties write the initial transaction, storing funds in a special multi-signature address (**multi-sig**), which redistributes the funds only if both of the parties have signed the new balance with their private keys. The introduction of the multi-sig along with *time*- and *hash*-lock transactions makes the channels bidirectional and trustless⁴². Time-lock allows a party to withdraw the initially deposited funds (when the pre-set lock-time expires) if anything goes wrong. Hash-lock allows one party to pass value securely to another (and vice versa) along a string of two-party channels. This way any two users wishing to transact do not have to establish a direct payment channel with each other. Instead they can use a chain of intermediaries with already established mutual channels. All they need is a route; the network does the routing automatically. The parties do not broadcast transactions to the network and commit only the final balance when they decide to close the channel.



The speed of state channel transactions is limited only by the Internet connection quality and the speed of light, since they are peer-to-peer off-chain communications. The payments should be reasonably cheap since one pays only to open or close a channel and to peers or nodes for using their channels. The latter fees should be cheaper than on-chain fees, given that the blockchain is not updated with every payment.

New virtual financial agents are likely to appear, creating payment hubs and threatening centralization. Peer-to-peer payment channels are more suitable for micro-to-medium sums than for large amounts. For a payment to go through a channel, each of its intermediary participants must have a balance at least equal to the amount of the transaction. While reasonable for small amounts, it might be difficult finding a P2P path with enough capacity for large sums. To meet demand, some participants will probably choose to become professional transaction brokers able to freeze large sums of money. Given zero credit risk, the cost of running such a business would be just the cost of the locked up funds. Contemporary financial institutions would be among the candidates to diversify into this area.

Such a network-topology-based economic model evokes fears and accusations of possible future centralization among both Lightning supporters and competitors such as Bitcoin Cash network miners, boasting higher throughput and shorter confirmation time on the protocol they secure. Lightning Network developers are working on automating

⁴¹ Technically, the Bitcoin payment channels *are not* state channels as they use the Unspent Transaction Output (UTXO) model for keeping record of who owns what, instead of a state. Bitcoin payment channels are formally a type of proto-state channels. Yet for the sake of simplicity, in this section we consider all two-party channel technologies on layer 2 of blockchains, as they are very similar in basic architecture. Additionally, see [Glossary](#).

⁴² For a more detailed breakdown of the technology in its Bitcoin implementation, please refer to the following series by Aaron van Wirdum in Bitcoin Magazine: [Part 1](#), [Part 2](#), [Part 3](#).

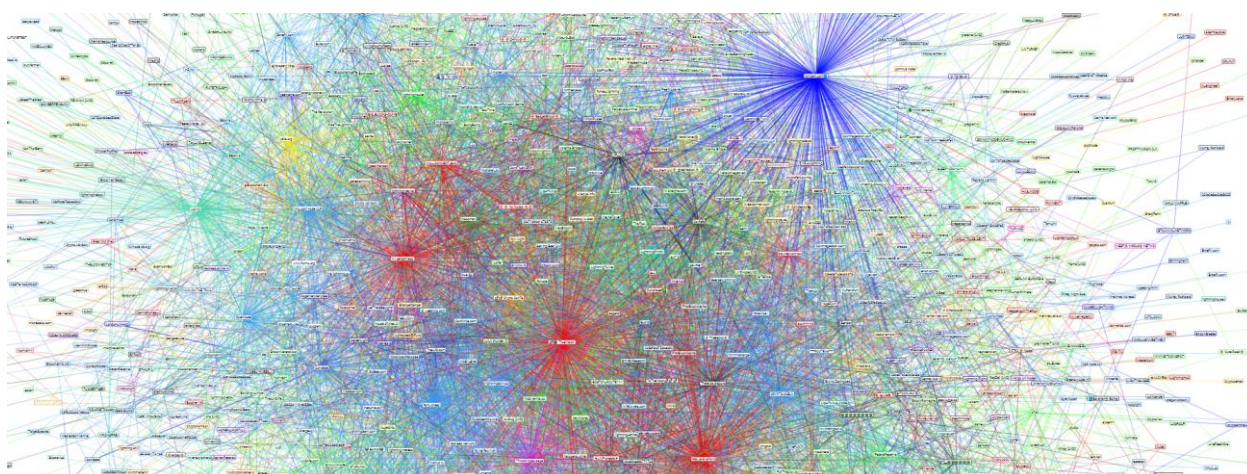
and anonymizing payment routing, which would presumably mitigate risks by making payment hub providers honor commonly established fee levels and disable their ability to censor (block) transactions.

Automatic routing is a challenge. Existing methodologies support routing for channels that do not transform the participants' conditions. This is not the case for state channels where conditions change after each transaction or even during the transaction. Therefore, after each payment (or other form of a state change) a new route must be found. As of now, we know no such dynamic routing solutions. The problem is known as Packing Based Routing on a Dynamic Network and is still a scientific research frontier.

Mainstream state channel networks

Most current efforts are directed at building state channels on top of the two largest blockchains, Bitcoin and Ethereum. Bitcoin Lightning Network is probably the most highly anticipated payment channel network. However, it will focus solely on payments and on payments with bitcoins and litecoins only. While rapidly growing, BLN is still under construction, although different developers have released a few user-unfriendly and limited capacity beta versions⁴³.

Snapshot of current Lightning Network state



Source: reckexplorer

There are several state channel projects on the Ethereum network. The landscape is competitive as different teams of programmers are developing a number of projects simultaneously. Such competition should benefit end-users, as proposed solutions tackle different aspects of state channel functionality on Ethereum.

Raiden is a work-in-progress Ethereum-based payment network. A member of the Enterprise Ethereum Alliance⁴⁴, Brainbot Technologies AG, is developing this project. Raiden's architecture, unlike that of BLN, allows the network to operate with ETHs and any ERC-20⁴⁵-compatible tokens. **TrueBit**, an off-chain computation and payment solution developer with a number of products already being tested, is developing layer 2 solutions for Ethereum that support scaling distributed smart contract computations.

The concept of sidechains, introduced in 2014 by Blockstream⁴⁶, has laid the ground for most of the layer 2 scaling and interoperability solutions that have followed. It proposed using an underlying blockchain (the Bitcoin network, to be exact, as the most decentralized and secure at the time) as a settlement layer for other blockchains. This concept generally inspired payment channels (which resulted in the Lightning Network project), we believe. But in its totality – having an actual blockchain on top of the Bitcoin blockchain – it was implemented by the RSK Labs team (formerly Rootstock), to enable smart-contract execution on top of Bitcoin with their second-layer protocol.

⁴³ Current implementations of Lightning protocol include Lnd, developed by Lightning Labs; C-lightning, developed by Blockstream; and Eclair, worked on by ACINQ. All three implementations are extensively being used and tested by the fast-growing Lightning network node-running community. There is also an implementation by MIT's Digital Currency Initiative, called Lit, presumably less developed at the time of writing.

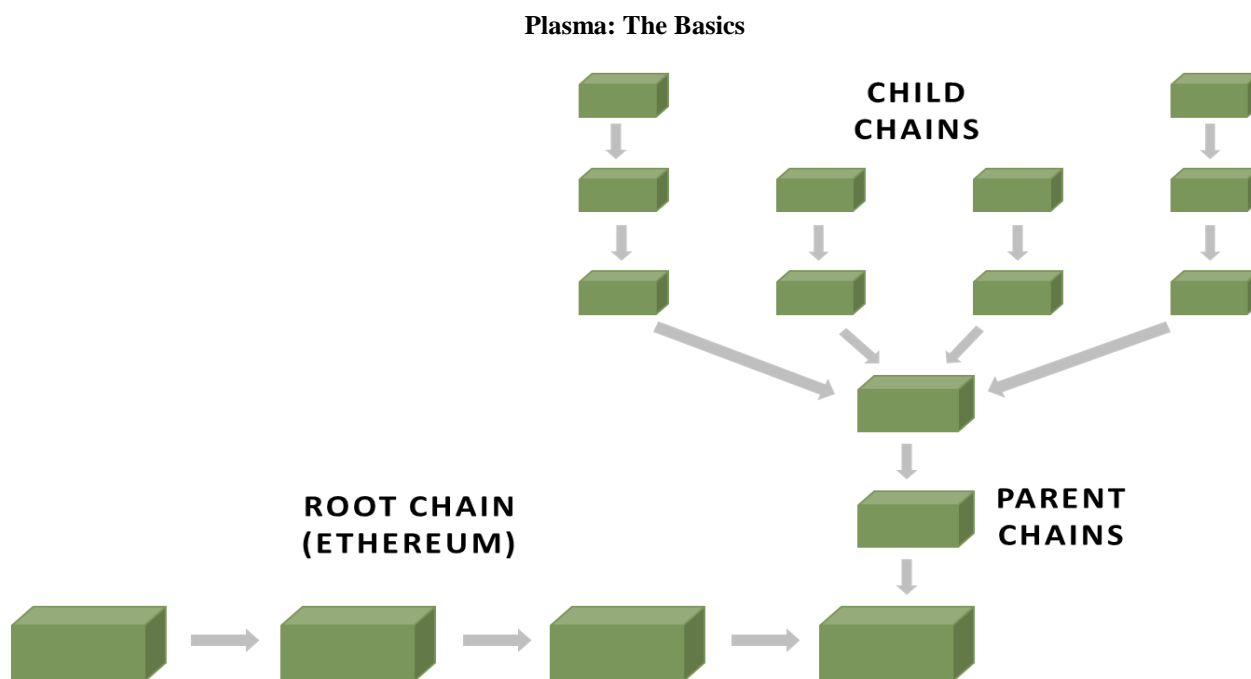
⁴⁴ A global organization exploring Enterprise Ethereum implementations, counting Intel, Microsoft and Accenture among its members.

⁴⁵ Ethereum's fungible token standard. See [Glossary](#).

⁴⁶ "Enabling Blockchain Innovations with Pegged Sidechains" by Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón and Peter Wuille.

Blockchains within blockchains. Announced in August 2017, **Plasma** is Ethereum's native solution to scaling computation⁴⁷ through connecting different solo-/multi-purpose chains with a mainnet (i.e. underlying Ethereum blockchain). Born out of the Lightning Network concept, Plasma expands the execution of smart contracts to multiple layers while maintaining the trustless and secure properties of the main network. Joseph Poon, one of the two BLN creators, has co-authored the original Plasma [White Paper](#) along with Vitalik Buterin.

Plasma allows for the creation of multiple sidechains. The “mother” Ethereum blockchain can generate “child” chains. These sidechains can, in turn, spawn their own sidechains and so on. In other words, Plasma is a hierarchical tree of blockchains branching from one root blockchain, Ethereum. As a result, many complex operations can be processed at the sidechain level with only minimal interaction with the main Ethereum blockchain. Each child-chain is faster and cheaper since operations on it do not need to be copied across the entire Ethereum blockchain. Such a blockchain architecture is much more scalable.



Source: [NullTX](#), HASH CIB

However, sidechain solutions to the scalability problem come at the expense of security. The security of the mainnet (Ethereum) can be evoked by any participant of a Plasma sidechain in order to protect their funds or prevent malicious behavior. However, there are a few potential vulnerabilities yet to be resolved in such a scheme. In the event of a large attack on Plasma sidechains, all their users would have to withdraw back to the main blockchain. Given a large enough number of users, there might not be enough space in the blockchain to process all withdrawals in time, and the system would become insecure. Therefore, Plasma can increase scalability only by a large but constant factor. Another problem is that each user must download and authenticate each Plasma block, wasting time and resources. And data unavailability (block withholding by parties responsible for their creation) cannot be mitigated on the Plasma sidechains other than by reverting to the mainnet. Given the complexity of these and other problems faced by the proposal, Plasma has transformed from a concrete project into a field of research and experimentation at this point.

Plasma Cash – an upgrade of an upgrade. In March 2018, Vitalik Buterin suggested a radical approach to making Plasma scaling exponential. Unlike the original Plasma, Plasma Cash would not require users to download all blocks; it would allow them to concentrate on the location of the specific **Plasma coin** relevant to them. When a user deposits ETH for a transaction, the blockchain creates a non-fungible Plasma coin with a unique ID. However, as of now, Plasma Cash remains also a concept under study, led by Ethereum developer Karl Floersch.

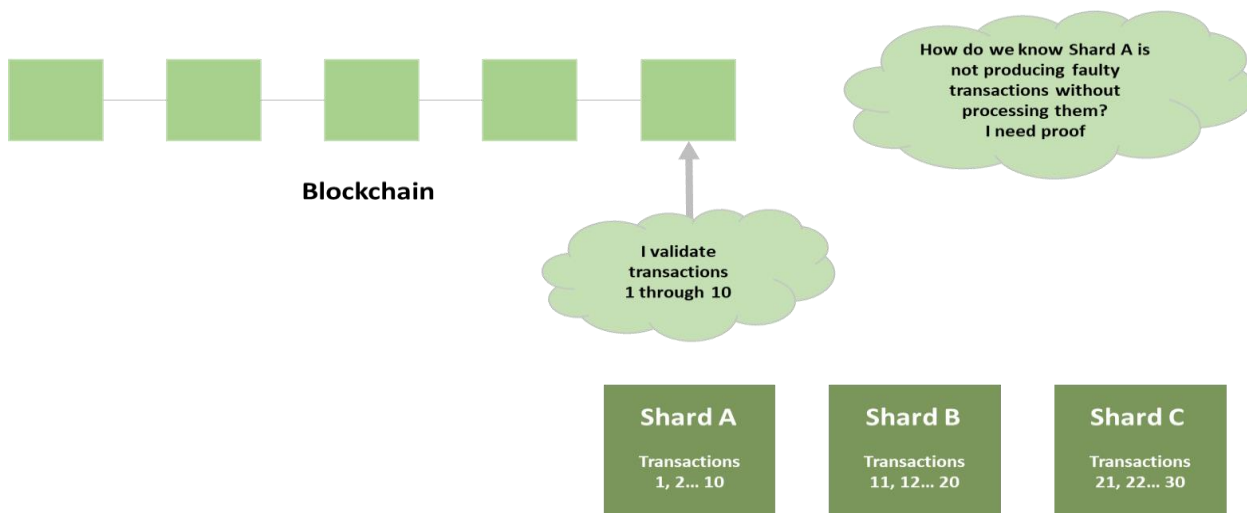
Sharding – an on-chain approach to tackling scalability

Sharding comes from the database management field. The concept is a type of database partitioning that separates very large databases into the smaller, faster, easier managed parts called data shards. In common use, sharding refers to having some data for an application on one database server, and other data on another, so that different parts of the database are requested separately. Optimization comes through having specific data tables hosted on specific servers, with a function determining which server contains the information being requested – thus eliminating the bottleneck of one server centrally processing all requests concerning different pieces of the same data set. Sharding is frequently

⁴⁷ Distributed computation is the main intended use case for Ethereum, as opposed to value transfer on Bitcoin network.

discussed with regard to large web-based applications, but it is not limited to any particular industry. However, it is native to data storage and management rather than performance of more complex, state-based code execution.

The idea of blockchain sharding is to split the network into a bunch of partitions, called shards, that contain their own independent piece of the network, conduct only parts of the transactions, and run in parallel. Currently, each blockchain node processes every single transaction going through the network. As said above, this gives the blockchain a high degree of security at the expense of efficiency and scalability. In a sharded system, certain nodes would process transactions only for certain shards, substantially increasing the throughput of transactions across all shards. Unlike state channels and second layer blockchains, shards are permanently linked to the main chain since they are just pieces of such a chain rather than solid separate constructs. Hence, sharding is called an *on-chain* approach.



Source: [Hackernoon](#), HASH CIB

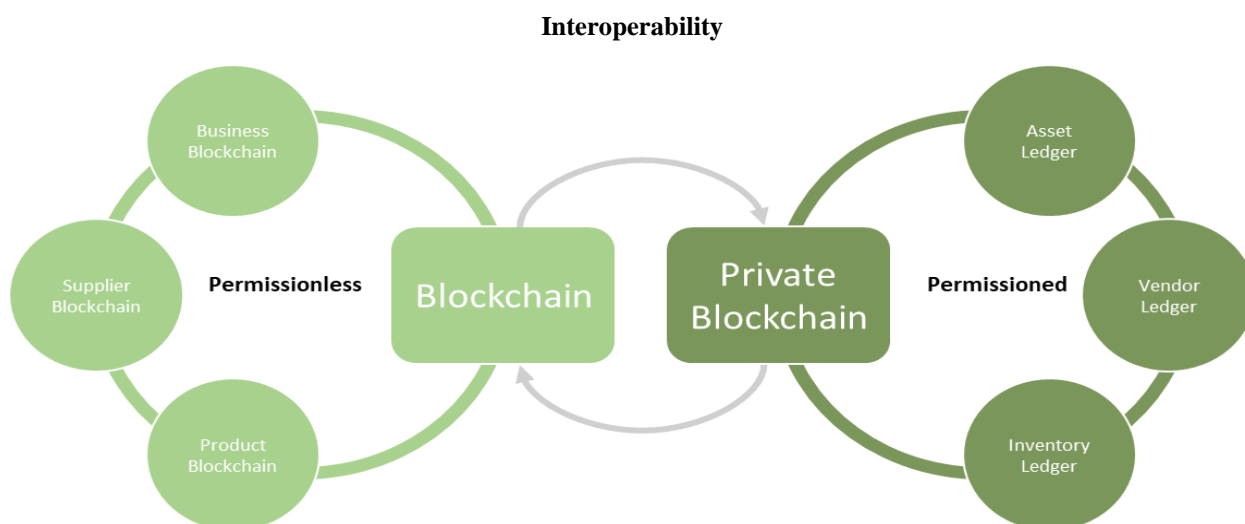
No blockchains have implemented sharding as of now. Yet, this promising solution is on the agenda for most high-profile projects, the biggest and most active of which is Ethereum. However, there are multiple hurdles on the way to execution, arising from having to split a single complete system into parts instead of adding supplementary systems on top of it. For example, one risk in a PoW sharded blockchain is a 1% attack: in a 100-shard system, it would take only 1% of the network hashrate to dominate the shard. Maintaining universal time across the network, i.e., the ability of multiple shards to have the same perception of time, is another extremely complex problem. Another flaw is that inter-shard communication is very difficult. Some special protocols are required to complete transactions between users of different shards. However, inter-chain communication is not just a sharding problem, it is the second main issue for the whole blockchain technology – the bigger problem of interoperability of separate blockchains.

However, sharding as a solution already has a specific protocol, the concept of which is being developed by Ethereum researchers. The main technological basis of this protocol is the concept of Simplified Payment Verification (SPV) light clients, introduced in Bitcoin and broadened in Ethereum. SPV's simplicity comes from the ability of a node to verify certain transactions by reviewing the compact data structure (called **Merkle tree**⁴⁸) stored in each block header without downloading the full block. The same approach is also the key component of blockchain interoperability solutions.

Interoperability – another must for blockchain's mainstream adoption

Blockchain interoperability refers to the ability of various blockchains to interact with one another and share information. Contemporary networks exist in isolation with no communication or interoperability between them. For instance, moving value between chains requires transferring coins or tokens to an exchange, trading the assets there, and then withdrawing the converted assets on a new chain. This is an expensive, time-consuming and risky process. Even if the scalability problem were solved, blockchain would not bridge the gap between core technology and actual application without interoperability in the ecosystem. On top of that, if we take into consideration wider Turing-complete network capabilities, certain smart contract-based solutions could expand blockchain capabilities if they could be leveraged across multiple chains.

⁴⁸ In cryptography and computer science, a **hash tree** or **Merkle tree** is a “tree” data structure in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the sum of hashes of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Merkle trees allow more efficient verification of the existence of certain data. The more optimized **Merkle Patricia tree** structure allows blockchain systems like Ethereum to compactly store proofs of complex state transitions, as opposed to simple value transfers, for which SPV client feature was first introduced in Bitcoin.



Source: *Rplanx Technology Private Limited*

Cross-chain Atomic Swaps and Cross-Chain Messaging/Transition Change are the two main methods to facilitate interoperability. In cross-chain atomic swaps, users exchange coins⁴⁹ without using a third party. Cross-chain messaging is a system inside one blockchain that can validate and read event and/or state change in another blockchain, then trigger a transaction in the initial blockchain. This system relays messages about the state of one chain to another chain.

In cross-chain atomic swaps, two parties existing on different blockchains communicate directly to each other. The word “atomic” is used in its original Greek meaning of “indivisible”. This method ensures that either both transfers happen or neither does. In the swap, user A (residing on the first chain) transfers digital assets to user B (residing on the second chain) in exchange for user B transferring digital assets to user A. The first cross-chain atomic swap took place in 2017 between the Litecoin and Decred networks.

The current implementation of cross-chain atomic swaps does not scale. The existing swap operation code presumes that both parties control or create addresses on both networks. Price discovery of the swapped digital assets is manual, with both ends of the deal to be determined by parties individually each time they want to swap. Most importantly, cross-chain atomic swaps are limited only to value transfer (transfers of coins) between chains.

With cross-chain messaging, two parties existing on separate blockchains communicate via an intermediary chain, called a relay. This process requires creating synthetic tokens. To a large extent, cross-chain messaging is a question of trust. Building a system that can trustlessly relay messages between different blockchains is one of the biggest challenges. Current technologies using relay networks include decentralized exchange (DEX) protocols used on a single blockchain (such as 0x on Ethereum).

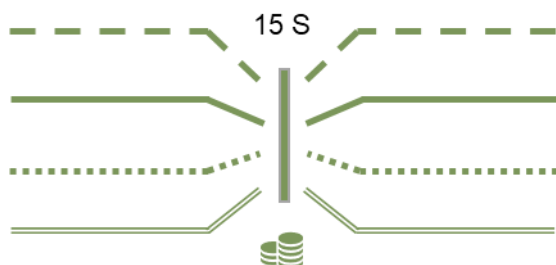
A “blockchain for blockchains” should solve the interoperability issue. A few high-profile projects, including Polkadot, Cosmos, and TON, are vying to become the “blockchain for blockchains” of choice. Relaying messages would be just one of the processes conducted by such a meta-blockchain. For such a system to be a success, it must gain recognition and be widely accepted by the blockchain community. The first big attempt of creating a blockchain (or rather a simpler distributed ledger) for blockchains can be attributed to Ripple Labs – the company behind XRP, one of the biggest cryptoassets in terms of market capitalization. Their Interledger protocol has been unveiled back in 2014 and basically describes an automated version of an inter-ledger account infrastructure, similar to what is used in correspondent banking. Its actual usage still remains to be seen.

Polkadot is a heterogeneous multi-chain technology expected to materialize by end-2019. This ambitious project, led by one of the key developers and co-founders of Ethereum, Gavin Wood, aims at solving the scalability and interoperability problems at the same time. Polkadot calls its main chain the **relay chain** and its sidechains **parachains** to emphasize that the latter chains process transactions in parallel/or have limited block validation capabilities in relation to the main chain. Such an architecture would allow spreading transactions across chains, greatly increasing throughput. To link independent chains, the network can create specialized parachains called **bridges**.

⁴⁹ Only the network’s underlying digital currency, not tokens.

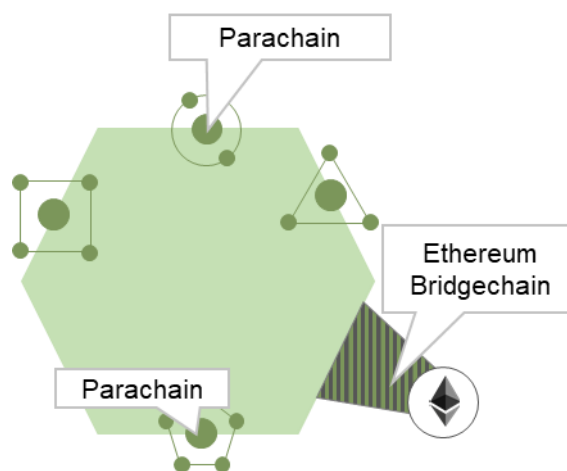
Multiple Parallelized Transactions

Multiple Parallelised Transactions



Source: Polkadot, HASH CIB

Relay Chain



Polkadot proposes solving the interoperability problem by connecting different blockchains to the main chain and offering its own consensus mechanism as a service to those blockchains, abolishing their native consensus algorithms as a result. Polkadot expands the set of blockchain participants in its architecture and consensus algorithm. **Validators** secure the main consensus-as-a-service chain by staking coins, validating proofs from collators, and participating in consensus with other validators. **Nominators** secure the main chain by selecting validators they trust and staking coins. **Collators** maintain parachains⁵⁰ by collecting parachain transactions from users and producing state transition proofs for validators. The whole concept of validation in Polkadot is based on the notion of state transition proofs – “snapshots” of the parachain before and after a new block has been committed by the collator. Such state transition proofs are submitted for validation via an SPV-like (remember Merkle trees mentioned earlier) compact data representation and should be enough for a validator to make sure that collators do not act maliciously. As a final security frontier, **fishermen** monitor the network (both collators and validators) and prove bad behavior – thus causing the network to slash collators for proposing invalid blocks, or validators for accepting such blocks.

Cosmos initially narrowed its use case solely to inter-blockchain value transfer, in contrast to Polkadot’s efforts to solve the interoperability problem on the level of smart contract execution. The two projects have much in common in terms of network architecture and underlying philosophy. The main concept in Cosmos – developed by the team behind the PoS Tendermint protocol – is also based on using the same consensus and networking of Tendermint to build different single-functionality/application blockchains on top of it. However, the main chain Cosmos Hub does not provide consensus-as-a-service to other Cosmos chains. Instead, they each use the Tendermint PoS consensus algorithm within their own group of parties, with a “result” of already finalized transactions then “transferred” to other chain(s) via Cosmos Hub. The Cosmos team initially emphasized narrowing interoperability to just value transfer; but it also plans to expand the protocol’s functionality to inter-blockchain computation.

TON’s approach is unique but to a large extent based on Polkadot’s proposed solution. However, certain aspects of TON’s functionality go beyond that of Polkadot, while seemingly rooted in the same approach to blockchain architecture. Given that Polkadot will be under development at least until 3Q19, this represents a risk for the whole TON project – as TON developers cannot use much of Polkadot’s implementation as a reference – fairly common practice in the open source public blockchain space.

The interoperability-compatible blockchain market remains an open playing field, with projects such as Icon, Zilliqa, Wanchain, and Block Collider holding successful ICOs in Q1 and Q2 2018. However, a full interoperability solution that involves value transfers, code execution, and consensus compatibility across various blockchains is yet to be proposed. TON is attempting to leverage on existing research in this area to introduce its own approach.

⁵⁰According to Polkadot’s vision, parachains could very well be the already existant, “old” blockchains, transformed.

Conclusion

Blockchain technology is a breakthrough capable of reshaping the world. It has garnered widespread attention and already raised huge sums of money on the back of just one use case – trustless value transfers. However, this is just the tip of the iceberg. To unleash its full potential and to become widely adopted, the technology must solve two main issues: scalability and interoperability.

The open source nature of the industry, combined with the rat race nature of value creation on the market, presents a daunting challenge to outsiders: figuring out what technological solution is actually a genuine innovation, as opposed to a newly branded open source code base or system architecture. A deeper dive reveals a more compelling picture of the very few actual innovations being used (and abused) by different teams to get their slice of the ever-growing pie. However, the teams that are coming up with slightly different versions of earlier envisaged solutions compete to be the first to put them into production. The array of Ethereum-based scaling solutions is the best example of that: Plasma, Plasma Cash, TrueBit, Raiden – all boil down to a broadly similar second-layer architecture with the Ethereum mainnet as the base layer. However, certain design choices in those projects and, more importantly, actual implementations, will be the true distinguishing factors in the race to market leadership. Potential investors should not be put off by the abundance of names: focus on doing proper diligence on the underlying principles in order to make sense of what is as yet a mostly theoretical competition.

The two largest blockchains in terms of user adoption and activity, Bitcoin and Ethereum, are probably the closest to launching native applied solutions. However, there are ambitious projects attempting to go much further. They aim to build blockchains whose architectures do not inherit existing problems and will allow the creation of blockchains of blockchains. Although these efforts are still at the research frontier, the future seems promising, partially thanks to billions of dollars of support. TON is in the forefront of this cohort.

Telegram Open Network – a technological breakthrough

*A community is defined by the cooperation of its participants,
and efficient cooperation requires a medium of exchange (money)
and a way to enforce contracts.*

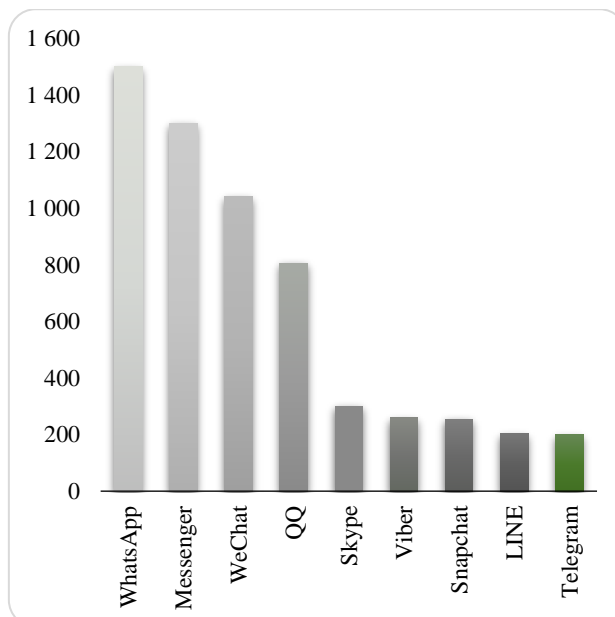
Wei Dai

Not only has five-year-old Telegram attracted 200mn monthly active users (MAU) and gained a reputation as one of the fastest and most secure messaging apps, it has also joined the battlefield of blockchain technology⁵¹. The company designed the Telegram Open Network (TON), which is much more than just a blockchain or payment channel network, but an ambitious ecosystem created with several technologies running in parallel and in multiple combinations. With its user base, Telegram already has the pre-existing critical mass necessary for such an ecosystem to quickly develop and gain widespread adoption. The blockchain platform is just one of the elements of the wider stack of TON technologies, and Gram – its native cryptocurrency – is its key cryptoasset. Telegram raised \$1.7bn in a very successful but unusual private coin placement, distributing 58% of Grams' initial total supply. The project's declared goals require complex engineering solutions, and TON developers have many issues to solve in the months preceding and following the project's launch.

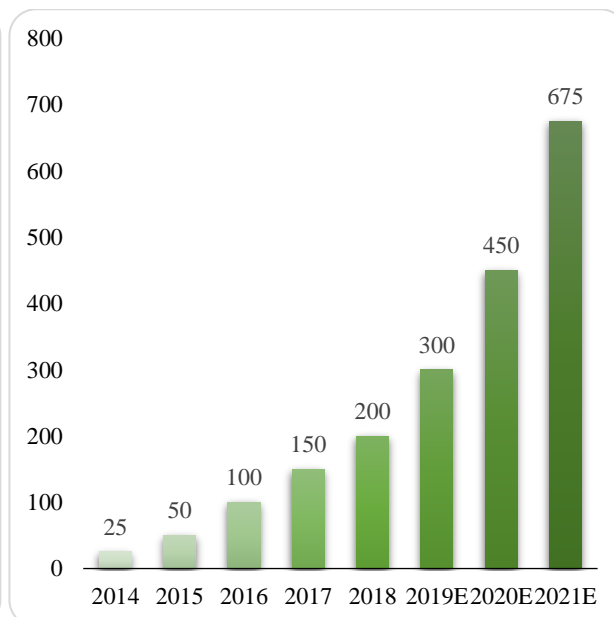
A fast and secure messenger

Launched in 2013 by a team of Russian software developers, by spring 2018 Telegram messenger had gained 200mn monthly active users worldwide. The same core team was behind the most popular Russian social network, VKontakte (VK), which has more than 80mn MAU – four times that of Facebook in Russia. The Durov brothers – Pavel, who leads the Telegram project strategically, and Nikolai, who oversees technology – finance the app's development and maintenance out of their pocket. [Selling VK for an estimated \\$360-480mn in 2014](#), the brothers have since used the money to finance Telegram, claiming it will always remain a non-profit and will never be sold. The messaging app has gone from a niche player to become one of the most widely used around the globe, with 500k new users reportedly joining daily. Telegram aims to have 675mn MAU and one billion active users by end-2021, according to the TON Primer.

Messengers MAU (mn)



Telegram MAU (mn)



Source: TON Primer, Statista

Telegram is a cloud-based messenger with seamless synchronization. As such, it was the first to allow simultaneous access to messages from several devices, and still is the only messenger to allow sharing of unlimited number of photos, videos and files of up to 1.5GB each, while storing all that data in the cloud. Telegram claims to be faster, more secure, and more reliable than most of its competitors thanks to its distributed, multi-data center infrastructure and encryption. However, security experts claim that cloud synchronization presumably comes at a cost.

⁵¹ Telegram never officially announced or denied its plans for an ICO. Our analysis is based on copies of the ICO marketing paper (the [Primer](#), often referred to as the "Investor White Paper") and the 132-page long actual [White Paper](#) (the Paper, "Technical White Paper"), both of which were leaked and posted widely on the Web.

The Telegram desktop app's (let alone the mobile version) "guaranteed" security and privacy have not been proven, while [claims of the opposite have surfaced](#) throughout Telegram's short history.

However, the technical advantages of any messaging app are unsustainable and unlikely to be the main reason for customer retention. People usually have more than one such application and quickly switch from one to another depending on their user-friendliness and/or speed. Any distinguishing feature can be replicated rapidly given the level of industry development. For example, Telegram's option to edit delivered messages – absent in both the WhatsApp and Facebook Messenger apps – is likely to appear in those messengers shortly, we believe. Therefore, messaging platforms must have other properties to ensure loyalty.

Encryption is now a prerequisite for any messaging app. WhatsApp has used client-to-client encryption for all conversations since 2016. Both LINE and Viber added end-to-end encryption to their platforms in 2017. Telegram uses client-server encryption for regular conversations and client-to-client encryption for Secret Chats. Even Facebook Messenger includes end-to-end encrypted communication options in the form of Secret Conversations for its mobile app.

Telegram has been criticized for not enabling end-to-end message encryption by default and storing all contacts, messages and media, together with their decryption keys on its servers, also by default. Pavel Durov has explained that this architecture both helps avoid third-party unsecure backups and allows access to messages from any device. If users want client-to-client encryption, they can always choose the embedded Secret Chat option.

WhatsApp, Facebook Messenger, and Google Allo implemented Signal Protocol, which, as a result, has become the most widely accepted encryption protocol, life-tested by billions of users. Telegram, on the other hand, uses a home-designed protocol, MTProto. Although cryptography experts criticize Telegram's protocol for not having proven its reliability and security (Telegram never revealed its encryption protocol for peer review, often the only way to prove the security of cryptographic techniques⁵²), no one has been able to publicly crack the messenger's encryption, despite a \$300,000 bounty for doing so. But since this encryption is not applied when using Telegram for seamless mobile-to-desktop switching by users, its use is still limited in Telegram.

However, there have been substantiated claims of hacks and privacy breaches throughout Telegram's short history. A well-known maxim among cryptographers is "Don't roll your own crypto!" meaning don't try to develop your own approach to cryptography, and in 2015, Telegram received some [criticism](#) in this regard. The same year it emerged its [Android users were vulnerable to stalking](#), due to usage data leaked to all of their contacts. And in 2016, 15mn Telegram users' phone numbers were [revealed in Iran](#) due to a user authentication flaw. Similar criticism surfaced recently in relation to Telegram's newest service, dubbed Passport.

Nevertheless, security and privacy are still the main differentiating features Telegram has to offer. Encryption is just the technical part of security; security policy is equally if not more important. The way a messenger protects private information sheds light on the kind of security it provides: the value of encryption is negligible if a messenger shares the encryption keys with third parties. Telegram manages to maintain its image through multiple proven instances of ideological resistance to breaches of user privacy.

Digital Resistance

Pavel Durov refused to give the protocol's encryption keys to Russian security agencies. In response, the authorities have been trying – unsuccessfully – to block the messenger since April 2018. The approach chosen by Russian officials to ban Telegram was straightforward and brutal. Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media (commonly known as Roskomnadzor) decided to block hosts appearing to have the same address range as Telegram's servers, rather than its usual procedure of sniping out direct server addresses. The government agency needed such a blunt approach because Telegram was too quick and efficient in changing single-server addresses. However, Telegram also turned out to be extremely rapid and efficient in changing the underlying hosting providers, which caught Roskomnadzor by surprise. As a result, the agency shut down whole subnetworks of servers, with Google, Amazon, and Twitter among the many collateral victims of the Telegram ban. Meanwhile, Telegram itself was able to quickly set up new proxy servers for its Russian users, causing only short-term disruptions in access to the messenger.

Telegram was well prepared for the attack. The state-level attack was unprecedented, in our view, as no other Internet company had experienced one of such magnitude. In the first week, the number of Internet Protocol (IP) addresses banned in the government's attempts to block the messenger reached 18mn, [The Moscow Times reported](#). However, Telegram was able to resist efficiently by rapidly setting up new instances of the Telegram proxy on different cloud providers' infrastructure. The cat-and-mouse game lasted for some time, but Telegram was able to survive and prove its expertise in operating a distributed (while centrally controlled) network of nodes. We believe

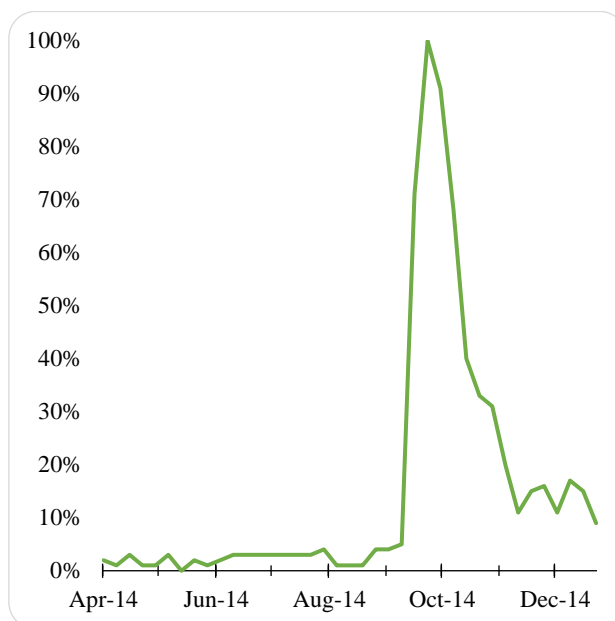
⁵² [Kerckhoffs's principle](#) holds that cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

Telegram may have used this opportunity to display its degree of distribution and resistance to censorship in anticipation of the launch of its blockchain network.

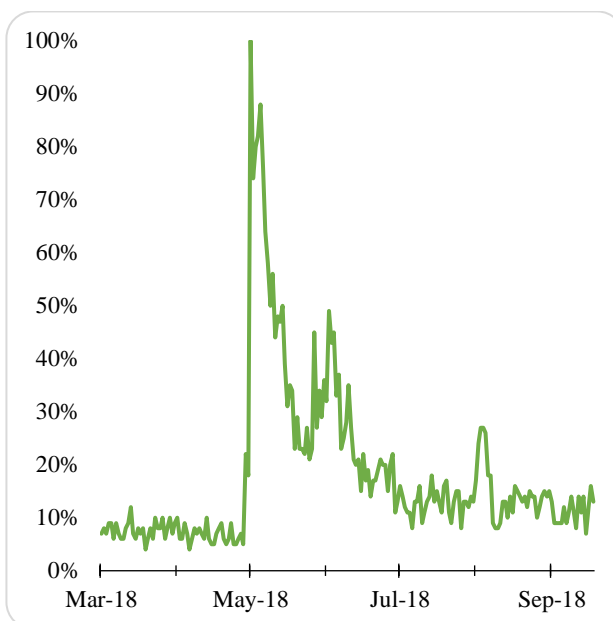
This confrontation, later called “Digital Resistance”, earned the trust and won the hearts of additional users, even leading to small protests in the country. At almost the same time, a similar situation emerged in Iran, where Telegram has 40mn users – half of the country’s population. The messenger’s popularity in Iran has also been fueled by the company’s [refusal to submit to Iran’s state censorship rules](#). “For many Iranians the Internet is Telegram, and Telegram is the Internet,” says Omid Memarian, deputy director of the Center for Human Rights in Iran, [told Wired](#) in June 2018. Even Iranian government officials [seem to agree](#) attributing 60% of the country’s Internet traffic to the use of Telegram back in 2016.

Telegram has become the messenger of choice when other services are compromised. In 2014, Telegram saw [a massive increase in its user base in South Korea](#) – reporting 1.5mn new users signing up in just 7 days – after the country’s president confirmed government surveillance of the region’s biggest messenger app, KakaoTalk, spurring a user boycott.

Telegram’s popularity spiked in Korea in 2014...



and in Iran in 2018



Source: [Google Trends](#)

Telegram agreed to cooperate with investigators in terror probes when ordered by courts, the company announced on 28 August 2018. If the messenger receives a court order confirming that a person is a terror suspect, it may disclose this person’s IP address and phone number to the relevant authorities. When such disclosures occur, the app will include them in a semiannual transparency report. [The new privacy terms](#) were adopted to “comply with new European laws on protecting private data”, while additionally including the new anti-terrorist clause. Previously Pavel Durov had [explicitly rejected](#) complying with such justifications for user privacy breaches.

But Russia remains an exception. Pavel Durov said Telegram would continue to withhold Russian users’ data from security services, [Meduza reported](#). “In Russia, Telegram is asked to disclose not the phone numbers or IP addresses of terrorists based on a court decision, but access to the messages of all users,” he wrote on his Telegram channel. He added that since Telegram is illegal in Russia, “we do not consider the request of Russian secret services”.

Telegram protects personal data not only from official but also from commercial parties. Subsidized by the Durov brothers and by the proceeds of the TON private placement, the messenger has no revenue streams and declares it will not have ads or other monetization schemes in the future (as opposed to the avalanche of ads in its competitor Viber, for instance). If it runs out of funds, Telegram might introduce non-essential paid options to support the infrastructure and finance developer salaries⁵³. The paradigm might vary with a change in control, of course. However, Pavel Durov confirmed in a December 2017 [Bloomberg interview](#) that Telegram is not for sale and never will be. Telegram chose a different way of raising funds to grow and expand its business, with the aim of making it eventually more public and decentralized than an acquisition by a major public company or its own IPO would have ever done.

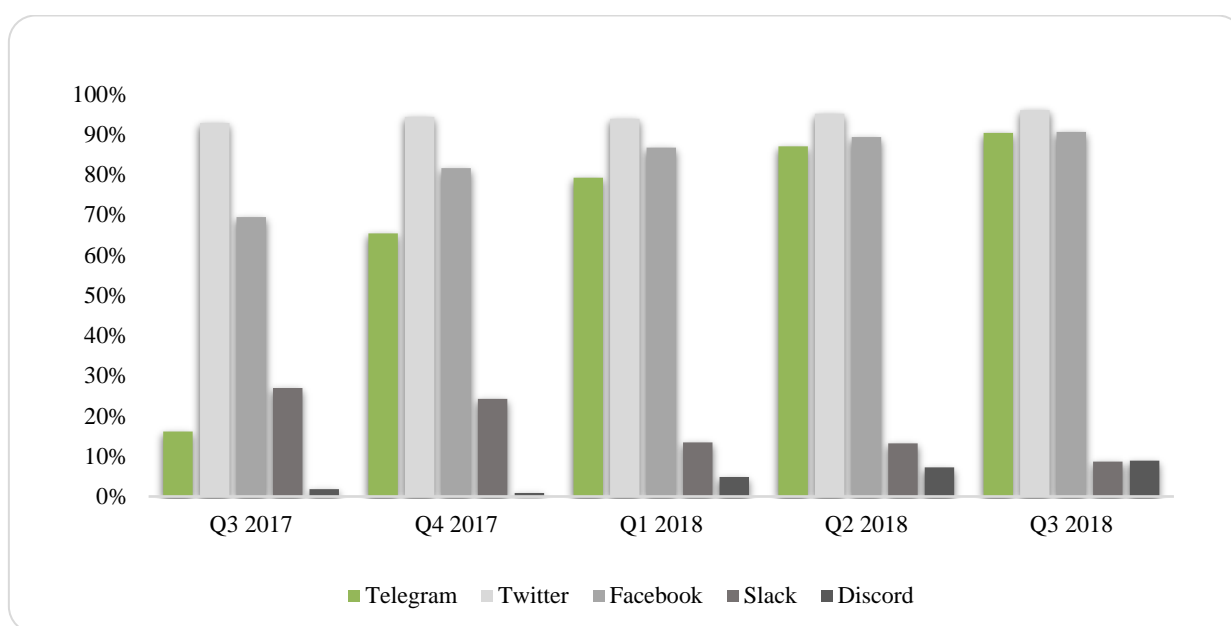
⁵³ <https://telegram.org/faq>

The Telegram Open Network ecosystem

Telegram plans to launch its own, entirely new blockchain platform and native cryptocurrency. The company designed the Telegram Open Network as a fast and secure blockchain and wider peer-to-peer network project able to meet the speed and scalability requirements needed for mass adoption. The TON coins exchanged by Telegram users will be called Grams (GRM). Grams will serve as the principal currency for the in-app economy and will be available for external use.

With its 200mn monthly active users, Telegram already has the pre-existing critical mass necessary for the ecosystem to expand quickly and gain widespread adoption. Moreover, the messenger has become one of the main communication platforms for official ICO discussion groups. Most actors in the digital economy already have Telegram accounts, and its popularity is rapidly expanding. Currently, 90% of blockchain-based projects have active communities in the messenger, compared to just 16% a year ago, according to ICObench.

Almost all ICOs have their discussion groups on Telegram



Source: [ICObench](#)

Much more than just a blockchain or payment channels network, TON is an ambitious ecosystem that creates several parallel technologies on multiple levels⁵⁴. TON is a stack of technologies to power a global community of users wishing to communicate, use applications, and buy and sell assets in a censorship-resistant and secure way. Telegram intends to build the very infrastructure and basic features for such *ecosystem of decentralized services over a distributed network* to thrive independently of the World Wide Web, while leveraging on the global reach of its messenger's 200mn active user base. Grams are the lifeblood needed for the ecosystem to exist, while on-chain smart contracts and off-chain decentralization are designed to protect it from abuse and censorship. TON plans to challenge VISA and Mastercard as an alternative for the new decentralized economy, but it will also support a wider array of functions needed for what is considered the Web 3.0 generation of distributed applications and services.

The project's declared goals require complex engineering solutions, which constitute the TON technological stack. For investors to monitor the project's development, to evaluate technological risks, and to make educated decisions when some of those risks inevitably materialize, we present our analysis of the technologies composing TON. But first we would like to present an overview of the project and the private placement held to fund its development.

An unusual but very successful coin offering

Telegram raised \$1.7bn via private placement and called off an expected ICO. Telegram sold 2.89bn Grams for \$1.7bn⁵⁵ with no prior public announcements to communicate the concept and generate feedback – as is usually the norm in the public blockchain tech community. Nevertheless, demand was so strong that the company increased the total number of coins it had planned to initially allocate⁵⁶.

⁵⁴ e.g. the infrastructure level, the application development level, the user level, etc.

⁵⁵ See our Valuation chapter for a detailed calculation.

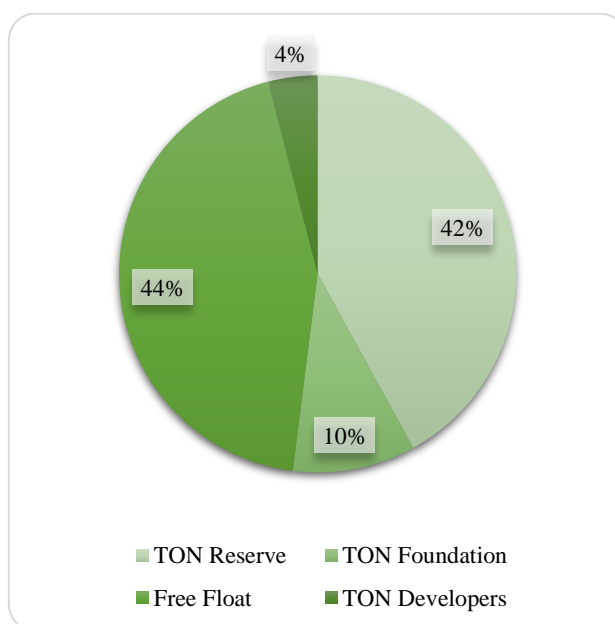
⁵⁶ According to the offering Primer, Telegram initially planned to sell 2.2bn Grams.

In the first round, which took place in February 2018, the company sold 2.25bn Grams to 81 purchasers for \$850mn at an average price of \$0.38 per Gram. During the second round in March 2018, Telegram distributed another 639mn coins for \$1.33 each, attracting another \$850mn from 94 investors. Telegram filed two Notices of Exempt Offering of Securities with the US Securities and Exchange Commission (SEC) for each placement. Such filings had only happened rarely before for a cryptocurrency placement⁵⁷, and never on such a massive scale.

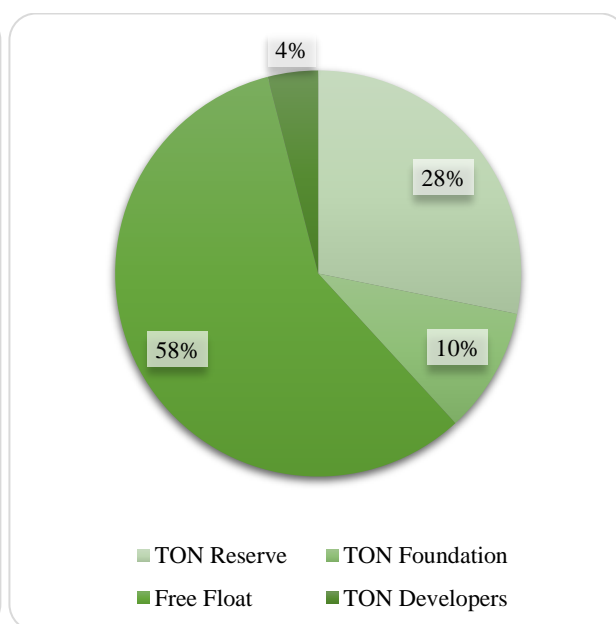
The overall nature of the placement was secretive, presumably for legal reasons. There were no official announcements or document postings made by Telegram or any affiliated parties. Before and after filing notices with the SEC, the company and its founders remained silent about the project. This has led to some controversy around TON-related updates, such as with the Telegram Passport service first mentioned in the offering Primer. More importantly, it allowed the emergence of several fake Telegram ICO websites⁵⁸. There have also been reports of secondary market private sales conducted by initial purchasers, thus creating a wider circle of investors than just the officially confirmed number of 175 accredited individuals and institutions. There have been public reports indicating there is a lockup condition at least for the first round of sale⁵⁹, suggesting a restriction of up to 18 months after the blockchain is launched (see Appendix for more background)⁶⁰.

Telegram distributed more than half of its original total supply of five billion Grams. During the blockchain's deployment, the network intends to allocate a further 200mn Grams to TON developers⁶⁰ as a remuneration and 500mn to the TON Foundation (a non-profit entity run by the TON team to oversee the network development). The remaining unallocated Grams will be kept in the TON Reserve (TON's treasury). Telegram expects that on average at most 10% of the total supply of Grams will be bound in validator stakes at any given moment. Validators are to be rewarded by approximately 20% of their stakes annually. This should produce an inflation rate of 2% p.a., and as a result, would double the total supply of Grams in 35 years. "Essentially, this inflation represents a payment made by all members of the community to the validators for keeping the system up and running," as noted in the Appendix to the White Paper.

Initially planned distribution of Grams



Grams distribution after placement



Source: TON Primer, TON White Paper, HASH CIB

The deadline for the project's launch is reportedly set at October 2019 the latest⁶¹. If the obligation is not fulfilled by then, reports suggest that investors would receive the sum they paid minus costs incurred by the issuer since the date of the investment (presumably, including the costs of maintaining Telegram messenger).

⁵⁷ For example, [Protocol Labs](#) filed three similar Form D notices in August 2017 for its over \$200mn Filecoin placement, making it the biggest token sale at the time.

⁵⁸ <https://ico-telegram.org> is just one of many examples.

⁵⁹ As reported before and after the first round sale by multiple sources, including [TechCrunch](#), [Bloomberg](#), and [Coindesk](#).

⁶⁰ Vested for four years, according to the Primer.

⁶¹ Although the Primer indicated a Q4 2018 target for the launch, some [media outlets](#) (such as Business Insider) have indicated the "legal" deadline to be in October 2019.

TON Project Roadmap

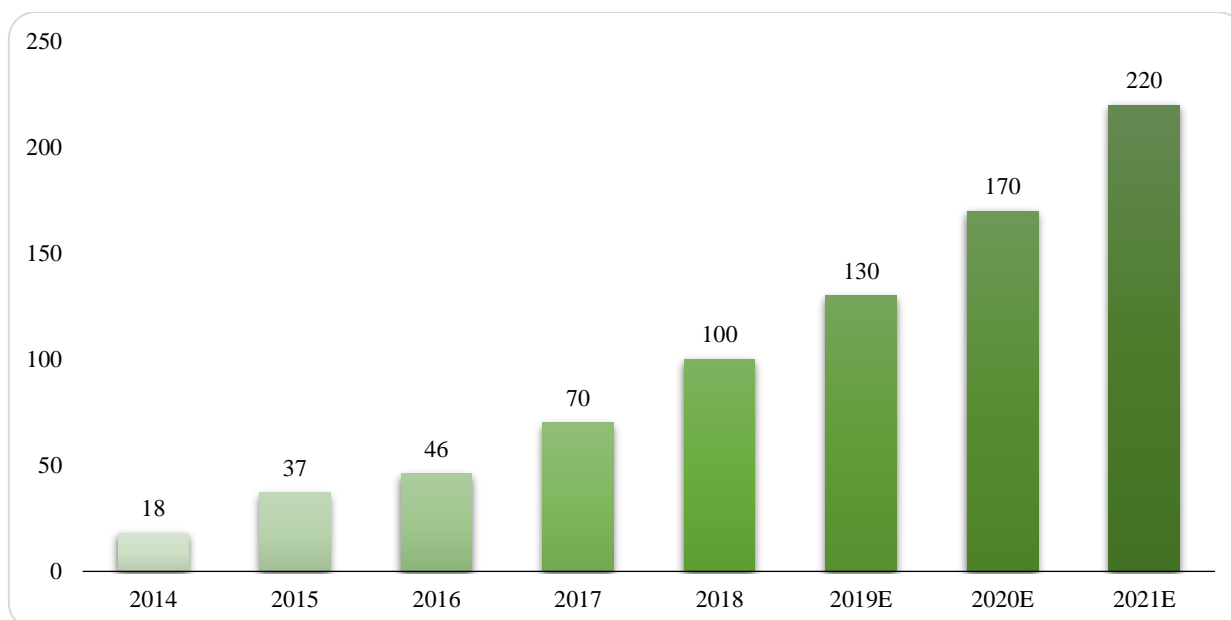
Q3 2013	↓	Launch of Telegram Messenger and the Telegram API
Q2 2015	↓	Launch of the Bot API and Platform
Q2 2017	↓	Launch of the Payments Platform
Q2 2017	↓	Start of the development of TON
Q1 2018	↓	Launch of Telegram External Secure ID
Q2 2018	↓	Launch of the Minimal Viable Test Network of TON
Q3 2018	↓	Testing and security audits of TON
Q4 2018	↓	Deployment of the stable version of TON
Q4 2018	↓	Launch of Telegram Wallet
Q1 2019	↓	Creation of TON-based economy in Telegram
Q2 2019	↓	Launch of TON Services, TON Storage, and TON Proxy

Source: TON Primer

Considering legal risks surrounding the sale and the amount of raised funds, Telegram appears to have called off the public placement of Grams⁶². In documents reportedly shared with purchasers, the issuer outlined eight critical risks for TON investors, [Coindesk wrote](#). One of the crucial risks is the legal uncertainty surrounding the secondary market trading of Gram cryptocurrency. In addition to risks related to the overall regulation of the cryptoasset space, legal risks associated with the legal status of Gram coins and possible government or private actions arising from that, Telegram outlines market and technological risks for blockchain projects.

A substantial part of the raised funds will be used to cover the costs of maintaining and developing Telegram messenger, in our view. Telegram needs around \$620mn to fund the app until end-2021, according to the company. This leaves it with a staggering sum of more than \$1bn for TON development. Nevertheless, the offering addendum outlining risks reportedly contains the following passage: “Telegram may not retain the services of developers with the technical skills and expertise needed to successfully develop the TON Blockchain and progress it to a successful launch” – even with a seemingly well-funded “war chest”. We believe such a risk poses a material threat given the ambitious technological scope of the project.

Telegram cash burn rate (\$mn)



Source: TON Primer

⁶² “Telegram Messaging App Scraps Plans for Public Coin Offering”, The Wall Street Journal.

TON project components

Both the TON White Paper and TON Primer describe the Telegram Open Network. We reiterate that neither of the documents has been officially released by Telegram. However, we are confident that the publicly available leaks are authentic. The Primer, naturally, seems to have been drafted later, with certain details added to the initial concept. We start with its brief overview, before diving deeper into analyzing the more technical White Paper (the Paper), authored by Dr. Nikolai Durov⁶³, which is the main source of information about the asset comprising the offering and the underlying technology.

The TON Primer outlines the core specifications of the technology as well as the terms of the offering. However, as a marketing document, it deals mostly with promoting the proposed ecosystem and highlights the most marketable features of TON as an investment:

- TON's native cryptocurrency, Gram (GRM), offering the potential for mass market adoption thanks to VISA/Mastercard scalability features and Telegram messenger's already over 200mn MAU user base;
- *"expertise in encrypted distributed data storage and 10-year experience in building user-friendly interfaces"* of the team behind Telegram;
- non-rent-seeking aspirations of its founders, *"libertarians who want to preserve freedom through encryption"*;
- Telegram's existing *"distributed server infrastructure to synchronize encrypted data across multiple independent server clusters spread across different continents and jurisdictions"*.

The Primer puts a scalable, and thus potentially widely adopted, cryptocurrency at the forefront of the project – the cornerstone for the whole TON ecosystem to build upon. Although the Gram cryptocurrency is the first of the key ecosystem components to be delivered with the network launch, the team behind TON envisions a broader use for its project than might initially appear after reading the Primer. After the peer-to-peer networking layer of the TON stack of technologies is laid down and the blockchain is running, the launch of the following protocols/features of the network should follow the anticipated distribution of Grams: TON Storage, TON Domain Name System (DNS), TON Proxy, and TON Payments (an additional payment channel network built on top of the blockchain). The order of those features is the order of actual delivery that we expect based on our reading of the White Paper. Worth noting is that the peer-to-peer payment network – a key component in making the Gram currency truly widely adopted – is to come later.

In addition, the Primer proposes an External ID service. Since the White Paper does not mention this service, we conclude that the idea came to the TON team later. Telegram [publicly unveiled](#) its new service, dubbed Telegram Passport, in July 2018. Passport is already integrated with *ePayments* – a UK-based regulated online payments service provider, noticeably integrated with the low-liquidity crypto exchange DSX. However, at present, we are unaware of any other major platform integrations that could drive up Passport's user base (see the appendix for more details on Passport^{A2}).

The White Paper outlines TON technologies as follows:

1. An interoperable *"Multi-blockchain platform (TON Blockchain),"* capable of *"processing millions of transactions per second"* (presumably, the aggregate capacity of all of TON's multiple blockchains), *"supporting Turing-complete smart contracts, upgradable formal blockchain specifications, multi-cryptocurrency value transfer, support for micropayment channels and off-chain payment networks"*.

We would additionally describe it as a blockchain platform for distributed a) computation, b) value transfer and c) governance (i.e. enforcement of the former two, hopefully distributed *and* decentralized as TON matures). It is basically the key, but not only, communication protocol within the Telegram Open Network's stack of protocols and technologies.

2. *"A peer-to-peer network (TON P2P Network), used for accessing the TON Blockchain, ... but also able to support arbitrary distributed services, blockchain-related or not"*.

We would define the TON P2P Network as a group of specific communication protocols – a particular stack within the larger TON protocol and technologies stack. Their function is to establish a set of networking layers and rules that define communication between nodes (on a lower level) and clients (i.e. software implementations for accessing the network as a user, validator, service provider, etc.) running those nodes (on a higher level) in the Telegram Open Network.

3. *"A distributed file storage technology (TON Storage), accessible through the TON Network, used by the TON Blockchain to store archive copies of blocks and status data (snapshots), but also available for storing arbitrary files for users or other services running on the platform, with torrent-like access technology"*.

⁶³ The project's co-founder and the CTO of Telegram.

TON Storage is an example of technology built on top of and connected through the communication protocols, such as TON Blockchain and P2P Network. The project's proponents nominally distinguish between services and applications so that: a) *services* cater to the needs of other applications while b) *applications* serve end-users. The distinction is nominal and is used solely for convenience, as TON Storage's functionality illustrates. It is a collection of distributed data servers, connected through the communication protocols of TON Networking to other TON technologies in order to facilitate storing and accessing data by TON's end-users, as well as other TON platforms, services and applications – including the TON Blockchain itself.

4. *“A network proxy/anonymizer layer (**TON Proxy**), similar to the I^2P (Invisible Internet Project), used to hide the identity and IP addresses of TON Network nodes if necessary (i.e. nodes committing transactions from accounts with large amounts of cryptocurrency, or high-stake blockchain validator nodes who wish to hide their exact IP address and geographical location as a measure against DDoS attacks)”.*

In line with the service/application distinction, TON Proxy would be a giant distributed service that can be also used as an application. It utilizes TON Networking communication protocols. We note that this most probably *adds additional privacy* to P2P communication within TON but does not actually *hide* the identities and IP addresses of nodes.

5. *A Kademlia-like distributed hash table (**TON DHT**), used as a “torrent tracker” for TON Storage, as an “input tunnel locator” for TON Proxy, and as a service locator for TON Services.*

This could be thought of as a part of TON P2P Network's built-in software, running on top of its communication protocols on any TON-connected node. It is built-in so that nodes can easily find other nodes and data within the whole of TON stack of protocols and technologies – e.g. Blockchain, Storage, Payment channels and other (all, eventually, supported by different nodes, possibly providing some of the TON technologies and services concurrently).

6. *“A platform for arbitrary services (**TON Services**), residing in and available through TON Network and TON Proxy, with formalized interfaces enabling browser-like or smartphone application interaction. These formal interfaces and persistent service entry points can be published in the TON Blockchain; ... Services may create smart contracts in the TON Blockchain to offer some guarantees to their clients”.*

In a stricter sense, TON Services is not a single platform, but rather a set of different technologies connecting with TON applications and users. Such services and applications can be purely on-chain (i.e. smart contract-executed and enforced), off-chain (operating in the “old-fashioned”, client-server centralized mode) or mixed (possibly, smart contract-enforced but client-server executed). The connection is enabled by the TON Networking and other underlying protocols. The idea behind TON Services is that Telegram Open Network users would not need to bother with “under-the-hood” implementation (on/off-chain or mixed) of applications and services, but just simply connect to them in a seamless generalized way. Actually, TON Storage or TON Proxy are good examples of “mixed” and “off-chain” apps or services. If, say a group of Proxy service providers (nodes) utilize TON Blockchain for (smart-contract automated) payments by users, it could be called a mixed application or service. If it does not use the blockchain for payments/automation/lookup etc., but still provides its services to TON network participants via a traditional web-page interface accessible through Telegram messenger, it could be considered an off-chain service.

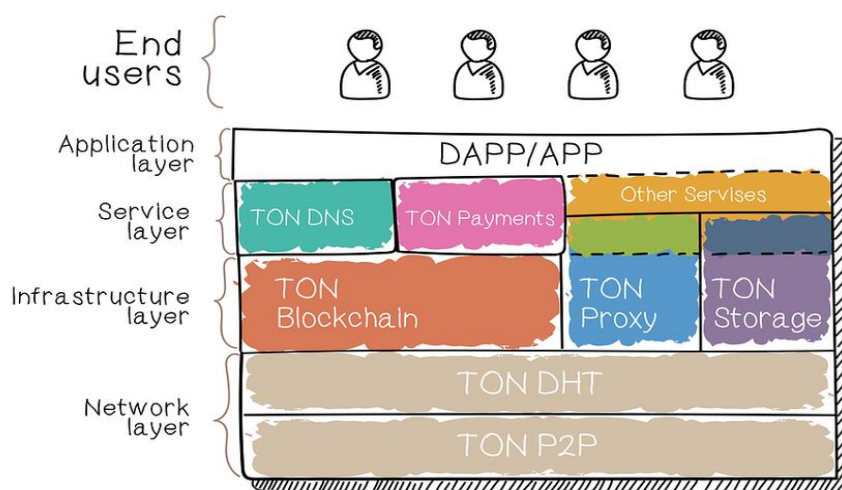
7. *“**TON DNS**, a service for assigning human-readable names to accounts, smart contracts, services and network nodes”.*

This is a service utilizing the whole set of underlying TON protocols and technologies to enable Blockchain user accounts and smart contracts (on-chain applications and services), as well as off-chain and mixed applications and services to connect with each other, with the rest of the Internet, and possibly other computer networks in a seamless way. That means that Telegram Open Network, while utilizing the same Internet infrastructure as the rest of the World Wide Web, could be thought of as its “own” Web, while connected to the wider Web in a seamless way thanks to TON DNS.

8. *“**TON Payments**, a platform for micropayments, micropayment channels and a micropayment channel network. It can be used for fast off-chain value transfers, and for paying for services powered by TON Services”.*

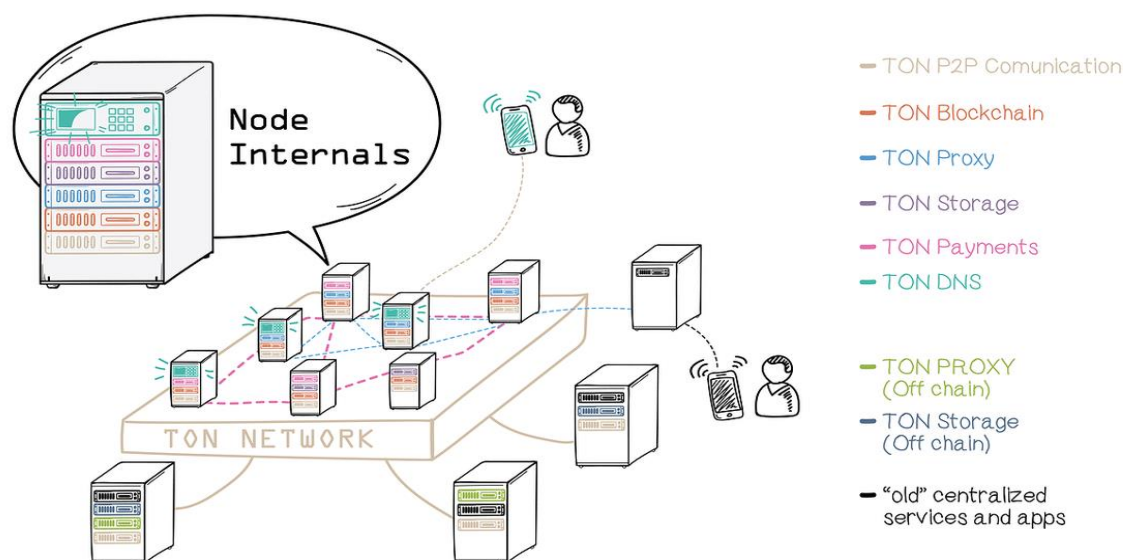
This is the Blockchain's second-layer state channel protocol plus a network of nodes utilizing this protocol, to provide scalable payment infrastructure to TON users. It is similar to the various state channel second-layer protocols built on top of the Bitcoin and Ethereum networks.

TON's stack of protocols and technologies



Source: TON White Paper, HASH CIB

TON Ecosystem utilizing TON's stack of protocols and technologies



Source: TON White Paper, HASH CIB

The Paper, when describing the Telegram Open Network project as a whole, emphasizes the much broader application of the proposed stack of technologies than just a scalable payments system. Also the blockchain platform is just one of the key elements of the wider stack of TON technologies, and the Gram cryptocurrency is the key cryptoasset – albeit not the only cryptoasset/token supported by TON – to facilitate the ambitious ecosystem. However, in addition to Gram being by design just *one* of the potential means of payment in the system, it serves additional functions in the network, uniquely realized with Grams only.

GRM cryptocurrency is the mandatory unit of value, to be used for posting validator stakes in the proof-of-stake consensus and for paying transaction fees to validators for securing the blockchain. The fees consist of a fixed payment, so-called "gas" (similar to Ethereum), to cover computation and account storage costs, and a remuneration part arbitrarily set by the payor. The remuneration component could be set in units of account other than Grams, but the amount should ultimately be exchanged into Grams and distributed among the validators. Moreover, one needs to use Grams to propose and vote on changes in the configurable parameters of the blockchain on its main chain – the so-called "masterchain", which hosts the global transaction history of all other TON blockchains. Other special masterchain transactions requiring Grams include the creation of "global" smart contracts – i.e. on-chain applications, compatible with all or most of the chains in the TON blockchain multiverse. Additionally, any account on the TON Blockchain must have a non-zero balance in Grams, with the ability to keep additional balances in other cryptocurrencies and tokens supported by the TON Blockchain.

Telegram plans to release a Wallet integration into its messenger before the TON Payments platform is developed, we believe. This means that Gram holders will initially be able to use their cryptocurrency not for “*instant money transfers and micropayments*” supported by TON Payments, but rather for more “regular” blockchain-based transactions, involving higher fees to validators, longer confirmation times and less transaction throughput. Nevertheless, if working as promised, throughput should still be well above that of today’s blockchain protocols.

Technology analysis

We derive all the technological concepts of the future Telegram Open Network solely from the White Paper. The document was authored by the older of the Durov brothers, Dr. Nikolai Durov. We have analyzed the version of the document dated 3 December 2017, which has been made [publicly available](#) on the Internet by unknown and unconfirmed sources.

The Paper explicitly states that it is not the ultimate reference in terms of actual project implementation, as during the development and testing of the TON stack of technologies “*some particulars are likely to change*”. Moreover, the project documentation is missing formal technical specification – a so-called Yellow Paper or an online-accessible repository⁶⁴. We believe that (as with most major projects in the space) TON is envisioned as an open source set of technologies (at the very least, with its blockchain component), although this has not been clearly articulated by TON proponents. So we would expect further low-level technical specifications for TON to be unveiled prior to the release of the core blockchain software. This is needed for the open source peer review common in the space, to prevent major bugs and failures *after* the project is launched⁶⁵. These missing pieces and subject-to-change clauses substantially limit our understanding of the concepts described in the Paper.

The White Paper is composed of four key parts, which outline the main software architecture underpinning TON. The parts are presented in what appears to be the order of importance for Telegram – TON Blockchain, TON Networking, TON Services and Applications, and TON Payments – with each chapter specifying the features of the corresponding technologies and their envisioned high-level implementation⁶⁶.

TON Payments – the killer app

The market typically views payments as the “killer app” for cryptocurrencies, and therefore we start describing the TON stack of technologies there. Solving the problem of *instant, scalable and trustless payments* will drive the widest adoption of the project, and therefore accrue the most value to it. However, nothing in the White Paper suggests that TON Payments will be used for facilitation of value transfers solely in Grams. Since the project will by design support multiple cryptocurrencies, the technology can be easily extended to other units of account for storing and transferring value.

TON Payments is proposed as a specific implementation of state channel technology. However, in TON terminology the payment channel technologies already under development should be considered *simple* in relation to more complicated TON Payments architectures described below. These simple payment channels can also make up a network of intermediaries between two parties wishing to transact without having a direct channel established between them – with the ability to bind the intermediaries by making them prove to each other (along the payment routing) that they have reliable knowledge of a “promise” of payment between the original two parties.

TON Payments is scheduled to be released *after* other core elements of the network are built. The reason for latency in releasing Payments is due to the nature of the technology driving it. The TON Blockchain is planned to be “*inherently scalable by design*” with 5-second block intervals, and Payments is envisioned as a second layer to that blockchain. That implies adding technology on top of the underlying protocol, which by then should have been built and working in order to support the facilitation of payment channels. It also implies that in order for the aforementioned technology to cater the masses an actual network of independent payment channel operators must be developed to provide the necessary liquidity⁶⁷.

Envisioned as a “platform for micropayments, micropayment channels and a micropayment channel network”, TON Payments would be used both for fast P2P transfers and to pay for services within the ecosystem. This is the reason why the payment network is designed *on top* of the TON Blockchain instead of being integrated into its base layer architecture: it allows decoupling value transfers from other transactions (computations on the distributed

⁶⁴ Such as [GitHub](#), commonly used by open source blockchain projects.

⁶⁵ As was, unfortunately, the case with another ambitious project and an even bigger fundraiser, EOS.

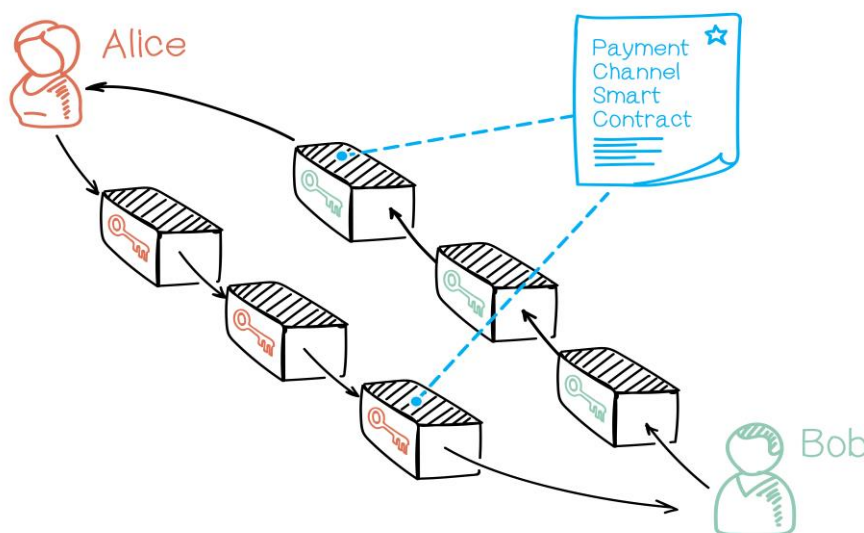
⁶⁶ The level of detail in the chapters is inconsistent, with instances of cross-referencing, while substantiation is sometimes lacking in the linked descriptions. This could be attributed to the massive size of the document, it being prepared by different teams, and/or time pressures. Although this has led to some criticism by blockchain technologists, we believe that conceptually the Paper presents a compelling set of ideas, even if the articulation at times leaves something to be desired.

⁶⁷ Even with payment channel-compatibility embedded in the initial design of TON Blockchain and with second-layer software development running in parallel with the main chain development, the implementation of TON Payments is still dependent on the successful operation of the main chain and other infrastructure elements. We believe this is why the product roadmap in the Primer does not include a release date for Payments.

blockchain computer), which need to first be committed and validated to appear in the next block. It also eliminates the necessity to pay blockchain-layer transaction fees – presumably excessive for micropayments – which *allows essentially a whole new set of monetization tools for online goods and services*, in particular, those available to TON users in the future.

Leveraging on the open source software of Bitcoin and Ethereum payment channel solutions, such as Lightning, Raiden, and Plasma Cash, TON’s proponents add some new features. Nikolai Durov proposes a system of *asynchronous payment channels as virtual blockchains* (containing, essentially, two *virtual* chains – one for each transacting party). This is basically just a common payment channel, but with some blockchain-like properties for each party’s side of the channel. This system would allow for trustless bi- and unidirectional payments between the two parties. Provided balances are enough, each party can sign as many transactions on its end as it needs, without having to wait for another party’s expressed acknowledgement. This is especially useful for unidirectional channels, such as customers regularly paying their service providers. A smart contract takes care of all the settlements and can “punish” the misbehaving party by sending *all* of its channel balance to the counterparty. This approach differs little from other smart contract-operated payment channel technologies, such as Raiden; however, the ability to use a fully-fledged blockchain verification toolkit out of the box in (usually simpler) state channels would represent an advance. That’s why they are called *smart* payment channels and are described as virtual blockchains, for having blockchain-like properties^{A3}.

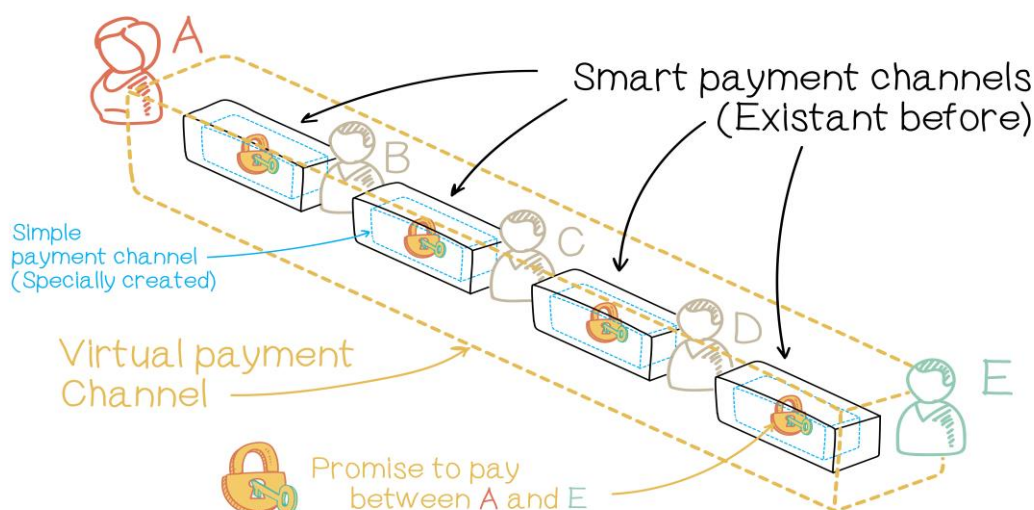
Smart payment channel as a virtual two-chain blockchain



Source: TON White Paper, HASH CIB

In addition to creating *smart* payment channels, the TON Payments platform would allow for *simple* payment channels to run “inside” the smart ones. This complicated architecture permits for two parties’ obligations to pay one another to form conditions (“promises”) bounding their intermediaries (a set of two *other* parties) into a network of simple channels. Such new simple channels are created inside the already established permanent smart payment channels between each of the intermediaries. This essentially allows the *original* two parties to use a payment channel network to transact with each other multiple times in a bidirectional way *without ever creating a direct channel* between each other. The latter is common for all payment channel network architectures; however, such networks require a massive number of two-party channels between nodes to function properly. The TON proposal represents an optimization of the size of such a network (i.e. number of nodes active), which would facilitate large transaction volumes. Additionally, this approach could bring more security to such a network: the main pain point of payment channel network routing is the necessity for the nodes in the network to trust their chains of intermediaries. This is why building such networks has taken so much time for Bitcoin and Ethereum communities. Thus, if TON arrives with a working solution to this issue, it could catch up with its competitors.

Virtual payment channel between A and E



Source: TON White Paper, HASH CIB

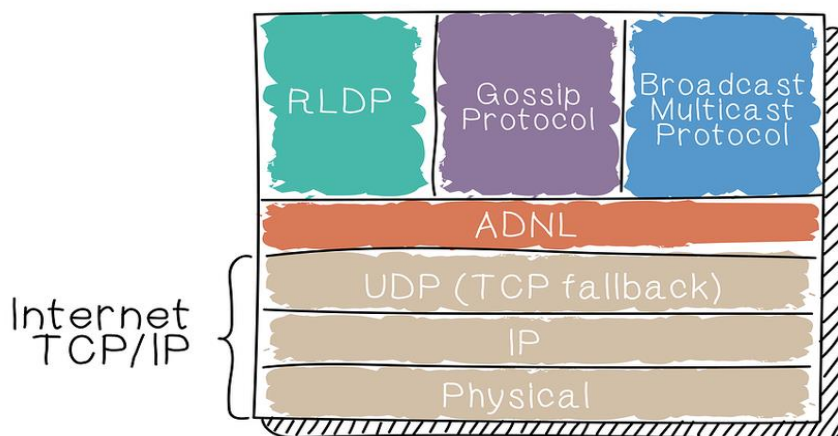
While TON Payments appears to be a compelling and logical solution to building trustless and complex payment channel networks, it remains just a concept. With TON developers proposing logical and seemingly consistent payment channel engineering solutions and overall payment network architecture, the technology has yet to be implemented. And implementation is hardly a trivial task. While TON programmers may have some *working* decentralized and trustless implementations available to study and improve upon during the development of TON Payments (such as the Lightning Network for Bitcoin), their additional solutions and improvements will have to be tested – something that can most likely be done only when launched on top of the functional TON Blockchain.

TON Networking

TON Networking is a set of communication protocols that connect all parts of the Telegram Open Network together like an organism's arterial system. A combination of several-layer infrastructure technologies on top of each other makes up the Networking stack. Most of these technologies are part of the current Internet protocol stack. While not directly associated with blockchain as a technology, these protocols are crucial in understanding how peer-to-peer networking works, especially for TON, which goes beyond just building a blockchain. TON Networking is based on the following protocols:

- *Abstract Datagram Network Layer (ADNL)* in TON will be built over one of the key modern network data transmission protocols – User Datagram Protocol (UDP) – which here is put over the Internet Protocol (IP) versions 4 and 6, with an optional Transmission Control Protocol (TCP) fallback in case of UDP unavailability. ADNL is a transporting layer abstraction, regulating how *all* the Telegram Open Network nodes connect and share data on the lowest levels (to TON infrastructure). While being based on top of UDP, ADNL shares the same network stack with commonly known Internet protocols like HTTP/HTTPS. Each node in the TON network identifies by ADNL address, represented as a 256-bit integer^{A4}.
- *Reliable Large Datagram Network Protocol (RLDP)* is used for TCP-like transporting over the default ADNL (UDP) protocol in TON^{A5}.
- *Gossip Protocols* (including *Broadcast Protocols*) and *Streaming Broadcast (Multicast) Protocols* are used for TON overlay networks. An overlay network is an arbitrary subnetwork built on top of the ADNL to connect TON nodes for a special purpose, e.g. blockchain validator networks for block propagation, payment channel networks for near-instant value transfers, storage networks for data uploads/downloads, etc^{A6}.
- *(Kademlia-like) Distributed Hash Table (DHT)* is a technology used in every TON-supporting node (whether it runs TON Blockchain, TON Storage, or any other Services and Apps separately or in arbitrary combination) but on top of the P2P Networking layer of the above-listed protocols, although it is not a communication protocol itself. DHT is a *virtual* table made up of smaller parts *actually* stored with each node in the network. When are virtually put together, it turns out such a table collectively keeps references to *all* of TON's data, where each data hash is combined with references to node addresses keeping the data. The data-address table entries are presented in a form of a key-value pair, where the key is presented with its “hash” (a reasonably unique index of a key), hence, the name of the table. DHT allows for fast data/node lookup in the network^{A7}.

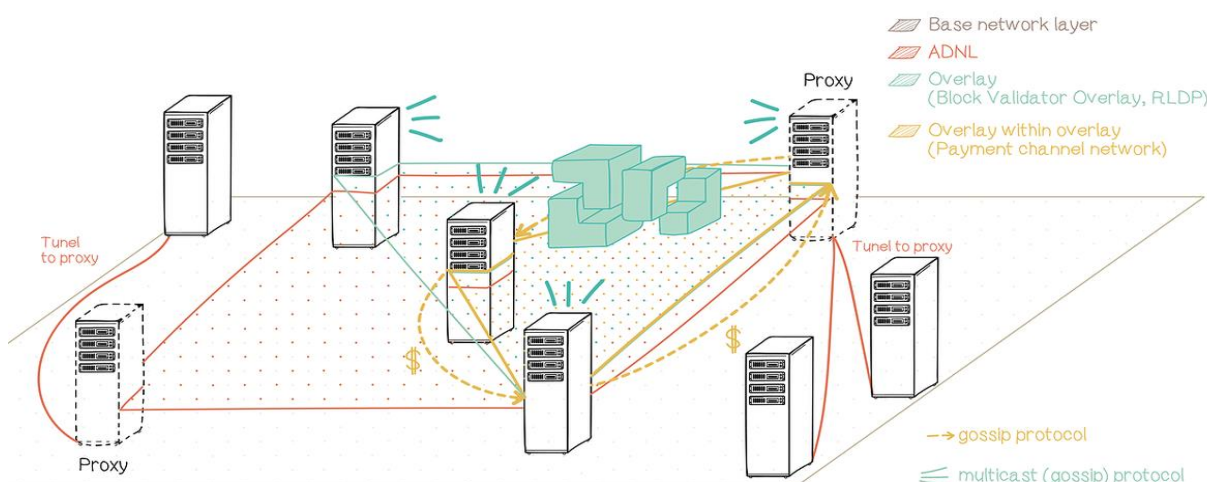
TON Networking stack of protocols on top of the pre-existing lower layers of the Internet infrastructure



Source: TON White Paper, HASH CIB

Moreover, TON Networking supports low-level network privacy features on the ADNL level through the creation of point-to-point and one-way communications that are routed via so-called channel identifiers (abstract network addresses). These channel identifiers could be used as proxies to actual (ADNL) node addresses. Using this channel identifier mechanism, one could build communication routes through various proxies (such routing is referred to as “tunneling”), combined with encryption steps for the communicated data and sender/receiver addresses along the way. This is similar to anonymizing routing technologies like I²P or TOR^{A8}.

TON Networking layers represented as logical abstractions between nodes



Source: TON White Paper, HASH CIB

The two most important features enabled by TON Networking are:

- The ability of nodes to quickly look each other up through DHT and create arbitrary overlay networks with different sets of rules to communicate in specific ways (e.g. more private, more reliable, etc.). Payments, Storage, and other TON platforms and services, as well as blockchain validation and other important functions in the system, are all enabled with the ability to create such overlay networks;
- The ability of different servers and software clients (on-chain, off-chain or mixed) to communicate, using a single routing, data transmission, and interaction infrastructure. This is truly unique for current blockchain designs with only special-purpose instances of on-chain and off-chain interaction mechanisms created. Other projects (such as Ethereum or Dfinity) are addressing the same problem differently – fully separating their new, blockchain-powered, services and applications’ back end from the “old” (centralized) World Wide Web, while adding intercommunication on- and off-ramps. TON seems to design its ecosystem so that “old” centralized Internet services can offer themselves to TON users alongside or even intermingled with distributed ones.

While TON Networking is a set of predominantly well-known and tested technologies, its complexity still creates some risk of underperformance. TON Networking meshes together many layers of protocols and technologies and asks them carry out a wider array of functions than they are usually used for. Such a complex system could result in slower performance or even halts under high loads, because these are physically dispersed distributed nodes running data transmissions over networking protocols over data transmission protocols over networking protocols, etc. At the same time, all the presented solutions could work well together, especially given the Telegram team's demonstrated expertise in maintaining high-performance distributed networks under even state-level attacks.

TON Services and Applications

The Paper's author described the formal distinction between *applications* and *services* as follows:

- *applications* are services that deal with end customers (i.e. human users)
- *services* are technological solutions and interfaces to be exploited by applications

TON's infrastructure is intended to facilitate building and using both. Developers will be able to create business models catering to either TON's end-users or the ecosystem's back end. However, the distinction is nominal, as certain services could be used by users, applications, and other services.

Three TON services (Storage, Proxy and DNS) will be built and provided by TON developers themselves, at least initially, we believe. To make sure that the ecosystem for future applications and services is running as soon as the network launches, the developer team will make some core services accessible from the start, via TON Foundation-operated servers or TON-developed smart contracts (for pure on-chain services)⁶⁸.

The TON White Paper also draws a distinction between:

- *on-chain* apps and services, which keep all their data and processing on the Blockchain;
- *off-chain* apps and services, which are connected to TON via Networking layers of technologies⁶⁹;
- *mixed* apps and services, for which only partial data storage and processing is done in the blockchain, with the rest of the interaction coming via a traditional centralized client-server apparatus connected to the TON Blockchain via TON Networking protocols⁷⁰ (all seemingly invisibly for the end-user).

Mixed TON Services: TON Storage and TON Proxy

TON Storage is a peer-to-peer service that not only handles data storage for TON users and other apps and services, but also is the key element in storing TON Blockchain history. A distributed storage service like [InterPlanetary File System \(IPFS\)](#) would be an extremely compelling utility for users wishing to maintain a certain level of immutability of data stored in the Internet while also being able to have reliable access to the data^{A9}.

TON Proxy can also be a distributed service with peer nodes providing their proxy bandwidth for micropayments by users. To ensure the utility of such so-called fog services, TON developers plan to let the P2P markets of resources needed for this and many more fog services and apps to be created as registries or exchanges (themselves to be on-chain, off-chain, or mixed) within the TON ecosystem. So, TON Proxy-providing nodes, other services, and service-providing nodes could be looked up through such special registries or marketplaces, *effectively powering the digital sharing economy* within TON.

⁶⁸ The White Paper contains multiple indications that TON's proponents aim at creating competition among network participants as the network evolves (or re-distributing the costs along with the rewards, depending on where the system decentralization slider is located at any point in time). However, comments such as "*initial set of TON Storage and TON Proxy nodes may be installed by TON Foundation*" and "*helper services that will be provided by TON, including TON DNS...*" also suggest that TON designers realize the importance of providing such services from the outset. We have no objections, as long as this helps jumpstart network utility and does not hamper healthy competition from other service providers further down the line. However, it does pose certain risks to network adoption.

⁶⁹ These Networking protocols allow off-chain applications (such as the current implementation of Telegram Passport, for example) to cater to TON Blockchain users. Or the other way around – creating a seamless on-ramp to blockchain technologies for off-chain app users (such as Telegram messenger).

⁷⁰ The White Paper also distinguishes between two kinds of mixed services – *centralized* and *decentralized*, according to Nikolai Durov's terminology. *Decentralized* mixed services are additionally called *fog services* in the White Paper, i.e. those powered by network peers' resources such as disk space, computation, and the like (see [Glossary](#)).

On-chain TON Service: TON DNS

TON DNS is a pure on-chain service, powered by smart contracts that map human-readable domain names to 256-bit addresses of ADNL nodes, TON Blockchain accounts, and other smart contracts. Since DNS is a key service for connecting users and applications both on- and off-chain, it is envisioned as a “*predefined service*”. That means that while any smart contract developer will have freedom to implement it the way they wish, TON developers take it upon themselves to create a “*well-known*” interface for such a smart contract class in order to introduce consistency to the service^{A10}.

The most important feature of TON Blockchain-powered DNS is the notion of user interfaces for smart contracts and web page-like representation of off-chain services as TON sites. Leveraging on the ability to access a smart contract via the so-called “get methods” executed as messages sent to a smart contract without causing a change in its state⁷¹, TON developers propose creating public interfaces for smart contracts that can display the various actions (computations) available for that particular contract. Similar public interface representations could be created for off-chain applications and services connecting to TON. These interfaces would allow for seamless interactions by the user – such as pressing a button or posting text – irrespective of the “under the hood” (on-/off-chain or mixed) execution caused by such action. All of this could be easily accessed in an indistinguishable way with the aid of TON DNS. Additionally, as TON’s TCP-like (RLDP) networking protocol would allow the display of an application’s interface in the form of a web page, it allows for a browser-like user experience with the aid of TON DNS. This would integrate Telegram messenger (and third-party social and messaging networks and World Wide Web sites) with TON via hyperlinks to TON-residing or TON-connected services.

Finally, with the help of TON DHT⁷², TON DNS could help building a torrent tracker-like system. Such a system could have multiple use cases, as it allows one to look up groups of nodes from all over TON based on any arbitrary indicator – a file, an indicated interest, or any other piece of information uniting a group and referenced as a key in DHT.

TON Payments can be also thought of as a pure on-chain service or DApp, as it is facilitated with blockchain-residing smart contracts for blockchain cryptocurrency/token users, and nodes providing such a service by default must be blockchain nodes. All of this while the payment channel network itself is an off-chain special purpose overlay.

Off-chain TON applications

The White Paper barely discusses the possible use cases for such apps if and when built or integrated with TON, although it lays out the foundation of services that would facilitate future end-user applications. However, based on the information provided both in the Paper and the Primer, we would highlight the following possible applications⁷³:

- **Telegram messenger** is anticipated to be the first “external” application integrated with the TON infrastructure, via a combination of TON Wallet, TON Passport, and possible TON-browser messenger app extensions (all of which could be viewed as separate applications in this regard, as the messenger itself turns into a platform with the advent of TON);
- **TON Wallet** is intended (at least initially) to be an in-app application of Telegram messenger and should accelerate wider adoption of TON via Gram purchases and storage. However, we note that the TON network of payment channels will not have been built (nor will have other apps or most of the services that would facilitate the utility of Grams) by the time TON Wallet is expected to be available via Telegram. We therefore believe that at this point, the wallet represents less an actual utility than a tool to reassure initial investors by fueling speculation that such an utility will eventually see broader uptake.
- **Telegram Passport** is currently being positioned for use with ICOs and crypto exchanges (at least, as we interpret it). Given Telegram’s large crypto community, it could serve as an additional tool for onboarding these Telegram users into the TON ecosystem. This would be the case mainly if Telegram Wallet supported other popular crypto currencies, which are often used for financing ICO purchases.
- **TON Browser** looks like another app that would be quickly developed. Whether or not the first implementation would be actually built by TON developers is never clearly stated in the White Paper or the Primer. But since TON is envisioned as its own Web-like ecosystem with a DNS service, a desktop/mobile browser would make sense, we believe.

⁷¹ i.e. a commit of a transaction into the next block of the blockchain where such a smart contract resides, as would normally be the case with other smart contract-operated blockchains.

⁷² As DHT can “attach” any arbitrary group of nodes to a value that corresponds to a certain key in its key-value mapping.

⁷³ Here we focus on Telegram’s current products to illustrate the utility of integration. We have no doubt that these will be the initial applications connecting to TON and providing interoperability with TON Blockchain, and other distributed services and applications in the TON stack. It remains to be seen, though, whether TON or third-party developers will come up with other compelling interoperability use cases that inspire other off-chain applications to connect with TON. We see micropayment technology enabling a Gram-driven marketplace as a potential driving factor.

TON Blockchain – among the most ambitious projects in the industry

We have purposefully left analysis of the TON Blockchain to the end because while “other components might be considered as playing a supportive role for the blockchain, they turn out to have useful and interesting functionality by themselves”. It is precisely the addition of a wide array of additional components into the initial design that makes TON stand out as one of the most ambitious in the space. However, the most technically challenging of the TON technologies is, of course, the blockchain itself.

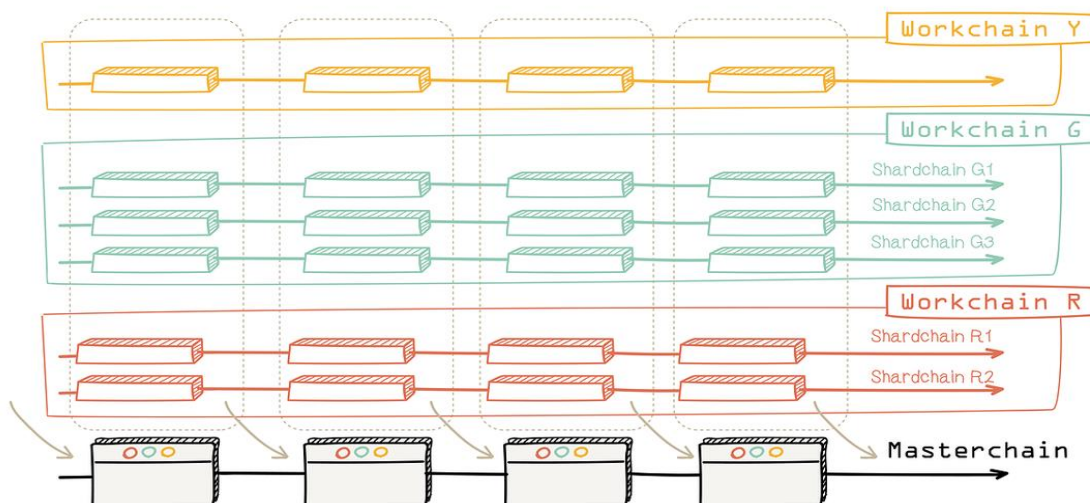
The TON Blockchain’s basic configuration consists of three levels:

1. The Masterchain, which contains hashes “of the most recent blocks of all workchains and shardchains” – think of it as a general ledger used just for tracking what is going on in the system and making sure it follows the rules;
2. Up to 2^{32} Workchains – actual blockchains with their own set of rules that nevertheless comply with the masterchain’s general rules and use it for settlement and harmonization within themselves and between each other;
3. Up to 2^{60} Shardchains – the working parts (shards) that make up the workchains, where *everything is actually happening* in the TON Blockchain.

The TON Blockchain will use a proof-of-stake consensus algorithm, employing a global distributed set of validators (from 100 at the beginning to possibly 1,000 or more as it grows) instead of miners to produce new blocks. The global set will be used to come to the masterchain consensus, and local groups of the global set will validate workchains in constant rotation among themselves. Additionally, the TON Blockchain will use other professional parties to assist validators in their task, in order to maintain decentralization while also achieving better performance.

The system architecture of the TON Blockchain is designed to solve two key issues: *scalability* and *interoperability*. The fundamental aspect of the blockchain architecture here is its ability to support multiple shards of a single workchain and their ability to then “come together” in the masterchain blocks. Such functionality is enabled by the so-called *Infinite Sharding Paradigm*. Sharding here refers to the ability of a blockchain to split into several parts while maintaining a single logical construction.⁷⁴ TON, in contrast, comes up with its own unique *bottom up* approach, essentially viewing each account in the blockchain like a separate shardchain. Then those shards (accounts) are grouped together based on the proximity of their 256-bit (blockchain) addresses (these are different from the network node addresses in TON DHT of the same representation format discussed earlier). This is a core design feature of the TON Blockchain concept, theoretically allowing it to scale to “millions of transactions per second”.

TON Blockchain as a combination of multiple workchains made up of shardchains



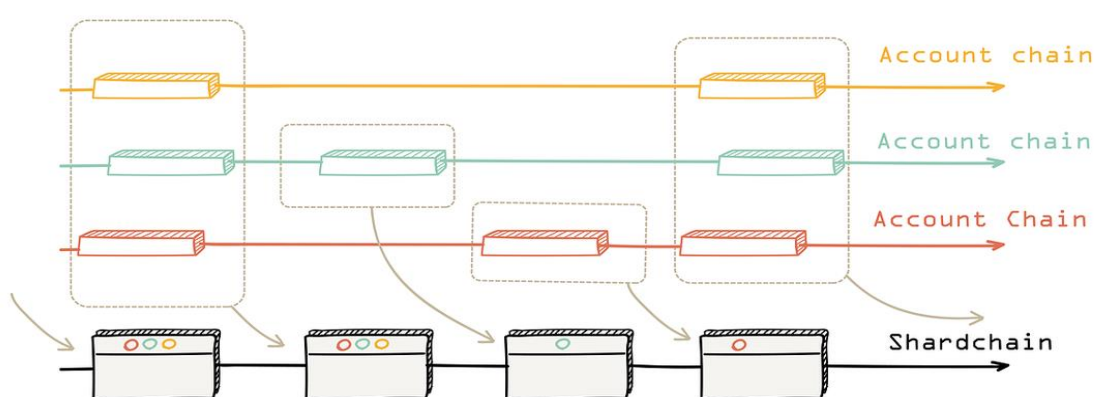
Source: TON White Paper, HASH CIB

⁷⁴ As opposed to classical database sharding – just assuming the name and basic principle of splitting a single complex architecture into logical parts in order to scale up usage.

Workchains⁷⁵ can be thought of as completely separate blockchains, run on different Turing-complete or limited-functionality virtual machines, using different programming languages and possibly having their own basic cryptocurrency protocols. This theoretically means TON could support up to 2^{32} cryptocurrencies and many more tokens⁷⁶. The White Paper states that with “*basic interoperability criteria*” workchains can be effectively combined together into the TON Blockchain. Thus, mainly following approach also taken by another interoperability-focused project – Polkadot – TON aims to solve the problem of blockchain interoperability. *Workchain Zero* is the Gram- and TON Virtual Machine-driven workchain, the single chain (2^{60} times scalable) that will be launched on TON Blockchain initially.

The accounts could be grouped into 2^{60} shardchains as a result of the *infinite sharding paradigm*. Account grouping is done on the principle that considers their addresses (specifically the 64 leftmost bits). “Each shardchain is identified by a couple $(w,s) = (workchain_id, shard_prefix)$ ” where the workchain id is a 32-bit integer (as there could be up to 2^{32} workchains) and a shard prefix is a $2^{0...60}$ shard identifier. The number would logically be 2^{64} , but for some, presumably technical, reason the 4 of 64 bits of any TON Blockchain address have been reserved for something other than shardchain grouping.

TON account chains making up a shardchain



Source: TON White Paper, HASH CIB

Finally, a shardchain can split in two if the transaction load on one chain is too high and two shardchains can merge into a single one if the combined load is too low⁷⁷. Such binary splitting is allowed almost infinitely up to 2^{60} times per workchain with similar ease of merging, thus providing for almost limitless *horizontal* on-chain scaling. There is a limit imposed on both splitting and merging operations per hour, yet a shardchain can sustain a *threefold increase* in load (split) and quickly cut cost of operation (merge) in case of *twofold fall-off*. This means that, even without second-layer Payment solutions, the TON Blockchain can inherently support a large transaction load by design. This is where the “millions of transactions per second” performance indicator comes from – it implies a *gross* metric of multiple shardchains and workchains combined. However, with TON first-layer scaling one would still need to wait *at least 5 seconds* (which is the block confirmation time in TON Blockchain) and pay (higher than off-chain) on-chain transaction fees (hence the need for the additional Payments infrastructure on top).

The TON Virtual Machine (TVM) and its basic principle for data representation⁷⁸ – “everything is a bag of cells” – are at the cornerstone of chain interoperability in TON. Although it is described only by certain criteria, we understand that TVM by design supports interchain compatibility by allowing data to be represented in such a way that Merkle proofs are supported out of the box. The ability to provide such Merklized (i.e. compactly presented) proofs of state transitions that have taken place in *originating* chains lets validators of different *other* chains (not knowing essentially anything about the originating chain) verify transactions on the *originating* chain and validate transactions on their chains dependent on transaction data in the originating chains, and do so both quickly and securely.

⁷⁵ However, Nikolai Durov speaks of workchains in TON solely as *logical abstractions* – combinations of shardchains that make up a workchain by following the *same set of rules*, like running the same distributed computer (virtual machine) or supporting the same cryptocurrency.

⁷⁶ i.e. smart contracts serving as units of account on top of each workchain’s basic currency – like Ethereum-supported tokens (see [Glossary](#)).

⁷⁷ “Too high” meaning over 90% of the block is full for 5 or more consecutive minutes, “too low” if the load is less than 60% of a block’s computation limit (size) for the two “sibling” shardchains combined.

⁷⁸ The so-called “*everything is a bag of cells*” principle represents data as cells with up to four pointers to other cells, which makes cells essentially interconnected on the lowest level.

To facilitate work(shard)chain interoperability, TON uses so-called Hypercube Message Routing^{A11}. Another blockchain innovation in TON is the concept of **Block Healing**, introduced to amend transactions already committed but later proven invalid^{A12}.

Smart and well-elaborated concepts in the TON White Paper are found side by side with ill-defined or poorly articulated approaches leaving room for both improvement and error. With all the innovative concepts introduced in the TON Blockchain architecture, there are elements of the technology that are still vaguely expressed, providing grounds for contradicting conclusions that are only likely to be resolved when the system is launched (or at least publicly tested and reviewed).

- **The TON Blockchain consensus algorithm and block validation and propagation rules are the least defined points in the proposed design.** Using the yet-to-be proven safe and effective proof-of-stake (PoS) system consensus, Nikolai Durov also suggests implementing either a Practical Byzantine Fault Tolerance (PBFT) leader-based consensus algorithm⁷⁹ or a Honey Badger Byzantine Fault Tolerance algorithm. But while the latter has received some acclaim in the computer science community for its theoretic propositions, no major working systems have been built on it⁸⁰.
- **A five-second validation interval for a block creation in TON seems unrealistically fast** for such a complex system planning to run “in the wild” of the physical distribution of no less than 100 validator nodes around the globe. Additionally, while shardchain blocks are limited in size⁸¹, masterchain blocks needing to contain “*hashes of the most recent blocks of all workchains and shardchains*” could – in the extreme case of all 2³² workchains being in operation – grow in size to approximately 137 Gb per block⁸². Such a huge block would have seconds to travel around the globe for at least two-thirds of 100-1,000 validators to expressly agree on its contents^{A13}.

Moreover, some of the complex engineering proposals, although conceptually making sense on a higher level, call for additional explanation. We understand such extreme over-engineering as a way for TON proponents to anticipate any issues and future industry competition long after the blockchain is launched, helping to make sure TON remains the ultimate scalable Turing-complete platform for the decentralized web. However, it is yet to be seen whether the proposed solutions actually would ever prove useful^{A14}.

TON developers have many issues to solve, both leading up to and immediately following the project’s launch, given that they have proposed a massively ambitious set of technologies with blockchain at their core. Some, if not most, of these issues could be resolved by the TON team engaging more openly with blockchain developers and the wider community, we believe. An open source peer review would help prevent issues faced by other recent ambitious projects⁸³. Despite developers’ hopes of carrying billions of dollars’ worth of value and serving millions of people in the future, teams can sometimes rush complicated blockchain systems into operation, in an illusory race for network effects and ultimate supremacy.

⁷⁹ With one validator ultimately signing and propagating a block while the remaining validator set members have to then come to an agreement whether or not they approve such a block based on the additional evidence (i.e. state transition proofs).

⁸⁰ There is an online repository for implementation of Honey Badger BFT, updated by one of the protocol creators Andrew Miller: <https://github.com/itnc3/HoneyBadgerBFT/> – which also contains links to other external implementations. To our knowledge, the only of all of these (both original and external) implementations currently being tested in practice is the one developed for one of Ethereum’s sidechains – POA Network (<https://github.com/poanetwork/hbbft>). It is not a perfect reference for TON developers to learn from as the aforementioned sidechain uses an already predefined and whitelisted set of validators – something a permissionless public blockchain like TON would try to avoid.

⁸¹ Relative to the amount of computations allowed per block, as in Ethereum, rather than limited in simple byte-size of transactions within a limited block size, as in Bitcoin.

⁸² Assuming hash size of 32 bytes for each of the workchain block references put into masterchain block – as suggested in the White Paper. See Appendix for an even extremier case example^{A13}.

⁸³ For example, when the EOS blockchain was implemented, some decisions that made sense on paper turned out to be errors in judgment by the developers. Such issues are inevitable in human-built systems, we believe.

Competitive landscape and risks

Withdrawing into technology is like pulling the blankets over your head. It feels good for a while, until reality catches up.
Hal Finney

An ambitious project in an embryonic industry, TON will emerge in an extremely competitive environment and faces many risks. We divide these risks into two broad categories, internal and external, and in turn into more specific concerns. The highest greatest risk for TON is internal, we believe: successful, timely execution of the project will be extremely challenging, given the magnitude and still theoretical nature of proposed technological and engineering changes. At the same time, the project faces external risks that are beyond the control of the Telegram team, including competition both from contemporary messengers and other blockchain projects, while legal risks also look considerable.

The TON project faces several risks

Internal				External		
Execution			Post-launch risk	Competition		Legal
Failure to hire enough talent	Theory doesn't meet practice	Failure to meet deadlines		Messaging Apps	Blockchain projects	Inability to trade Gram
Substantial	Very substantial	Very substantial	Substantial	Average	Substantial	Substantial (US only)

Source: HASH CIB

We omit the myriad of minor issues to focus on those that should be of primary importance to investors in Grams. We also note that while there have been [reports](#) of a document shared by Telegram with investors in TON's private placement, which outlines eight major risk factors for the project, we did not rely on these reports. We rather focus on *our understanding* of what an investor doing “deep-dive” diligence on the asset they hold or would want to acquire should be interested in.

Internal risks

Technological concept

The Blockchain protocol and Networking set of protocols that form the foundation of the project pose the most significant risks in terms of TON working as intended. These elements are the infrastructure on which the remaining technologies are to be built, and therefore the most fundamental risks come from any major issues related to them. We also highlight some of the “trickle-up” effects these might have on the higher-level functionality of TON.

The following major issues pose risks to Blockchain implementation on the conceptual level for the proposed technology:

- *TON Blockchain's inherent scalability is both its major selling point and possible Achilles' heel.* Maintaining multiple sets of blockchain states while being able to quickly expand or merge them without discrepancies is a complex task even for a centrally controlled distributed system, let alone a globally distributed, permissionless network. Just the combination of layers of software engineering techniques needed to support the *infinite sharding paradigm* should present a daunting challenge to its builders, with the complexities of reaching consensus among multiple distrustful strangers coming as an additional major task.
- *A scalable yet truly decentralized proof-of-stake consensus algorithm is still effectively a field of scientific research* as Ethereum, Cosmos, Dfinity, and other high-profile projects claiming to offer working solutions still have not presented them so far. By only briefly referencing the approach to choosing a consensus algorithm, TON's White Paper leaves much ambiguity on this issue.
- *Since the interoperability criteria for the multiple different workchains TON should support are not clearly defined*, it is hard to say whether multiple chains will actually be able to run in parallel in TON Blockchain while maintaining their own “integrity” (with own virtual machines or basic currency and token designs), different from TON's *Workchain Zero*. Major projects such as Polkadot and Cosmos, which have been in development since before TON, still have not released any substantial evidence that such a level of interoperability is possible within a single framework, while they have released significantly more theory and code on how they plan to achieve this.

- *TON's documentation currently lacks the technical specification* for us to confirm that the TON Virtual Machine will be able to support the proposed *everything is a bag of cells* data representation technique, which, it is claimed, will be able to support multiple important functions out of the box, such as smart payment channels or near-instant computations between multiple chains via hypercube message routing. The same conclusion applies to its proposed TL-B type language and serialization TL-scheme (for serialization of virtual objects written in other languages), aimed at harmonizing code written by the anticipated global community of third-party developers that will build their services and applications on TON. Even these developers appear only in the future, the success of both TVM and the TL-B language are important in the short term for adoption of TON, as they are important for the creation of generalized user interfaces for on-chain applications.

The above issues represent the main set of technological risks to be addressed by TON Blockchain developers, in our view. There are important but less critical technological obstacles to overcome – such as on-chain enforcement of the off-chain availability of TON Blockchain's archived history if/when TON Storage is decentralized – but they do not pose existential risks to the Blockchain on the conceptual level, in our view, and could be resolved after the project is launched.

The following implications of Networking protocols could pose risks to the proper implementation of TON:

- From one perspective, the *TON Networking architecture described in the White Paper uses a common networking stack* that currently powers such protocols as HTTP/HTTPS (used across the Internet on a daily basis), since TON's Abstract Datagram Network Layer (ADNL) itself is an abstraction over the commonly-used UDP protocol. However, ADNL is a much larger concept than any similar networking abstraction on top of common Internet communication protocols currently used in other projects. TON's "sandwich of technologies," which involves Reliable Large Datagram Protocol (RLDP), Kademlia-like DHT lookups, proxy routing, overlay networking over ADNL, etc., looks both massive and fragile. We know of no examples where such a combination of technologies worked in a production environment. Of course, there have been many experiments, even proofs of concept and test networks – just none of TON Networking's scale. The combination of so many technologies and layers of networking, its complexity and interdependency, could pose technological implementation risks for TON.
- Another example of potential fragility could be *the UDP communications protocol (as a basic layer, separate from the other technologies used), which is used as a workhorse for ADNL (which is on top of it)*. It is fairly easy to censor UDP on a network hardware layer. To prevent that, TON offers a TCP fallback option, but TCP itself brings a significant slowdown in communication speed, which is important given limited block propagation time and consensus-related messaging between validators, among other things. And as we saw from Telegram's wars with different governments, TON's ability to resist censorship is a key factor in driving adoption, so relying so much on UDP for TON Networking could be detrimental to that.
- *Adding abstraction layers separates us more from the real world.* For example, two nodes with minimal Kademlia-distance in TON DHT (which is used for *any* routing in TON) could be on different continents in the real world. In that case, network communication would decrease dramatically, since the laws of physics still apply. Admittedly, most modern-day blockchain protocols use Kademlia-like DHT tables in their networking implementations, both for node lookup and routing. But none rely on it as extensively as TON, we believe: in other projects the overlay networks stack looks much lighter.

Although the described networking architecture seems elegant and technically smart, it's a long way from testing and production to wide adoption. And adoption is what will drive the growth of the TON ecosystem, which in turn would drive the appreciation of Gram and other TON-based assets. The current description of TON Networking means functioning as presented is not a given.

TON's development and launch

In terms of execution, there are two major risks related to project development, testing, and rollout: schedule and recruiting. The project is *already behind the schedule* presented in the offering Primer. Telegram Passport – referred to as Telegram External Secure ID in the Roadmap – was scheduled for Q1 2018, but it was not announced until Q3 2018. This implies that other milestones, such as the Launch of the Minimal Viable Test Network of TON (MVTN, scheduled for Q2 2018) and Testing and security audits of TON (scheduled for Q3 2018) have fallen behind the schedule.

TON Project Roadmap

Q3 2013	↓	Launch of Telegram Messenger and the Telegram API
Q2 2015	↓	Launch of the Bot API and Platform
Q2 2017	↓	Launch of the Payments Platform
Q2 2017	↓	Start of the development of TON
Q1 2018	↓	Launch of Telegram External Secure ID
Q2 2018	↓	Launch of the Minimal Viable Test Network of TON
Q3 2018	↓	Testing and security audits of TON
Q4 2018	↓	Deployment of the stable version of TON
Q4 2018	↓	Launch of Telegram Wallet
Q1 2019	↓	Creation of TON-based economy in Telegram
Q2 2019	↓	Launch of TON Services, TON Storage, and TON Proxy

Source: TON Primer

As there has been no public indication of TON launching, testing or auditing the minimal viable version of its network, the technological challenges could be catching up with developers, we believe. The market professionals and independent developers that we have spoken to argue that TON's team should prefer public releases, given how important peer review will be for their product. However, it is possible that both the launch of the MVTN and the testing/auditing phases of development may have been held secretly. This would be consistent with the team's past behavior, which has seen Telegram's developers remaining silent about their progress and proprietary products before releasing them.

We continue to believe the TON Blockchain protocol (if nothing else out of the larger TON stack of protocols and technologies) will be open source. An open source rollout ensures access to constant peer review and community-driven updates – almost mandatory for such complex technological systems as blockchains. Open source would also drive the wider adoption of the platform by developers and service providers wishing to build on top of TON. We also note the White Paper's multiple mentions of blockchain forks and mechanisms to prevent them embedded into the protocol. Since open source is effectively what makes forks possible, such mentions paint a compelling picture of TON developers that *intend* for the Blockchain to be open source.

Difficulties recruiting developer talent could be another reason why TON appears behind schedule. Even though TON's set of technologies, especially TON Blockchain, require additional recruitment by Telegram, our technology counsel suggested that it would be natural for Telegram's CTO to plan out the building of TON as a natural extension of current Telegram's set of technologies. Such an approach would naturally require more involvement from the core Telegram team members. So even though Telegram has demonstrated the resilience of its distributed server infrastructure during the height of the banning campaign, the effort might have affected the pace of TON development.

We note that a fifth of Telegram's core 15-man developer team as presented in the TON Primer could have been overwhelmed with the April-May 2018 state-level attacks on Telegram by Russia and Iran. Even if Telegram was prepared for the bans, three core team members (one dedicated to each mobile app platform – iOS and Android, respectively – and one back-end engineer) would have probably been needed. It is unclear to what extent Telegram's remaining developer team (i.e. outside of the people presented in the Primer) would be prepared to take up these functions. Moreover, if Telegram did not expect the bans, the number of core team members dedicated to maintaining a presence in those key markets (Iran alone accounts for 20% of Telegram's 200mn user base) could rise to one or even two thirds of the core team's total headcount (5-10 people). So this factor alone could have slowed down the development of TON significantly.

Telegram probably needs to recruit additional developers to its core messenger app team in order to fulfill its ambitions for TON. Similarly ambitious projects in the space intend to grow their tech headcount to 100 developers or more, our sources say. Given that the actual size of the *total* Telegram developer team is unknown, even a rough quantitative approach to figuring out the gap is impossible. A qualitative analysis is no easier without an understanding of the pools of competence within the team (and the holes that need to be filled).

Quality blockchain-focused developer talent is scarce, as our conversations with some of the developer teams on the market have confirmed. Moreover, while TON's competitors are visibly hiring, our sources say there has been little talk of TON hiring among the developer communities that one would expect Telegram (predominantly EMEA-based, as we understand) to draw from: in St. Petersburg, Russia – the home of the Durov brothers and presumably, most of their core team – Parity (the company behind Polkadot) has a developer team. In Berlin – Europe's blockchain developer hub – Parity and Ethereum have a strong developer presence, and Cosmos is also openly hiring. In Switzerland, Dfinity has one of its camps and is openly hiring, as are some other better-financed projects in the space. We are also unaware of TON-related hiring going on in Eastern or Central Europe or in Silicon Valley. Telegram is either secretly hiring talent, or they selectively prefer to seek talent outside of the more commonly known developer

communities. That said, we do not believe they can rely solely on internal resources, given the sheer ambition and tight schedule of the project.

Telegram could fail to obtain the talent necessary to develop the TON project. Telegram initially sought to raise about \$800mn, with \$620mn reserved for costs related to the organic growth of its core messenger app. Following the Primer, we assume that initially only 20% of the remaining \$180mn were intended for “*wages, offices, and legal and consulting services*” for TON development. This implies that the Telegram team intended to spend around \$36mn on costs related to external consultants (with a large portion probably going to legal counsel) and internal talent. In fact, massive investor interest meant that Telegram ended up with a little over \$1bn for TON, instead of \$180mn. Even assuming that only 20% out of that sum would go to recruiting talent – probably a conservative assumption since equipment and infrastructure requirements would not necessarily have changed – Telegram is extremely well funded to hire the best people in the space.

Nevertheless, **talent is a scarce resource in a nascent industry oversaturated with ambitious projects.** And the ambitions of many developers in the space are driven by those projects engaging with the community more openly. Additionally, while the TON White Paper puts forward complex technological concepts, it lacks the detail and approach that technologists would have expected, meaning the project may not have appeared as truly technically challenging (and thus not as interesting) to top-tier blockchain developers. Even with pure technological ambition in mind, we believe most developers will look for a sustainable career rather than a series of well-paid one-offs. So we still believe that the risk of the TON developer team being understaffed remains and is quite material.

We assume that TON is behind schedule: due to the challenge of hiring proper talent and/or the technological challenges. It is difficult to assess actual extent to which this issue is present with TON, so we just underline here the existence of such a risk. If material, it presents a significant challenge for TON as a project.

Post-launch risks

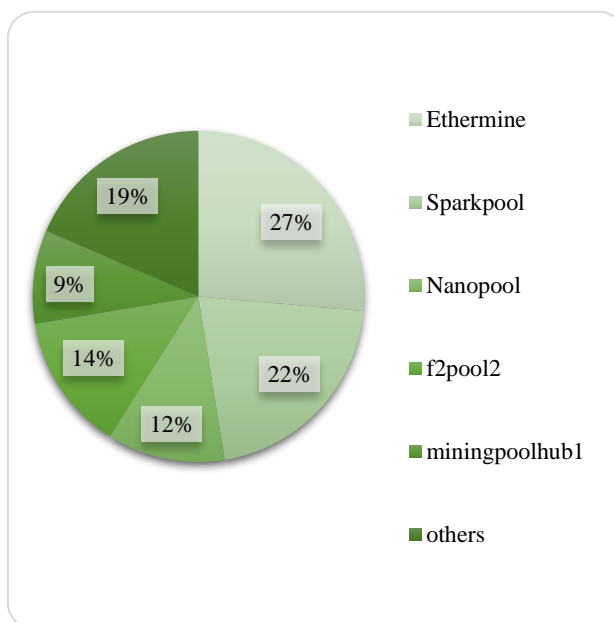
TON is envisioned as a complex system where multiple parties need to collaborate in order for it to thrive and expand. How third-party developers and service providers integrate with the TON ecosystem does not appear to pose a material risk for the project, given more than adequate funding to incentivize these third parties, at least for some time after launch. Of more concern are those potential risks related to the actual maintainers of TON – the nodes and parties providing their resources and services for blockchain validation and storage. These are risks that could materialize after the network is launched.

The industry has seen a well-publicized discourse around off-chain blockchain governance bottlenecks and various on-chain experiments to resolve them. Some research has argued that even the biggest Bitcoin and Ethereum networks are not as decentralized as is publicly presented⁸⁴ and that much greater network node decentralization is needed, be it via mining machines participating in block creation or user computers keeping and updating blockchain history. Both networks are governed off-chain – as being initially envisioned to provide for on-chain Nash equilibrium for different participants via PoW-based consensus algorithms and miner remuneration systems. Although we personally believe both networks are fairly decentralized⁸⁵, those concerns (especially the mining pool centralization narrative) have driven experimentation both around blockchain consensus and governance. TON also proposes an innovation in this regard, one very much inspired by the block creation collective approach proposed by Polkadot. However, on a technological level, TON proposes additional mechanisms as well as a somewhat different PoS consensus mechanism *on top of* the Polkadot-like network maintainers structure. However, we believe that such a grouping of multiple parties responsible for block creation and validation is the key to looking into possible risks with what could go wrong with the TON project as an ecosystem after its launched.

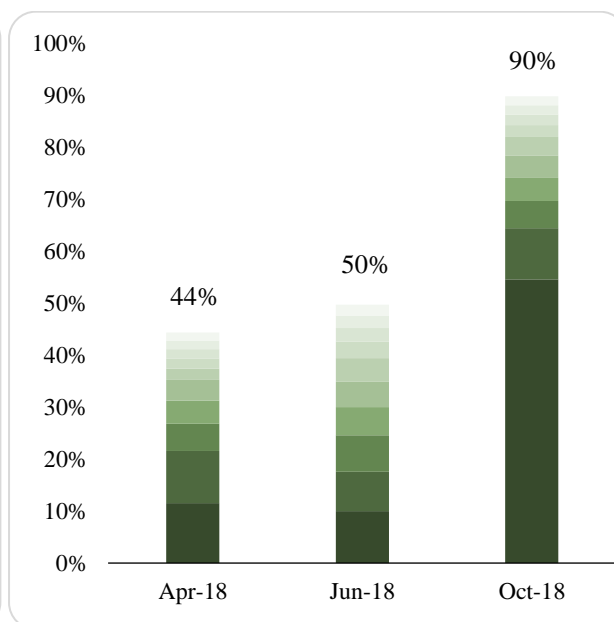
⁸⁴ Probably the most authoritative of such research has been conducted by the Cornell University computer scientists. See: [“Decentralization in Bitcoin and Ethereum Networks”](#) by Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert Van Renesse, Emin Gün Sirer (2018).

⁸⁵ Which is true for the Bitcoin network’s miner-user relationship as evidenced by the block scaling debate, which peaked in August 2017 with the so-called User Activated Soft Fork and the Bitcoin Cash hard fork (discussed [here](#) and [here](#)). Ethereum, on the other hand, is regarded as having a much broader developer community. While being built around the project’s co-founder and “benevolent dictator”, Vitalik Buterin, the Ethereum community is said to be far more democratic and widely spread out than the Bitcoin developer community (which, by the way, is less true about the Bitcoin Lightning Network development). So, both blockchains, in our view, stand out in different factors that equally make up for their respective platforms to be considered fairly *decentralized* – i.e. not controlled by a single party or faction.

Ethereum miner pool centralization (PoW)



EOS held by top 10 wallets (vs. total supply) (PoS)



Source: [Etherscan](#), [Etherchain](#), [eosflare.io](#), [EOS Tracker](#)

The following parties ensure the decentralization of TON Blockchain: validators, collators, fishermen, and nominators. Validators are the parties actually running the nodes that contain the recent state and validate the combined state transitions of all of the shard(work)chains and the main – master – chain of TON Blockchain. A global set of *validators* is responsible for putting together and validating the global state – i.e. the masterchain blocks. Additionally, local groups of validators, no less than five in each such “task group”, are randomly rotated and tasked with validating blocks in different shardchains. *Collators* should put together shardchain blocks of transactions with the state transition proofs of validity of those transactions, while validators would limit their involvement in just checking the correctness of such blocks and committing them into the chain. *Fishermen* are the watchmen of the whole network, responsible for making sure neither collators nor validators meddle with the network by posting proofs of such misbehavior to the network. Finally, *nominators* are a wider group of network participants that nominate certain validators by sponsoring them – for them to buy and maintain dedicated hardware or participate in staking (at most about 0.1% of the total capitalization of TON per each validator – no less than roughly \$9mn⁸⁶).

Global validators are chosen and known about one month in advance, local task groups – about an hour. Each global set of validators is chosen on the basis of an auction, where validators anonymously post their stakes and the proportion of the total system load they are willing to take up to a special smart contract. Then, top T of validators are chosen by the contract. T is a configurable parameter, based on network’s size, initially planned for 100 nodes, with the option to increase to 1,000 validators eventually. The global set is known 2^{19} masterchain blocks (about one month) in advance, while the local set is established 2^{10} masterchain blocks (about one hour) in advance. The validators’ stakes are frozen for two months – a month more than to the actual month they are chosen to fulfill their duties – in order to make sure that validators are slashed if they are found and proven guilty for misbehavior by fishermen or other network participants – even after they give up their responsibilities, but not more than a month. Additionally, the algorithm to select task group validators each hour is (pseudo-)random. All of the parameters for choosing validators could be later changed by special masterchain voting proposals by any network participant with sufficient Grams to post such a proposal for a change, which takes effect if a majority of validators ($2/3$ of the total number of network validators) and other network participants ($>50\%$ of other network participants) agree to it.

We see possible flaws in the block validation mechanism in TON that heighten the risk of attacks, network centralization, or corruption. Given that validators are known a month in advance and they need to post their public key to the rest of the network (for it to make sure that its actually them signing new blocks) and that additionally they would need to maintain the same public-private key pair to maintain their duties for a month more while their stake is frozen – all of this makes the network vulnerable to hacks and other forms of attacks via direct attacks on the validators. Basically, since the global set of validators is publicly unveiled a month in advance, there is a bounty on their heads for at least three months (without them being able to change the “mark point”).

⁸⁶ Our lower-end estimate based on the current Gram price set at \$3.62, per pricing formula presented in the White Paper (actually, at half of this price, as TON Reserve is committed to never let it go below that mark).

Also, since any network user can create a direct payment channel (or use the payment channel network) to remunerate validators, this could lead to bribes that would for the most part be “invisible” to other blockchain participants. The White Paper includes an explicit reference to users being able to open payment channels with any validator or collator in the TON Blockchain in order to incentivize them to include the user’s transactions. Because validator sets (both global and local) are known in advance, we believe this creates possibilities for bribe attacks on the network. This could significantly hamper decentralization, as any party could corrupt a validator without the rest of the network knowing. For example, a participant could pay to have the transactions of another shardchain participant censored and their own transactions included in each block over some period of time; such a scheme could be used to undermine a competing service provider using the same shardchain. This would be more difficult with direct payment channels (due to the higher visibility of final settlements between two parties), but with a payment channel network such bribes could be executed more realistically without attracting too much attention.

The proposed segregation of nominators and validators that should drive decentralization could have the opposite effect initially. The White Paper suggests that since a) validator stakes are expensive and b) not all of the third parties wishing to make sure the network operates as promised would want to buy and maintain the hardware and bandwidth necessary to operate a validator node, some parties could pool their funds behind certain validators instead, in exchange for a percentage of their returns. Such nominators could only come from among Gram holders, as validator stakes can only be posted in Grams. This mechanism is viewed as more democratic, allowing a wider group of network users financially participate in its maintenance and benefit from such participation. However, as it currently stands, only 175 of the project’s investors are sure to receive Gram coins as soon as the network goes live – as TON Reserve (i.e. TON’s treasury) has the right to maintain the remaining supply of Grams in its possession. Additionally, some investors could be incentivized to keep their funds and use them as nominators instead of re-selling them to a wider to-be-nominator crowd – as the secondary market for Grams at least in the US could be restricted for some time from the network’s launch, we assume. But these concerns could all be moot, as there is a high possibility that TON Reserve and “*some other accounts explicitly linked to it*” will use *some of* the unsold TON Reserve coins (holding total of 2bn Grams currently) for staking on the blockchain⁸⁷ during the “*first deployment phase of TON Blockchain*”. And the validator nodes will be installed and maintained by TON Foundation (i.e. a non-profit entity run by the TON team to oversee the network development). All of these measures are proposed as necessary to bootstrap the ecosystem, but could pose the risk of a less-than-tolerable level of centralization of TON.

Third parties such as fishermen will be “incentivized” at least initially by the TON Foundation, which also presents centralization risks. Collators and fishermen are proposed as a means of decentralization for the TON ecosystem. Collators are effectively validators, i.e. professional parties operating nodes capable of complying with system requirements and not having obtained/posted a large enough stake to participate as a validator. Fishermen should make sure that validation is correct and submit invalidity proofs in case of validators’ misbehavior. For that, fishermen obtain a reward – a fraction of validator’s stake. Potential fisherman would need to comply with less rigorous system requirements to perform their duties and deposit relatively small amounts of coins in order to get selected, but their participation is crucial to maintain the democratic ethos of the network. During the initial deployment phase, no collators are envisioned, as low network load should allow validators to be able to put blocks together themselves. However, to ensure that validation is fair, fishermen are needed from the very start to monitor the network’s operations.

The TON Foundation is expected to use up to 500mn Grams (presumably *on top* of the funds to be used by TON Reserve for staking on behalf of TON Foundation) in order to incentivize third-party network participants, including fishermen. With the TON Foundation already controlling validators in the initial phase of operation, initial TON investors would ideally use their Gram holdings to finance fishermen (or provide such services themselves). But if truly independent third-party fishermen nodes are not installed, then TON Foundation would have to finance the installment of such nodes. The problem is that if the parties necessary for making sure a system works in favor of its users become dependent on the service providers (i.e. the other side), this will inevitably lead to corruption of such parties, or, as is more likely, a lack of trust in the network.

TON Proxy and TON Storage nodes will be initially installed by TON Foundation, as explicitly discussed in the Appendix to the TON White Paper covering the use of funds from the placement. TON Storage will be the repository of all of Blockchain history beyond the most recent two months of blocks kept with current set of validators, we assume. The risk is that even the third-party fishermen would not be able to prove that someone has tampered with history if there is a single “owner,” i.e. a single point of failure (even while distributed from the topology standpoint). TON Proxy presents less of a concern, we believe, given Telegram’s track record of preserving users’ privacy.

Network participants must approve changes to the system’s key parameters, but the TON Foundation may initially be able to win any vote. The White Paper explicitly says that the TON Reserve will use unallocated Grams (again, around 2bn Grams currently) to back changes to the network’s configurable parameters proposed by the TON Foundation. Given that validators and possibly other network participants will also be controlled by the TON

⁸⁷ With up to ~500mn needed initially for such staking purposes.

Foundation, any changes it proposes should pass with ease. It remains unclear how long such a concentration of power, described as necessary to prevent system forks and other undesirable events, would remain. As with other risks, it raises concerns about potential system centralization, which could slow adoption and affect valuation.

Some parameters governing the processes among network participants and even some aspects of its technological concept could be resolved as the network evolves. However, easy adaptability comes at the cost of centralization. We are confident that *centralized* distributed ledger systems will be less valued by users over the longer run, even this characteristic does not affect their valuations amid the current market euphoria. Decentralization and immutability are the reasons why the Bitcoin and Ethereum networks are valued so much more than their more efficient centralized counterparts. While the blockchain craze makes up for some of the more centralized public blockchains still gaining and retaining value, we believe such valuations are overblown in terms of fundamentals, so eventually would tend to evaporate if the issues are not resolved. So, to summarize, initial technological concepts and after-the-launch network exploitation mechanisms – both as they stand right now and in light of the very mechanism that would allow them to be changed subsequently – pose significant risks to whether TON is a truly decentralized system in the longer run, which would imply pressure on its value.

External risks – messaging app competitors

One of a kind in a crowded competitive landscape

Although TON Payments is not the only service the blockchain will offer, nor is it likely to be the first to appear, it is the most marketable and one of the most value-added. It is unlikely that Telegram would have raised almost \$2bn without providing a payments service, we believe. And the long-term success of the Telegram Open Network to a large extent depends on the success of the TON Payments service in the mobile payments segment.

Mobile payments is currently one of the most dynamic segments in financial services. The global market will reach \$3.1 trillion by 2022, growing at a compound annual growth rate (CAGR) of around 32%, according to Zion Market Research. Allied Market Research arrived at a similar forecast for a market value of \$4.6 trillion by 2023, with a CAGR of 33.8%. Unsurprisingly, such a bright future has attracted a countless number of players into a now-crowded industry. Although customers do not need that many different solutions, none of the mobile payment systems has become dominant so far.

Mobile payments ecosystem

Mobile wallets	Stores credit card or bank information and uses different technologies to pay online, or through a smartphone app	WeChat Pay, Messenger Pay, WhatsApp Pay, LINE Pay, Kik, GooglePay, Alipay, Tenpay, ApplePay, PayPal, SamsungPay, Square, Venmo
Card payments	Authorizes the use of credit or debit card to pay	Visa, Master Card, Amex
Bank transfers	Uses bank's mobile app to send money to someone else's bank account directly	Sofort, Trustly, Deal
Carrier billing	Buy something on your mobile phone, get it billed to you by your mobile service provider	DaoPay, Boku

Source: *Acapture; HASH CIB*

We consider large messaging apps, especially those able to build blockchains, to be the main conventional competitors for TON Payments. We believe that making payments with a messenger is a different user experience than using, for instance, a mobile wallet, which is just another version of a bank card, for regular purchases. Moreover, TON Payments is intended for micro P2P transfers – the focus segment for messaging systems.

The largest messengers belong to two corporations, Facebook Inc., and Tencent Holding Ltd. Facebook owns WhatsApp, Facebook Messenger (Messenger) and Instagram. Tencent Holding owns WeChat (WeiXin for Chinese), QQ, and 12% of Snap Inc. The next in line in terms of total number of users (300mn) is the Canadian messenger Kik. However, monthly active users make up only a fraction (15mn) of the total, which raises questions about its real adoption rate. Viber has around 260mn MAU. Korea's NAVER (KRX: 035420) controls Japan's LINE Kabushiki Kaisha, which operates LINE messenger with over 200mn active users. Telegram, the next largest, is the only one in this list that does not have a payment service.

Largest Messaging Apps

Corporation	Messenger	MAU, mn	Payment Service
Facebook	Messenger	1 500	Messenger Pay
	WhatsApp	1 300	WhatsApp Pay
	Instagram	1 000	
Tencent Holding	WeChat / Weixin	1 040	WeChat Pay
	QQ	806	QQ Pay
	Snapchat (12% ownership)	200	Discontinued Aug 2018
			Tenpay
			WeBank
Rakuten Viber	Viber	260	Payments via Western Union
NAVER	LINE	203	LINE Pay
Telegram	Telegram	200	TON Payments
Kik	Kik	15	Kin cryptocurrency

Source: Statista, HASH CIB

Not all messengers can call the payments business a commercial success. In fact, for some, it may be loss-making, as they offer rewards for using their payment services while paying fees to operate on established infrastructures. Setting up their own infrastructures, probably based on blockchains, appears to be one of the solutions considered by most messengers. However, given the commercial nature of the corporations owning the messengers, we expect them to always try to monetize the user base one way or another, meaning they are unlikely to surrender control of their networks to the public. Therefore, if built, their blockchains will be centralized and as such, censored.

TON Payments could become one-of-a-kind in the mobile payment segment, we believe. First, its payment channels will be built upon a decentralized, censorship-resistant blockchain. This is a very valuable feature in the payment industry: no one can stop, seize, or refuse payments. Second, TON is a nonprofit structure, and as such, monetization of users is not on the agenda, which leaves the messenger ad-free and puts control over payment fees in the hands of the peer liquidity providers, creating a free and competitive fee market. Third, TON should have a something like a first-mover advantage if it executes and deploys its blockchain in a timely manner (as current messenger app cryptocurrency efforts by Kik and LINE are unconvincing). Last and not least, Telegram's massive commitment to TON means there is much more to lose if its payments service fails. In contrast other companies (especially the Asian stories) that other messengers belong to are more diversified. If these corporations fail to deliver a high-quality payment service or blockchain, the impact would be less. If Apple delivers one disappointing product across its entire portfolio of businesses, its share price falls. If Sony produces an underwhelming cell phone while making virtually anything that can be plugged into a socket, no one cares. Given all these factors, we believe that the main risk for TON Payments is not the competitors in the messaging space, but the project execution itself.

Facebook appears to plan strengthening its P2P payments

Facebook Messenger launched a US-only P2P payment service back in 2015, about a year after Snapchat began to offer a similar service. Now it is 2018, and Snapchat shut down this feature in August 30, and Messenger seems to have troubles with monetization. Payments and other fees represented only 1.5% of Facebook's total revenue in 1H18. According to a May 2018 JP Morgan survey, only 3% of respondents in the US had used FB Messenger for P2P payments in the previous three months, a far cry from PayPal's 38%. Moreover, only 3% consider Messenger a main P2P payment service compared to 58% for PayPal. In other words, users simply do not see the added value in Messenger Pay's run-of-the-mill service. However, unlike Snap, Facebook does not want to give up: international payments on FB Messenger are now possible in the US, Europe, Canada, and Australia via London-based money transfer service TransferWise.

Moreover, WhatsApp plans to launch a payment feature and currently is testing it in India. In February 2018 the messenger began a pilot project in partnership with ICICI Bank, initially intending to offer the service to the public by end-March. However, the project has been delayed as Facebook faces concerns, including the storage and sharing of user data, owing to the [Cambridge Analytica scandal](#). With more than 200mn MAU, India is the largest market for the messenger. If tests go well, WhatsApp is likely to roll out the service worldwide.

Facebook is able and probably plans to build a blockchain, which could be used for payments on WhatsApp or Messenger. There have been some signs that the company is moving in this direction. A few months after banning cryptocurrency and ICO ads on its platform, Facebook not only removed the ban, but also moved further to set up a separate blockchain division and explore how P2P payments could benefit the network ecosystem. The company appointed David Marcus, former VP of messaging products and Facebook Messenger, as head of the blockchain

group. Marcus, who formerly served as a PayPal CEO and a director at Coinbase, one of the biggest cryptocurrency mobile wallet apps, seems to have the right experience to help the network build a blockchain and introduce cryptocurrencies as part of payments facilities.

However, if Facebook creates a blockchain, it is most likely to be controlled by the corporation and regulated by all jurisdictions the company operates in. Thus, decentralized TON Payments will be preferable. We would expect Facebook payments to be more expensive than TON's simply because of Facebook's commercial nature. Still, given the social network's user base, worldwide penetration, and technological strength, we regard it the strongest competitor for TON among messaging apps.

800mn people use WeChat Pay monthly

China's largest messenger, Weixin (known as WeChat outside of its motherland), launched its payment service in 2014. By end-2015, the service had around 100mn monthly users. In its 2Q18 results presentation, parent company Tencent Holding reported that more than 80% of messaging app users (more than 850mn people) also use WeChat Pay. As such, unlike Facebook, Tencent does not seem to have a service adoption problem. However, we cannot say that mobile payments monetization is not an issue for Tencent, as the company does not disclose the revenue from WeChat Pay.

Revenue from all of Tencent's payment-related services totaled \$2.5bn in 2Q18, representing around 10% of the company's total revenue for the period, according to its financial results and our estimation. However, we believe that mobile payments represent only a small fraction of the total. This revenue includes all fees from on- and offline retail and corporate payments through WeChat Pay, QQ Pay, WeBank, and Tenpay. The latter probably brings most of the revenue, as it is China's second-largest payment system after Alipay, with 37% local market share in the \$2.7tr mobile payments sector as of end-2016, according to JPMorgan.

WeChat is a predominately local player with only 10% of its 1bn MAU located outside of China. We think it will continue to remain mostly a domestic messenger, since it will encounter far greater competition abroad. Back home, WeChat benefits from restrictions imposed on main competitors: WhatsApp use has been banned in China since June 2017, with the app joining a host of other social media platforms, such as Facebook, that have been blocked in the country. Moreover, WeChat is both highly censored and centralized. It even has two privacy policies: for locals and foreigners. Therefore, whatever service WeChat offers would be controlled from China, we believe. If it builds a blockchain, it would most likely be centralized and ultimately monitored by local authorities. We doubt that there will be many outside of China eager to share their personal or financial information with Chinese officials. Therefore, we do not consider WeChat a serious threat to TON Payments.

Viber, LINE, and Kik – even less of a threat

Viber has not disclosed plans to build its own payment service, nor have they commented on the possible use of blockchain technology. Viber users can make P2P payments within the messenger via Western Union, and this is probably as far as Viber wants to go. It monetizes its user base through advertising and its Viber Out service, which allows users to make calls to phone numbers.

Japan, Thailand, Taiwan, and Indonesia are the main four markets for the LINE messenger. It launched LINE Pay in December 2014 and now has over 30mn accounts in Japan and 10mn in Taiwan. However, transaction value remains low and usage is based almost entirely on prepaid cards. Transaction volume totaled ¥228bn in October–December 2017, but Japan accounted for just around 20% while Taiwan remained the key driver. Use of LINE Pay in Taiwan got a major boost in July–September 2017 when it became possible to pay personal income tax through it. In Japan, use of LINE Pay prepaid cards is gradually expanding, centered on young people, but app-based use remains very limited.

LINE is trying to increase penetration and is investing heavily in the service in an effort to secure merchants and increase use among consumers. Beginning in June, LINE Pay purchases via the app were eligible for point awards of 0.5-2.0% as part of the incentive program. LINE also began a promotional campaign (10-Yen Ping Pong), offering users who send ¥10 to anyone on their LINE friends list a free item at participating businesses (McDonald's and Lawson). However, cash payments are deeply rooted in Japan, and it lags other countries in the shift to cashless society.

LINE built its blockchain and opened a captive crypto exchange, BITBOX, where its LINK coins, are exclusively available. The messenger did not conduct an ICO and plans to allocate the coins as rewards among LINE ecosystem participants. Around 4mn out of the 100mn total coin supply had been distributed as of 1 October 2018. LINE intends for LINK to become the main cryptocurrency within its ecosystem (for instance, one can pay trading fees on BITBOX in LINKs). However, so far, we see little interest in using the exchange, where daily crypto trading volume is around \$1mn but little interest in LINKs, with zero volume. We see LINE's blockchain and its native

cryptocurrency as a way to digitalize the messenger's rewards program rather than a serious attempt to become a worldwide player in the blockchain industry.

Kik usage is very low. Although the messenger has 300mn accounts, MAU is only 5% of that. With such a small user base, it cannot become a competitor to Telegram or to its Open Network, in our view. Kik launched its Ethereum-based cryptocurrency, Kin, in autumn 2017, raising around \$100mn with private and public rounds of its token sale. The messenger intended Kin to become the first mainstream-adopted cryptocurrency. However, the reality has been disappointing. The Ethereum network proved itself unusable as payment infrastructure for Kin due to slow transaction confirmations and high fees, so the cryptocurrency announced a move to the Stellar network in December 2017, which was then reframed to concurrent use of the two public blockchain infrastructures to power Kin. Later, in May 2018 Kik announced it would fork Stellar protocol to build a proprietary blockchain to better accommodate its micropayment driven in-app marketplace. While Kin made some headlines with all of those announcements, the demand for the coins is weak, with daily trading volume about \$300-500K and price over 90% off its January 2017 peak.

All in all, with the notable exception of WeChat, no messenger can brag that its payment service is widely adopted and used. However, we would argue that WeChat is a special case, given the regulatory environment in China and the country's leap to a cashless society. Whether it can repeat its success abroad is still to be seen. However, even negative experience is good, as it allows newcomers to learn from others' mistakes. Therefore, we believe TON Payments is in a good position: competition is not that strong and TON can try to use accumulated knowledge and avoid mistakes.

External risks – blockchain project competitors

TON's Blockchain-based competitors fall into three major categories, reflecting three core aspects of TON as a project: scaling of payments, scaling of distributed computations, and inter-blockchain communication. However, from the software architecture standpoint they fall into two categories:

- Layer 2 (L2) solutions on top of the already existing blockchains – predominantly solving for *scalability* rather than *interoperability*. These projects are at development stages closer to production than the majority of projects in the other group. Key competitors here are **Bitcoin Lightning Network** and **Raiden** (Ethereum payment channel network).
- Layer 1 (L1) scalability and interoperability-enabling blockchain projects. Effectively, new blockchain architectures that solve both two problems within their basic mainnet layer. Although all projects address both issues, we divide them into groups according to their focus:
 - a) better performance of smart-contract execution and distributed computations (**EOS**, **Dfinity**)
 - b) horizontal scaling and interoperability-enabling infrastructure projects – blockchains for other blockchains to be built on top of them (**Polkadot**, **Cosmos**)

Although TON seems to be the only project out of the ones mentioned so far to explicitly reference building both L1 and L2 architecture elements within its Blockchain platform to provide for all of the three of the major components of next-generation distributed ecosystems, **Ethereum** is moving toward a series of major updates to also solve for general mainnet scalability (on L1) and payments/smart-contract execution scalability (on L2).

Just as TON tackles all three of these major blockchain-based solutions, each of the competitor projects could be used successfully for three of these as well. However, we categorize and review them primarily based on their unique selling points, just as TON used scalable payments as its core marketing hook (noting again that the most marketable technology is not necessarily the most important or innovative in a stack). We believe that in reality such selling points are what usually drive the initial market success of a software platform, with its array of services later expanding as the platform gains momentum⁸⁸. While we believe that blockchains, as more fundamental and widely-applicable tech platforms, will probably undergo a more complex series of transformations in their path to market success – just because there are many aspects and elements to each – we believe the initial line of thinking makes sense. Therefore each of the competitors below could present a challenge to TON, if successful with their own goals.

This is not an exhaustive list of possible category winners amid the Cambrian explosion of tech innovation that is current blockchain space, but rather the most compelling set of projects at this moment that should be released, updated, or ramped up on the same timeframe with TON. Some notable new blockchain projects have been intentionally omitted because they do not (yet) appear to be key players in the competitive landscape, with the exception of RSK network on top of Bitcoin (L2). It is a smart contract execution platform that aims to expand to a whole ecosystem very much resembling that of TON. In our view, it deserves a more in-depth approach than what we present below, which we would like to follow up on in future reports.

⁸⁸ Marc Andreessen, one of the developers of the first mass market Internet browser, proposed a perfect, yet simple, series of theses using current tech incumbents as examples: [On selling points determining the early big winner](#), and [on such winners then adding up new services on top of the initial single major product](#).

Payment Channel Networks: Bitcoin Lightning Network

While we have roughly described Bitcoin Lightning Network (BLN) in some detail in the industry overview chapter of this report, here we would like to provide the product update and current status. Bitcoin Lightning Network is a network of specially designated nodes (all having wallets, i.e., addresses, on the underlying Bitcoin network) that lock up some of their bitcoin liquidity in a set of direct payment channels between each other. In this way they form a combination of routing paths for fast and easy provision of payment routing services to other Bitcoin users. While the network itself is growing exponentially, with more and more liquidity being locked up⁸⁹, the technology itself is still predominantly in test phase with nodes installed mostly by early adopters. Because the Bitcoin ecosystem is open source, some node owners installed the beta-phase software on their actual Bitcoin network-connected nodes, thus rushing its adoption before it was production-ready. Before that BLN was being developed on Bitcoin's copycat "valueless" fork networks, which were used for testing.

Three major software clients developed by three independent companies currently dominate. The key software versions of Lightning clients and their developers are: C-lightning (by Blockstream), the Lightning Network Daemon (Lnd, by Lightning Labs) and Éclair (by ACINQ). Another notable BLN software client is Lit (backed by the MIT Digital Currency Initiative), which was announced back in 2016 but active development seems to have picked up only recently (judging by their online GitHub repository).

In addition to protocol-level software clients – most of which have been in development since 2015 – some end-user applications supporting BLN have emerged recently. While most of them are just Github open repository software code-level projects, some could be tested and possibly even used, namely:

- [CoinMall](#) – a P2P marketplace that supports BLN deposits and withdrawals
- [Strike](#) – a BLN wallet for online businesses with 1% transaction fees
- [Bitrefill](#) – a crypto-payment processor for prepaid phones and some other services, primarily games, that supports five cryptocurrencies and recently introduced support for BLN

There is also an ever-growing [list of online merchants](#), such as [Swiss healthy snack bar with actual physical pickup locations](#), or a [store with Bitcoin-related T-shirts](#) and other merchandise, and many largely similar gambling sites like [Lightning Roulette](#) and [Lightning Spin](#).

While early-phase applications often appear insignificant, they break ground in terms of adoption and can be the start of a snowball effect, as the world saw with L1 Bitcoin. However, there are technological hurdles for BLN software client developers to overcome, while bitcoin itself must become less volatile to drive the use of such payments. Bitcoin still has a long way to go to become accepted by main street businesses such as Starbucks⁹⁰, while users' willingness to spend their bitcoins, given their deflationary nature, is questionable. But BLN does have major supporters, with Jack Dorsey, the co-founder of Twitter and payment provider Square, being among the investors in BLN software developer Lightning Labs. The shared ownership teases the potential of a connection between BLN and Square's Cash app (and its millions⁹¹ of users) in the future.

BLN appears to be the biggest rival to TON Blockchain's instant payment platform, as it is already in production and gaining adoption⁹². TON has yet to unveil its main Blockchain, only after which can it build payment channels on top – not a trivial task in light of the almost three years it took BLN to build up to its current beta phase.

Payment Channel Networks: Raiden

Raiden is a proposed implementation of Bitcoin Lightning-style payment channels and a network of such channels on top of Ethereum developed by a single company, Austria-based Brainbot Technologies AG. However, Ethereum is a different protocol from Bitcoin, and applying even an already tested solution on a different technology is not a trivial task. Currently Raiden is still under development, with two technologies being built in parallel:

- A general Raiden bi-directional payment channel network to be used mainly for human-to-human value transfers, and
- μ Raiden – a one-way channel protocol for costless (micro)payments to service providers, aimed at human-to-machine or machine-to-machine interaction.

The general Raiden technology and payment network is currently being tested on one of the three most widely used Ethereum testnets. It is already at version 0.12.0 with the first mainnet Ethereum beta release (to be dubbed Red Eyes) being prepared. This release is likely to remain largely a testing ground, as developers attempt to solve

⁸⁹ Current BLN status can be seen on [recksplorer](#).

⁹⁰ Starbucks has explicitly [denied that it is working on accepting bitcoin](#).

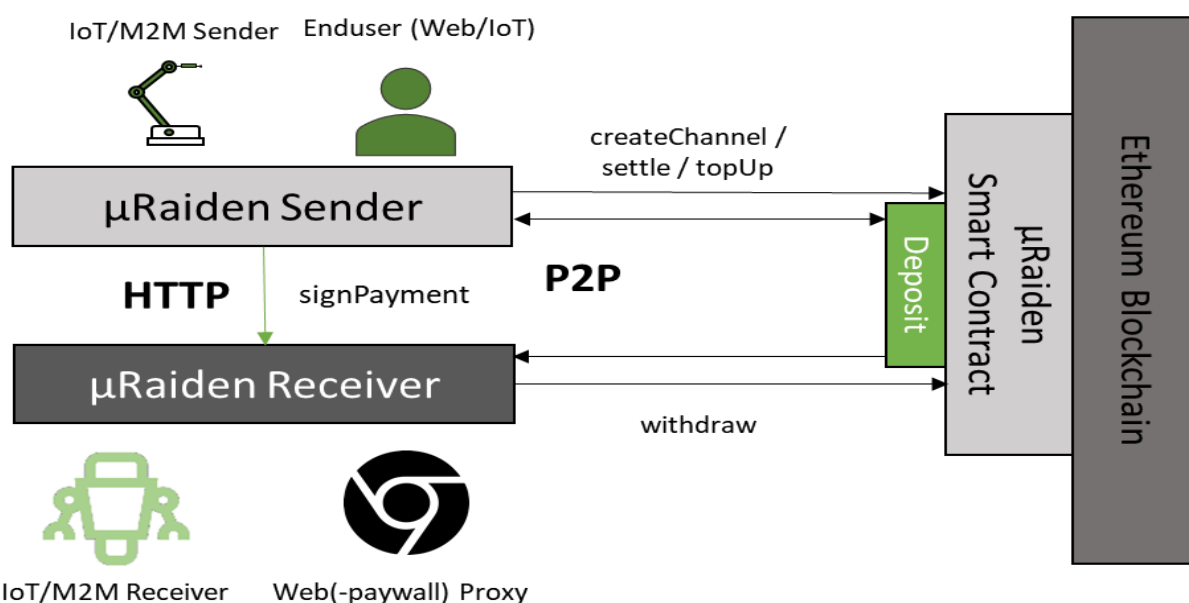
⁹¹ Square [reported](#) seven million monthly users in December 2017 and [later said](#) monthly spend tripled from December to June 2018.

⁹² Another simple, yet informative BLN stats resource: <https://1ml.com/statistics>

routing and liquidity availability issues. Eventually end-users will see a more complete release (to be called Ithaka), which should include a mobile wallet application and a light client protocol (for third-party wallet apps to build upon).

μRaiden is a no-fee micropayment technology. Since it uses one-directional payment channels, the only costs that parties should incur are mainnet Ethereum channel opening and closing (final settlement) transaction fees. While μRaiden remains a work-in-progress technology at this point (version 0.2.0 version at the time of writing), it is rapidly being developed and tested. On top of just being a significantly simplified version of Raiden, it was also released as an open source framework (set of libraries, documentation and code). So, it currently has an implementation on each of Ethereum's three major testing networks, as well as the mainnet.

μRaiden is aimed at facilitating micropayments for digital services on the web or machine-facilitated services – the possible new market with huge opportunities, also targeted by TON Payments. There are two major technology examples at this point (test versions): a Wikipedia-directed channel for thanking contributors and payments towards an IoT-enabled device – both in form of demos.



Source: Brainbot Technologies AG

As both Raiden payment channel technologies are aimed at solely ETH and ERC-20⁹³ tokens value transfer facilitation, the developer team also plans to build more generalized state channel technology on top of Ethereum – for distributed computation to be executed by smart contracts across various L2 chains. In this regard it is somewhat similar to TON's multi-blockchain architecture, however limited, and has the potential to expand towards blockchain interoperability functionality. The project for such generalized state channels network is called Raidos and currently is mostly a concept, as we understand it.

We assume that while being in development for some time now (from 2016) Raiden has yet a long way to go before getting to production and starting to get actual adoption like BLN is already doing. However, Brainbot AG seems to be determined to publicly release the network in 2019 and seems to have both the developer team and funding to do so. Since Raiden is built on Ethereum – a platform that is aiming at a wider niche of applications to be built on top of it, rather than just value transfers (as is the case for BLN), Raiden runs a risk of being “leapfrogged” by newer-generation protocols like Dfinity and EOS that solve the same host of scalability problems out of the box, before picking up steam. Additionally, Ethereum developers themselves are building competing solutions to Raiden's second layer payment and generalized state channel technologies, which could also shatter rather than provide healthy alternative to Raiden's solution. Nevertheless, it is still a possible competitor to TON Payments, leveraging on Ethereum's wide network effects with its 35+mn unique addresses⁹⁴.

Blockchains: EOS

EOS held a massively successful fundraiser, which lasted for almost a year and raised roughly ETH 7mn (at one point equivalent to \$4.2bn) with tokens being sold through special auction window periods while concurrently being traded on some of the biggest cryptocurrency exchanges – thus creating price arbitrage opportunities. The sale was surrounded by controversies, which saw the issuer and developer of the protocol, the Cayman Islands company Block.one, referring to the

⁹³ Ethereum fungible token standard. See [Glossary](#).



⁹⁴ According to 1 June 2018 data from [ConsenSys](#).

fundraiser proceeds as “revenue” (seemingly due to legal restrictions), while its CEO reportedly said the funds would be reinvested into ecosystem development through a billion-dollar fund. As of now, Block.one has [officially announced](#) only a \$200mn JV partnership to incentivize EOS-related development activity in Asia.

As a Delegated proof-of-stake system, EOS needs additional governance mechanisms to guarantee fairness and reliability to its participants, resulting in a trade-off of decentralization, as only 21 nodes (so-called “block proposers”) are nominated by the stake-weighted votes of other network users. Therefore on top of a software protocol, it has an offline-world-like Constitution and Core Arbitration Body (ECAAF). However, as it turned out, Block.one was not well prepared for the long-awaited network launch in June 2018, either with its software or the initial version of the system’s Constitution.

China’s largest Internet security company, Qihoo 360, [announced critical security vulnerabilities](#) with EOS’ Block.one-developed protocol, just days prior to the official launch. In addition to fixing the bugs, Block.one launched [a bug bounty campaign](#) on an open source hacker community platform – with a \$10,000 maximum reward tag on the gravest vulnerabilities found. In its first days (and prior to the launch of the network) a single bug hunter was able to collect \$80,000 worth of bounty in a day and [\\$120,000 in just a week](#). The current tally is well over \$400,000 in bounties paid, with critical bugs still being found on a regular basis.

Critical bugs are still being found in EOS, months after the network launch (as of 27 September 2018)

10		By francois_proulx-eoscanada to Block.one	\$10,000	closed 16 days ago
10		By tjps to Block.one	\$10,000	closed 18 days ago
7		By francois_proulx-eoscanada to Block.one	\$10,000	closed 22 days ago
3		By humblefirm to Block.one	\$1,000	closed 22 days ago
3		By chengjia4574 to Block.one	\$100	closed 22 days ago
5		By talko to Block.one	\$250	closed 23 days ago

Source: [HackerOne](#)

In addition to buggy software, the network had multiple major operational issues, including:

- a delay in the network’s launch due to some of its 21 block producers being offline during the set launch time
- the network completely halting, with no blocks being produced just days after the postponed launch, [due to a bug in a software update](#)

Beyond the overwhelming [number of technical issues](#) with EOS, additional criticism came from the project’s own CTO and ideologist Daniel Larimer, previously responsible for building BitShares and Steem blockchains, who decided to scrap the platform’s Constitution because of multiple issues surrounding the EOS Core Arbitration Forum – a judiciary body within the network.

The main series of issues arose after the network’s block proposers violated the EOS Constitution by singlehandedly “freezing” several user accounts without putting the issue before the arbitration body⁹⁵. Moreover EOS’ top 10 account holders (including Block.one and top crypto exchanges that had facilitated EOS’ secondary sales amidst its fundraiser) were [accused of controlling around 50% of all of the platform’s monetary supply at network launch](#) giving them ability to control the stake-weighted voting for the 21 block proposers. As of 1 October 2018, the top 10 “richest” accounts have only increased their control, which is now at 90% of the network’s circulating coin supply. The combination of those two factors have led to near-consensus in the community that EOS is a far more centralized platform than advertised by its proponents. Moreover, these governance and technological issues have led to multiple instances of users and third-party developers [forking the EOS protocol](#) on their own terms, in order to fix the technology or to get rid of the oligopoly.

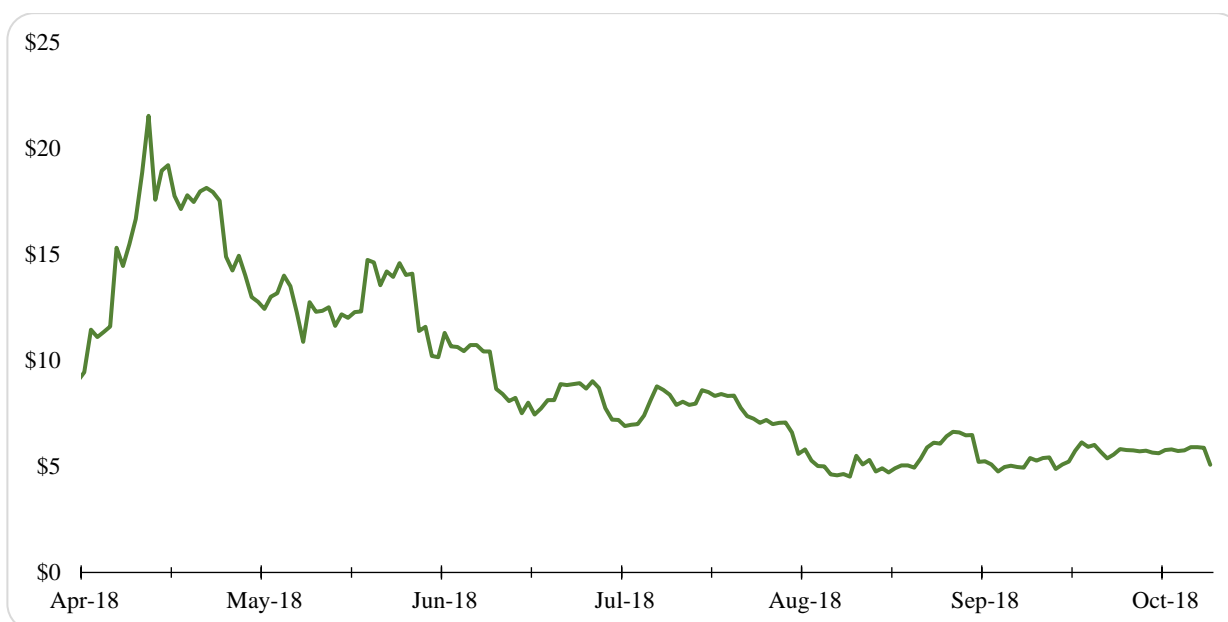
⁹⁵ [“EOS freezes 7 accounts in violation of its own “constitution”](#), The Next Web.

Despite the criticism, we believe that EOS still offers a compelling set of technological concepts. Because it is built on the more developer-friendly WebAssembly framework (as opposed to Ethereum’s Virtual Machine) and utilizes DPoS (which is reported to enable EOS to reach thousands of transactions per second⁹⁶), EOS may be better suited for hosting multimillion-user DApps than its competitors. EOS optimizes for network account management and usage more suitable to general users than the rigid one-mistake-can-cost-you-everything general blockchain user experience. It supports *costless* transactions for users, effectively eliminating fees, and allowing users use its capacity in full, unless the network reaches maximum load, when their percentage of network capacity is limited by their share in the total network’s monetary supply. Network nodes providing the CPU, storage, and bandwidth necessary for its operation have a steady revenue stream from EOS inflation (1% p.a.), distributed among its standby block producers (network nodes with capacity that do not participate in current block creation and validation processes – just running the computations and storage for the network) and block producers (network validators).

The market currently finds EOS less convincing and promising, due to the combination of an extremely successful fundraiser and the stark contrast between the developer’s as-yet unproven claims of superiority and its messy launch. Block.one should have all the funding and incentives to deliver on its promises (assuming it is acting in good faith). If EOS actually builds out an ecosystem of massive DApps for ordinary users in the way [some recent announcements suggest](#), it could present significant competition to TON’s intended *distributed, mixed* and *centralized* app and service ecosystem. However, at this point, how EOS handles massive loads of real user activity has yet to be seen – presumably the “stress-tested” capacity is yet to get a real test in the wild⁹⁷. However, EOS’s top DApps are [reportedly already serving a few thousand users daily](#) – entirely possible given its strong presence in the Chinese-speaking part of the world.

The EOS cryptocurrency currently trades significantly below its pre-launch price levels. Such sentiment could be protracted, due to the market being deeply scarred by EOS’s messy launch. It took Ethereum almost two years to overcome similar technical issues and grave governance crises before it actually functioned more or less as intended. But since Ethereum’s developers were less brash about the project’s goals and more open and engaging with the developer community, it caught significantly less flack, even with the whole of then-dominant Bitcoin community set against it. Consequently, such controversies had less impact on ETH’s valuation.

EOS is just a quarter of its peak level



Source: [CoinMarketCap](#)

⁹⁶ While the [EOS Network Monitor](#) (the website experiences downtimes) shows the all-time high record of tx/s at 3,996, at the time of writing the actual load on the network (providing a block roughly each 0.5 seconds) is a moderate 7 transactions per second (much like the current Bitcoin maximum load).

⁹⁷ EOS supporters also commonly point to [Blocktivity](#) as an independent reference source. The site has historically listed Bitshares and Steem, projects created by Block.one’s former CTO, among the most widely-used blockchains in the world with massive tx/s results. However, we question whether the reported loads reflect real user interest or just DPoS delegates’ artificial activity: it is unclear that Bitshares is ever actually used, but it nevertheless holds the #1 position even after the massively marketed EOS was launched.

Blockchains: Dfinity

Much like EOS, Dfinity aims at creating a completely distributed but extremely well-performing platform for future applications and services. The core difference between the two (technological differences aside) is that while EOS aims to cater to end-users by providing access to applications, Dfinity seeks to become a backbone service and infrastructure provider for applications, without creating an actual ecosystem for users, but rather seamless off-chain to on-chain transitions. The project's founders call it the "Internet Computer".

While aiming to disrupt the fast-growing Internet infrastructure big businesses of Amazon Web Services and Microsoft Azure, Dfinity has been marked by sequential yet material progress since setting up a non-profit Swiss foundation in Autumn 2016 (pre-dating to 2015 as an actual project). Their step-by-step progress illustrates the thoughtfulness of its founders and the seriousness of their aspirations. Ahead of the ICO craze of 2017, it held a "seed" crowdfunding round in February, moderately capping its capital requirements at CHF 1mn and receiving four times more in ETH and BTC in just a few hours. The timing, however, coincided with a market rally, following the Enterprise Ethereum Alliance's⁹⁸ announcement at the end of February 2017 – seeing ETH skyrocket threefold in a little over a 3-week span. Eventually, according to the project's president and chief scientist Dominick Williams, Dfinity ended up with approximately \$40mn worth of fiat and crypto cash. Since then the project received another, private round of funding led by Polychain Capital – one of the blockchain industry's leading Silicon Valley investment funds – which left it with over \$100mn in funding. And then in August 2018, the project raised another \$100mn from institutional and accredited investors, including Andreessen Horowitz's newly established crypto fund. With its host of respected backers, Dfinity seems to remain keen on rewarding their "seed" investors with a constant ~25% of total token supply when the network is launched.

Dfinity aims at innovating on multiple levels with its own PoS consensus algorithm (a complicated hybrid of existing algorithms on top of Dfinity-specific randomizer technology) and on-chain governance model (the so-called "Blockchain Nervous System"). Without attempting to dwell on these complex system innovations, we note they represent original approaches to solving scalability and governance issues that existing public blockchains have not been able to resolve.

Dfinity's massive scale and its holistic approach are the main reasons it looks like a TON competitor. Dfinity built its foundation on top of the WebAssembly (Wasm) virtual machine that is used as the main engine to run DApps. WebAssembly compiler⁹⁹-based applications are compatible not only with popular web-browsers such as Google Chrome, Microsoft Explorer, Apple's Safari, and Mozilla's Firefox, but also with end-user operating systems, which at the end of the day will allow running them not only on the Dfinity platform environment but virtually everywhere. By using Wasm, Dfinity makes its infrastructure seamlessly compatible with the rest of the world's software. At the same time, we note that the WebAssembly standard remains itself a work in progress. Dfinity currently employs one of WebAssembly's creators, working with the team on allowing a browser extension-powered seamless transition to websites (and subsequently applications and services) hosted on its distributed cloud.

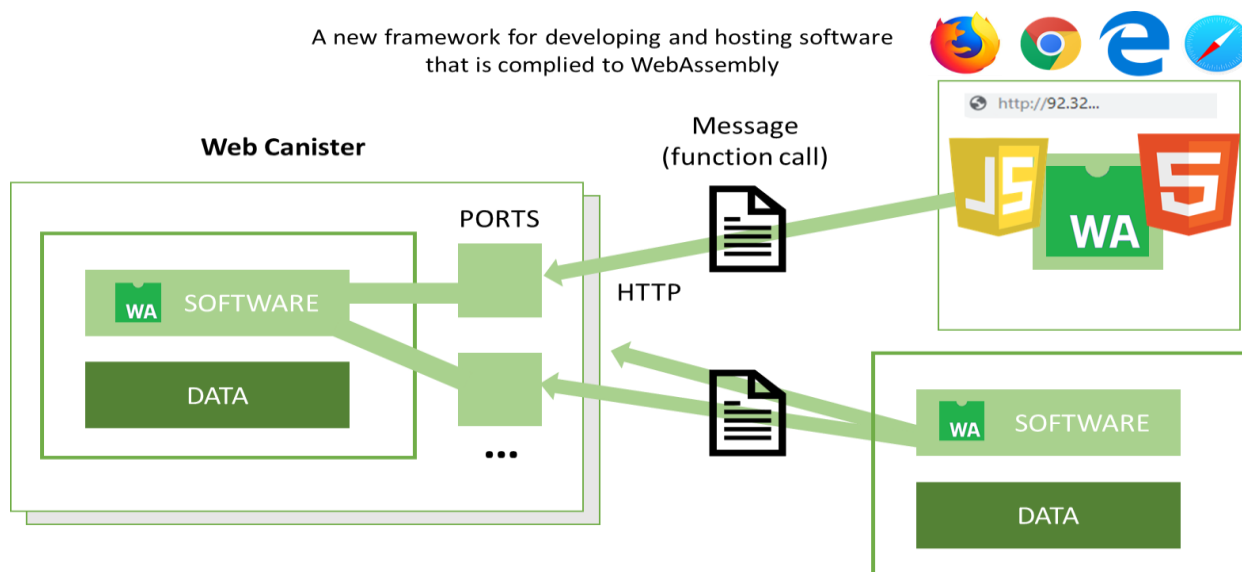
In this way Dfinity could enable truly censorship- and failure-resistant distributed (and even decentralized) applications, as current Ethereum or EOS DApps, for example, still rely on centrally hosted website interfaces to link users to their applications. If the hosting provider of such a website decides to shut it down for whatever reason (e.g. it is banned, as Russia and Iran did with Telegram), it would take time and incur additional costs for the DApp developer to move it to a different hosting provider, where the risk would only reappear – just as Telegram had to play a cat-mouse game with the authorities. Dfinity aims at eliminating such risks. Any app or service developer will be able to host their app or service on a Dfinity-distributed cloud and maintain all the properties of a commonly used website/app interface and performance, yet with a truly distributed infrastructure underneath it.

⁹⁸ An effort by businesses to experiment with Ethereum's technology, which counts Microsoft, JP Morgan, Intel, Deloitte and many other multinationals among its members.

⁹⁹ A tool for web development recently gaining wide adoption outside of the blockchain industry. Wasm effectively allows a programmer to use any programming language they prefer when building web pages and applications. It is being developed by engineers from Mozilla, Microsoft, Google and Apple.

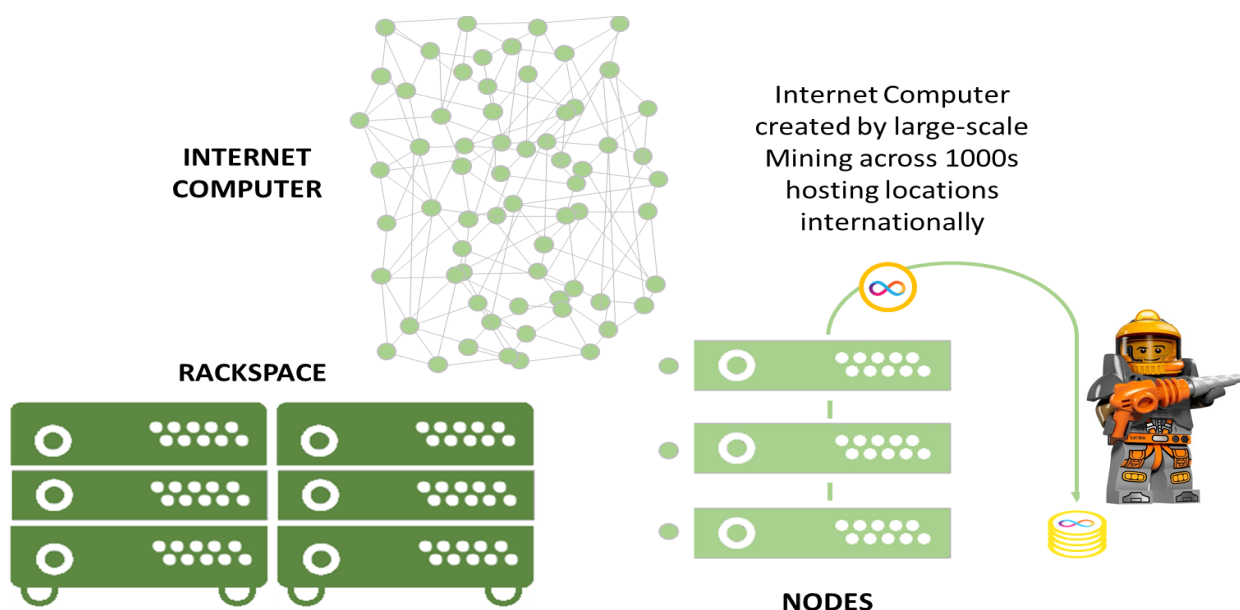
Dfinity website and app-hosting “web canisters” seamlessly connected to popular Internet browsers

A new framework for developing and hosting software that is complied to WebAssembly



Source: Dfinity

Dfinity treats each node on the network as a separate service provider, using cryptographic algorithms to make sure that they comply with its high system requirements. This replaces relying on a virtual machine to perform sequential blockchain state changes within blocks, with *all* of the network’s nodes computing the same transactions, as in Ethereum. This approach allows Dfinity to distribute hosting and computation services but with dedicated loads imposed on the network, rather than simple replication that is “useless” but necessary to keep the blockchain secure and robust. Dfinity claims it can maintain the security and robustness of blockchains without any tradeoffs.



Source: Dfinity

The project is set to launch its first public version in Q1 2019, with limited functionality – currently focusing on hosting websites rather than full applications, with the rest of the network to be gradually built up. With private and seed token distribution already complete and ICO plans scrapped, in order to incentivize adoption the team has been hosting series of “airdrop” signup events (free token distributions) for its supporters.

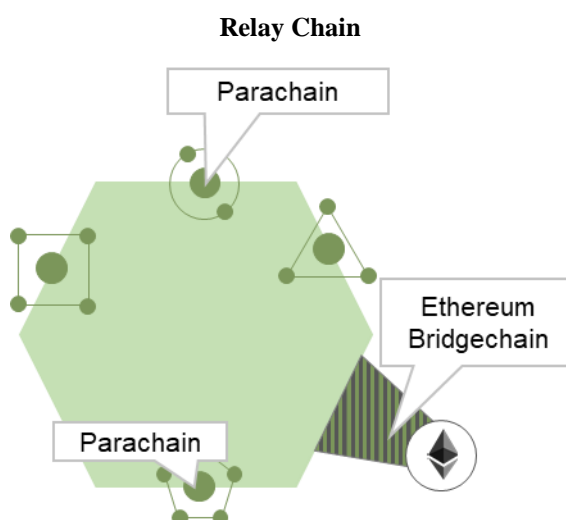
Dfinity would represent serious competition for TON if it manages to implement seamless WWW-to-distributed network transition for users. The possible advantage of Dfinity’s infrastructure here vs. TON’s is that it would host fully distributed applications and services (again, with the possibility of expanding to truly decentralized versions, in terms of governance) – the so-called Web 3.0 generation of censorship- and control-immutable, democratized Internet.

Blockchains: Polkadot

Polkadot is an ambitious project aiming to build a blockchain for other blockchains. Unlike EOS and Dfinity, which focus on promoting themselves as platforms for distributed apps and services, Polkadot can be thought of like a connecting hub for other platforms to be built upon. Its core premise is that it provides consensus-as-a-service to blockchains docked at Polkadot.

Architecturally TON Blockchain seems very much Polkadot-inspired. The main chain is a relay chain that hosts blocks containing the recent states of all blockchains within the Polkadot ecosystem, which are called parachains. Any parachain can grow down (scale) vertically by becoming a relay chain to its parachains. If this happens, then instead of actually processing transactions (distributed computations), such a parachain-turned-relay becomes a consensus-only layer to lower level execution chains. Parachains are maintained by collators, which put together transactions and send them to the relay chain with state transition proofs for verification of their validity, which is done, with subsequent transaction commit into the next block, by validators.

Polkadot uses its own PoS consensus algorithm, generally based on validators reaching a minimum of 2/3 consensus among themselves on the validity of a transaction based on its state transition proof – i.e. verifiably true description (which itself is based on prior history, also recorded on the relay chain and thus available to validators) of the state of accounts related to a transaction before and after it takes place. The Polkadot consensus algorithm should be fast, but currently there are no particular block propagation interval time limits or transactions per block throughput count, mostly because Polkadot is currently more of an approach, with concrete implementation yet to follow.



Source: Polkadot

Polkadot is being developed by Parity – a company widely known for maintaining the biggest third-party Ethereum network client software and popular multi-signature wallet. Parity is run by Ethereum co-founder Gavin Wood, who authored Ethereum's initial technical specification and its subsequent updates – the Ethereum Yellow Paper. Wood and his team are considered among the best blockchain developers in the industry. Yet the Parity team are responsible for a software bug that resulted in almost [514,000 ETH being “frozen”](#) – effectively lost at this time, but possibly retraceable via a “hard” fork¹⁰⁰ Ethereum protocol update. The irony is that over 300,000 ETH out of that sum – almost \$400mn at peak ETH prices of January 2018 – were funds collected through the Polkadot ICO. Users had reported the bug responsible for the loss months before it happened, but Parity did not fix it in time. Earlier, in July 2017 some 150,000 ETH (worth \$30mn at the time) were stolen from Parity wallet users due to a vulnerability in one of its updates. Both issues, as our technology counsel has suggested, illustrate the complexity and vulnerability of coding in Solidity (Ethereum's home-cooked programming language) more than the level of competence of the Parity team.

The Swiss non-profit behind the Polkadot project, Wood's Web3 Foundation, [confirmed](#) that it is dead set on continuing the development of Polkadot and plans to deliver on the initial schedule, thanks to the availability of additional funds to finance the project, despite the freezing of ICO proceeds. Parity does seem to be well funded, with multiple developer teams working in the UK, Switzerland, Germany, and Russia. The key differentiating factor for Polkadot is that its currently available codebase is neatly written, its Parity Substrate framework for building blockchains within Polkadot contains a ready-made library for developers to build upon, their version of libp2p (an

¹⁰⁰ In order to introduce changes to the protocol in a hard fork, the changes must be accepted and effectuated via software update by the majority of network participants for others to follow the new chain as well, because it would require *every* network participant to update their software clients in order to continue participating in such a blockchain.

open source networking layer stack somewhat similar to TON Networking, but less complex) implementation is a robust example of proper engineering, while the whole Polkadot project supports WebAssembly compiler for easy integration of other developer tools within its ecosystem (with additional compatibility provided by Parity Substrate framework).

The Parity developer team's approach to their project seems rigorous and that is why it will probably take so long for Polkadot to go live – perhaps in Q4 2019. In July, the team unveiled a second version of Polkadot's proof-of-concept implementation (still mostly code at this point) with an important milestone – a bridge parachain to connect Polkadot with Ethereum, and some testing activity on Parity-curated Ethereum testnet Kovan. And in October, Parity announced the launch of a testnet for its Substrate framework for building blockchains (that could be easily integrated with Polkadot). This way third-party developers will be able to experiment with the Wasm virtual machine for Polkadot and build parachain implementations. While it appears that Polkadot project will take some time to be released, its architecture and Parity's approach to implementation have attracted both much attention and top-notch blockchain developer talent to work on it.

Since TON which takes after Polkadot in many ways, we would not be surprised to find out that TON's **workchain zero and second-layer solutions were actually envisioned as a Polkadot-compatible blockchain**, and that the teams are actually working more closely with each other than it seems from the outside. One possibility is that the Polkadot infrastructure represents a "backup" option for TON Blockchain to maintain much of the advertised ecosystem and payment channel functionality, should the team encounter too many problems along the way to product.

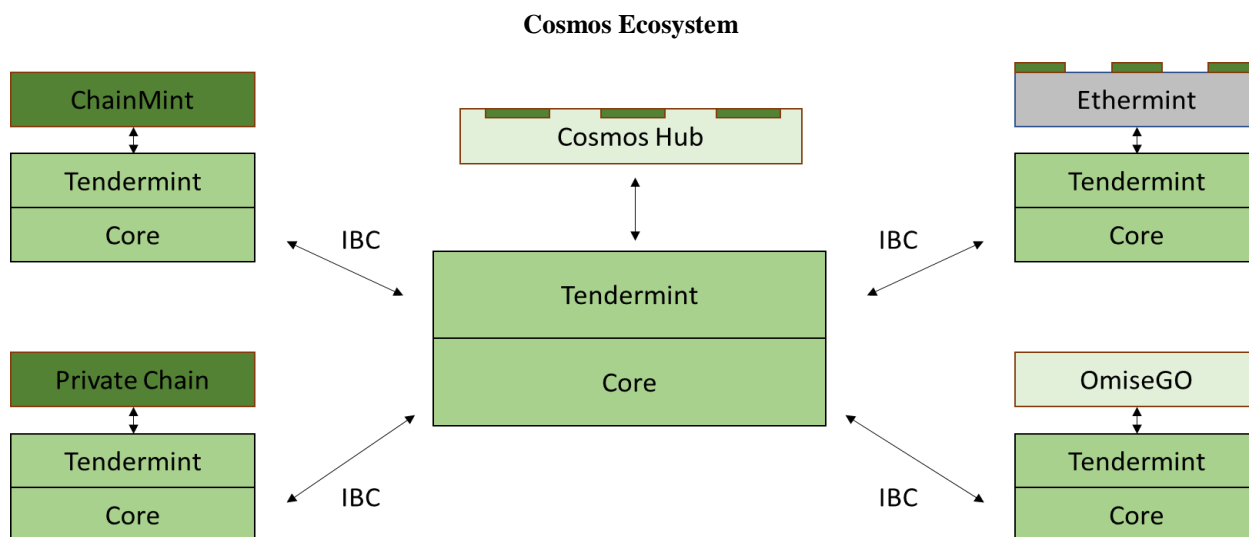
Blockchains: Cosmos

Cosmos grew out of founder Jae Kwon playing with the idea of introducing proof-of-stake to Ethereum. In 2014 he proposed the first implementation of a blockchain-based *BFT algorithm¹⁰¹, inspired by the general computer scientific research on distributed consensus and Practical Byzantine Fault Tolerance. The groundbreaking consensus algorithm proposal resulted in the creation of Tendermint – an Ethereum Virtual Machine-based blockchain project aimed at private and sidechain implementations.

While the Tendermint project itself did not pick up steam, its consensus algorithm inspired major projects in the space – namely, Ethereum's Casper research and Polkadot. Tendermint's PoS Ethereum implementation, dubbed Ethermint, gained the attention of the wider developer community. Tendermint's network architecture allows the decoupling of application execution from the networking and consensus layers of the blockchain (whereas on Ethereum, such processes are closely intertwined). Additionally the Tendermint algorithm theoretically allows for over 1,000 transactions per second. So, in 2017 Kwon and team announced they would build an ambitious inter-blockchain platform Cosmos, leveraging on some of the best technologies of the Tendermint protocol and proposing some new ones to advance inter-blockchain compatibility. Cosmos raised almost \$17mn worth of crypto in an ICO held in April 2017.

Cosmos seems to have architectural similarities with Polkadot – the main interoperability chain (the so-called Cosmos Hub) connects the network's other chains (called "zones") to each other – but also some important distinctions. The main differentiator for Cosmos initially is that the zones already establish consensus within them using a Tendermint leader-based PoS algorithm. As Cosmos was initially intended solely to facilitate value transfers between chains, it leveraged on in-zone consensus to enable fast and reliable verification of compact (i.e. Merklized) transaction-proving data (much like TON's TVM-enabled bag of cells inter-chain facilitation approach). In other words, Cosmos Hub acts as a light client node to each of its zones – receiving proofs of value being properly "frozen" on one chain in order to release it on another chain, with everything done in an automated, smart contract-operated way. All the communication between the zones is done via Inter-Blockchain Communication protocol (IBC, for short).

¹⁰¹ As discussed in the section covering probabilistic vs commercial finality in the chapter covering blockchain industry.



Source: Cosmos

In addition to zones – blockchains adopting Tendermint PoS protocol – other public blockchains like Ethereum can be connected to Cosmos via so-called “peg-zones”, i.e. Cosmos chains performing the special function of pegging their tokens to these outside blockchain’s cryptoassets (again very much like Polkadot’s “bridge” parachains).

Cosmos has generally been more focused on light client-like simple verification and value transfer rather than inter-chain computations. However, recently the team announced that they were working on enabling inter-blockchain messages – i.e. smart contract calls in addition to just value transfers.

While being the least financed project out of the analyzed group of public blockchain initiatives, Cosmos is the one closest to actual launch, thus breaking ground in solving for interoperability. In terms of scalability, its horizontal scaling can in theory allow it to support an extremely high load of transactions – which is to be proven right or wrong after the network is launched or more openly tested. No release date has been set for Cosmos, but we expect the network to launch Q1-Q2 2019, if all goes as expected. It could capture the first-mover advantage or, alternately become a learning experience for other projects in the space (namely Polkadot and TON).

Blockchains: Ethereum

All of the above discussed projects, each in their own right, present challenges and even possible threats to TON gaining traction and achieving market dominance (as probably most of its investors and supporters would hope), rather than just becoming one of the many second-best platforms out there¹⁰². But we believe the biggest threat still comes from the platform whose architectural, lower-level technological, and governance issues were initially put into a roadmap to be resolved later, and whose additional defects were revealed only after it was launched, providing major “inspiration” and points of reference to all of the above newer generation projects – Ethereum. The Bitcoin network, thanks to a combination of Bitcoin Lightning Network and an RSK-built second-layer infrastructure (referenced earlier in the current section, but left outside of this report), in our view, presents a serious threat to TON as well. But Ethereum comes off as a more immediate one, but *if and only if* it solves its scalability issues, looming over all of its future. All of the innovations it plans to undergo in order to accomplish that will put it right back into the same bucket of leading-edge blockchain technology with the other projects discussed here. We believe that on top of already existing network effects (probably *all* of Telegram’s ICO-hungry users have used ETH at least once – and those are TON’s would-be early retail adopters) and resources behind it, Ethereum also has the technological developments in place to be able to do so.

In November 2018, Ethereum will reach a major milestone on its roadmap: Constantinople. It is a hard fork software update, assumingly implemented by all of the network without any objections because it will not introduce any drastic changes. But it will lay the ground for a key platform update expected by end-2018 or Q1 2019 – the long-awaited switch to the Casper the Friendly Finality Gadget (CFFG) PoS+PoW hybrid consensus.

While proof-of-work is currently viewed as the most secure consensus algorithm, it only provides for *relative finality of the blockchain’s history*, as a party with a majority of computation power *always* presents a threat. While such a party would not have financial incentives to do so, the mere possibility of such an attack represents a constant vulnerability for a PoW blockchain – especially if, for whatever reason, it quickly loses the computational output (the

¹⁰² As we know from the dot-com era, in tech second-best products usually tend to die slowly or become niche players, while the emerging winners end up dominating their respective categories or markets.

so-called hashrate) provided by miners¹⁰³. In case of what we called the “commercial finality” (see the chapter covering the blockchain industry overview for more background) provided by PoS, there is a significantly smaller risk that such finality will be broken. If the PoS network stops being valued (and thus maintained and updated by all of PoS consensus-participants), then there’s no need for it – so why bother with finality? In PoW, argued by supporters of the above-presented line of thinking, the cause-and-effect relationship is less direct – with the amount of computational resources used to secure the network being a reasonable straightforward proxy of its value. So true PoS finality, if figured out, is actually a more secure and immutable blockchain consensus algorithm, its proponents argue. That is exactly what makes it so desirable for Ethereum – far more than just cutting the electricity consumption externalities of PoW.

Any second, third, and further layering on top of a PoW blockchain could simply collapse like a house of cards if you break the security of the underlying network by obtaining enough computational resources. Proof-of-stake proponents would argue that you do not take chances if you build those layers on top of commercial finality. So in order to keep expanding and building, Ethereum needs to figure PoS out. And while projects like Tendermint provide for fairly secure and more or less useful PoS algorithms, true *decentralized* PoS is much harder to achieve, as there are far more mathematics and actual game theory involved: the attack vector for PoS is much wider than for PoW. This is why it has taken Ethereum so long.

However, the Friendly Finality Gadget “lighter” version of its Casper PoS algorithm seems actually not far from being put into place. It provides finality through PoS validation of a block once in 100 blocks (~20-25 minutes). All the Casper FFG logic will be governed by a smart contract. Basically, validators deposit some amount of ETH (yet to be finalized, but 1500 ETH as of right now) to that smart contract and then vote only for each 50th block (the 49 blocks that come before it are mined the usual PoW way). If this block gets the necessary 2/3 of the votes, then it gets committed as the so-called epoch check point. Each epoch is linked to the previous one, so after validators commit the second epoch in a row the first one gets finalized and so on. That’s why it takes exactly 100 blocks for finality. And you only need to vote for the latest block to confirm the validity of the whole chain of blocks in the epoch.

As soon as the Casper FFG is effectuated, Ethereum is locked in for the most major of its updates – the switch to sharding. While having its own specialties the major of which being that those are actual shards¹⁰⁴ of *one single* blockchain, it basically resembles projects like Polkadot and TON in that there is a common consensus-layer to rule the whole divided thing. However, being that it is not a blockchain layer for other blockchains to settle on, but rather the actual division of a single blockchain into parts, it presents a set of complex issues that, if solved, will make for significant innovation in blockchain architecture.

For example, **Ethereum needs to solve for universal time synchronization, which has long been deemed impossible in distributed networks; data to be available for access between its sharded parts; switch to a totally different virtual machine**¹⁰⁵ for different developers to finally be able to build DApps on Ethereum in any programming language they want instead of just its own Solidity. The latter has been the reason for multimillion-dollar bugs. All of that needs to be introduced to a system that is already up and running with billions of dollars’ worth of value being attached to it. That is why while being actively worked on by Ethereum team, sharding is still a research frontier, but one successfully, though sequentially conquered.

In terms of allowing for interoperability, Ethereum relies on Plasma and Plasma-inspired solutions to be built as second layers, which, with the introduction of Casper FFG and hopefully later with the actual “full” Casper¹⁰⁶, it will become much more secure, and thus possible. We note that the project has evolved from an actual protocol proposal to something more like a set of recommendations for the wider Ethereum developer community by the core Ethereum team – in order to allow them to experiment and build their own L2 chains with varying functionality on top of Ethereum. Additionally, some of Ethereum’s developers¹⁰⁷ are building two Plasma-style second layer networks: Minimum Viable Plasma (Plasma MVP) and Plasma Cash – both of which are really just *payment-channel network* implementations, drastically differing from each other for the sake of healthy experimentation¹⁰⁸. Both protocols currently run on Ethereum test networks. Eventually Ethereum intends to solve for much more functional blockchain interoperability with second-layer solutions based on Plasma functionality.

None of the aforementioned projects has a particularly identifiable timeline. While we expect Ethereum to switch to Casper FFG by end-2018 – Q1 2019, this timeframe is not guaranteed, given how long it has taken since initially

¹⁰³ For example, if a ban on mining equipment production and operations was suddenly imposed by the government of China, where the majority of Bitcoin’s mining equipment is manufactured and then used to mine bitcoin.

¹⁰⁴ i.e. groups of network accounts, put together based on their leftmost address identifiers – much like in TON.

¹⁰⁵ EWasm, which stands for Ethereum-flavored WebAssembly virtual machine.

¹⁰⁶ A truly decentralised PoS, or Casper Correct by Construction (CBC), on Ethereum is a research project led by Vlad Zamfir, working on the complex mathematics of its game theory.

¹⁰⁷ Led by Karl Floersch.

¹⁰⁸ Plasma Cash is Unspent Transaction Output (UTXO)-based like Bitcoin, while Plasma MVP uses a state machine. See [Glossary](#).

promised (since 2016 has been “a year”, “quarters” and “months” away while repeatedly postponed). But as soon as it does go through, it will trigger a 5x reduction in miner block reward, done in 4 quarters since committed – in effect reducing Ethereum’s current almost 6% yearly inflation rate to less than 1.2% p/a when over. This could reduce Ethereum-backing mining power significantly, which at the same time reflects the reduction in need for it, other than for maintaining network security for the 100 most recent Ethereum blocks.

The network faces some short-term risks, with the potential for an even further correction in prices¹⁰⁹. In a presumable effort to overcome possible short-to-medium term negative effects of switching to Casper FFG for miners (among other things), Vitalik Buterin himself has actively proposed capping the network’s total ETH supply at 120mn (the current number of ethers outstanding is 102.3mn) as well as [changing its transaction fee model](#), which has been a reason cited in [a well-known essay by John Pfeffer](#) for valuing Ethereum down.

Ethereum could introduce a working payment channel infrastructure with Plasma Cash and Plasma MVP sometime in 2019. Late 2019 may also see it implement the first instance of sharding. If so, Ethereum would automatically take the lead among all the projects presented herein, – including TON – given how widely adopted it already is. All of the above factors playing out in Ethereum’s favor could significantly drive up its valuation.

Legal Risks¹¹⁰

Any investor looking at the crypto market is forced to confront a range of legal issues surrounding this entirely new field of investing and trading. With lawmakers and regulators across a range of jurisdictions turning their attention to cryptoassets, the ground can shift from week to week. This means the industry remains a grey area often requiring due diligence outside of investor’s regular comfort zone. A crypto investor has to be a renaissance man in some respects, able to understand various aspects of the industry, while it is nascent and thus unfamiliar to domain-specific experts. And we believe any discussion of the potential attractiveness of Grams as an investment calls for an attempt to highlight potential legal issues around secondary market sales of the coins. Our notes below rely entirely on a [recent article](#) by Alfredo B. D. Silva and Dario de Martino of Morrison & Foerster LLP, who pioneered the public discourse on legal implications of post-ICO trading of tokens in the US. We found their analysis sufficiently compelling to derive high-level conclusions and point our readers’ attention to. We just present our limited understanding of the above-mentioned lawyers’ assumptions – to highlight the possible areas of further research, to be done by law experts. **Please consult a legal professional if it presents any relevance to you, before making your own judgments.**

We focus our brief overview of legal issues possibly arising for TON and its investors *only* in relation to secondary market sales of the Gram cryptocurrency in the US or by the US entities/persons. Since the US Securities and Exchange Commission (SEC) is the only securities market regulator actually “aware” of the TON private offering (through two Form D notices of exempt offering – see Appendix for context¹¹¹) and also since there have been reports of at least two respected US institutional investors participating in the offering¹¹¹, we assume that US securities regulations apply to the placement and possible secondary market of Grams at least for some of its investors (although we do not exclude that other national or international legal regimes could be applicable as well). So, we stick to illuminating some of such US federal regulations possibly applicable to Telegram as an issuer and at least two of its reported investors – top US venture firms – as it could be relevant to the rest of the market as well. Furthermore, to justify our focus, we note that the SEC is one of the most actively referenced government agencies in today’s crypto markets, whose “presence” is well felt beyond the United States, as most of other financial regulators trying to tackle governing the space within their respective jurisdictions seem to follow the SEC’s lead.

The market already understands that any initial coin offering raising funds for the development of a future blockchain platform, that accepts investments or promotes itself in the US, falls under US federal securities laws. Thus offered tokens, whether in the form of Safe Agreements for Future Tokens (SAFTs), which is the case with TON, or actual digital assets, are deemed securities under US jurisdiction. However, verbal comments made by the SEC officials, namely [the commission’s Chairman](#) and [Director of its Corporate Finance Division](#) have introduced additional considerations. They indicated that some digital assets put in circulation *after* the underlying platform is launched and thus having *actual* utility (as opposed to speculation on their *future* utility), could still be considered securities and regulated as such by the SEC. The reason for such a possible treatment of digital assets already put into circulation could be the insufficient degree of decentralization of the underlying platform – pointing to the fact that

¹⁰⁹ At the time of writing, Ethereum has lost most of its price gains since May 2017.

¹¹⁰ We stress that this section is not intended to provide formal legal analysis or opinions on whether or not certain laws and regulations apply to the issuance or trading of TON coins or any other cryptoassets, and urge readers to obtain qualified legal counsel before making any investment decisions.

¹¹¹ [Crypto Utopia report](#) by Autonomous Next mentions venture capital firms Sequoia Capital and Benchmark Capital among the 175 TON investors.

its future (and thus utility and value) still remains in the hands of its initial promoter, thus making it a security under the benchmark [Howey test](#).

Taking into account the above comments by the SEC officials – which are just comments and not actual regulations – Grams could bear the risk of being considered securities under US federal laws even *after* the network is launched... The TON White Paper expressly states that the TON Foundation would initially¹¹² maintain the network's core services and perform blockchain validation duties – single-handedly proposing and effecting changes to the underlying protocol if needed. This could imply that indeed during at least such deployment phase and possibly sometime after (presumably, at least for a few months or more after the network is launched) Grams bare the risk of being considered securities under the US federal regulation.

...and US federal securities laws could also apply to secondary market sales of Grams by their holders (investors and possibly TON Reserve, developers and other staff). A security subject to an *unregistered* initial offering (which applies to TON) falls under general restrictions in relation to secondary sales by its non-affiliated holders (i.e. TON investors) and the issuer or its affiliates (i.e. TON developers, other staff and affiliates). The reason why we believe this is important is the fact that both Telegram (as the TON issuer) and, presumably, at least two of its US institutional investors will be keen to remain compliant with any and all of such restrictions – judging by the way the private placement was held and the status of reported investors. Since TON issued its SAFT agreements to purchasers without *registering* its offering in the US – exercising its right for an exemption¹¹³ – such agreements, and later the underlying Grams, fall under the “restricted securities” category. Generally, each secondary sale of restricted securities needs to be registered by the seller with the SEC. Registering sales with the SEC, as we understand, almost prohibits the secondary market, as each registration is very time- and resource-consuming. However, there are some exceptional circumstances under which restricted securities could be sold without registration, but *only* if certain conditions are met.

Generally, restrictions imposed on investors are related to a full-year holding period if a legal exemption applies. If not, they must register their secondary sales with the SEC, the earlier [referenced article](#) on Bloomberg Law suggests. The broadest of such exemptions¹¹⁴, as we understand it, stipulates that there is a year-long lock-up period on the holding of restricted securities by investors. Generally, since we are convinced that TON is substantially behind schedule for delivering its tokens (which should take place after the network is launched), we believe that the term of such a restriction – approximately until Q2 2019 at the latest (as the second round of sale was reported in March 2018) – could be met by its US investors without additional compliance assessment on their behalf. We note that [media reports have suggested](#) that TON imposed lockup periods on at least first-round investors. So, one way or another, TON's US investors (at least) may want to wait until Q2 2019 to sell their GRMs.

However, there is another possible obstacle. Alfredo Silva and Dario de Martino, the authors of the [cited article](#), stress that above discussed exemption from registration is not available “*for tokens of issuers who may have issued tokens prior to commencement of operations, or operating companies who have structured the tokens to be issued through a subsidiary that itself has no meaningful operations*”. Since at least one of the *two* TON issuers (the Telegram company and its specially created TON Issuer entity, according to the [filings](#)) could possibly fit such a description, we assume there could be a restriction imposed on unregistered resales of Grams. This could mean that TON's US investors would not be able to resell their tokens under the above discussed exemption without registering such a sale with the SEC (which, again, we understand is almost prohibitive to a sale in terms of cost and time).

There is also a separate group of legal exemptions for registration-free resales of Grams. One of them¹¹⁵ allows TON US investors to resell their GRMs to qualified institutional buyers (QIBs), which still limits secondary market opportunities for non-TON-affiliated US Gram holders, if the option is realistic at all, as the [article](#) by Morrison Foerster lawyers suggests. Additionally, TON's US investors could possibly rely on *two other* exemptions for unregistered secondary sales: provided the deals are either effectuated privately or offshore of US, we derive from the article. One of them¹¹⁶ is said to open opportunities similar to the QIB-resale options, just possibly less strict – to a wider circle of institutions and sophisticated private investors – but is less certain to apply to cryptoasset sales given other conditions are met, as it is based on case law (which hasn't yet been widely applied to cryptoasset sales, we assume) and not actual codification, as Silva and De Martino point out. The other exemption¹¹⁷ of the two, in relation to Grams seems to more reliably allow for unregistered resales, but only to persons known to be “non-US persons”, individually identified and *verified via privately negotiated* transactions.

¹¹² During the vaguely defined “*first deployment phase of TON Blockchain*”, according to TON White Paper.

¹¹³ Following the Rule 506 (c) exemption clause of the US Securities Act of 1933.

¹¹⁴ Rule 144 under Section 4(a)(1) of the Securities Act of 1933.

¹¹⁵ Rule 144A under Section 4(a)(1) of the Securities Act of 1933.

¹¹⁶ The so-called “Section 4(a)(1½)” developed by US case law.

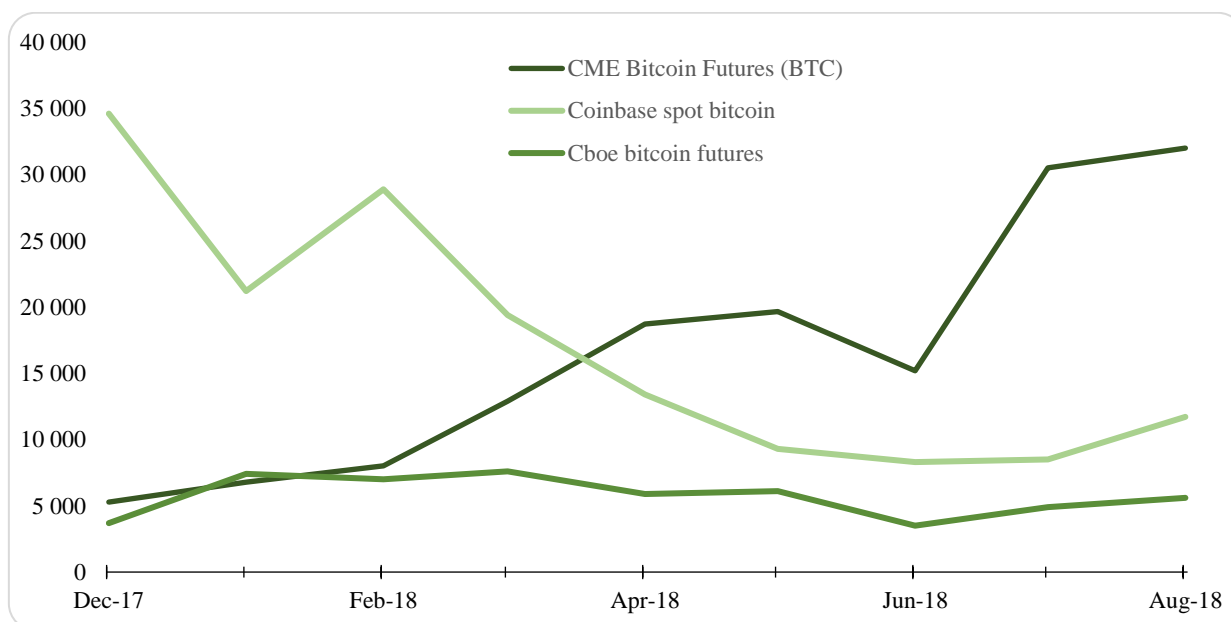
¹¹⁷ Regulation S under the Securities Act of 1933.

We therefore understand the [article](#) on Bloomberg Law to imply that TON's US investors may *reliably* be able to sell their GRMs *only* to identified foreigners if they want to stay fully compliant with the US federal securities laws. With the advent of Telegram Passport this could actually be made possible – identified *and verified* foreign Telegram messenger users could possibly buy Grams not only from TON Reserve, but directly from non-TON-affiliated US investors, thus opening arbitrage opportunities. So, it all boils down to how exactly the Telegram Passport service will be able to verify the status of the buyer in order for reselling US Gram holders to safely rely on it (since we assume it would be institutions possibly reporting to SEC and thus needing to comply with not only the secondary market sales regulations, but also their KYC/AML legal obligations). Not a total ban on secondary market sales of Grams for American TON investors, we assume, but yet a possible serious restriction.

We are not sure whether *insider trading and market manipulation* restrictions, extensively discussed in the [referenced article](#), apply to TON's Foundation (i.e. developers and other staff) and Reserve. However, since TON SAFTs are sold to US investors, SEC could have jurisdiction over TON in this regard. If so, then it triggers a whole host of other restrictions imposed on the so-called affiliates of an issuer. In an extreme case, this could mean that sales and other forms of distribution of Grams directly effectuated by TON Reserve or TON developers (of the 200mn GRMs allocated to them after the private sale with a subsequent four-year vesting period, according to the offering Primer) could be hampered. However, we do not possess any legal expertise in order to stipulate whether such risks should even be discussed here.

Additionally, even if restrictions don't apply, any resale of TON to public (for the time it bears a risk of being deemed a security) in the US would require a registered securities trading market. To our knowledge no US virtual currency (spot) exchange has been registered as the so-called [National Securities Exchange](#) or [Alternative Trading System](#) – two types of securities trading facilities allowed in the US, as we understand. Coinbase, the company behind the biggest US spot market for cryptocurrencies, Coinbase Pro, has recently [announced](#) acquisitions of a registered broker-dealer, an alternative trading system and a registered investment advisor in a presumable attempt to become the first cryptocurrency exchange to become fully compliant with the securities market regulations. But it still has some [ground to cover](#), as reported. Other big US virtual currency exchanges are under regulatory scrutiny¹¹⁸, while still enjoying some freedom in a relative grey-area outside of Know-Your-Customer, Anti-Money Laundering and Tax reporting obligations they seem to comply with for the most part. However, even if granted a proper license to trade securities (i.e. cryptoassets deemed securities under the US federal laws), Coinbase Pro or other US cryptoasset exchanges currently still present a pretty narrow market in terms of liquidity.

Biggest US bitcoin spot market volumes vs bitcoin derivative markets



Source: Financial Times, Bloomberg, [Coinalyze.net](#)

¹¹⁸ Just recently The Office of the New York State Attorney General, a regulator with possible jurisdiction (where the United States' SEC or Commodities and Futures Trading Commission, CFTC, might lack such jurisdiction) over crypto exchanges that offer their services to New York state residents, has published a critical [review](#) of practices implied by such exchanges, including in legal compliance, general transparency and fairness of procedures related to listings of new coins.

How much a Gram weighs

Valuation is vague and arbitrary, when there is no assurance that it will be generally acquiesced in by others.

Jean-Baptiste Say

Cryptocurrency valuation is the key conundrum for traditional investors who have only recently begun paying attention to the new asset class. But even pure crypto players recently entering the market need to start appreciating the problem, now that the astonishing returns delivered by a shotgun approach are no longer a given in the maturing market. Despite attempts by a few research enthusiasts, a mainstream valuation method still needs to be developed. To value TON, we use our in-house model, which represents a modification of the models offered by crypto researchers¹¹⁹. The model offers a Rational Value (we do not dare to call it Fair Value yet) of \$5.90 per Gram for end-2019, which implies 4.4x upside for investors that participated in the second financing round.

Valuation methods lag, as usual

Equity markets had existed for four centuries and the New York Stock Exchange operated for 130 years before Discounted Cash Flow (DCF) methodology became the mainstream in equity valuation, spurred by the market crash of 1929. Irving Fisher in 1930 and John Burr Williams in 1938 first formally expressed the DCF method in modern economic terms. So it is unsurprising that after less than 10 years no one really knows how to value cryptoassets yet.

So far, crypto research has proposed original relative valuation metrics. It has introduced two new multiples applicable to blockchains: Network Value to Transactions (NVT) and Network Value to Metcalfe (NVM) ratios. Although these ratios could be used for valuation in the future, reality as of now does not allow for their use in deriving cryptocurrencies' fair values.

Cryptocurrencies do not intend to deliver cash to their holders and cannot be valued as equities¹²⁰. The absence of financial metrics – cash flow in particular – is the main issue in cryptoasset valuation. While various approaches exist to appraise non-cash generating businesses, all of them implicitly assume that those businesses will eventually deliver positive cash flow. This is not the case for cryptoassets. Not only does cash flow to token holders not exist at the initial stages of the projects, it is never meant to appear¹²¹. Coins issued to miners or validators for the work they perform for the blockchain is remuneration, and as such, meaningless for valuation. In other words, the classical DCF approach does not apply to cryptocurrencies.

The name itself suggests the right approach: cryptocurrencies should be valued as currencies. Money serves three main purposes: a store of value, medium of exchange, and unit of account. For instance, cash serves as both a store of value and a medium of exchange, while gold is nowadays only a store of value. Having assumed that cryptocurrencies perform one or all of these functions, crypto researchers devised their absolute valuation methodologies: Store of Value and Equation of Exchange. Both approaches have their limitations and require further development before they deliver cryptoassets' fair values. However, we believe they point in the correct direction and raise the right questions.

The emerging field of multiples

Ratio-based valuation generally offers a good proxy for fair value, although it lacks the details offered by DCF analysis. Since traditional multiples do not apply to cryptoassets due to the absence of financials such as revenue, profit, or book value, new ratios need to be developed. Cryptoasset researchers Chris Burniske, Willy Woo, and Dmitry Kalichkin, and Clearblocks' and Coin Metrics' respective teams introduced their original cryptocurrency ratios and approaches to ratio analysis. At the same time, they reasonably did not use multiples to obtain fair values of coins but studied them to find technical over- or undersold states.

¹¹⁹ Namely those of [Brett Winton](#) and [Chris Burniske](#).

¹²⁰ While there are a few cryptoassets trading on the market that have equity-like features, the absolute majority serve as currencies or "internal" currencies for whatever the underlying network/distributed application provides.

¹²¹ Again, we are generalizing for simplicity's sake: there are some cryptos designed specifically for capturing value for the projects' backers, but they represent a negligible fraction of the overall market at this point.

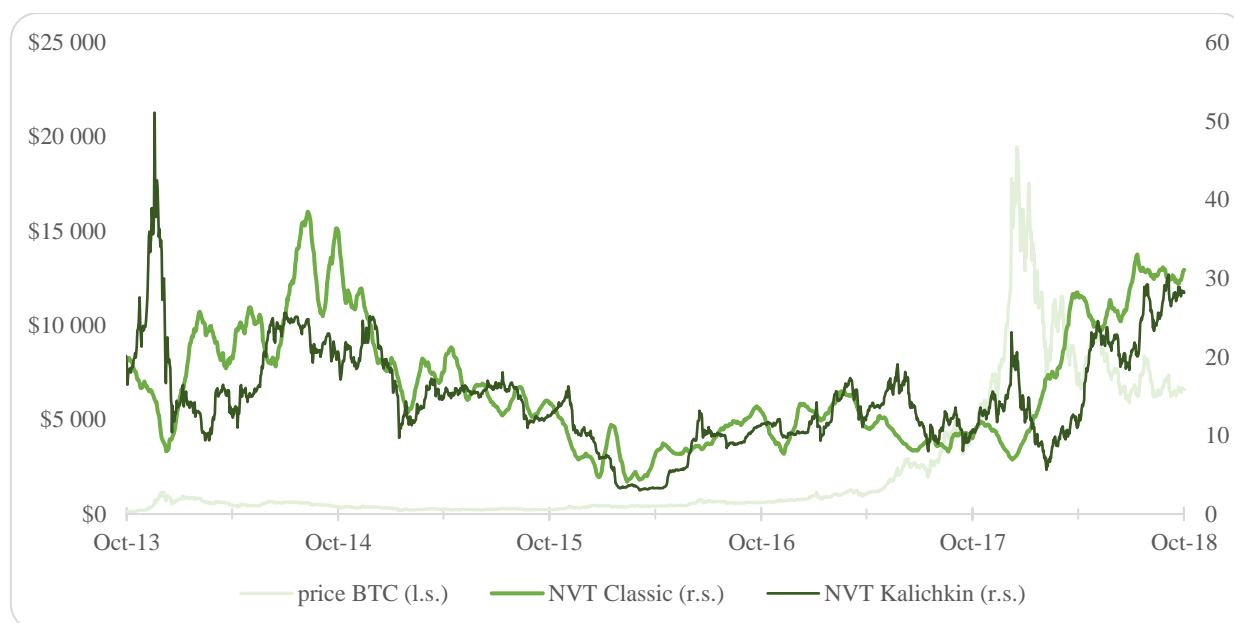
NVT ratio

Researchers popularized the Network Value to Transactions (NVT) ratio, which is now one of the most widely known approaches to looking at the new asset class. Willy Woo came up with the ratio and used it solely for the Bitcoin network, as it has the most historic data¹²². However, the use of the ratio could be extended to other cryptoassets as long as they have enough history of multiple “bullish” and “bearish” seasons. The argument is that transactions are the metric of economic activity of essentially any blockchain. Thus, a blockchain can be valued as a multiple of all on-chain transaction volume, much like an entity established for earnings is valued as a multiple of those earnings. In other words, NVT for a network is the analog of P/E for a company. A network’s value is how much users can derive from the chain, and transaction volume is a good proxy for this value.

$$\text{NVT} = \text{Network Market Cap} / \text{Daily Transaction Volume}$$

The ratio can be fine-tuned to smooth the effect of volatility in daily transaction volumes. Dmitry Kalichkin of Cryptolab Capital has suggested using a 90-day moving average (90MA) for the daily transaction volume as the denominator. Given that the author uses NVT to predict price movements and to detect bubbles, this new smoothed ratio makes sense as it serves this goal better. Moreover, the smoothed ratio should be more suitable for cryptoasset valuation, since NVT with a 90-day moving average in denominator is closer to a P/E multiple, which uses annual income as its denominator.

NVT Ratio (Classic & Kalichkin) vs. BTC price



Source: [Coin Metrics](#)

NVT considers only on-chain transactions, disregarding all off-chain activities such as trading on exchanges, and potentially leaving aside most speculative activity as a result. Thus, the multiple should capture fundamentals and give a network intrinsic value. However, we cannot value cryptoassets using NVT ratios yet, because we do not know this multiple’s fair value and we cannot claim that existing on-chain transactions are not speculative. In fact, we can and will claim the opposite. We cannot say that current values for NVT multiples represent their intrinsic values, as speculative components are likely to be large (if not dominant). We need other methodologies to value networks first, and then we can derive fair values for NVT ratios. Or we need much more data and a more mature market to empirically obtain fair values for NVT ratios.

Nevertheless, we can use NVT ratios to compare different blockchains’ valuations. Let us take Ethereum (ETH) and its 2016 hard fork Ethereum Classic (ETC) as an example. Since both blockchains are fundamentally identical, it is logical to assume that their NVT ratios should be similar. And they are: ETH’s 90-day moving average Kalichkin NVT of 35x is close to ETC’s NVT of 36x. The picture is different for Bitcoin (BTC) and its fork Bitcoin Cash (BCH). The former has an NVT of 27x, while struggling BCH had an NVT of 45x as of 11 October 2018. As such, we can say that BCH is roughly twice as expensive as BTC. We also applied 90-day moving average to classic NVT, which means using it for the whole network value to transactions ratio, rather than just the denominator (as in Kalichkin NVT).

¹²² Woo, an independent cryptoasset analyst, estimated top and bottom levels to come up with a “real value” corridor for the NVT, based on seven years of bitcoin trading data, beginning in July 2010 with the launch of the first crypto exchange Mt. Gox.

Main cryptocurrencies' NVT ratios under different calculation methods (as of 11 October 2018)

	NVT	90MA NVT	Kalichkin NVT	90MA Kalichkin NVT
BTC	22	31	28	27
BCH	31	78	54	45
LTC	30	61	51	37
ETH	30	31	41	35
ETC	25	73	37	36
DASH	85	77	42	27

Source: [Coin Metrics](#)

We introduce the concept of the **Network Value to Future Transactions (NVFT) ratio**, which is a better approach to cryptocurrency valuations, we believe. The NVT valuation method would only be used to estimate current intrinsic values of active blockchains, much like P/E ratio can only be used to value profitable entities. Traditional finance places more value on price to future earnings ratios than on price to historical earnings. By the same token, it makes sense to use NVFT to value cryptoassets, as this ratio should be applicable to both existing and emerging networks. However, with NVFT even more unknowns appear. The cryptocurrency market has to be mature enough for the analysts that cover blockchains to estimate their future transaction volumes and to arrive at a consensus forecast. So, we will leave it as a concept for now.

Network to Metcalfe ratio

Metcalfe's Law states that a telecom network's value is proportional to the square of the number of connected users, n^2 . The underlying rationale is that the value of a network with n users grows with the number of its unique connections, which equals $n * (n + 1) / 2 \sim n^2$. In the context of social networks, Andrew Odlyzko as well as Robert Metcalfe himself argued that this formula estimates the number of *potential* connections, while the value of the social network should be proportional to the number of *active* connections. They suggested using $n * \ln(n)$ instead of n^2 for large n . There are other modifications of the law, playing with different degrees of n , such as the so-called Generalized Metcalfe's Law using $n^{1.5}$. Researchers from the Chinese Academy of Science have validated the law with actual data using Facebook and Tencent as samples¹²³.

Blockchains that have reached critical mass behave like social networks, we believe. As such, their values depend on their usage, which should be reflected in transaction volume. Given that a user can and usually does have more than one account, the number of daily active accounts (DAA) seems to be a better metric to measure the usage of a blockchain than a total number of users. Classic Network Value to Metcalfe multiple is then a ratio of a blockchain's market cap to DAA squared. Analysts have also [experimented with different modifications of Metcalfe's Law](#) using various functions of DAA as a denominator.

$$\text{NVM} = \text{Network Market Cap} / \text{Function of Daily Active Accounts}$$

We calculated the correlation between the market caps (MC) of the most developed and most liquid cryptoassets, BTC and ETH, and six blockchain metrics:

1. Daily on-chain transaction volume in USD (TV\$), which gives us NVT ratio.
2. Number of daily transactions (TX).
3. Number of daily active accounts (DAA), a Metcalfe's Law modification.
4. Squared number of daily active accounts, (DAA^2), which is Classic Metcalfe's Law.
5. $\text{DAA} * \ln(\text{DAA})$, or Odlyzko's modification of Metcalfe's Law.
6. $\text{DAA}^2 * \text{Average daily transaction size (AT\$)}$. [Inspired by Tom Lee of Fundstrat](#).

To smooth the volatility of each of the variables above, we also used their 30- and 90-day moving averages. We also calculated correlation between DAA and TX. We used the data from 28 April 2013 to 3 October 2018.

¹²³ ["Tencent and Facebook Data Validate Metcalfe's Law"](#) by Xing-Zhou Zhang, Jing-Jie Liu, Zhing-Wei Xu, J. Comput. Sci. Technol (2015).

BTC (as of 3 October 2018)

Bitcoin	without MA	30D MA	90D MA
MC - TV (\$)	81.9%	86.6%	89.0%
MC - TX	49.9%	50.7%	49.7%
MC - DAA	70.1%	71.5%	71.4%
MC - DAA ²	76.7%	79.5%	79.5%
MC - DAA * LN(DAA)	70.8%	72.3%	72.2%
MC - DAA² * AT (\$)	79.4%	84.0%	86.7%
TX - DAA	94.2%	95.4%	95.6%

Source: [Coin Metrics](#), HASH CIB¹²⁴

Around 90% of bitcoin's market cap is explained by both the blockchain transaction volume in USD and a modification of Metcalfe's Law. Although the number for BTC seems incredibly high, it is still lower than the practically perfect correlations between ETH's market cap and some of its network metrics. 98+% of Ethereum blockchain value can be explained by 90-moving averages of either of the following: daily transaction volume, daily active accounts, the product of daily active accounts and their natural log. Such strong correlation can be very effective for quantitative trading, but it is of little use for valuation purposes.

ETH (as of 3 October 2018)

Ethereum	without MA	30 MA	90 MA
MC - TV (\$)	68.2%	73.2%	75.2%
MC - TX	94.8%	96.4%	98.3%
MC - DAA	94.5%	96.5%	98.4%
MC - DAA ²	87.6%	92.4%	96.3%
MC - DAA * LN(DAA)	94.4%	96.5%	98.5%
MC - DAA ² * AT (\$)	68.2%	73.9%	77.3%
TX - DAA	99.3%	99.7%	99.9%

Source: [Coin Metrics](#), HASH CIB¹²⁴

No magic, mostly speculation. We can offer two hypotheses to explain the abovementioned 90%-100% correlations. First, the markets for both BTC and ETH are semi-strong efficient, and their prices instantly reflect all publicly available information. In this case, both coins are almost always fairly valued, and their prices simply fluctuate around their intrinsic values. Second, the market caps of both cryptocurrencies are simply a function (likely linear) of money inflow into the respective asset. In this case, the price does not depend on fundamentals and speculatively moves as new funds come aboard. We see the latter theory as much more realistic.

The high correlation between bitcoin's popularity and its price serves as an indirect proof of our thesis that recent price movements are primarily speculative. We calculated correlations between the seven-day averages of the daily search requests for the word "Bitcoin" on Google and the cryptocurrency's market cap. The data available since August 2013 shows that 83% of the cryptocurrency's price can be explained by its popularity. The correlation between searches and prices two to three weeks later grows to 87%, suggesting that an increase/decrease in popularity preceded the corresponding changes in market caps. Moreover, before the peak in December 2017, the correlation was 95%.

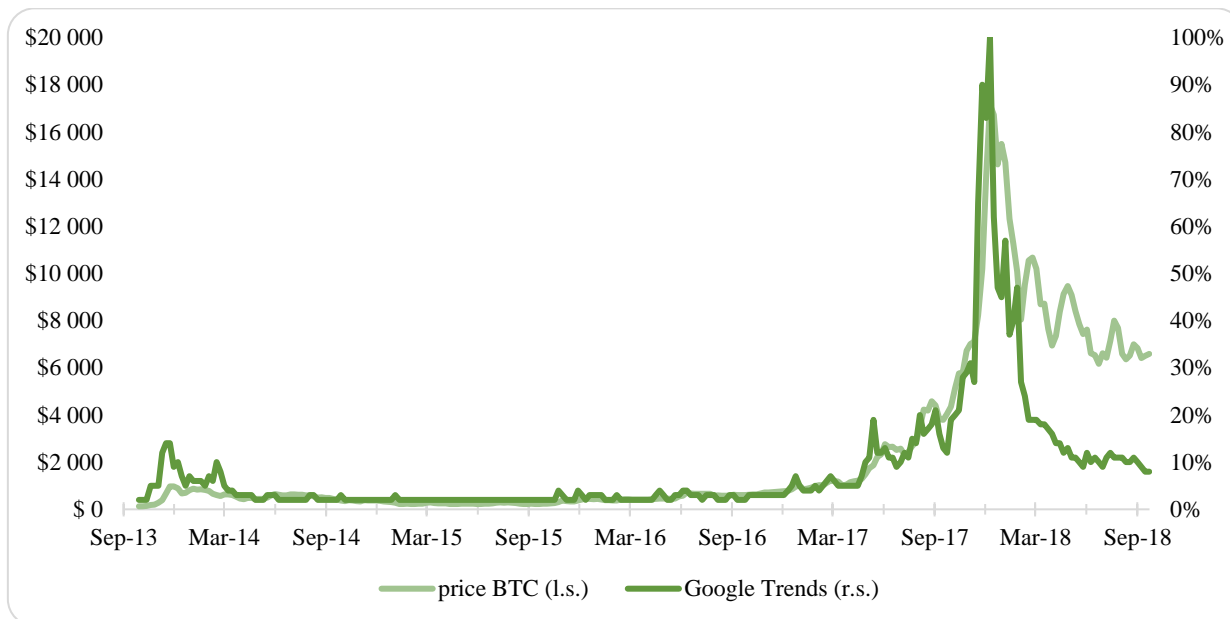
Correlations (as of 3 October 2018)

Aug 13 - Sep 18	Aug 13 - Dec 17	Dec 17 - Sep 18	Shift (weeks)
83%	95%	89%	0
86%	96%	85%	1
87%	95%	83%	2
87%	93%	88%	3
85%	89%	86%	4
83%	88%	82%	5
81%	86%	76%	6

Source: [Google Trends](#), HASH CIB¹²⁴

¹²⁴ The reader should use caution when considering these correlations. Such valuations may vary from valuations performed by other parties for similar types of investments.

**Both BTC's price and the number of search requests peaked in the second week of December 2017
(as of 3 October 2018)**



Source: [Coin Metrics](#), [Google Trends](#)

We are unlikely to determine the fair values of blockchains using ratios until investors decouple from users. Facebook or AMEX's shareholders are very distant from their users. The process of trading their stocks has nothing to do with AMEX transactions or activities on Facebook. The networks' users, not their investors, create their value. However, investors in and users of contemporary blockchains largely overlap, using their accounts to mainly buy and keep coins rather than to purchase goods or services. In other words, the on-chain transaction volume tends to equal inflow from investment funds. Hence, the near-perfect correlation is the consequence of the fact that the speculative money from blockchain investor-users is the main variable defining a coin's market cap.

We abstain from using ratios to value Grams. Unless a blockchain is used for its intended purpose(s) rather than investment in the coins, we cannot separate intrinsic transaction volume and active accounts from speculative ones. As such, we are unable to estimate fair values of those ratios. However, we do believe that suggested multiples will be helpful in roughly estimating cryptoassets' fair prices at some point in the future.

Store of value

The monetary store-of-value approach, although straightforward, is very sensitive to assumptions. It argues that cryptocurrencies will, to some extent, substitute traditional assets in storing monetary values. The key here is to correctly estimate this extent, and as such, the total value of all assets to be replaced by their digital counterparts. If this is done, the next step is just to divide the obtained results by the number of coins outstanding to arrive to the fair value of each coin.



Gram is unlikely to be the cryptocurrency to replace contemporary monetary store-of-value, nor does it intend to be. Therefore, the store-of-value approach is not applicable to TON and beyond the scope of this report. However, this method is used to value bitcoin, and as such, we believe it deserves to be presented at least as a rough example. We base this example on [John Pfeffer's paper](#).

Let us assume that bitcoin will substitute only for non-fiat store of value assets. Unlike fiat money, bitcoin is an asset with no interest payments, and therefore there should be less incentive to switch from fiat to bitcoin to store value. Gold dominates non-fiat monetary storage mainly due to millennia of tradition; it has no real advantages over other precious metals or durable assets. Because of bitcoin's superior characteristics compared to gold (e.g. ease of storage and transportation, as just one example) and its additional utility for payments, we can assume that it should at least partially displace gold as a store of value.

The value of all aboveground gold in the world was around \$7.4 trillion in September 2018. Around \$2.8tr (38%) of this in the form of bullion holdings, and the rest is fabricated products such as jewelry. We think that bullion is the only likely candidate for replacement by bitcoin, although some jewelry is kept as investments. Bullion holdings are roughly divided into \$1.1tr held in the national reserves of the 28 largest economies and \$1.7tr held privately. Assuming that in ten years, all private and a quarter of national holdings will be replaced by bitcoin, we arrive at \$2tr value for the cryptocurrency in 10 years. Discounting this number backward at a 40% annual rate and dividing the outcome by 21mn (the maximum number of bitcoins) we arrive at a fair price of \$3,250 for bitcoin.

Different assumptions will drastically change the fair value output. One can easily double or triple the target price by assuming that bitcoin will replace not only some gold but also some fiat currencies as a store of value. However, we leave this exercise for our future valuations of other cryptoassets.

The equation of exchange

The equation of exchange addresses the relationship between money and price level, and between money and nominal GDP. The equation states that $M * V = P * Q$, where M is the monetary supply, V is the velocity of money, P is the average price level of goods, and Q is real output (i.e. quantity of goods produced by the economy). The product on the right side of the equation (PQ) is the nominal GDP of the economy. Velocity is the number of times the average currency unit is spent in a given year to buy final goods and services.

A cryptoasset serves as the currency within its native blockchain, fulfilling all three money functions – a store of value, means of exchange, and unit of account. Therefore, we can apply the equation of exchange to value cryptocurrencies. In this case, M is the size of the asset base, V is the velocity of the asset, P is the price of the digital resource being provisioned, and Q is the quantity of the digital resource being provisioned, as described by [Chris Burniske](#). The product PQ is the blockchain transaction volume or its nominal GDP. The price of a cryptocurrency is a division of M by the number of coins available, where $M = PQ/V$. The equation should work well to value mature blockchains.

Ambiguity arises when a network under consideration is in the embryonic or even at an alpha stage of its development. In this case, we need to somehow derive blockchain's present value from its future value(s), which, in turn, are obtained by means of the equation of exchange. Specifically, we need a DCF-like model. Burniske and [Brett Winton](#) separately proposed a model that derives each year's blockchain current utility value (CUV) and then discounts the CUV in arbitrarily chosen distant year to the present time to determine a rational market cap. CUV at any given year t is forecast by the equation of exchange: $CUV_t = P_t Q_t / V$. Although we are in favor of the idea of discounting CUV, we have some issues with this model.

The Burniske model in reality considers only one future period and assumes a constant velocity, and the single future period bothers us the most. The model forecasts the CUVs for all the years up to the one when the network matures, i.e. reaches its assumed market share. Then the model discounts the CUV only for an arbitrarily chosen distant year effectively disregarding all intermediary and subsequent CUVs and making irrelevant all the complicated calculations used to derive them. We are not unique in our criticism. Burniske himself acknowledged that the model needs to be improved upon, and [Alex Evans of Placeholder introduced his own way](#) to account for dynamic velocity. Yet, again, the latter model considers only one period in the future, ignoring the interim and subsequent periods. We offer our in-house version of the model that, we believe, deals with this issue.

The rational utility value of a network is not just the discounted future CUV¹²⁵ of a particular year, nor is it the sum of discounted CUVs of all projected years¹²⁶, we believe. We think that blockchain's rational utility value is better modelled as **today's utility value plus discounted additional current utility values (ACUV)** for every year to infinity. $ACUV_t$ in a year t equals the difference between CUV_t in the year t and CUV_{t-1} in the year $t-1$.

$$ACUV_t = CUV_t - CUV_{t-1}$$

To account for infinity, we calculate the terminal value (TV) of ACUV at the period of network maturity. In this case, the model captures all the years. The approach is similar to the one used to value banks, for which traditional DCF is not applicable. A financial institution is valued as a sum of its current shareholders' equity and the present value of future excess returns on equity (returns in excess of those required by the cost of equity).

The commonalities and differences of our approach are easier to explain with a simple example. Consider a network that matures in five years and subsequently grows with the annual rate g indefinitely. CUV_t is network's utility value for the end of year t . The additional utility value $ACUV_t$ for the period t is equal to $CUV_t - CUV_{t-1}$. TV for the end of the year five equals $ACUV_6 / (r-g)$. This is a classic formula for terminal value, where r is the discount rate. We can simplify the formula for TV. Given that $ACUV_6 = CUV_6 - CUV_5$ and $CUV_6 = CUV_5 * (1+g)$, we arrive at $ACUV_6 = CUV_5 * g$, and $TV = CUV_5 * g / (r-g)$.

¹²⁵ As in Burniske and Winton.

¹²⁶ "0x (ZRX) Analysis and Valuation" by Miles Snider, Multicoin Capital (2017).

	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5	Terminal Value
CUV	CUV ₀	CUV ₁	CUV ₂	CUV ₃	CUV ₄	CUV ₅	
ACUV		CUV ₁ minus CUV ₀	CUV ₂ minus CUV ₁	CUV ₃ minus CUV ₂	CUV ₄ minus CUV ₃	CUV ₅ minus CUV ₄	CUV ₅ *g / (r-g)
Discount rate	1	1+r	(1+r) ²	(1+r) ³	(1+r) ⁴	(1+r) ⁵	(1+r) ⁵

Source: HASH CIB¹²⁷

We hesitate to call the number generated by this approach a “target” or “fair” price, given that the model only applies to coins with utility value and to developing blockchains. We would instead call it a **Rational Network Value (RNV)**. In the example above, the RNV would be as follows:

$RNV = CUV_5 / (1+r)^5$. Burniske model

$RNV = \sum CUV_t / (1+r)^t$, where $t = 0 \dots 5$. Multicoin Capital model

$RNV = CUV_0 + \sum ACUV_t / (1+r)^t + CUV_5 * g / (r-g) / (1+r)^5$, where $t = 1 \dots 5$. HASH CIB model

The Burniske model also assumes a constant cryptoasset velocity over time, which is unlikely. A cryptoasset’s velocity – another complex, disputed topic – will most probably increase with growing transaction volume and a blockchain’s approaching maturity. Pfeffer reasonably argues that a utility blockchain at equilibrium will have a very high velocity and its PQ will equal the cost of computational resources needed to run the network. Even if a fraction of utility tokens are permanently held, for staking in PoS consensus for instance, the rest should change hands often, which would drive up overall velocity.

We use a dynamic and increasing velocity to value cryptoassets in our in-house model. The rationale is simple. Only investors, not end-users, buy tokens during an ICO, and only investors hold tokens while the blockchain is under construction. Even if they trade, the average holding period is months rather than days, we believe. Thus, velocity is relatively low during the initial stages of the project. If the project is successful and the network is up and running, end-users come aboard, and the tokens are used for their main purposes. As a result, end-users gradually substitute investors as token holders, and velocity grows. In our model we assume that a cryptoasset’s velocity increases concurrently with blockchain adoption according to a logistic S-shaped curve.

We see a few advantages in our version of the Burniske model. First, it captures all the years including infinity, thus avoiding underestimation. Second, it summarizes only additional utility values, not the whole utility values for every year, thus avoiding overestimation. Third, it uses dynamically rising velocity, which is a more reasonable assumption, in our view. The obvious drawback is that the model is not universal: it would not apply to mature networks where fair values are simply today’s utility values derived from the equation of exchange.

NVT ratio is a function of velocity; they have inverse relationship. The right side of the monetary equation of exchange ($MV=PQ$), PQ , is simply an annual transaction volume for a blockchain. If we assume that daily transaction volume is just 1/365 of an annual volume, we obtain that $M/PQ = NVT/365$. At the same time $M/PQ = 1/V$. Therefore, $NVT = 365/V$. As a blockchain matures, its velocity should rise and its NVT ratio should fall. Therefore, when using this ratio to compare different networks, we have to take into account their maturities. If we use an annual transaction volume, then:

$$NVT = 1/V$$

Equipped with the NVT / Velocity equation, we can make much more reasonable judgments on NVT ratios and cryptoasset values. Although without velocity values we still do not know the fair values for the ratios, making assumptions on tangible velocity is easier than speculating on abstract NVT ratio values. Utility tokens should have high velocity and as such their NVT should be low. If a token changes hands every day, its velocity equals 365 and NVT equals one.

¹²⁷ Based on our own valuation model, described herein. This approach may not reflect actual results and is not a guarantee of future results.

Gram placement sets up the minimal price for the next issuance

Telegram has already sold more than a half of its intended total supply of five billion Grams, we calculate. The company raised \$1.7bn in two rounds attracting \$850mn in each. To place the tokens Telegram used a formula:

$$1) \quad P_n = P_0 * e^{(10^{-9} * n)}$$

where P_0 is the price for the first token and is equal to \$0.10. Therefore, the amount received by selling the first n Grams can be calculated by the formula:

$$2) \quad S_n = P_0 + P_0 * (e^{(10^{-9} * n)} - 1) * 10^9$$

Thus, the number of tokens sold in the first round can be derived from the formula:

$$3) \quad n = 10^9 * \ln(1 + S_n * 10^{-9} / P_0)$$

Given the \$850mn attracted in the first round, we arrive at $n_1 = 2,251,291,799$ Grams sold during this round at the price of \$0.377561 per token (\$850mn/2,251,799). The price for the first token in the second round, P_{n1} was exactly \$0.95 (calculated by formula (1)). Substituting P_0 with P_{n1} in formula (3) and taking into account that the second round raised another \$850mn, we calculate the number of tokens sold during the second step as $n_2 = 639,079,959$ and the price per Gram as \$1.330037 (\$850mn/639,079,959). The total number of Grams distributed via both placements was therefore $n_1 + n_2 = 2,890,371,758$.

700mn Grams will be allocated to TON developers and the TON Foundation. The former will receive 200mn Grams¹²⁸ and the latter 500mn¹²⁹. The total amount in circulation will be 3,590,371,758 after the allocation. TON Reserve, i.e. treasury, planned to sell only up to half of the total supply according to the price formula (1). It reserves the right not to sell any of the remaining Grams at all, or to sell them at a higher price than calculated by the formula, but never at a lower price. Given that it has already passed this threshold, the Reserve has the obligation to sell the next Grams at the price above the price of the 3,590,371,758th token, which should be \$3.62, per formula (1). At that price, TON's market cap should be \$13bn (\$3.62*3,590,371,758).

Second-round investors are guaranteed at least a 36% return, according to the White Paper. After the allocations to the TON Foundation and the founders, the minimum price for Gram should be effectively set at \$1.81. The issuer committed that TON Reserve will buy back the coins if their price drops below 50% of that calculated by formula (1). Given the above-calculated number of Grams in circulation, the buyback should start at \$3.62/2 = \$1.81, or 36% above the second-round price of \$1.33.

The amount raised by Telegram could negatively impact Gram's adoption in the short term, in our view. To satisfy enormous demand, the issuer sold 58% of total coin supply and, consequently, has already set the price for Grams at a relatively high level. All Grams in circulation are currently in the hands of just 175 investors in the form of agreements for future tokens. These investors bought in hoping for a cryptocurrency-like return of hundreds of percent. Many of those investors are likely to hold their positions awaiting such returns to materialize. To drive mass adoption of the blockchain, TON needs to place new tokens through the TON Reserve to make a substantial number of Grams available to the network's potential end-users.

Rational Network Value gives 63% upside on conservative assumptions

We derive TON's Rational Value using our in-house modification of the Burniske model. We divide network development into three stages: current condition, the future, and terminal growth. Given the October 2019 target for the project's launch, we consider the first stage to be the year 2019. The second period covers 2020-2028 and the last runs from 2028 to infinity.

First, we forecast TON's PQ for every period to calculate each year's current utility values (CUVs) using the equation of exchange. Then we calculate the ACUVs (additional CUV) for each year as well as the terminal value of ACUV, and divide the results by the average number of Grams outstanding during each of those periods and by corresponding velocity. Finally, we discount the outcomes to the present time and sum them up to arrive at the Rational Value of a Gram. We assume a 5% terminal growth rate and a 40% discount rate – a rate large enough to account for the risk associated with the project. We also presume Gram's adoption rate and velocity with S-shaped concurrent

¹²⁸ With a 4-year vesting period, according to the Primer.

¹²⁹ Presumably, the TON Foundation will use the funds to encourage third-party node owners to provide services to TON during the initial phase of project development. The Foundation will also have its nodes perform validator duties during the deployment phase of the Blockchain, using *other Gram funds* (outside of the discussed 500 million), specifically transferred from the TON Reserve for such purpose.

growth from zero in 2018 to 90% and 365 respectively in 2028. We believe the latter assumption is rather conservative as it means that Grams will change hands just once a day at maturity.

To predict TON's total PQ, we forecast and summarize the PQs for each of Gram's use cases:

1. **TON Payments:** Instant (micro) payments for any and all digital or physical assets or services sold within the TON ecosystem, which includes TON users, services and apps built exclusively on TON, and other applications and services/merchants integrated with TON
2. **TON Storage:** Payments for storing data securely in a distributed way
3. **TON DNS:** Payments for blockchain-based registration and management of addresses both on-chain (on-chain apps and services, user addresses) and off-chain – TON apps, services and TON sites
4. **TON Proxy:** Payments for obfuscating identity for bypassing censorship imposed by local ISPs or for security precautions
5. **TON Applications and Services:** Payments for services (other than the ones listed above) provided by apps and in-app purchases as well as for infrastructure services for apps and end-users

TON Payments should create the largest demand for Grams – the main cryptocurrency used within the Telegram ecosystem. The annual transaction volume or PQ of TON Payments is just the monetary volume of payments conducted through the blockchain, which should effectively become a marketplace for goods and services, both online and offline. To forecast payment volume, we assume that a) Telegram reaches one billion monthly active users (MAU) by end-2021¹³⁰ and 2.3bn by end-2028, b) payments adoption among users grows from 0% to 90% by 2028 according to S-shape, c) average annual account spending starts at \$2,300 in 2019 and increases to \$7,000 by 2028. We used PayPal as a P2P proxy for online spending and growth assumptions, given its similar base of 244mn active users and average annual account spending of around \$2,200, according to [Statista](#), with growth of more than 14% p.a.

Year	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Monthly Active Accounts (MAU), bn	0.30	0.45	0.68	0.99	1.20	1.39	1.57	1.75	1.93	2.11	2.29
Growth		50%	50%	47%	21%	16%	13%	11%	10%	9%	9%
Adoption Rate			0%	0%	1%	7%	34%	64%	80%	87%	89%
Average Transaction p.a., in \$'000	2.00	2.30	2.65	3.04	3.50	4.02	4.59	5.18	5.80	6.44	7.09
Growth		15%	15%	15%	15%	15%	14%	13%	12%	11%	10%
Total Transaction Volume, \$tr			0.00	0.00	0.04	0.36	2.43	5.80	8.98	11.80	14.44
Growth				1196%	963%	860%	567%	139%	55%	31%	22%

Source: TON Primer, HASH CIB¹³¹

TON Storage consists of two lines of service (presumably offered by the same set of Storage nodes): storing the whole blockchain and storing third-party data. The former will have a few orders less volume (possibly, tera- vs. exabytes) and therefore can be ignored for valuation purposes. The global cloud storage market was \$30bn in 2017 and is forecast to reach \$101bn by 2023, according to [Mordor Intelligence](#). Assuming a 20% CAGR for 2023-2028, 5% terminal growth and TON's market share expanding S-shape from nothing to 10% by 2028, we predict the blockchain's PQ in this particular business line. The storage service adds \$0.01 to GRM's value.

Year	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Cloud Storage Market, \$bn	37	45	55	68	83	102	122	146	176	211	253
Growth		22%	22%	22%	22%	22%	20%	20%	20%	20%	20%
TON Market Share	0%	0%	0%	0%	1%	5%	8%	9%	10%	10%	10%
TON Storage Transaction Volume, \$bn	0.0	0.0	0.0	0.1	1.0	5.1	9.4	13.4	17.1	20.9	25.2

Source: Mordor Intelligence, HASH CIB¹³¹

¹³⁰ Telegram's goal, according to the Primer.

¹³¹ This table contains forward looking statements and actual results may differ, because such a statement is derived from mathematical modeling techniques of the economic or financial markets that may or may not reflect actual conditions or events.

The global DNS market is forecast to reach \$2bn by 2027, according to [Market Research Future](#). Assuming terminal growth of 5% for the market and TON DNS' share increasing from 0% to 10% by 2028, we arrive at network's DNS transaction volume of \$225mn in 2028. This number is insignificant for the value of GRM.

Year	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Global DNS Market, \$bn	0.7	0.8	0.9	1.0	1.2	1.3	1.4	1.6	1.8	2.0	2.3
Growth		12%	12%	12%	12%	12%	12%	12%	12%	12%	12%
TON Market Share	0%	0%	0%	0%	1%	5%	8%	9%	10%	10%	10%
TON DNS Transaction Volume, \$mn	0.0	0.0	0.2	1.7	13.3	64.6	111.0	148.1	175.8	200.3	225.2

Source: Market Research Future, HASH CIB¹³¹

The global VPN market should hit \$36bn by 2022, according to [Statista](#). Using the same assumptions for terminal growth and market share as with the DNS market, we obtain proxy service transaction volume of \$8bn in 2028. This use case adds \$0.005 to GRM's valuation.

Year	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Global VPN Market, \$bn	20.6	23.6	27.1	31.1	35.7	41.1	47.3	54.3	62.5	71.9	80.3
Growth		15%	15%	15%	15%	15%	15%	15%	15%	15%	12%
TON Market Share	0%	0%	0%	0%	1%	5%	8%	9%	10%	10%	10%
TON VPN Transaction Volume, \$bn	0.0	0.0	0.0	0.1	0.4	2.1	3.6	5.0	6.1	7.1	8.0

Source: Statista, HASH CIB¹³¹

The fact that reasonable predictions for other TON Services and Applications seem problematic mean we disregard them for valuation purposes. We cannot forecast what kind of end-user apps and back-end services or how many of them will be built on TON and what demand for Grams they will generate as a result. However, the number of such apps and services will most likely be substantial and quickly growing. We believe that they should generate the second-largest demand for TON native tokens after TON Payments, given the natural assumption that GRMs will be the main currency for such services and applications. Therefore, by not including these use cases, our valuation looks conservative and should underestimate the network's rational value.

The next step is to estimate the number of Grams in circulation for every year. The inflation rate will be at most 2% of the total supply, according to the White Paper. While the document's wording is not explicit, we decided to apply this rate to the *total* GRM supply as opposed to the *circulating* supply. We assume that the secondary market will be formed by existing investors, by future validators selling their Gram rewards in excess of what is needed for staking, as well as by the founders selling 50mn Grams annually from their 200mn vested pool for four years. As a result, we calculated a time-series of the number of coins in circulation.

Period	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Total Supply, bop, bn	5.00	5.00	5.10	5.20	5.31	5.41	5.52	5.63	5.74	5.86
Total Supply, eop, bn	5.0	5.1	5.2	5.3	5.4	5.5	5.6	5.7	5.9	6.0
Stake	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
Reward	20%	20%	20%	20%	20%	20%	20%	20%	20%	20%
Number of Grams, bop, bn	3.59	3.69	3.79	3.89	4.00	4.10	4.21	4.32	4.43	4.55
Issued Grams, bn	0.10	0.10	0.10	0.10	0.11	0.11	0.11	0.11	0.11	0.12
Number of Grams, eop, bn	3.7	3.8	3.9	4.0	4.1	4.2	4.3	4.4	4.5	4.7
Number of Grams in Stake, mn	500	500	510	520	531	541	552	563	574	586
Number of Grams in circulation, bn	2.99	3.14	3.28	3.43	3.57	3.67	3.77	3.87	3.97	4.08
Price per first Gram, \$	3.6	4.0	4.4	4.9	5.4	6.0	6.7	7.5	8.4	9.5
Price per last Gram, \$	4.0	4.4	4.9	5.4	6.0	6.7	7.5	8.4	9.5	10.6

Source: HASH CIB¹³²

We estimate a Gram's Rational Value at \$5.90 as of end-2019. We summarize each Gram utility line transaction volume to arrive at aggregate CUVs and Additional CUVs for each period. Dividing ACUVs by the corresponding average number of coins in circulation and discounting the result to the end of 2019, we obtain \$5.90 per Gram. The result implies 63% upside to the \$3.62 minimal issuance price given by formula (1) and 4.4x upside to our calculated second-round placement price of \$1.33.

Year	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	TV
Current Utility Value (CUV), \$bn		0	4	45	436	2 523	4 993	7 501	9 837	12 162	14 603	
Growth			1221%	1176%	864%	479%	98%	50%	31%	24%	20%	5%
Additional Current Utility Value (ACUV), \$bn		0	3	42	391	2 087	2 470	2 508	2 335	2 326	2 440	2 086
Velocity	0	0	1	6	42	183	281	335	356	363	365	365
Number of Grams, bn (average)	2.89	2.99	3.07	3.21	3.35	3.50	3.62	3.72	3.82	3.92	4.03	4.03
Discount Rate	40%											
Discount Factor	1	1	0.71	0.51	0.36	0.26	0.19	0.13	0.09	0.07	0.05	0.05
Discounted ACUV, \$bn		0	2	21	142	543	459	333	222	158	118	101
Value per Gram, \$		0.86	0.95	1.09	1.01	0.85	0.45	0.27	0.16	0.11	0.08	0.07
Rational Gram Value, \$	\$5.90											

Source: HASH CIB¹³³

¹³² Based on our assumptions, derived from the publicly available information presented in the TON White Paper.

¹³³ Based on our own valuation model, described herein. This table contains forward looking statements and actual results may differ, because such a statement is derived from mathematical modeling techniques of the economic or financial markets that may or may not reflect actual conditions or events.

Appendix

A1: Telegram has never officially announced or denied plans for an ICO. However, the news was eventually widely reported on the tail end of what seems like a staged PR campaign. It kicked off with a December 2017 [Bloomberg article](#) in which Telegram founder Pavel Durov indicated he had rejected investment proposals valuing the messenger at \$3-5bn. Just 10 days later a [report](#) on the upcoming ICO appeared, featuring what seemed to be an official promo-video for the fundraiser. Finally, on 8 January 2018, one of the biggest tech media outlets, TechCrunch, [provided details](#) of the project and its upcoming pre-sale, which would value the total supply of Gram cryptocurrency at \$3-5bn. Subsequently, still-unconfirmed copies of the ICO Primer (often referred to as the “Investor White Paper”) and the 132-page long actual (dubbed “technical”) White Paper were leaked and shared over the web. The Primer implied that a possible offering of unregistered securities in the form of the so-called Simple Agreement for Future Tokens (SAFT) investment contracts – i.e., individual agreements between a cryptocurrency/token-promoter and the purchaser – would follow soon in 1Q 2018. However, since Telegram did not make any official statements at this point, it remained unclear whether or not an offering was actually taking place.

On 13 February 2018, a Notice of Exempt Offering of Securities was filed with the United States Securities and Exchange Commission (SEC). [The Form D notice](#) referred to TON Issuer Inc., a British Virgin Islands (BVI) company, incorporated in 2018, and Telegram Group Inc., also a BVI company, incorporated in 2014 – both with the same legal addresses – as the two issuers. Pavel Durov was indicated as a director in both companies and the signee of the notice. The notice also confirmed that the offering consisted of “Purchase Agreements for Cryptocurrency” – meaning investors would get their coins *after* the network was up and running. The notice indicated that the agreements had been executed with 81 purchasers. The indicated date of the first sale confirmed that the sale had been going on since 29 January 2018. The exemption for issuing unregistered securities, claimed by the notice, is Rule 506(c) of Regulation D under the Securities Act, which limits the offering to accredited investors without imposing limitations on advertising and publicly soliciting investments, as long as the issuer verifies the purchaser’s accredited investor status. TON Issuer Inc. and Telegram Group Inc. would not disclose their size in the notice, but they claimed to have raised \$850mn. No finder’s fee or sales commissions to be paid out to third parties were indicated in the notice – meaning the sale was executed directly with the issuers. Additionally, as to amounts to be paid to executives or other types of the companies’ promoters it was indicated that such amount was unknown at the time of notice – but not equal to zero. The clarification on the Use of Proceeds stated: “*Unknown at this time. The issuers intend to use the proceeds for the development of the TON Blockchain, the development and maintenance of Telegram messenger and the other purposes described in the offering materials*”. The notice also indicated the possibility of the following offerings of the same security, which came in just a month.

On 29 March 2018, the second notice was filed with the SEC. [The second notice](#) was virtually identical to the first one with minor additions. The minimum investment amount from outside investors was indicated as 0 during *the first round*, while the March notice indicated a *minimum \$1mn “ticket”* for the second offering. 94 investors accepted the terms, with the first sale taking place on 14 March. The sum raised was identical – \$850mn, bringing the total funds raised for TON to \$1.7bn. The second filing also indicated the possibility of future sales of the same security, although none have been disclosed to date.

A2: A short blog post in July 2018 announcing Passport has been Telegram’s only public announcement related to TON since the fundraiser¹³⁴. While providing links to the [developer manual](#) for Passport service integration, the post only briefly described the already-available Telegram ID integration as a (centralized, not blockchain-powered) end-to-end encryption service, which would store user data “in a decentralized cloud” sometime later in the future. Quickly following the unveiling of the technology, a report by the data security firm Virgil Security [pointed out](#) a critical vulnerability of the service’s password encryption algorithm, a criticism we found compelling. Additionally, the product launch came two quarters behind the Roadmap schedule presented in the Primer¹³⁵. However, we are reluctant to write the service off as a failure at this point: there have been similar hiccups with Telegram historically during the launch of new messenger features, which were later successfully resolved by the team.

Telegram seems to prefer to leverage its ever-growing base of users in the crypto community to integrate the service with ICOs’ and crypto exchanges’ sign-up processes for their Know-Your-Customer (KYC) procedures. To this end, in addition to integrating with online payments service ePayments, which is used as an on- and off-ramp for a relatively low-liquidity UK-regulated crypto exchange DSX, Passport has already been integrated with the crowd-investing platform for crypto projects, ICOEngine. At the time of writing, [the platform](#) lists nine small-to-medium ICO projects that, the website claims, have raised anywhere from a few hundred thousand to more than \$10mn since 2017. While both the integrated platforms seem small compared to the grand scale of TON, they represent compliant and regulated businesses. Additionally, their small-to-medium size customer load serves well for testing a new service.

A3: The smart payment channel functionality requires the support of Merkle state transition proofs for the channel’s smart contract to be able to verify asynchronous balance changes by the parties in the channel. We have given a brief

¹³⁴ However, TON is never mentioned in the [announcement](#).

¹³⁵ The almost half-year latency in unveiling what seems to be a “regular”, centralized service – initially promised within just three months after its announcement – raises concerns discussed among the project’s risks.

overview of what Merkle binary and Patricia tree data structures are and why they are so important for blockchain design in one of the footnotes in the chapter of the report dedicated to the blockchain industry overview (see footnote 48, additionally see [Glossary](#)). It is worth noting that support for Merkle proofs (i.e. compact data structures proving the existence of transactions in the blocks) for payment channel architecture – usually simplified for speed and security optimization – is not a trivial task. Nikolai Durov boasts of being able to use such functionality in payment channels due to the specific data representation capabilities of the TON Virtual Machine (TVM)¹³⁶. So, while payment channel functionality should be available to any cryptocurrency or token in the TON ecosystem of interoperable blockchains, the currencies and tokens running on TVM should have an edge in how quickly they will be able to implement smart payment channels for their purposes. TON also supports the use of other Turing-complete virtual limited-functionality virtual machines using different programming languages in its multiple chains within the TON Blockchain. This, of course, gives a first-mover advantage to Gram as the very first (and naturally, TVM-supported) cryptocurrency in the TON ecosystem.

A4: Abstract Datagram Network Layer (ADNL) in TON will be built over one of the key modern network data transmission protocols – User Datagram Protocol (UDP), which here is put over the Internet Protocol (IP) versions 4 and 6, with optional Transmission Control Protocol (TCP) fallback in case of unavailability. This means that all TON nodes will connect forming their own network within the larger Internet by using the contemporary Internet IP v4/v6 as its basic networking protocol. This implies that *physical node connection* and their *data link layers* (in the respective order, two of the lowest levels of communication networking¹³⁷) is not being built anew by Telegram, but implemented over the Internet. On the higher, so-called, transport layer all the communication between TON nodes will be done through UDP protocol that presents the transmitted data as datagrams. Datagrams can be thought of as “raw” pieces of data *as it is* with no additional information exchanged between the nodes. So UDP makes it possible to send those arbitrary packets from any node to any other node without having to confirm any connection – instead, presuming it is “established” by the sender node knowing the address of the receiver in the Internet Protocol. This makes UDP efficient in use of bandwidth while being unreliable in relation to data interpretation (allowing for mixed ordering, duplication or errors) and confirmation of connection. These data transmission issues are solved by using the more complicated TCP protocol, but speed suffers as a consequence.

A5: Reliable Large Datagram Network Protocol (RLDP) is used for TCP-like transporting over the default ADNL (UDP) protocol in TON. It is important for sending larger size datagrams over ADNL in a more reliable manner than the usual UDP datagram transmission, as it eliminates doubling of data (thus saving download time) and secures the integrity of the transfer in case of network partitions. Other TCP-like functionality that defines the utility of a higher level RLDP protocol over the ADNL is its ability to send Remote Procedure Call (RPC) queries (i.e. “pressings of virtual buttons”) and transfer Hyper Text Transfer Protocol (HTTP) queries (i.e. web page-like visual presentations of data) to TON nodes. *This basically allows RLDP to enable integration all of TON’s on-chain, off-chain, or mixed services into a generalized common web interface.*

A6: Gossip Protocols (including Broadcast Protocols) and Streaming Broadcast (Multicast) Protocols (for larger chunks of data) are used for the so-called TON overlay networks (i.e. arbitrary, special purpose node connections freely put up and broken up by nodes when necessary). Gossip protocols are a well-established group of technologies used for fast and efficient communication between nodes in any network (using only neighbor-to-neighbor node messaging, which effectively enables faster propagation of messages to *all nodes* of the network). This is why gossip protocols are widely used in blockchains. Streaming Broadcast Protocols are the ones used over TON’s RLDP to split different data for faster transmission and then reconstructing it without errors with the aid of data coding technologies. Such data coding¹³⁸ is used to split data into small chunks and then follow certain logic to consistently put it back together. This is how Streaming Broadcast (Multicast) Protocols offer fast and reliable way of sending larger datagrams (for example, blocks in a blockchain validator overlay network).

A7: (Kademlia-like) Distributed Hash Table (DHT) is a virtual table made up of actual shards (in the database management meaning) kept with all TON nodes. These shards of table entries reference the data and addresses (assumed node identities) corresponding to (i.e. storing) such data. The shards contain only references relevant to each particular node (forming their immediate network of connected nodes and account of data communicated between them), keeping and updating such a shard. When combined together these shards form a virtual DHT table. This enables TON DHT to store references to *all* of TON nodes’ data along with the all of the addresses of the nodes keeping it. It must be noted that a single node can assume multiple DHT identities, to easier distinguish between each of its particular functions in the network. The data-address combination is a key-value pair table, where each key is presented in the form of its hash (i.e. a reasonably uniquely computed index of a key). It is additionally optimized for grouping nodes based on their 256-bit ids in DHT¹³⁹, as routing paths are created between particular addresses (values of the key-value pair), using the most proximate nodes in their 256-bit address resemblance. Data (keys of the key-value pair) lookup is also optimized by using 256-bit string resemblance of the hashed data references. So both the keys and values in DHT have a 256-bit representation in order to enable fast data or node lookup and routing. This is what makes TON DHT a Kademlia-like key-to-value mapping table.

¹³⁶ The Turing-complete virtual machine that will be built specifically for TON (like Ethereum’s EVM)

¹³⁷ https://en.wikipedia.org/wiki/OSI_model

¹³⁸ Nikolai Durov mentions Reed Solomon code or RaptorQ fountain code as possible implementation references.

¹³⁹ Which are different from the lower-level ANDL addresses, assigned to each node in the network as well.

Kademlia is a technology widely used and long-tested in popular peer-to-peer distributed file sharing systems such as BitTorrent, eMule, and most recently InterPlanetary File System (IPFS). It is also used in blockchains, Ethereum being the most prominent example. While allowing effectively any node to be looked up and pinged for certain data, Kademlia routing does not take actual physical routing into consideration. That means that sometimes nodes physically located close to each other (and thus experiencing lower latency during direct data transmissions) could be further apart in Kademlia-like DHT than, say, two nodes physically located on different continents while being Kademlia-like DHT neighbors. This could cause additional network latency while being efficient for faster data/node lookups.

A8: TON Proxy is a network routing mechanism implemented through the use of “tunnels,” similar to I²P (Invisible Internet Project) or TOR (The Onion Router). Such routing protocols could be briefly described as those where nodes offering themselves as proxies along a certain path, do not “know” anything about the actual sender and receiver of a communication – just the preceding and the next node in the routing path. Additionally, the communication itself could be protected by encryption. This way a node that wishes to obfuscate its identity (i.e. make it harder to reveal but *never* completely hide – as is overstated in the TON White Paper) would use a tunnel identifier and its entry point (a 256-bit address), which would be posted in the TON DHT table. Additionally, nodes could assume multiple such proxy addresses for different “roles” they perform within Telegram Open Network or for security purposes. We cannot ascertain how much the TON anonymizing protocol will differ from I²P, which is cited as its main reference, but we note that the latter protocol has been exposed as susceptible to attacks¹⁴⁰. Another important note in this regard is that systems like I²P have never been used for “hiding” large stake validators in major blockchain networks, or even for simply transmitting value-containing messages. These factors could tempt possible attackers into trying to crack TON’s anonymizing technology.

A9: A distributed storage service like InterPlanetary File System (IPFS) would be an extremely compelling utility for users wishing to maintain a certain level of immutability of data stored in the Internet while also being able to have reliable access to it. This is not necessarily users’ data, but data maintained by applications, websites, and so on. Peers wishing to provide their data storage capacities as a service to the rest of the TON community can “participate” in a special smart contract that facilitates payment for such a service (for example, micropayment transactions sent for every Kb of uploaded/downloaded data) and automated provision of the service according to parameters set by the user (for example, according to their preferred replication factor). However, the most important feature of such trustless execution is the *enforcement of data availability* from the parties wishing to store it. Unfortunately, the White Paper does not provide details on how exactly this problem could be solved in TON. There are multiple potential approaches, but none of them reliably provide fully trustless certainty (being based on game theoretic measures imposing costs on misbehaving parties while also relying on optimal replication thresholds).

Moreover, the main reason this issue is important is because Storage will also be used for keeping TON Blockchain archived data (the so-called block snapshots). It could be preserved in a centralized manner during the ecosystem buildout phase with a TON Foundation-controlled distributed set of nodes up for the task, as suggested by the Paper. However, if this particular functionality is to become truly decentralized (for a whole host of reasons, but mainly to maintain trust in the blockchain’s history), it would need to be outsourced to the network of Storage providers. Here data availability enforcement becomes key. That’s why we think that the possible implementation of blockchain history storage use case could be reserved for professional blockchain maintainers – e.g. the validators – to keep and update such data in a Byzantine Fault Tolerant manner. The tradeoff is obvious: it would lead to centralization with the rest of the wider network dependent on this smaller group of parties. None of this has been clearly addressed in the White Paper.

A10: DNS is contemplated as an on-chain service because one simply *cannot* create such a service off-chain that can integrate both off- and on-chain addresses. While making transitions between the World Wide Web and TON (or off- to on-chain) seamless, DNS connects two very different networks of nodes. Web domains and subdomains are highly regulated pieces of virtual property, with regulation trickling down from the Internet Corporation for Assigned Names and Numbers (ICANN, a private non-profit U.S. organization, effectively responsible for granting DNS registry entry rights) to domain holders and their multiple “agents” (domain registrars) all over the world. ICANN also monitors the space for abuse or malpractice. So, in order to make sure that domain names are actually held¹⁴¹ by the entities claimed as their holders and are being used by these holders for their intended purposes – as opposed to facilitating phishing and other forms of online attacks on users or other malicious activity – a high degree of regulation is needed. A trustless system is the perfect alternative here, with the authenticity of a domain name verified using blockchain-powered validation. That is why such a system, if implemented correctly, will have a compelling use case in TON.

Each smart contract effectively governs its own domain space. This means that if we wanted to create a domain space *.hashcib* in TON, we would simply post a smart contract on the TON Blockchain, dedicated to governing all the subdomains of that domain. “Governing” here essentially means assigning anyone’s address in any of the TON stack of technologies – whether a user, a smart contract or a mixed/off-chain application or service – a human-readable representation within that

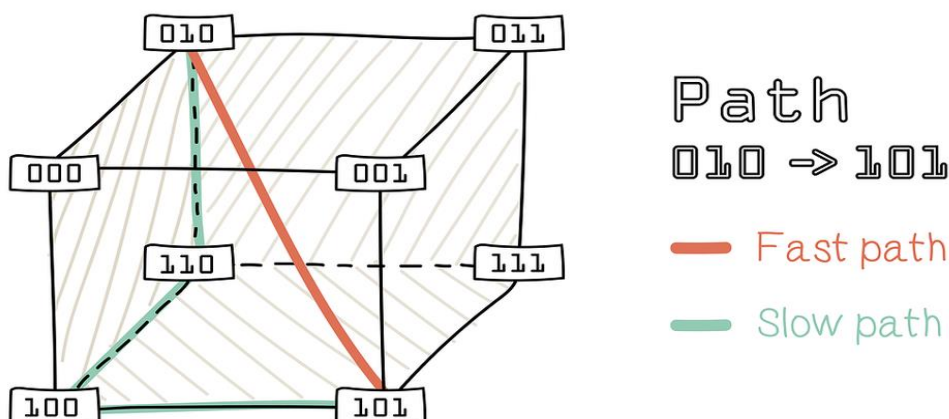
¹⁴⁰ “[Practical Attacks against the I2P Network](#)” by Christoph Egger, Johannes Schlumberger, Christopher Kruegel and Giovanni Vigna (2013).

¹⁴¹ Usually “leased” from the owner via an intermediary, a domain registrar.

domain space (say, *research.hashcib*) to be addressed from anywhere in TON¹⁴². Subdomains are registered on a first-come, first-served basis and could automatically update (via the DNS smart contract) links to the subdomain holder's actual underlying (bit-string represented) address in the network each time it changes – so the human-readable link to it stays the same and is not broken each time such underlying address changes. Also, domain-governing smart contracts could automate extracting regular payments for the use of subdomains. Additionally, a “root” DNS smart contract is created and hardcoded into the network's cache for any node to be able to easily look it up – as it keeps track of all other DNS smart contracts possibly residing in different chains of the TON (multi)Blockchain.

A11: TON uses so-called Hypercube Message Routing, which is a particular functionality to facilitate work(shard)chain interoperability. For a user's account in the blockchain to interact with a smart contract, or for a smart contract to cause another smart contract to execute, they need to share *messages*, i.e. execution calls limited only by the purpose of the smart contract being called. (Actually, any account-to-account interaction – including between two human-controlled accounts – requires messages to be sent between them as well). Value transfers are also done via messages and sometimes value-attached simple messages can also call a smart contract to act – say, provide a single service this contract “knows” to provide, for as much as it has been remunerated. For messages to be able to travel through *any* and *all* of the existing shardchains (which make up the differing workchains of TON (multi)Blockchain) in a fast and reliable manner, the message routing uses a *maximum* of four steps¹⁴³. This effectively means that the message sequentially travels “through” neighboring shardchains¹⁴⁴ until it gets to the destination shard. With validators of each shardchain along each step *mandatorily* having to monitor neighboring shards and include such messages coming from them (in threat of their stakes getting *slashed* for not complying) into the next (available) block in their respective shard. This is called *slow path* hypercube routing. The sender can additionally “speed up” their message by sending it along with the corresponding Merkle proof (effectively, proving the origin of the message and the validity of the inbound transaction to the receiving account) to the destination shardchain validators. This way the message is delivered in just one step (i.e. 5 seconds, the desired block confirmation time in TON Blockchain).

Simplified illustration of Hypercube Routing in TON with shard ids represented by 3-digit integers¹⁴⁵



Source: TON White Paper, HASH CIB

A12: Another blockchain innovation in TON is the concept of *block healing*, introduced to amend transactions already committed but later proven invalid. With punishing the misbehaving validator who committed a transaction that was later proven invalid¹⁴⁶, TON blockchain can also re-write the blockchain history related to only this particular transaction and any subsequent transactions that reference the initial invalid one. This allows altering the blockchain's *immutability* in a presumably fair and secure manner – to prevent so-called “hard forks”. For example, blockchain rollbacks due to some events “forever” embedded in the blockchain history but deemed unwanted or even disastrous by part or whole of the network's community – thus causing network to split with some or a majority of the network participants agreeing to roll history back to the block preceding the unwanted change and effectively deleting all subsequent *valid* transactions along with it¹⁴⁷. TON's proposed solution allows for the valid entries into a block deemed flawed by a single invalid entry to be

¹⁴² However, creating top level domains, compatible to the rest of the Internet (outside of TON) depends on whether or not TON will acquire DNS registry rights from ICANN.

¹⁴³ Each time by changing a hexadecimal part of a 64-bit destination shardchain id. The number of steps could be less than four if the shardchain ids are “close” to each other in terms of id resemblance.

¹⁴⁴ Differing only in one hexadecimal element of the leftmost 64-bits of their ids.

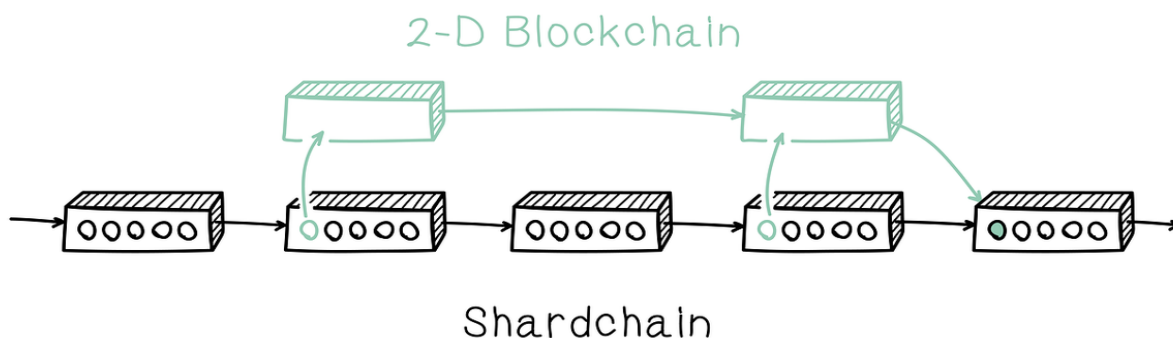
¹⁴⁵ An actual illustration would imply drawing a 4-dimensional [hypercube](#), which would need 4-digit representation and 4 maximum “hops” on the slower path – not 3, as presented above.

¹⁴⁶ i.e. being a misrepresentation of the network participants' desired state, like account balances or transaction outcomes, in effect possible only with validators' active participation in putting together and confirming transactions in the block.

¹⁴⁷ Ethereum's DAO hack story offers context on public blockchain forks due to extraordinary filues and their implications. Good overviews can be found at [BitDegree](#) and [Quartz](#).

left unchanged, as well as the sequence of all “correct” blocks that follow¹⁴⁸. A re-written transaction is committed to an otherwise empty new “vertical” block on top of the “old” one, with additional “corrections” to the subsequent transactions linked to the initial “wrong” one taking place in the same manner – with new vertical blocks on top of the old ones, creating the so-called “history rewriting ripples” until they reach the most recent shardchain and corresponding masterchain blocks (See illustration below). This is essentially a mechanism to prevent “*true forks of all shardchains involved*” in the extreme case of blockchain ambiguity.

Creation of vertical blocks on top of “horizontal” blocks



Source: TON White Paper, HASH CIB

A13: Work(shard)chain and masterchain blocks are to be created in proposed intervals of 2-3 seconds between them, while maintaining a 5-second block creation time within their chains, by a global validator set of 100 nodes (for the masterchain) and local subsets of no less than five validators (for shardchains). Complications here could arise from having to propagate blocks between these groups, with a global set possibly becoming prohibitively large for fast distributed consensus¹⁴⁹ in case of a larger block size. In the extreme case (purely theoretical, of course) of all shardchains being in operation (i.e. the TON Blockchain reaching its maximum capacity), the imaginary masterchain block would grow to a staggering $1.585 \cdot 10^{17}$ terabytes in size¹⁵⁰ if all the shardchain block hashes of 32 bytes each were included into the masterchain block! On a more realistic note, we assume that networking complications could add to latency in validator communication. Imagine an overlay network for validators that uses reliable large datagram protocol (RLDP) on top of the basic transporting (ADNL) protocol with additional proxy tunneling (possibly, effective for some of the validators)^{A4 A6 A8}.

A14: Moreover, some of the complex engineering solutions, although conceptually making sense on a higher level, call for additional explanation. Aside from the software engineering innovations, take, for example, the proposed new TON Virtual Machine and its type language (a TON-tuned version of Telegram’s current programming language TL) TL-B, which is used for *formal description* of core Blockchain underlying structures using a so-called TL-scheme. Effectively, this makes it possible to use *any* programming language in TON by transforming¹⁵¹ those languages to TON VM intermediate language. So, rather than requiring programmers to learn coding in a pre-defined new language set or a single language – thus limiting and slowing down ecosystem development in the ever more competitive blockchain platform space – it offers an easier learning curve for programmers. But the TON VM programming language is yet to be created (with only its high-level properties outlined in the White Paper), while TON Blockchain would still remain a whole new system architecture for outside developers looking to build on it. This approach does not fully mitigate actually having to grow a whole new developer community, even as many of TON’s newer generation competitors are coming out with more common, and thus well-understood, and supported approaches¹⁵². Introducing its own virtual machine and set of programming languages and allowing for other languages to be integrated by as-yet undeveloped special transition tools, TON still faces the risk of a longer adoption phase by the outside developer community. Moreover, TON developers could also face graver issues with their home-cooked VM and programming language, and this time the consequences could be different from the technical “hiccups” Telegram had to face with its messenger app – there could be billions of dollars on the line.

¹⁴⁸ Even if a series of invalid entries are all committed within a single block, making the whole block replaceable, it would make no difference. The following “correct” blocks – *all* inevitably referencing the “wrong” one – remain intact.

¹⁴⁹ Eventually planned to grow to up to a total of 1,000 nodes – adding even more network latency.

¹⁵⁰ The whole of global Internet traffic was 10^9 terabytes in 2016, according to [Cisco](#).

¹⁵¹ Creating [transpilers](#) or [compilers](#).

¹⁵² Like the WebAssembly compiler that sometimes makes it easier for more experienced and qualified wider (non-blockchain) programmers to quickly adapt their used and well-tested set of tools to building these new systems, which operate on a WebAssembly virtual machine. This newer approach represents an evolution after Ethereum’s hard-learned lessons of coming out with their own unique set of programming languages and virtual machine. It took Ethereum years to build its own developer community with a lot of costly programming “disasters” like [the \\$150mn DAO hack](#) or [the \\$230mn Parity wallet bug](#).

Glossary¹⁵³

Address can have multiple meanings throughout this report:

- In the context of **blockchains**, address is a unique identifier of a user. User's account = address + balance. On a **smart contract**-supporting blockchain (as opposed to value transfer-centric chains like Bitcoin) accounts can be externally (user) owned or smart contract-operated. Technically, a Bitcoin network, which by default is managed by user owned accounts, can also have automated accounts – such as multi-signature **payment channel** escrows, but they are less self-sustained than smart contract-operated accounts.
- Additionally, in the context of wider networking, addresses are unique indexes of **nodes**, **services** and **applications** in the general network topology (like TON ADNL) or additional routing databases (like TON DHT).

Block – a package of data, bundled together in a perimeter and structured within that perimeter a certain way. In the context of a **blockchain** – a block is a set of data organized with special rules, that contains information about current set of **transactions**, **proofs** of their **validity**, references to previous sets of transactions (blocks), and some other information needed to identify the block itself, its creators, the data set it contains and other parameters depending on system requirements.

Blockchain – a network (system, platform) of peer **nodes** that keep and update a common (**distributed**) **ledger** with **transactions** specific to the blockchain's functionality and communicate those changes to each other. In blockchains such changes to the ledger are introduced with putting transactions into the next **block** - "chained" to the previous one by referencing it, with that previous block referencing the one before it and so on (which differentiates blockchains from other types of distributed ledger systems) Depending on the context it could also mean:

- a **protocol of communication** for nodes wishing to keep and update a common ledger, which has specific functionalities to accommodate the purpose of such a ledger, differentiating such a protocol from another blockchain protocol.
- a software system, implementing program logic that compiles such a protocol (described above) in a way that allows different nodes to use it according to their roles in the network through special software clients (applications integrated with such a software system to interpret it according to their use cases).

Centralized vs. decentralized network (governance):

- **Centralized network** – a **distributed** (peer-to-peer) network of **nodes**:
 - run by a piece of software developed and updated by a single party, or
 - otherwise governed by or dependent on such a single party or faction.

A peer-to-peer network could be viewed as centralized if a single party/faction effectively decides the rules of data management and communication (or other ways the network operates) for the rest of peer **nodes**, or is able to abuse such rules in their own favor.

- **Decentralized network** – a peer-to-peer network of nodes (not necessarily a distributed ledger system):
 - running on a piece of software developed and updated by multiple parties, or
 - otherwise governed by or dependent on multiple parties in such a way that no single party or faction can introduce changes to the way a network operates, set or abuse its rules.

Centrally processed vs. distributed network (topology):

- **Centrally processed network** – a network of **nodes** connected to each other in a way that one or more nodes (but significantly less than a majority) have preference in terms of how they connect to other nodes or maintain commonly shared data.
- **Distributed network** – a network of **nodes** interconnected as peers in terms of their ability to access other nodes on the network and maintain commonly shared data.

Coin (Cryptocurrency) – a unit of value and account that is algorithmically issued by the blockchain protocol to **miners/validators** as a reward for their **consensus**-providing services to the network. Such an algorithmic issuance inherently connected to the **blockchain**'s operation makes it the underlying currency of a particular blockchain. That is how we distinguish between cryptocurrencies and other blockchain-based units of account (**tokens**). To date, each blockchain has supported only one underlying coin, but projects like TON and possibly other blockchain **interoperability**-focused **protocols** will be able to support multiple blockchains, each with their underlying coin.

¹⁵³ If a definition contains terms **in bold italics**, this means you can also look them up here.

Consensus – in *distributed networks* (not necessarily *blockchains*) where *nodes* need to agree on certain updates/changes to the network, consensus is a communications algorithm that allows different parties (nodes) to come to a single, non-conflicting view on the chain of events.

DApp – Distributed Application. A set of *smart contracts* combined for a particular set of functions, that “lives” on a *blockchain* and operates within it.

Distributed ledger – a ledger that is kept and updated simultaneously by a network of multiple *nodes*, so that each update corresponds to the *consensus* of effectively all of the nodes (a threshold to deem consensus universal depends on the consensus algorithm utilised by a particular network). All blockchains are distributed ledgers, but not all distributed ledgers are kept and updated in a form of a blockchain.

Finality – the irreversibility and rewrite tolerance of a *blockchain*.

- **Probabilistic finality** means that there is a non-zero probability that a chain of blocks could be replaced with an alternate, parallel chain, due to a technological advance by the party building the parallel chain, allowing it to add new blocks faster, and the *protocol*’s fixture on following the longest chain. This probability is relatively small and could be ignored in some scenarios.
- **Commercial finality** is finality achieved by placing an economic incentive on a particular chain of blocks, thus making the probability of such a chain being replaced by a different one directly linked to the economic significance of the network to the multiple parties using it.

Fog service – a digital service provided by a *distributed network* of peer *nodes*, possibly in different capacity or quantity, depending on the fog service’s function or technical implementation. The term takes its origin from the concept of “cloud service”. Cloud services are provided by companies such as Google, Amazon, Microsoft, etc. using their hardware; fog services are usually provided on the user (i.e. network peer) hardware itself. It is not necessary to have high-end servers to provide fog services, even a laptop could do so in some case.

Fork – a general term meaning a different version of a *blockchain*. Forks are possible due to the open source nature of most blockchain *protocols*’ software implementations.

- **Soft Fork** – a backward-compatible software update to a blockchain protocol that does not cause any disruption in the network’s operations, because *nodes* that have not updated their software can still maintain the network along with the updated nodes.
- **Hard Fork** – a parting in blockchain history from a certain point (i.e. a *block*) into two separate chains of blocks due to changes in the underlying protocol, which are incompatible with the previous version of the protocol (due to technological incompatibility, (political) incompatibility of the desires of different network participants, or a combination of both). Nodes that have not updated their software to the hard-forked version follow a different chain from the ones that have, due to such incompatibility.
 - *Purely technological* hard forks most of the time lead to universal software updates within a network with minor disruptions in the network’s functions (i.e. a minority of nodes lagging in updating their software clients and thus unable to function).
 - *Purely political* hard forks usually correspond to a specific event in the blockchain history rather than a technological update, e.g. the distribution of funds (as with the hard fork between Ethereum and Ethereum Classic, due to a buggy *smart contract* being misused to effectively steal millions of dollars’ worth of ETH). Purely political forks can also “start anew” instead of building on top of already generated history, if the reason for a fork is to introduce general improvements in blockchain’s on-/off-chain governance, issuance model and so on (as with the hard fork between EOS and Telos, due to user accusations of unfair centralization of EOS by the biggest stake owners and their designated validators).
 - *A combination of technological/political* factors playing into a network fork are usually driven by technological parameters of the network affecting governance (as with the hard fork between Bitcoin and Bitcoin Cash, due to different approaches to making the Bitcoin protocol more scalable, which could lead to higher/lower network centralization).

Hash – a probabilistically unique index with a specific, defined size (dependent on the function applied) that is created through application of a hash function to a dataset of arbitrary size. Hashes of data are used to reference a dataset in its entirety in a compact form – without needing to store the actual data, while making sure it is accurately and fully referenced. If a hash function is cryptographic, then the hash can be called a cryptographic hash, and its uniqueness is more certain that way. *Blockchains* predominantly use cryptographic hashing functions to create hashes, which they use to reference data in a compact form (like the hash of a previous *block* that is stored in the current one), without compromising the accuracy or completeness of data.

Interoperability – The ability to connect between different *blockchains* to execute *smart contracts* and/or transfer value.

Layer – in the context of the current report, a layer means:

- The same level of hardware or software intercommunication (see *stack of protocols*).

- The base **blockchain** (settlement) layer (layer 1) and special purpose software architecture built on top of it (layer 2 and on) that settles to the underlying blockchain (like payment channels, for example).

Merkle proof – the set of hashes you need to provide (besides the hash of a certain data item itself) in order to prove that a data item belongs in a particular set, presented in a Merklized (i.e. **Merkle tree**) form. In blockchains Merkle proofs are usually provided as proofs of existence of certain transactions (which also implies their **validity**).

Merkle tree – a way of organizing **hashes** of items in a set that allows for a more efficient representation that proves that the hash of a data set includes a hash of a particular data item. Usually in **blockchains** Merkle trees are used to reference a block and its transactions, but Ethereum keeps **Merkle (Patricia) trees** of transactions, a current state, and transaction receipts (i.e. the effect of a particular transaction) in a block.

Merkle (Patricia) tree – a more optimized version of a Merkle tree.

Miner – a **blockchain** network **node**, whose role is to put together a **block** of user **transactions** and propose it to the network in a way that is acceptable for the network to reach **consensus** on the proposed changes within the block. In order to be allowed to update the chain with such a block, a miner needs to be the first to solve a mathematical puzzle by applying brute computational force to it. The miner's chance to win gets higher the higher the amount of computations (CPU-power) per limited period of time the miner possesses. As soon as the block is “found” by one miner, all other miners rush to build the next one on top of it, and so on, which results in **probabilistic finality** under a proof-of-work consensus algorithm, which can only be broken if some miner possesses more CPU-power than the rest of the miners. For being the first to put a block together, the miner is rewarded with newly created (“minted”) coins – hence the name.

Node – any computing machine connected to any network of computing machine. In **blockchain** networks we distinguish:

- **Full Node** – a computer that stores the full history of the blockchain and participates in updating the blockchain with created blocks. Other software clients can be connected to a full node to provide current blockchain status to their users. Such reliance on a node is usually mitigated by connecting software clients to multiple full nodes.
- **Light Node** – computing machine (including a mobile device) that stores only **block hashes** and maybe additional compact data that allows them to check (with **Merkle tree**-structured **proofs**) whether **transactions** relevant to such a light node were included in the corresponding blocks. A light node participates in the blockchain update, but all software clients connected to such a node (i.e. apps of devices connected to it, such as a blockchain wallet on the user's mobile phone, or a browser-extension wallet on a desktop computer) can only rely on limited data on the current blockchain status.

Payment channel – a channel used to transfer a means of value. A payment channel could be implemented as a **state channel** that operates with **tokens** or **cryptocurrencies**, or it could be implemented on a **stateless** basis with utilizing the **UTXO** account balance change model.

Payment channel network – a network of two-party **state**/or **stateless** payment channels that allows two parties that are not directly connected to transact via a network of intermediaries.

(Communication) Protocol – a technology using a particular set of rules governing anything a network of **nodes** can do (store data, transmit data, communicate something about the data, update data, etc.).

Scalability – The speed at which a **blockchain** can process dozens of thousands of **transactions** in a distributed, spread out and **trustless** environment.

Sharding – has two meanings throughout this report:

- In database management sharding is a type of database partitioning that separates very large databases into the smaller, faster, easier managed parts called data shards. In common use, sharding refers to having some data for an application on one database server, and other data on another – so that different parts of a database when worked with are requested separately, which eliminates the bottleneck of one server centrally processing all requests concerning different pieces of the same data set.
- In **blockchains** sharding means the splitting of one logical system (a blockchain) into minor parts for performance optimizations, while maintaining a single system structure. This way not all of the blockchain **nodes** execute all of the blockchain's transactions (as in default blockchain setting), but only some of transactions – allocated to different node groups (i.e. shards) based on certain logic - while maintaining consistency (i.e. security and immutability) of the whole system.

Sidechain – a **blockchain** that settles to a different blockchain, and is thus subordinated to the settlement chain.

Smart contract – a computer program with a predefined set of outputs (virtual actions) each responding to a certain type (or groups) of input(s), which thus automates the execution of virtual actions if conditions precedent for such actions are met. Smart contracts allow for **trustless** execution of programmed code.

Stake – the economic or reputational resource a *blockchain* network participant is ready to place on some statement (like *validity* of the next *block*, for example) to prove its agreement with it. Various implementations of staking algorithms are used in the proof-of-stake (PoS) consensus algorithm.

State (of a digital entity/system) – a current set of parameters that make up such a digital entity/system in its entirety, with it being “aware” of such set of parameters.

Stateful (system) – a system that has a current state, with all future changes to the system made based on that state. In case a state is lost, the system will need to start over in order to operate. A good example of a state system could be an operating system with a RAM memory: if a computer loses power after a reboot, you will need to open programs once again and you will lose all unsaved changes.

Stateless (system) – a system that does not need to have (and be “aware” of) its current state in order to operate properly. It acts completely independently by applying some inputs and producing some outputs.

State channel – a peer-to-peer, off-chain communication channel between two parties used to update the state of balances, computations or other *smart-contract*-executed variable values.

Stack of protocols – a hierarchy of communication *protocols*. A hierarchically-set logical grouping that combines the protocols in a way that more specific (higher-level) use case-oriented protocols are built on top of the more broadly used (lower-level) protocols, defining the basic rules of communication within a system.

Stack of technologies – a hierarchy of technologies used to implement a desired technological solution or multi-solution system.

Token – a unit of account/value that is created through a special *smart contract* that keeps track of accounts and balances corresponding to parties using the token for a specific purpose (e.g. payment for digital services provisioned by a *decentralized application*) within a broader underlying *blockchain*.

- **Fungible** – characteristic of a *token* issued by a *smart contract*, meaning that such a token is no different from any other tokens issued by the same smart contract. Ethereum has a widely adopted technical specification for fungible token smart contracts, which is now a standard on Ethereum network – ERC-20. Fungible *coins* refers to cryptocurrencies that are untraceable in terms of their history, i.e. true privacy-preserving coins like the ones issued by Monero network, and not pseudo-private coins like bitcoins, where each owner of a coin throughout its history is known, even though those owners are hidden by a bit-string virtual address.
- **(Non)-fungible** – characteristic of a token issued by a smart-contract, meaning that any token issued by this smart contract has properties that uniquely identify it as such. Such tokens are used to create crypto collectibles, for example, like *DApp* non-fungible tokens in “Crypto Kitties”, that are virtual mascots each having unique set of properties (eye color, hair style and others – defined by their breed). Ethereum has a non-fungible token technical standard – ERC-721, widely used for creation of crypto collectibles and other non-fungible token use cases on Ethereum.

Transaction – in the context of *blockchains*, it is an atomic change of the blockchain’s state or balances (for example, due to blockchain account interactions, whether human owned or *smart contract*-operated), which is committed to a *block*.

Trustless – in the context of *blockchains*, not dependent on any party that needs to be trusted in order to deem something correct, easily and fully verifiable.

Turing-complete – a Turing-complete or computationally universal computer system is one that can process, store while using (multi-task), and long-term store data – like CPU, RAM and disk storage systems on a personal computer. The main property of such a system is the ability to implement any deterministic program or algorithm (algorithm that always ends - with no so-called “infinite loops”, no crashes and so on). It means that such a system can be used to implement any programmable business logic.

UTXO (Unspent Transaction Output) – a method of accounting in *stateless distributed ledgers* for input and output balances of a *transaction* in a way that the input minus the output should be exactly zero, thereby ensuring that no balance was produced inside the transaction and nothing is forgotten. Such a scheme does not require a system to store an actual balance but rather have an unspent output that can be verified by going through the *blockchain* history.

Validation/Validator – a *blockchain* network *node*, whose role is to put together a *block* of users’ *transactions* and propose it to the network in a way that is acceptable by the network to reach *consensus* on the proposed changes within the block. In a proof-of-stake algorithm, validators perform the initial work of reaching consensus, then present it to the rest of the network. In PoS validators check the correctness of a given statement or approve blocks proposed by different validators. Such a statement could be a whole new block proposal, a state transition within a block, or any other change in the underlying.

Verification – the process of verifying the correctness of *blocks* after they have been added to the blockchain.

DISCLOSURES

This report (hereinafter – “this report”) was prepared by ICO B@nk, LLC and/or its affiliated persons (collectively – “HASH CIB”).

This report accurately reflects analysts’ personal opinions about the company (companies) analyzed and its (their) securities and financial instruments. Analysts’ compensation is not in any way, directly or indirectly, related to the specific recommendations and opinions expressed in this report. The personal views of analysts may differ from one another. HASH CIB may have issued or may issue reports that are inconsistent with, and/or reach different conclusions from, the information presented herein.

The facts described in this report, as well as any opinions, estimates, expectations and forecasts expressed in it are provided as of the date hereof and are subject to change without notice. Due to its simplification, this report is partial and thus the information presented in this report can be subjective. No representation or warranty, express or implied, is made as to and no reliance should be placed on the fairness, accuracy, completeness or reasonableness of the information, opinions, estimates, expectations and forecasts contained in this document, and neither HASH CIB nor any other person accepts any responsibility or liability whatsoever for any loss howsoever arising from any use of this document or its contents or otherwise arising in connection therewith. This report does not take into account the recipient’s objectives, financial situation or needs.

HASH CIB is not committed to update the information or to correct any inaccuracies contained in this report. HASH CIB’s reports are published at irregular intervals as appropriate in the analyst’s judgment. Some information has been provided by HASH CIB, information furnished by third parties has not been verified by HASH CIB or any person for the accuracy and completeness. All accounting information, except otherwise specified, is un-audited.

Neither this report nor any information contained in this report shall be considered as advertising the securities mentioned in this report within the territory of the Russian Federation or outside the Russian Federation. The Product does not constitute an “appraisal” or “evaluation” within the meaning of the Federal Law of the Russian Federation of 29 July 1998 No. 135-FZ (as amended) On Appraisal Activities in the Russian Federation or similar laws of any jurisdiction.

HASH CIB is not licensed to carry out any banking or broker services or similar activities in the Russian Federation or anywhere in the world, is not a regulated entity in any jurisdiction, and does not hold any licenses or other permits from any regulatory bodies of any jurisdiction.

Both shareholders of HASH CIB occupy managerial positions at QIWI Blockchain Technologies, LLC, a direct subsidiary of QIWI PLC. The controlling shareholder and CEO of QIWI PLC, Sergei Solonin, holds a significant position in the securities and financial instruments covered in this report. Two of the analysts that have worked on this report are also employed by QIWI Blockchain Technologies, LLC.

Furthermore, from time to time, HASH CIB or its principals or employees and/or their respective connected persons (the “Connected Investors”), may have or have had positions in the securities or other instruments referred to herein or otherwise act or have acted as principal in transactions in any of these securities or instruments or may provide or have provided consulting and other services to, or have otherwise been involved with, a company referred to in this report, in addition to the relationship of HASH CIB to QIWI PLC and its controlling shareholder described above.

HASH CIB’s representatives may provide oral or written market commentary or trading strategies, and such commentary and strategies may reflect opinions that are contrary to the opinions expressed in this report. Neither the Connected Investors, nor HASH CIB, nor any of its analysts, are under any obligation to inform you of the identity of such Connected Investors, and the Connected Investors are under no obligation to notify you or to otherwise disclose to you that they are affiliated with HASH CIB and/or its analysts, including when transacting with you in securities or other financial instruments covered by this report.

Financial instruments may afford the opportunity to generate positive returns, they also provide the opportunity for increased volatility and significant risk of loss. The information described herein is also subject to the risk of counterparty or issuer default. This brief statement does not disclose all the risks and other significant aspects in connection with the information described in the report.

All information, analysis and conclusions herein present analysts' current knowledge and market estimation at the time of its production. Nevertheless it can contain unintended erroneous statements or presentations and the information may change at any time without previous announcements and/or notices to the recipient of this report. Information contained herein may vary from previous or future published versions of this report. Although the information has been obtained from sources believed to be reliable, there are no guarantees of accuracy, completeness or fairness.

The data and information, including but not limited to scenarios set forth in the report, are presented for illustrative purposes only and such data could vary significantly from the actual results.

Where past performance, past experience and track record information is provided, this is not necessarily representative of future results: performance is not constant over time and the value of investments may fall as well as rise. No representation is made that any results or other figures indicated in the report will be achieved and that investments will achieve comparable results to targeted returns.

Past performance does not constitute a representation or guarantee as to future results or performance. The data provided above is only intended to give the recipient information concerning the general experience of analysts and is not intended as a representation or warranty by HASH CIB, or any other person or entity as to actual results.

Any hypothetical illustrations, forecasts and estimates contained in the report are forward looking statements and are based upon assumptions. Hypothetical illustrations are necessarily speculative in nature and it can be expected that some or all of the assumptions underlying the hypothetical illustrations will not materialize or will vary significantly from actual results. Accordingly, the hypothetical illustrations are only an estimate and HASH CIB assumes no duty to update any forward looking statement. This report may also contain historical market data; however, historical market trends are not reliable indicators of future market behavior.

Except as otherwise specified, any companies, sectors, securities and/or markets discussed are solely for illustrative purposes regarding economic trends and conditions.

Further information on the securities referred to herein may be obtained from HASH CIB upon request. This report may not be reproduced or copied in whole or in any part without written consent of HASH CIB.

© HASH CIB