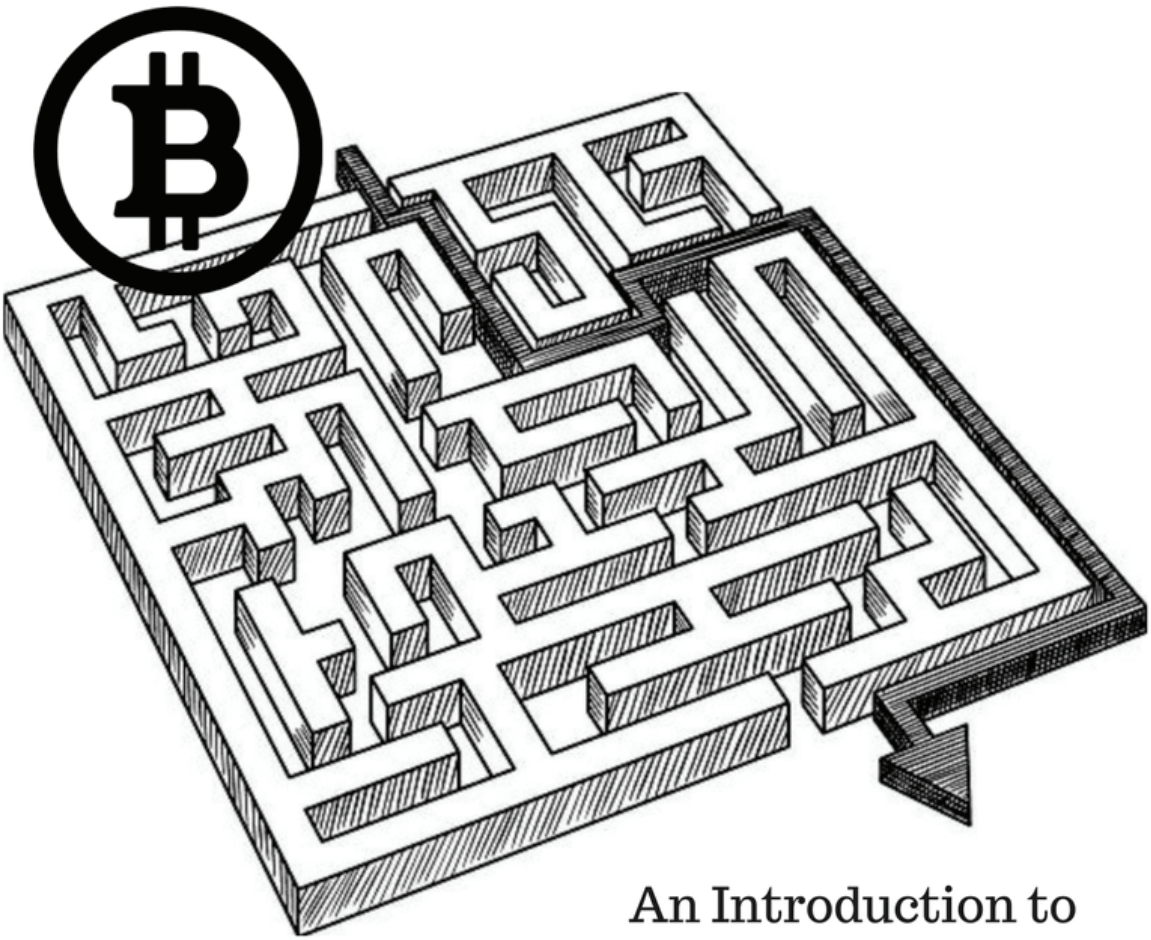


An Introduction to Bitcoin Valuation

Sath Ganesarajah
www.riskmeeting.com

Intrinsic Value

It is worth knowing that the price of a classic car should be between $80k - $90k. Otherwise, we will be left watching the quoted prices be anywhere between $50k - $150k, with no clue when it is a bargain or when it is expensive

Bitcoin

With public opinion on bitcoin reaching levels of near hysteria, we think it has never been more important to understand 'intrinsic' value. We think bitcoin is an extremely dangerous investment, at the moment. The price volatility, lack of widespread education, regulatory uncertainty and most pertinently, the speculative and leveraged money already invested make it difficult to "keep your shirt on."

Nonetheless, we agree that the technologies underlying Bitcoin and, more broadly, 'Cryptoassets', are truly revolutionary. Cryptoassets are set to become a genuine asset class, in fact, at over $500 billion in combined market capitalisation, they arguably already are. This paper aims to introduce some of the key concepts for building an approach to valuation.

While the potential of blockchain is only beginning to be understood, the technology is the product of a broad range of ideas that go back far in history and span many fields of study. Strictly speaking, Bitcoin[1] has been around since 2009[2] but much of the philosophy of the latent mechanics has been lifted almost directly from the pages written by Adam Smith over 200 years ago. 'Self-interest as impetus' and 'competition as regulator' lies at the heart of the technology's ability to self-govern and maintain a decentralised system. The computer science aspects of blockchain date back to the early 1990s[3], around the same time the internet began. For this reason, it is sometimes described as "how the internet should have been."[4] Blockchain combines ideas across cryptography, computer science, mathematics, complexity theory, economics and political science. The intersection of so many sciences, rather than the price volatility, could explain why it is such a provocative and divisive subject.

While the title suggests this paper is specific to bitcoin valuation, the ideas presented apply to any public blockchain. There will need to be a different emphasis on different factors depending on specific features of the blockchain in question and how far along it is in adoption. The analysis

of an Initial Coin Offering (ICO) will look very different to the work involved in the analysis of bitcoin. This is analogous to how appraising a new startup is different to Apple stock.

The precise protocol defined at inception can vary between blockchains and carry great significance. The protocol is what governs the system. A key feature of blockchain technology is the absence of a central authority, with governing power instead distributed across the network. It does not have or need regulation, as decentralisation makes it hard to abuse the system. The system is stable because the protocol is hard coded.

The protocol also determines the economic incentives embedded within the entire system and therefore has a considerable impact on both the sustainability and valuation of its native assets - which are called 'tokens', or bitcoins in our case. Some examples of protocol design decisions include supply schedule of tokens, amount of pre-mined tokens, throughput, and mechanism for miner selection. Any change in these variables may impact the approach taken in token valuation.

We do not think blockchain valuation can be explained in a few pages. This paper therefore only serves as an introduction. We do not spend much time explaining the ins and outs of how blockchain works as plenty of literature on this topic exists in the public domain. Instead we offer insights into the mechanics if and when they pertain to aspects of valuation.

This paper explores building a framework to approach the valuation of fundamentals. Factors outside of the scope of this paper must be considered when completing the thorough analysis required for investing. At the current time this includes understanding market factors and the market ecosystem. Understanding the ecosystem may be the greatest area of research needed that we do not detail in this paper.

Understanding the market ecosystem is important because it is highly unregulated. There currently is little oversight concerning exchanges, wallet providers or token originators. It is far too easy to be exposed to both bankrupt or fraudulent firms. Price manipulation and selective access to markets is also a major concern. Price manipulation is an issue that has beleaguered even the most regulated and advanced markets in the world. Michael Lewis' Flash Boys famously illustrates some of the more sophisticated techniques used in developed markets. In contrast, the Cryptoasset market has nearly zero protections. Many of the exchanges were nothing more than a garage operation only a few years ago[5]. The entire ecosystem is 'a startup' and therefore carries all the same risks as one. The technology might be state of the art but the market itself is not, and therefore there are further factors to consider when making the 'investment' case for bitcoin. We think regulation is inevitable and that will be a strong positive signal for the asset class rather than negative.

Current Approach to Valuation

The conventional method to appraise bitcoin has been to compare it to currency and therefore to measure its use as:

1. A store hold of wealth
2. A medium of exchange

We have not quite understood why this is the convention. If we know it is not a currency, then why are the same metrics we use to measure currency applied?

A more accurate description of Bitcoin is to say it is comparable to a payment network like Visa, MasterCard or PayPal. Further than that, it has embedded some currency-like features.

Traditional payment networks store most of the value created at the centre. They are centralised systems. At the centre is where all personal data is held, and it allows for the central authority to dictate payments rules and charges. The system, by design, allows the central body to extract an inordinate amount of value for themselves.

Bitcoin shares value across its network through its native ‘currency’. Value is apportioned across network users rather than to a central authority - this is the primary tenet of understanding Cryptoasset valuation.

Bitcoins are formally called Tokens. Tokens are artefacts of the blockchain. The blockchain is the generic name of the technology. Since cryptography underlies the technology, the tokens have become popularised as 'Cryptocurrency'. Commentators have interchangeably described tokens as Cryptocurrencies, Cryptoassets, Cryptocommodites and Coins. In this paper, we refer to all tokens as Cryptoassets.

Bitcoins neither generate cash-flows like stock and bonds nor are backed by the trust of government or gold, like currencies. Bitcoins are resource allocators. In bitcoin’s case, the use of the payment network is the resource to be allocated.

No asset class shares the same features as Cryptoassets. Therefore, we cannot superimpose methodologies used to appraise other assets to try to value bitcoin. A new approach is required.

Some History to Establish a Tool Kit

The modern concept of money and wealth creation came about around the 18th century. Up to that point, gold was considered money and 'hoarding' gold was considered how to create wealth. In 1776's *The Wealth of Nations*, Scottish economist and moral philosopher, Adam Smith identified labour and commerce the creators of wealth, and money a vehicle to facilitate the exchange of the products of labour. Labour essentially creates an asset, which is either consumed or exchanged for other assets.

Adam Smith proposed an asset can be valued by 'value in use' and 'value in exchange'[6]. Money itself is an asset, but with nearly always the inverse properties of the assets it was designed to facilitate exchange.

An Inquiry into the Nature and Causes of the
Wealth of Nations
by Adam Smith 1776
Book 1, Chapter 4

The word **value**, it is to be observed, **has two different meanings**, and **sometimes expresses the utility** of some particular object, and **sometimes the power of purchasing other goods** which the possession of that object conveys. The one may be called "**value in use**"; the other, "**value in exchange**." The things which have the greatest value in use have frequently little or no value in exchange; and, on the contrary, those which have the greatest value in exchange have frequently little or no value in use. Nothing is more useful than water: but it will purchase scarce anything; scarce anything can be had in exchange for it. A diamond, on the contrary, has scarce any value in use; but a very great quantity of other goods may frequently be had in exchange for it.

Money measurable by this metric is:

1. Its value in use: as a store of labour, and therefore, wealth
2. Its value in exchange: being an effective and deliberate medium of exchange.

We arrive at the metric we used earlier for understanding currencies.

Adam Smith proceeded to describe the principal components of exchangeable value as rent, labour and profit. These factors combine to determine the effectual supply and demand of a market. Supply and demand, in turn, sets the market price.

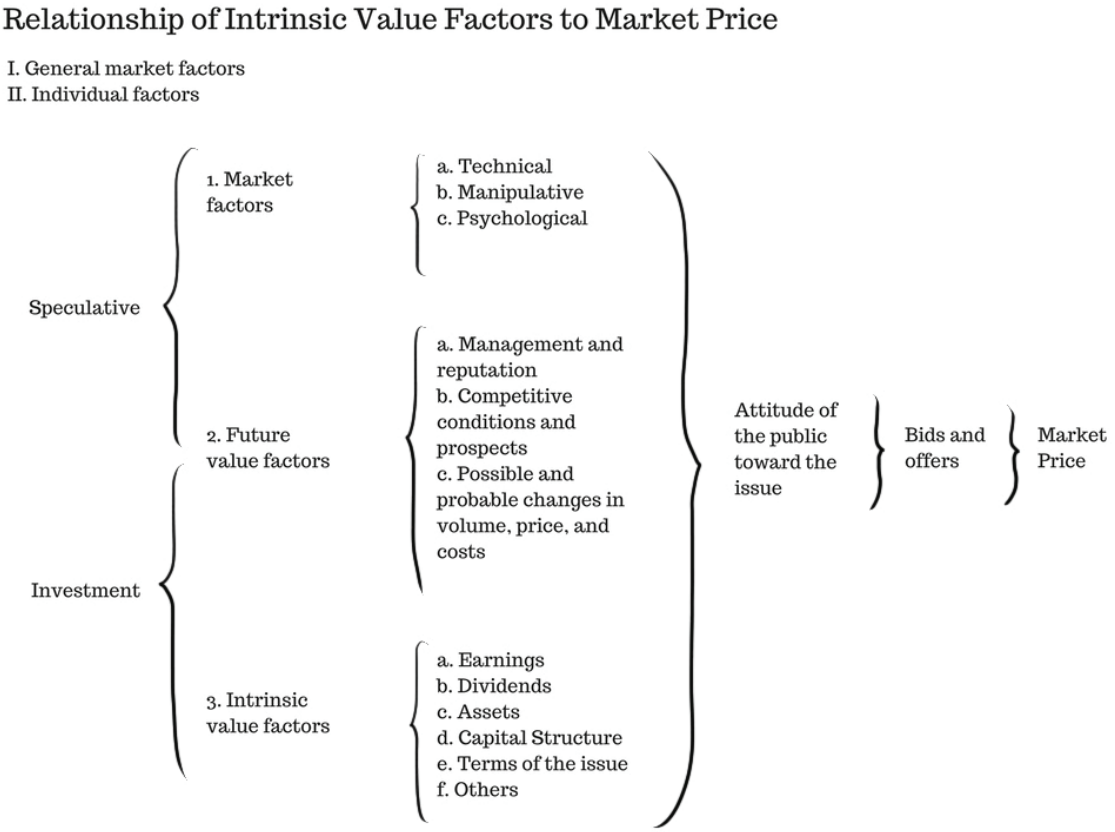
To appraise an investment, we care less about how we arrive at the market price on an aggregate level and more about how the market price relates to building an investment case.

We need a framework that allows us to think about how the market price relates to investment value for the individual.

Prescribing investment analysis is inherently a difficult task because investment decision making comes down to the particular philosophy of the person undertaking the research. What is a good investment for one person might not be for another as investment comes down to, among other things, individual attitudes towards risk and reward.

Investment Analysis from Security Analysis, 1934

In the seminal work, *Security Analysis*, Benjamin Graham and David Dodd suggested a framework that identified the relationship of intrinsic value factors of a company issued security to the market price[7]. If on a macro level, Adam Smith supposed that 'value in exchange' determines the market price and the 'value in use' determines intrinsic value, we can use Graham's framework is a natural progression of the same ideas but on a micro level.



Graham described the effect of the market price, as determined by the factors in the diagram, as both partial and indirect. Partial, because it frequently competes with speculative factors which

can influence price in the opposite direction, and indirect because it acts through people's sentiment and decision.

Graham argues that "the value of each factor is not recorded by an exact mechanism." He was recognising the market as a voting machine rather than a weighing machine. The market functioned 'with countless individuals registering their choice with reason and emotion.'

Intrinsic value is the value justified by the facts. It defines asset quality and is distinct from market quotations which can be driven by psychological excess. Graham admitted intrinsic value is an elusive concept and the point was not to determine an exact number but only to ensure value was adequate. Adequate value is what protects a bond holder from loss or justifies an expected return to a stockholder. Graham wrote anecdotally that one does not need not know someone's precise weight to know they are overweight or know someone's precise age to know they are old enough to vote.

The philosophy underlying Security Analysis is that investment implies expected safety while speculation connotes acknowledged risk. The value of analysis in determining intrinsic value in investment is to leave as little to chance as possible. After all, if everything was left to chance, then there is no value in analysis at all.

Graham does not suggest speculation as an unviable activity or a process that cannot be equally analytically rigorous. Speculation is not 'wrong.' Speculation has become a science in its own right. Quantitative methods to speculate are constantly evolving using cutting-edge mathematics and the latest technological advances. The point, however, is it will always remain the study of chance.

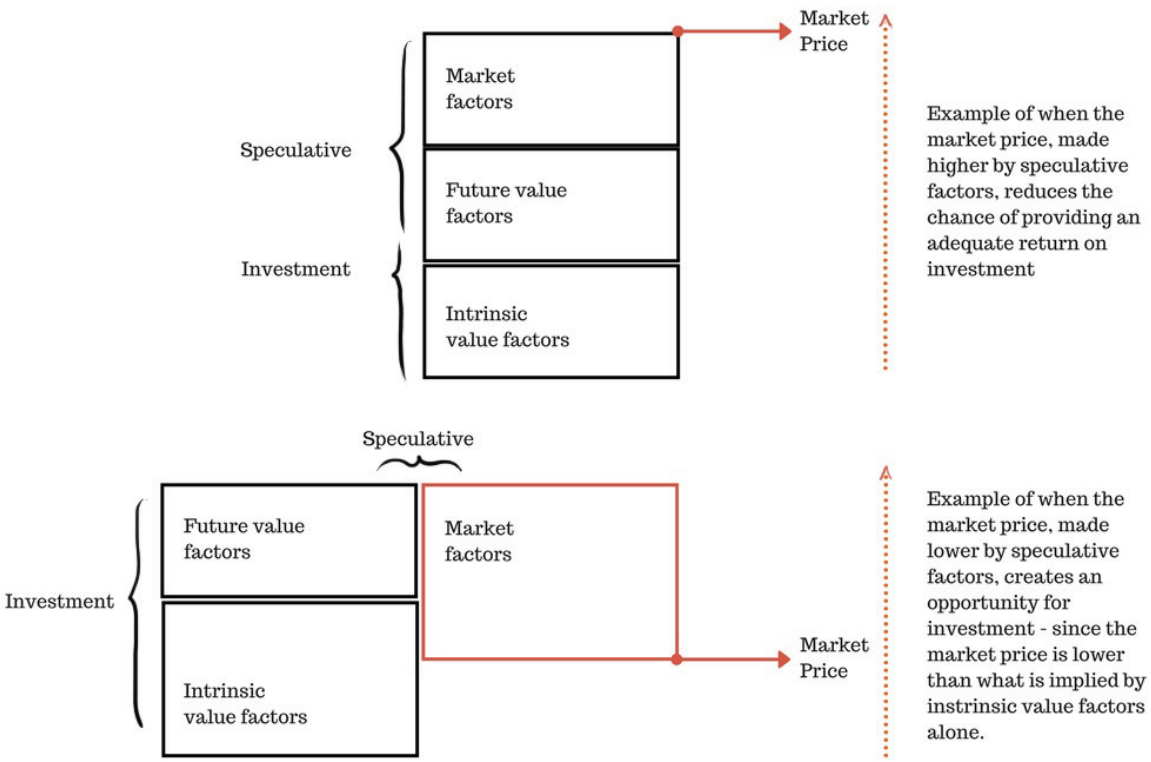
Graham's school of thought dictates a good investment is when the market price is substantially lower than the intrinsic value. This scenario maximises the chance of generating a satisfactory return while providing safety of principal.

Benjamin Graham's Definition of Investment

"An investment operation is one which, upon thorough analysis, promises safety of principal and a satisfactory return. Operations not meeting these requirements are speculative."

The difference between the market price and the intrinsic value is what creates the 'margin of safety'. High-quality assets do not by themselves make great investments. The market price can equally make safe assets risky and risky assets safe. Graham summarises this as, "nearly anything can be cheap and therefore a good investment in one price range and expensive and a bad investment in another price range."

Relationship of Intrinsic Value Factors to Market Price



When the market price has been inflated by speculative value the hard facts that make up intrinsic value no longer provide a source of protection. Therefore it does not qualify as a good investment - even if it might continue to make sense for a speculator.

Investing is about safety. Speculation is about risk.

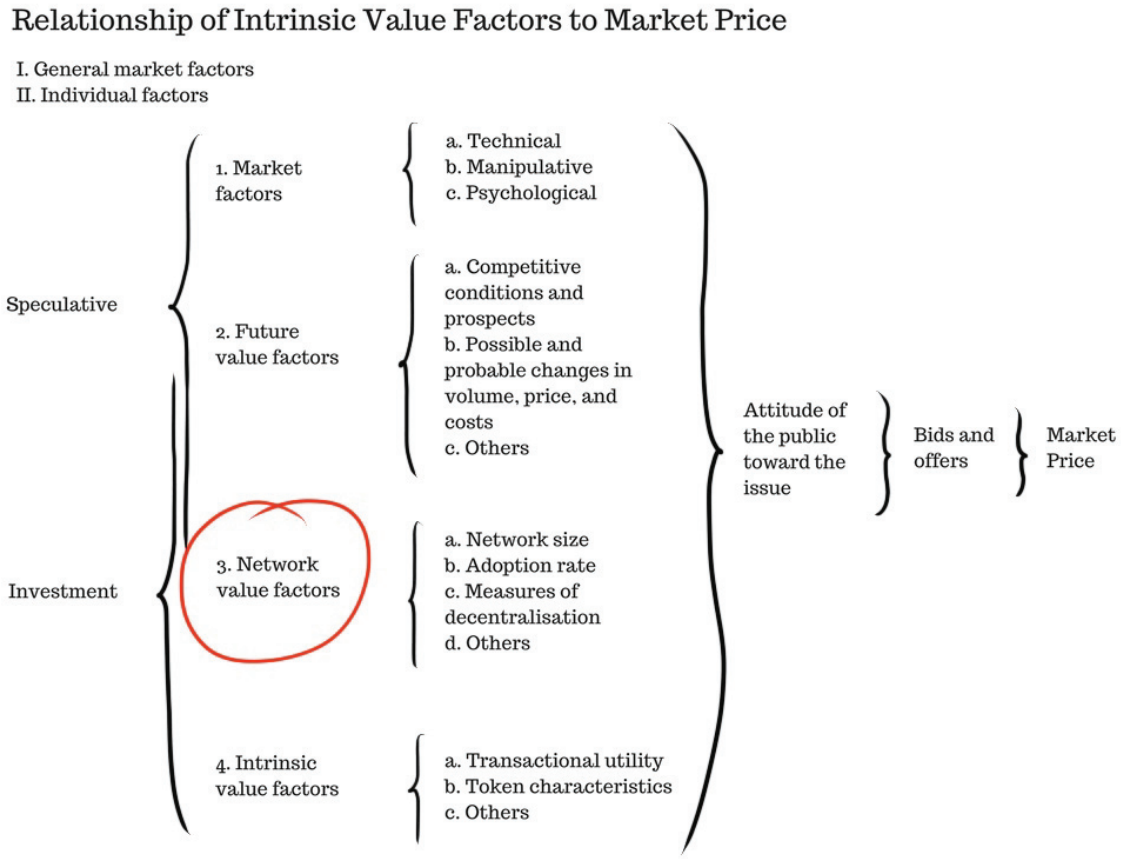
We adopt the philosophies of Benjamin Graham when considering how to extend the asset appraisal framework. We prize margin of safety and ascertaining minimum value. By appraising investments with safety in mind, the analysis should logically be fit for anyone regardless of their attitude towards risk.

An Introduction to Bitcoin Valuation

Cryptoassets have an inherent economic feature that makes them unlike any other asset that exists today. It is this feature drives it's supporters grandiose claims that the technology is a revolution to current economic and business models.

As the blockchain network increases in size, the value created by the network is distributed across the network's native assets which are the tokens known as Cryptoassets. Network Value is apportioned, in egalitarian fashion, across token holders. This feature is exceptionally compelling; as users increase, there is an exponential increase in value for individual asset holders.

We augment Graham's framework to include this feature as an additional component.



Network Value

Metcalfe's Law[8] states that the value of a network is proportional to the square of the number of users of the system: n^2.

Metcalfe's law
From Wikipedia, the free encyclopedia

The law has often been illustrated using the example of fax machines: a single fax machine is useless, but the value of every fax machine increases with the total number of fax machines in the network, because the total number of people with whom each user may send and receive documents increases. Likewise, in social networks, the greater number of users with the service, the more valuable the service becomes to the community.

Over the last few years, we have seen the network effect displayed with incredible potency. The platform revolution was built entirely on the power of networks. Some of the largest companies in the world, Uber, Facebook, Google, Netflix, capitalise on the network value they create and harness. These formidable enterprises, built on top of internet technology, have been powered by the rapid and centralised collection of consumer data. The sizeable data they hold within their respective networks is the most prominent source of their value.

The top internet companies have essentially created a digital asset by harvesting data. Not only are the digital assets why these companies have multi-billion dollar valuations, it is also why the internet itself is increasingly becoming controlled by them.

Until now, a way to create robust networks where network value can be distributed equally across the users has not existed. In effect, value distribution is the 'problem' blockchain solves by way of a decentralised system.

The Fairground without a box office.

Imagine a fairground that requires tokens for access and use of all the rides, but there are only twenty-one tokens. Only one person can use any one token, at any time. Initially, all the tokens are left at the front gate.

If there are only twenty-one people who want access to the fairground, then the price of the token is actually zero. The twenty-one free tokens supplied has met the demand of the twenty-one people.

Now imagine someone new arrives at the front gate and wants access to the fairground. The price of the token is now equal to the lowest price at which any of the original twenty-one holders will sell.

Let's assume one of the original holders sells the token for $1. The seller now exits the fairground, and the buyer takes the sellers place inside. If we assume that the seller currently has no use left for the fairground and will never return, what is now the price of the tokens?

It should, in theory, be zero. We are back to the state of twenty-one tokens having exhausted the marginal demand.

Now imagine one-million people are waiting outside the fairground wanting access. Transactions can now happen very frequently as the token prices rise and fall depending on the effectual supply of sellers (who are inside the fairground) and the effectual demand of the abundant buyers (who are outside of the fairground).

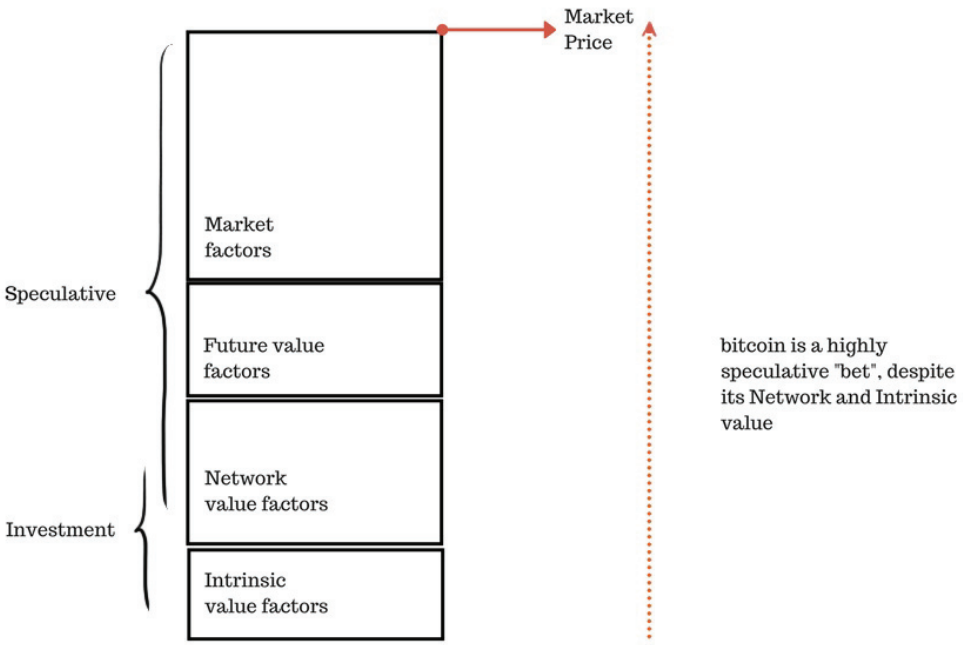
Note that everyone who holds tokens shares the appreciation and depreciation in the market price. The value is both determined by the market and distributed among token holders.

This is a stylised illustration of some of the economic aspects of a decentralised system. It shows how the value created by demand for using the fairground becomes shared by all current users, rather than a central authority - usually 'the box office'.

In a centralised system, access to the fairground would be via the box office at the entrance. The box office can set the admission policy, governing rules of the park and the prices. The box office can create new tokens and even issue them with expiries and non-transferability, for example.

Network Value adds to the investment and speculative case. If everyone on the network is a speculator, then the Network Value is still something positive even if the nature of the network is speculative. For an investor, what is preferred is a network made up of users deriving real utility from it. Without this, the long term investment case for any blockchain is questionable. Currently we believe this is the fundamental difficulty when making an investment case on most Cryptoassets. However, we are confident the landscape for investment will change as the adoption of the technology becomes more widespread.

Relationship of bitcoin's Value Factors to Market Price



The Intrinsic Value is the study of what attracts users and miners to the network.

The Network Value is a study of the adoption rate and sustainability of the network.

By combining these factors, we can arrive at a better understanding of the minimum value of a Cryptoasset. Comparing this to the market price gives us our margin of safety concerning investment.

Aspects of Intrinsic Value

Usefulness of the Network

What is the network for? For Bitcoin, it is a payment network. It is 'instant' in the sense that it is direct - peer to peer. Payments are not subject to costs and lead times associated with approval from a trusted third party. While cryptocurrencies have come under fire for being only useful for criminal activities, we see at least three categories of transactions which require modernisation of current payment systems.

1. Cross-border transactions generate around $300 billion in revenues for banks[9]. When a financial institution carries out a transaction on behalf of another (who is unable to complete the transaction themselves as they have no local presence), this is called 'correspondent banking'. Correspondent banking represents around 20 percent of all transactions in the payments industry, yet they generate around 50 percent of all transaction-related revenues. While this highlights the costs associated with such dealings, what is even more striking is that correspondent banking has remained largely the same, with little innovation, since the mid-18th century, .

2. The $500 billion remittances market[10] could also benefit from reduced costs and innovation in the payments industry. The global average cost is 7.5% of the money sent but can be as high as 20% depending on the country. For many emerging market countries, remittances are a sizeable source of foreign financing and have a significant impact on development .

3. Around 2.5 billion people in the world still lack access to formal banking services[11]. For the unbanked, mobile phones are increasingly being used to increase access to low-cost financial services: this includes payments, insurance, credit and savings. However, mobile money has struggled to reach scale due to low levels of investment, lack of industry collaboration, and regulatory barriers. Innovation is again urgently required.

When researching any blockchain project, the white paper is usually the first place to start. Outside of the technical standards employed, it should detail the precise problem it is solving.

A 'Back of Envelope' Measure of Utility Value

For a quick measure of network utility value, we can calculate a straightforward ratio. We simply divide the total market capitalisation of blockchain tokens by the number of transactions over a period.

Seeing how this ratio evolves allows us to see if the market capitalisation, and therefore the value of all tokens, is growing faster than the number of transactions. Since the purpose of the network is facilitating transactions, and not to grow market capital, this gives some indication of whether coins have become artificially inflated.

It is essential the network has turnover rather than market capitalisation. Low turnover and high market cap (and therefore high ratio), indicates the amount of 'hoarding' in the network. It means the network is less useful and is made up of mostly 'buy and hold' users - i.e. speculators.

Tokens as Resource Allocators

The Bitcoin blockchain is commonly referred to as Bitcoin (upper case B)[12]. Bitcoin represents the underlying network that carries the shared data and protocol.

Users access and transfer value on the blockchain using tokens. The token is called bitcoin (lower case b). These tokens are what gets quoted with a market price. It is the network's native asset and what a user 'owns'. Unlike stocks and bonds, bitcoins do not have cash flows. It is a resource allocator.

Brief Digression, Gold

Metals, specifically gold were the original resource allocators of labour. Gold is sometimes described as the 'original money' or 'one true money'[13]. Historically gold was seen as the ultimate resource allocator due to its atomic qualities, that allow it to stand the test of time, and its finite quantity.

It becomes difficult to allocate variable resources with an allocator that is also a variable. The resource allocator should be fixed, or the resource to be allocated should be fixed.

Since money was created to allocate labour, which is an inherently tricky variable to measure, money, in theory, should be a set quantity. This concept is one of the most prominent problems people have with current fiat money systems. We have given central monetary authorities the power to control both the worth of money and labour.

In many ways, gold should still be the measure of all value, but it's physical properties, once its virtue, have made this impractical for the connected and digital world in which we live. However, for the people who create money, central banks, it has arguably never lost its status. We only need to study global central bank reserve holdings and buying patterns to see this.

Gold's physical nature and now limited exposure to the ordinary person make it ineffective as a general yardstick for value. For this reason, bitcoin is seen as a potential way of measuring value in the future.

The fixed quantity of tokens makes bitcoin excellent for allocation of resources. We know there are twenty-one million bitcoins or sixteen quadrillion satoshi (the minimum denomination of bitcoin). The resource is access to the payment network. Bitcoin is digital and highly portable, and ingrained in its ideology is transparency of verified data. Advocates of bitcoin argue that in

the future it may become far easier to understand the value of dollars, sterling, euros and barrels, in terms of bitcoins than in terms of each other (variables against variables).

Token Characteristics

Tokens will have different characteristics depending on the blockchain to which they belong[14]. The use case of the blockchain will determine the token characteristics. Tokens may provide access to a digital service, the right to contribute work to a decentralised organisation or a combination of both. Tokens can also be used to represent a physical asset digitally.

Users

The unique number of users of the network, and who they are, is an essential part of utility and intrinsic value. No payment system is useful if the people we need to pay are not on it.

Quantifying Intrinsic Value

The Bitcoin blockchain is a two-sided system. There are users and miners. Both sides have a quantifiable aspect of intrinsic value that encourages them to be part of the network.

Intrinsic Value for Users

One approach to quantifying the utility of the network is to consider the cost of the alternative.

Suppose a business needs to send $100 million to a Sri Lankan supplier within the next 90 minutes or they could miss out on a profit opportunity of $20 million. The sensitivity of timing may be related to perishable goods, for instance.

The business calls its bank, but the bank won't immediately arrange the transfer because there are due diligence checks to run, credit costs involved and more pertinently, the bank is closed on a Sunday.

Suppose the business finds some intermediary that will arrange the transfer, but they will charge 10% of the notional amount to be sent. The cost is therefore $10 million.

Now consider Bitcoin. The business can buy $100 million worth of bitcoins and send the coins across the network to the supplier. The supplier will then sell the coins for dollars. The dollar amount will be $100 million +/- the exchange rate fluctuation during the transaction, plus transaction fees. What is this exchange rate risk worth? There are also transaction fees involved, but on the blockchain, fees are a function of data size rather than the notional transfer size. As

long as these costs combined is less than $10 million, then the Bitcoin network is useful for this company.

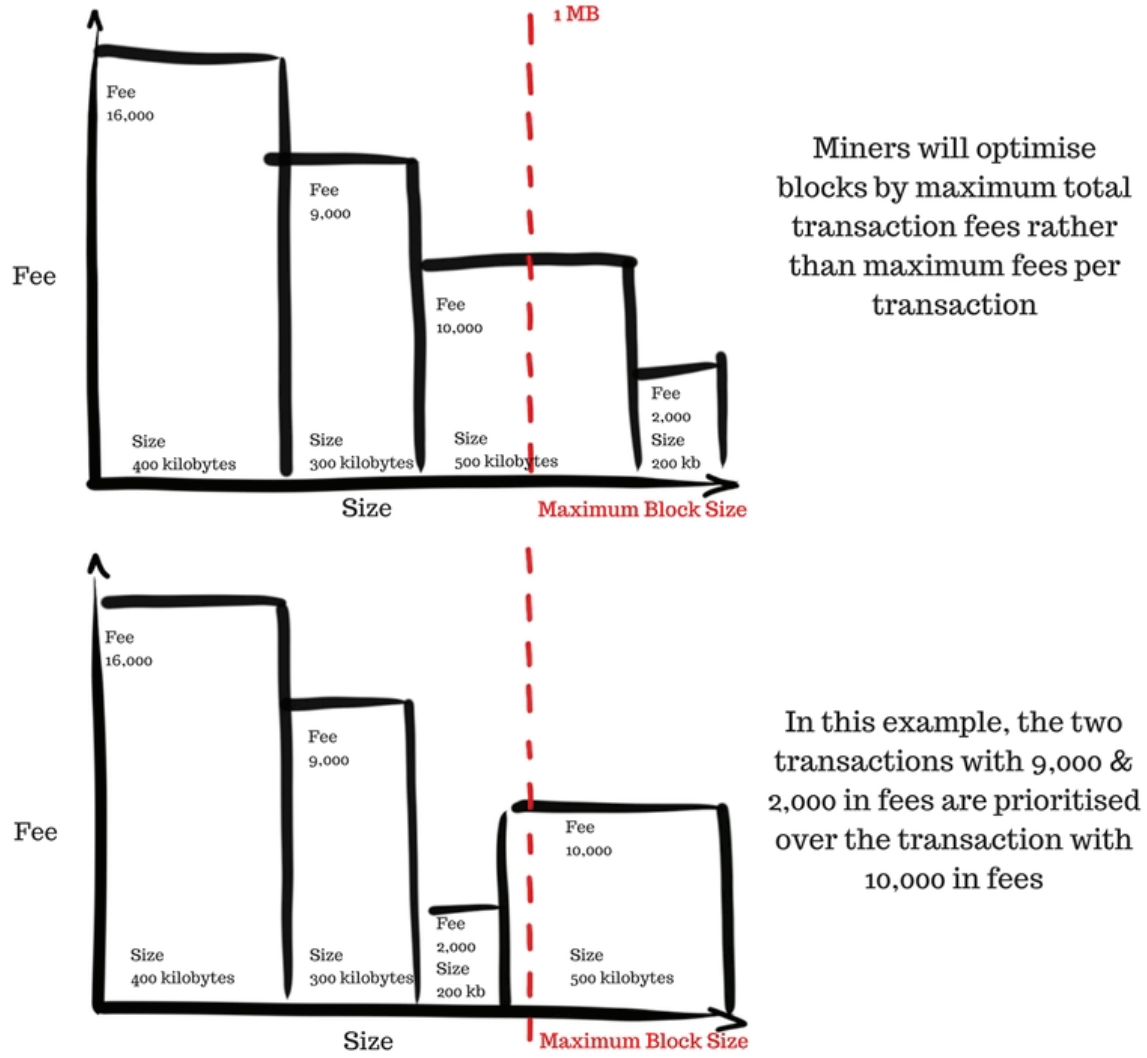
Understanding Transaction Fees

The cost of using the network, for the user, is the time it takes for the transaction to be approved

Transactions on the Bitcoin network are not instant. For transactions to be completed (approved), it needs to be collected into a block, validated, mined, and then added to the blockchain. Because of the way blockchain prevents double spending, a user might have to wait for six blocks - which can take up to one hour - for approval[15]. If there are a large number of transactions that require processing at the same time, this will cause congestion and users will have to wait their turn. Therefore the wait at busier times could be considerably longer than one hour depending on traffic.

To get around this problem, users can provide the miners with a transaction fee. Transaction fees are the de facto way orders are prioritised in the system[16]. The simple logic being that miners will attempt to add the blocks in order of those that generate them the most income. The fee set by users is what incentivise miners on the network to mine.

Unlike in traditional payment systems where the transaction fee is a function of the value of the transfer, on Bitcoin the fee depends on the size of the transaction data (in bytes)[17]. There are a few nuances. The Bitcoin protocol dictates that the maximum block size is 1 Megabyte (MB, which is 1,000,000 bytes), and only complete transactions can be included in a block. This means the transaction with the highest transaction fee does not always get into the next block. Given the transaction size in bytes will vary, miners optimise for the maximum combined fees possible from as many transactions that can fit into the next 1MB block.



The Bitcoin protocol limits block creation to one block every 10 minutes on average. Knowing this, we can start to do some analysis on transaction congestion.

For simplicity's sake, let us assume the average transaction size is 500 bytes and the variance is low. Since we know that the block size limit is 1MB, the maximum transactions per block every 10 minutes, is around 2,000. We can combine this information with data from the blockchain ledger to understand network traffic. The ledger tells us the number of transactions that have recently been processed and the transaction fees paid. From this we can calculate the expected wait time as well as deduce the transaction fee required to fast track to the front of the queue[18].

Since the user sets the transaction fee, a rational user would set the fee equal to their expected cost (or 'transactional utility' foregone) in waiting for the transaction to be approved.

To provide some context, Bitcoin transaction fees, in dollar terms, for prioritisation (10 minutes maximum expected wait time for processing) have recently varied between $10 and $35. Low priority transaction fees meanwhile, could be as low as $3.

Since transaction fees are the precise value being paid by users to use the network, this is the most important aspect of intrinsic value.

Intrinsic Value for Miners

We see much written about the 'wasted resources' of the blockchain due to electricity costs associated with mining. The Bitcoin network's mining costs are well known and estimated to be around $3.4 million a day (or the equivalent of electricity supply to 600,000 households in the US)[19]; 'all for the sake of producing coins which derive their entire value from market-driven speculation' - or so the argument goes. This analysis widely misses the mark.

It is important to remember the principle purpose of mining is to produce a block, not the coin. Verifying transactions and producing blocks is fundamental to maintaining the blockchain infrastructure. It is real computational work and what keeps the network intact. Because miners have real world direct costs such as hardware and electricity, they require an incentive to provide this service. In the long run, the incentive will become transaction fees alone. However, the Bitcoin protocol contains a design feature which adds the incentive of coin rewards over an initial 'growth' period (125 years) of the blockchain. This clever design feature simultaneously achieves a number of objectives including the following:

Firstly, the coin reward period ensures system stability during the network adoption phase. The mining network is essential to the security and stability of the blockchain. In the early stages of the blockchain's adoption, there may not be enough transactions to generate fees for mining to be worthwhile - since mining activity incurs financial costs. All networks start from only a few users. For transaction volumes to grow, the network must grow. However, this growth will not be possible without miners. The network needs to grow while also instantaneously providing enough transaction fees to cover mining costs. We have described a classic 'chicken and egg' problem. The coin reward period solves this problem by rewarding miners with coins. The value of the coins increase as the value of the network increases and therefore permeates growth of the entire ecosystem.

Secondly, the coin distribution over time also solves the problem of having too many of the finite coins appropriated to the early adopters. Early adopters would, therefore, have inordinate 'power' over the network. For instance, giving all the coins to the first miner would allow this miner to dictate the price.

We analyse transaction fees as the exclusive source mining revenue to understand the long-term sustainability of the Bitcoin blockchain.

Intrinsic Value for Miners in the Long-Run

We established earlier the mining revenue is the transaction fee paid by the users, which is in turn determined by the user's cost. The user's cost is the time for a transaction to be approved.

The time for a transaction to be approved is a function of the miner community's ability to make enough revenue to cover mining costs.

Mining Costs

The miner revenues are denominated in bitcoins while the mining costs are denominated in the local currency of the miner. A miner in the US will have dollar costs, and a miner in China will incur costs in Chinese Yuan.

The miner first needs to buy the computer hardware, which is currently estimated to be $2,000 for one 'rig'[20]. The hardware cost is recurring as it can be assumed to need replacing every 1-2 years. Electricity consumption is the other significant input for a mining operation. Electricity cost will vary depending on local factors: country, region, energy provider.

In the US the marginal cost of bitcoin mining is estimated between $2,000 - $5,000. That is the average cost of hardware and electricity used in producing the next block - and therefore the cost of 10 minutes mining activity on Bitcoin.

Since costs vary geographically, so will expected profit. Chinese miners have a competitive advantage in electricity costs. The Bitcoin mining network has a large concentration in China for this reason.

It is important to remember that miner selection, which drives revenue, is entirely random. Miner selection is the process which dictates which miner will add the next block and therefore collect the transaction fees. So while the number of computers a miner has does increase their chances of being chosen, revenue will always be an 'expected value' rather than guaranteed income. Costs are certain, while revenues are not.

Mining Revenue

We can estimate the probability of a miner being chosen to add the next block as:

The one winning computation out of the total number of calculations the network runs in a 10 minute period.

By multiplying these odds with the expected transaction fees, we arrive at expected revenue, or what is called expected value in statistics.

We know from earlier, the transaction fees are determined by the wait time (the congestion).

The congestion in the system is a function of the block size limit, size of transactions (in bytes), the number of transactions at a given time, and the number of blocks permitted within in a time frame. The average block production time is determined by an algorithm hardcoded in the protocol, which in Bitcoin's case results in 10 minutes on average.

Continuing from the earlier example, with the average transaction size being 500 bytes, we know that on average the maximum number of transactions will be around 2,000 for each 10 minute period. If we assume the network is generally running at maximum traffic and the average transaction fee is $10, the total fees in each block will be approximately $20,000 (2,000 transactions on average, 10$ per transaction).

Over each 10 minute period the transaction fee will, therefore, be very low when far fewer than 2,000 transactions are waiting to be processed and the fee will start to increase once we are ‘at limit’. The limit is the point at which wait times begin for users, and they will necessarily bid for real estate on the next block. The bidding process is what will drive fees higher. So in our example, if the number of transactions exceed well past 2,000, the average transaction fees can be expected to climb significantly higher than $10.

The wait time is set by the mining community because the system will not mine at a loss. If there are not enough transaction fees, miners stop mining or exit the system such that it slows the system down and ‘congestion’ returns. Therefore transaction fees will always maintain a level where mining will continue.

The Bitcoin protocol's ability set the average block creation time is by way of an algorithm that changes mining ‘difficulty’. The difficulty level is based on moving averages of block production frequency. This difficulty level can run in both directions. The difficulty increases if there are many miners but also falls as computing power leaves the system. The falling difficulty level simultaneously increases expected revenue, creating an automatic stabiliser against too many miners leaving the system.

Calculating Expected Mining Revenue

Expected Revenue = average transaction fees per block x probability of being the chosen miner that creates the next block

the probability = one chance out of total computations of the network

$$\text{Expected Revenue} = \text{average transaction fees per block} \times \frac{1}{\text{total network computations per 10 minutes average}}$$

10 minutes average to create next block

Bitcoin Example.

$$\text{Expected Revenue} = \$20{,}000 \times \frac{1}{\text{total network computations per 10 minutes average}}$$

$$= \$20{,}000 \times \frac{1}{600 \times 20{,}000{,}000 \times 10\text{^}12}$$

600 seconds x Terahash of Bitcoin network per second

= $$0.00000000000000000167 per 10 minutes

Finding Equilibrium & Zero Profits

The users determine the transaction fees and the miners determine the wait time. The system is a delicate balancing act between the cost for users and the opportunity for miners. This balance, through the many intricate in-built mechanisms, is what creates a system that is forever trying to remain in a beautiful equilibrium. The beautiful equilibrium is what makes the system stable, secure and a veritable marvel.

Economic theory suggests that the mining market is in 'perfect competition'. Perfect competition is when there are low barriers to entry and many competitors. Because the mining network is open and permission-less, the expected profit of the system as a whole is zero[21]. If there were extraordinary profits from mining, new miners would join the network and erode, through competition, the system's earnings back to zero. The number of miners and computing power in the system will increase and decrease based on potential profit. However, this does not mean individual miners do not profit. Cost structures and strategies will differ between miners. So while the system in aggregate should not make extraordinary profits, individual miners may.

We can model mining costs against the total transaction fees of the system to understand if the blockchain is sustainable.

Modelling

While many of the numbers used in protocol features are arbitrary (10 minutes, 1MB), the consequences are not. The growth of the network is almost like a living organism. Much of the beautiful equilibrium we described earlier is a consequence of the protocol's initial settings.

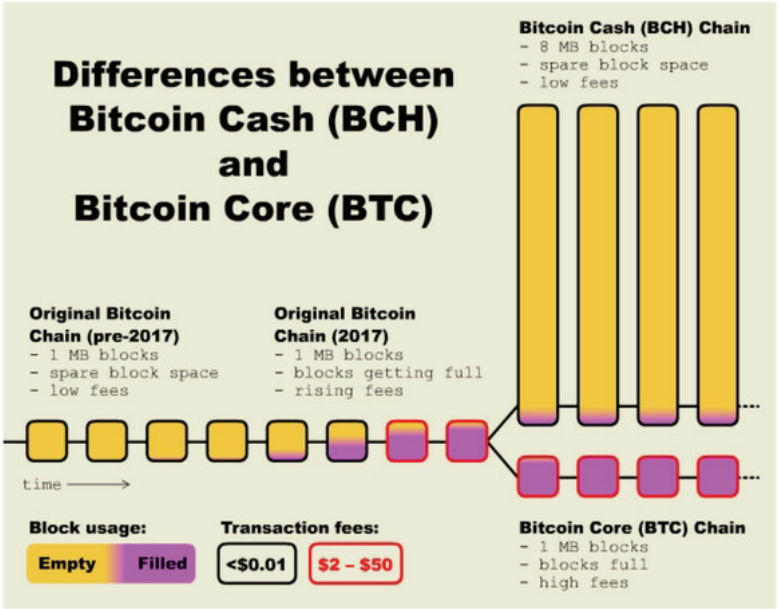
Modelling will require considering these settings together with the external environment - the process of the blockchain's adoption in society.

We see throughput as the most crucial aspect of network sustainability. The throughput is directly a consequence of the protocol settings: the average block creation time and the maximum size of a block - 10 minutes and 1MB in Bitcoin's case. For the system to function properly, the throughput needs to deliver adequate congestion to generate enough transaction fees to cover the mining costs and therefore maintain the overall infrastructure. If there are not enough transactions, then there is no delay in creating a block and transaction fees fall. If fees drop below mining costs, miners start to exit the system. If a sufficiently large number of miners exit the system, the entire network can become unstable or compromised.

Modelling will help highlight the consequences of protocol differences between blockchains.

'Bitcoin Cash' was the creation of a new blockchain by what is called a hard fork. A hard fork is when a blockchain permanently splinters off from the 'parent' blockchain to become independent. The Bitcoin community, long divided on the issue of scalability, reached a consensus to create a user activated fork. Users could choose between remaining on the existing Bitcoin blockchain or migrate to Bitcoin Cash. The motive of Bitcoin Cash was to improve throughput and reduce transaction fees. It did so by making a change to the protocol to increase the block size limit to 8MB from 1MB, making the 'pipes wider' by allowing eight times as many transactions per block. While at first glance this seems like a logical way to solve scalability issues, we know from our earlier discussion that it may, in fact, make the system unstable if transaction fees fall too low in the long-run.

Advocates of 'Bitcoin Cash' highlight how transaction fees fall under the 8MB block - without maybe consideration that in the long run transaction fees are an essential part of maintaining equilibrium of user/miner participation



source: https://twitter.com/Bitcoin

Intrinsic Value for Miners Under Coin Reward Scheme

We have described how miners provide the infrastructure of the blockchain, while also bearing the costs of mining. The supply schedule of coins is a clever design feature to support the network in its growing stages, where transaction fees alone may not sufficiently fund the infrastructure.

The economics during the coin reward stage for miners will differ from the economics in the long run. Understanding the short-run is also crucial for valuation. We use the same methodology from earlier, but we now factor in the market price of bitcoin into expected mining revenue. The expected revenue will be the total amount of transaction fees in the next block plus the market price of the coin.

Calculating Expected Mining Revenue, with coin reward scheme

Expected Revenue = (average transaction fees per block + market price of coin reward) x probability of being the chosen miner that creates the next block

Bitcoin Example.

$$\text{Expected Revenue} = (\$20{,}000 + \$10{,}000) \times \frac{1}{\text{total network computations per 10 minutes average}}$$

$$= \$30{,}000 \times \frac{1}{600 \times 20{,}000{,}000 \times 10\text{^}12}$$

$$= \$0.00000000000000000250 \text{ per 10 minutes}$$

The coin reward stage of the network needs to be modelled together with the longer term scenario.

Exercise Extreme Caution When Looking at New Cryptoassets (ICOs)

The Cryptoasset market is highly unregulated[22]. The most seemingly obvious yet easily overlooked step when looking at new Cryptoassets is determining whether it is a fraud. It is incredibly easy for criminals to set up fake white papers, companies, websites and generate a community following. The danger of Crypto 'boiler rooms'[23] is very real and the lack of regulation means there is no recourse.

Initial Coin Offering (ICO) is the name given to the process in which a company raises money to develop or continue to develop a decentralised project that will utilise Cryptoassets. The acronym deliberately sounds similar to IPO (Initial Public Offering), which is the process in which companies raise money when they sell shares in their business.

ICOs are a hazardous area of investment since there is no certainty that the coin or technology will have the sufficient community support to grow. In many cases the coins provide access to a service that does not exist yet. There is a risk these projects may never get finished.

The attraction of the ICO market is obvious for both participants (buyers) and issuers (sellers). For the seller, they raise money quickly, efficiently and even fraudulently. The current hype around the technology has made this all the more easy. For the buyers, ICOs offer a market with opportunities similar to those found in the venture capital (VC) world but with the added benefit of secondary trading: the ability to both buy and sell these opportunities frequently and quickly. If we consider typical VC returns are expected to be 20%[24], ICOs are also turbocharged by the network value effect. It may be more accurate to describe ICOs as penny stocks on rocket fuel.

Network value, which we discuss next, is what can allow Cryptoassets of even fraudulent companies to perform well. Network value can make a Cryptoasset that will never be fit for investment remain lucrative for speculation. A speculator can buy a coin with a market price driven purely by network growth and sell it before its zero intrinsic value becomes apparent.

Network Value

Network value is the defining feature of the asset class. The assets are a finite number of blockchain tokens (bitcoins) that allocates access to a network (the Bitcoin payment network). As the network grows, because tokens are limited, any increase in demand and access to the network will be reflected by an incremental increase in value across all tokens. This is the unique and extraordinary feature of the Cryptoasset asset class.

The features of the network determine how the system grows and remains sustainable. It also determines how the native asset becomes valuable.

There Are No Coins and There Is No Database

On closer examination of the technology it becomes apparent there are in fact no coins or a public database with account balances. The public database and coins are implied artefacts generated by the way the system works. Most blockchain explainers focus on these aspects to avoid talking in abstract terms. The one thing that actually exists are transactions. The immutable list of all these transactions in the history of a blockchain is called a ledger.

The public database is implied from the transaction history, and the 'coins' are differences between inputs and outputs that make up the transactions. It is the transactions or the 'flow' rather than the 'stock' that gives the system its value. Without users, there are no transactions, and without miners, there are no blocks. We established earlier how utility and economic incentives bring together these two sides to the blockchain. We now consider how the network grows and becomes sustainable. Understanding the scaffolding that allows network value to flourish is the most vital aspect of valuation.

The Allure is also the Security

For the network to be reliable and secure the number of miners needs to be large. A large number of miners ensures consistent service even when some mining nodes occasionally fail or exit the system. A large aggregate computational power also ensures the system is prohibitively expensive to hack, as it would require an equal amount of computational resources to be acquired to overtake the system. This is described as the '51% attack'[25].

In order to compromise the blockchain, an attacker would need to own over half the system's processing power. Only with 51% can an attacker upend the miner selection process and control which blocks become valid. For this reason, each miner needs to remain small. A large number of small miners describes a highly decentralised network or what we described earlier as perfect competition in economics.

Decentralisation is the virtue of the technology, but it is also the system's security. Decentralisation is required to ensure protection against attackers. An essential feature of the

technology is to make sure nodes are independent. While we know “one CPU is one vote”[26], it is crucial to understand the concentration of CPUs among mining entities.

Studying Network Value involves measuring network size, adoption and measures of decentralisation.

Aspects of Network Valuation

Hash Rate

A computation is expressed as a hash. The hash rate represents the number of computations performed per second when mining a block. One Terahash represents one trillion hashes. We can use hash rates to measure the combined processing power dedicated to the network. We expect a viable network to have a hash rate that is high and trending higher. If the hash rate is trending lower, it means processing power is leaving the network.

The hash rate is directly affected by the protocol specifications. The Bitcoin protocol is designed to ensure blocks are only created, on average, every 10 minutes. The algorithm within the protocol achieves this by modifying the difficulty level of the computations, in what is called the 'proof of work'. Therefore the difficulty level increases in line with an increase in processing power. Conversely, if processing power starts to trend down, the proof of work becomes easier for those remaining on the network. This elegant design feature ensures ‘brute force’ cannot be used to compromise the system. Measuring hash rates over time can be used to monitor the evolution of blockchain activity, security and participation.

Proof of Work Difficulty History

The time series of the difficulty of proof of work can provide additional insight. It allows us to see the efficiency of deployed computing resources. Hash power can vary from rig to rig, as different computers use different computer processing chips. Since rig prices and electricity costs differ from country to country, combining difficulty level with hash rates, we can imply the efficiency of mining. If the difficulty level is going up faster than the hash power, that translates to cost efficiencies for miners. Costs efficiencies allow miners to stay in business and remain on the network longer. If hash power is going up faster than the difficulty level, then computing resources and associated costs may outstrip the revenue opportunity or usefulness to be on the network.

Not all blockchains use proof of work in the block creation process. Ethereum is famously considering moving to a 'proof of stake' protocol[27]. Protocol changes such as this will impact valuation.

Cash Value of the Mining Network’s Physical Assets

A bitcoin mining unit capable of 14 Terahash/second costs roughly $2,000[28]. We can use this cost and the associated hash rate to estimate the dollar value of the combined computing power dedicated to the network.

To hack the network, an attacker would need to buy the entire size of the network, to gain 50% of computing power. When a single entity controls over half the system, it can create blocks on the blockchain faster than other miners. The attacker can create blocks with invalid or fraudulent transactions, while still maintaining the longest chain. The blockchain always assumes that the longest chain is the valid chain. This type of hack is the single biggest security risk to any blockchain and what we described earlier as the '51% attack'.

The 51% attack highlights how, the larger the mining network and the more physical assets associated with it, the more secure it is. The total physical asset value associated with the bitcoin network can be estimated to be $1.5 billion.

Number of Nodes & Geographic Distribution

The number of unique users is an important aspect of both utility value and network value. Nodes are not made equally. Most of the nodes on the Bitcoin network are in the US but most of the computing power is in China[29].

Having a high concentration of nodes in one country increases 'country risk' for the network. The network can become sensitive to government policy. For example, China's crackdown on mining could potentially disrupt the network. Commentators attribute the large mining network in China to the country's competitive mining cost advantage[30]. Economics dictate that if miners in China began to exit, the second lowest cost country would likely replace the Chinese miners on the network.

From a user standpoint, if the US outlawed using the bitcoin payment network, that would potentially be even more disruptive since it undermines the usefulness of the network.

While economic competition will always try to protect the system from disruption, disruption of large enough size may be enough to effect the viability of the entire network.

Quantitative Measures of Decentralisation

There are a number quantitative measures of decentralisation that can be explored across various disciplines, such as the study of market structure in economics, the Herfindahl-Hirschman index, the Gini Coefficient, the Lorenz Curve, and metrics used in the analysis of complex systems.

Developer Community & Support

The most crucial aspect of building a network is having the appropriate scaffolding. Since Cryptoassets are open source projects, the developer community is a vital part of ensuring the platform's success. The protocol design process needs to foster collaborative work between both miners and developers. Elements such as the programming language used and social media

attention are essential aspects of creating a community that will drive the network's adoption. Bitcoin famously does not have a Turing Complete programming language[31], likely due to extendability not being a design consideration. Ethereum, on the other hand, is designed to work like an operating system for decentralised applications, and therefore a Turing Complete programming language was essential[32].

Understanding the interoperability of the technology gives insight into how intellectually invested communities are and how easy it is for new contributors to invest in the network. Interoperability is an integral part of growing a foundation for new technologies. If there have been notable forks on the blockchain, as there has been with Bitcoin, then understanding why it happened and what determines the popularity of each chain, also provides insight[33].

Token Issuance Model

Divisibility means the number of finite tokens set at blockchain inception is arbitrary. However, distribution and the number of tokens pre-mined before going public with the blockchain will vary. The process of coin distribution will affect the network's level of decentralisation and can easily compromise the system in its early stages.

Consider if one miner retained all the coins at the start of the network. The miner will have inordinate control over the price of tokens and de facto become the central authority. Bitcoin's over time issuance model ensures there is a mechanism that promotes both network growth and competition to keep it decentralised.

Bitcoin's supply schedule is what allows it to grow organically and not reward early adopters egregiously. So while the 10 minute block average and coin reward for Bitcoin is arbitrary, it does serve a higher purpose. The time needs to be large enough to compensate for network communication latency (transactions details reaching enough nodes globally) while also not being too large that it slows down transaction time and utility[34]. If the block creation time was 1 minute, then nearly all of the coins will be in the hands of those who joined and mined the network in the first few years. A very short block production time would also increase the risk of geographic concentration due to co-location risk: 1 minute may not be enough time to transmit messages globally. Messages would be picked up and mined by the closet network members. Bitcoin's 10-minute blocks equate to roughly 25 years to mine 99% of all coins[35]. Network growth needs to allow for a higher chance of widespread use and a higher chance of surviving the transition out of the coin reward phase.

Virality of Network and Self-sustaining Ecosystem or, Feedback Loops & Emergence

An understanding of all of the factors we have discussed is necessary when examining how feedback loops of incentives are created within the network to allow it to grow.

The theory of emergence in complex systems is the study of how things go viral[36]. The ability to make something go viral and create a self-sustaining network and ecosystem is crucial for blockchain success. It is also the most challenging aspect of network valuation.

The technology itself is not the most difficult component of a Crypto-project. In fact, the Ethereum Foundation through their 'crowdsale' initiative[37], has made it very easy for anyone to create an ICO. The blockchain technology creates digital consensus but its success depends on consensus in the real world.

Using google search trends and analysing social media is the easiest way to measure adoption rates and virality. As detailed earlier, the scaffolding needs to be in place to convert social virality to network use, and therefore the creation of a valuable Cryptoasset.

How the System can Implode

We described earlier how the system is entirely reliant on transaction flow and transaction fees. Users need to pay enough fees so that the mining infrastructure remains intact or the network implodes. If enough users and miners exit the system, all value is destroyed. If users stop making transactions, no further coins are produced, no fees are available, and no additional 'blocks' are created. The system will grind to a halt and all 'token value' is lost and all that remains is a list of historical transactions (the ledger). This scenario is similar to the situation described in the fairground analogy, where everyone who wants to be in the fairground already has a token (and therefore the token price is zero).

If the network implodes, re-starting the network will not be much different from starting a brand new network. This dynamic underscores again why the dollar cost of the entire network or invested assets is so relevant. It is harder for a mining network of $1 billion to cease to exist than one of $100,000. Miners will continue to operate at zero cost or losses for longer if there is a lot more to lose.

To truly understand network value we may need to study further areas such as psychology, complexity theory and empirical work on social networks. However, it is also important to keep in mind the risk of overthinking the mechanics - let us not forget what we are really studying is 'Consensus'.

Gold is maybe the best example of how enduring consensus can be. It has very little industrial use but has for thousands of years kept its place at the heart of global monetary systems. This trust has held because the consensus among people, governments and central banks has always prevailed. Digital consensus may be no different. If bitcoin can become 'digital gold', it could conceivably remain digital gold.

Value, Distributed

Blockchain is not just about transferring value. It is about the allocation of value and how decentralisation can completely transform existing business and economic models.

True decentralisation, however, is hugely complex and it remains to be seen if it is possible or even sustainable.

Decentralisation has many advantages. It can transform the way we approach public goods, merit goods[38] and incomplete markets[39]. Bitcoin shows us how incentive structures can be used to change the way markets are designed, allowing for innovation where before the economics did not allow it. Open Source projects can now reward the researchers driving them, thereby, attracting more researchers to Open Source projects.

Decentralisation is not a panacea. It will solve some problems while creating new ones. Not everything needs to be decentralised. Optimal outcomes will depend on the utility of something being decentralised instead of being centralised.

Decentralisation of Money

We do not know if money is the obvious candidate for decentralisation. While Bitcoin's origin stems from the near collapse of the financial system in 2009, a genuine need for an alternative monetary system has not materialised. While Bitcoin remains a pioneer of the technology, decentralising money is a particularly complex undertaking.

We highlighted earlier worthwhile use cases for a decentralised payment system: for the unbanked, remittances and cross-border transactions. However, taking over the high street and replacing existing forms of cash has far-reaching implications that likely will not make sense in the long run.

If decentralising money is really the end goal, there are actually much easier ways to achieve this. We can go to the bank, withdraw all our money, convert it into gold, and hide it under the bed. Bitcoin is in some ways a lot like physical cash or physical gold - since we can lose it and once a transaction is done, it is near impossible to reverse.

Users who own a substantial amount of bitcoins also have the same security risks as storing physical gold. The private keys[40] that protect a user's bitcoins will need to be kept in what is called 'cold storage'[41], to be fully secure. Cold storage is where access to unspent bitcoin is kept off the grid. Only off the network can the risk of being hacked be reduced to zero. Holding private keys on a portable hard drive is an example of cold storage. A bar of gold or a portable hard drive, whichever metal we want under the bed, the problems are similar.

Achieving real decentralisation of money means assuming all responsibility and associated risks with it. Is it in our benefit to keep all our money under the bed? Should we pay a custodian and

pass the responsibility on to someone who specialises in security or is insured? How about an agency that is protected by our government? Maybe even a bank? Perhaps centralisation is not such a bad idea after all.

It should be noted that keeping bitcoin with a wallet provider is not decentralisation. Cutting out the third party in bitcoin means having specialised software and becoming a legitimate node on the network, something that will likely struggle to find widespread adoption.

The final point we will make about decentralising money is that it will compromise the banking system. As vilified as banks are, they play a vital role in the economy: to facilitate the creation of credit. Credit is the lifeblood of economic growth and prosperity. Modern monetary systems are based on what is called Fractional Reserve Banking (FRB). FRB is what allows for banks to take deposits and create loans by lending out a percentage of those deposits. It remains to be seen if FRB is possible in the Bitcoin ecosystem. FRB systems usually require a central authority else the viability of a 'Cryptobank' business model will be unclear. We should also note that building a banking system within the bitcoin ecosystem is fundamentally contradictory to the entire ethos of its creators and current users.

Jamie Dimon, the Chairman and CEO of JP Morgan, famously once said "Remember that banks aren't markets. The market is amoral. The market doesn't care who you are. You're a trade to the market. The market will sell you if they think you're riskier. Banks didn't do that"[42]

Dimon makes a crucial point, society works on relationships. When people come under hardship, we cannot help them through code or algorithms. Human decision sometimes overrules economics and politics is something very difficult to code.

Money is not the most obvious candidate for blockchain. Some parts of the payments system might be, but not money in its entirety.

This paper serves as an introduction to some of the considerations involved in blockchain valuation. We have proposed aspects that now need to be measured and examined in further detail - in both quantitative and qualitative terms. The next step would be to determine minimum value. The minimum value can be compared to book value in stock valuation or recovery value in bond valuation. Understanding Cryptoassets as a fixed quantity resource allocator provides the anchor from where this work can begin.

Graduation Day, Timing the Cryptoasset Market

Widespread adoption of Cryptoassets is obviously an important aspect of valuation. For many, it is still an unproven technology with no real use cases. Bitcoin has been around for eight years but is not a legitimised payment system. Unless the assets support networks of practical use, then valuation work is mostly in a speculative case.

Blockchain's real potential will become apparent when we start seeing decentralised applications (dApps); the decentralised internet or "how the internet should have been".

The theory is, dApps will empower users. Ownership of data will be returned to individuals. Commissions usually charged by middlemen, and known as 'take rates' in e-commerce, will be substantially lower or nonexistent. There will be minimal switching costs and significant consumer market power.

So far we have not seen any 'killer' decentralised apps. The reason for this being the technology stack required to create them has not until very recently existed. Blockchain needs software engineers to rethink almost the entire software development process. Some estimates suggest only around 5,000 developers globally really understand blockchain[43]. For comparison there are roughly 18.5 million software developers worldwide. This anecdote gives us an idea of how early we are in the dApp product development cycle.

The Decentralised Application

The technology stack is a term used to describe the components required to build a computing service or application. There are broadly three components[44].

1. Communication: user front-end software (browser)
2. Processing: executes commands, controls operations (operating system)
3. Storage: data file system (file storage, file transfer) & database

The traditional open-web development stack that make up these components, comprises of Linux (Operating System), Apache (Web Server), MySQL (database) and PHP (programming language). The stack is commonly abbreviated as the LAMP Stack and is what software is built on top of.

The decentralised development stack would need a reworking of the same three components.

1. Communication is already decentralised through the internet. Google, Facebook, and Airbnb have all built software, on top of the internet, that exploits the value created by decentralised communication.

2. To decentralise processing, the Ethereum Foundation developed a programming language called Solidity. They created a development environment that allows processes and smart

contracts to run across the network. Exploratory use cases for this technology have been around since 2015.

3. To decentralise storage, three main elements were required;

a. A ledger that holds tokens (part of the blockchain technology)
b. A file system to store large files
c. A searchable database that can handle high volumes of transactions being written to the database

The first element has been around since Bitcoin. It is integral to blockchain. The second element was introduced in 2015 (Interplanetary File System). The third element has been around since 2016 (BigChainDB).

All the components for an open-source decentralised stack on top of which applications can be built now exists. The crucial point to highlight, however, is how recent the pieces have come together. The timing coupled with the limited number of experts who can work with the technology underscores how early we are in the Cryptoasset life.

Many specialist investors are closely monitoring the development of dApps[45]. The creation of the first "killer" app is seen as the real signal validating Cryptoassets as an asset class, as users will need to own tokens to use the app.

Once we start to see dApps becoming mainstream along with the widespread adoption of Cryptoassets it will be easier to assess the investment case, as only then will Crytoassets be generating significant intrinsic value and network value. At the moment, we see Cryptoassets being driven nearly exclusively by future value factors and market value factors. Therefore, the case for speculation is more evident than for investment.

Digital Consensus

Digital Consensus may be the more appropriate name for the asset class. Bitcoin is the largest open blockchain by market capitalisation, and there are thousands of blockchains behind it with various potential uses and nuances. However, blockchain is part of a broader set of technologies that share one feature: digital consensus.

Digital consensus is what allows for a distributed system that is as a whole trustworthy but requires no trust at individual nodes; a trust-less decentralised system. Other emerging technologies in this space include tangle (IOTA), hash graph and private blockchains. Different technologies deployed to achieve digital consensus require adjustments to valuation approach - since variations of the philosophy and economics of each system are crucial to understanding value.

Digital Assets

Digital assets and their value have been appreciated for a long time already[46]. For instance, it is the digital asset on the Netflix balance sheet that allows the stock to consistently trade at an optically ludicrous price to earnings ratio. Digital assets are what makes Amazon, Google and Facebook the incredibly powerful forces they are.

As we described in our opening paragraphs, digital assets are the result of powerful networks which have so far only been configurable as a centralised system. Digital assets represent the value created out of personal data. Data is often described as the new oil due to its immense worth in the digital economy. The innovation that cryptography and computer science has provided is distributing the value of these digital assets. What before was concentrated at the centre - on the company's balance sheet - can now, via decentralisation, be taken off the balance sheet and into tradable assets.

Cryptoassets simultaneously share access to a network's use and value.

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008

[2] https://en.wikipedia.org/wiki/History_of_bitcoin

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, 1991

[4] https://www.coindesk.com/can-blockchain-save-us-from-the-internets-original-sin/

[5] https://www.wired.com/2013/11/mtgox/

[6] Adam Smith, “An Inquiry into the Nature and Causes of the Wealth of Nations”, 1776

[7] B. Graham, D. Dodd, “Security Analysis: Sixth Edition”, 2008

[8] https://en.wikipedia.org/wiki/Metcalfe%27s_law

[9] McKinsey & Co., Global Payments 2016: Strong Fundamentals Despite Uncertain Times, https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx

[10] https://qz.com/775159/theres-a-500-billion-remittance-market-and-bitcoin-startups-want-in-on-it/

[11] http://www.worldbank.org/en/news/feature/2012/04/19/three-quarters-of-the-worlds-poor-are-unbanked

[12] https://blog.blockchain.com/2014/12/29/drawing-the-distinction-between-the-uppercase-b-and-lowercase-b-in-bitcoin/

[13] J. Rickards, “The New Case for Gold”, 2016

[14] https://blockchainhub.net/tokens/

[15] https://en.bitcoin.it/wiki/Confirmation

[16] https://bitcoinfees.info/

[17] https://en.bitcoin.it/wiki/Transaction_fees

[18] https://bitcoinfees.earn.com/

[19] ETF Securities Outlook December 2017, https://www.etfsecurities.com/retail/dk/en-gb/news/outlook-2018--disruption-driving-rare-metal-appetite-in-2018---but-mainstream-commodities-likely-to-stay-flat

[20] https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/

[21] https://open.lib.umn.edu/principleseconomics/chapter/9-3-perfect-competition-in-the-long-run/

[22] https://en.wikipedia.org/wiki/Cryptocurrency#The_legal_concern_of_an_unregulated_global_economy

[23] http://www.telegraph.co.uk/technology/2017/08/11/police-shut-scam-cryptocurrency-boiler-room-city/

[24] https://www.linkedin.com/pulse/venture-capital-risk-return-matrix-hans-swildens/

[25] https://en.bitcoin.it/wiki/Majority_attack

[26] Direct quote from Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008

[27] https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

[28] https://99bitcoins.com/2016-bitcoin-mining-hardware-comparison/

[29] https://bitnodes.earn.com/

[30] https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china

[31] https://en.bitcoin.it/wiki/Script

[32] https://thetechpanda.com/2017/12/29/explainer-ethereum-turing-complete/

[33] https://coincentral.com/the-upcoming-bitcoin-hard-forks-what-you-need-to-know/

[34] C. Decker, R. Wattenhofer, “Information Propagation in the Bitcoin Network”, 2013

[35] https://en.bitcoin.it/wiki/Controlled_supply

[36] http://complexitylabs.io/

[37] https://ethereum.org/crowdsale

[38] https://www.huffingtonpost.com/entry/blockchain-and-a-renaissance-of-the-social-commons_us_5a4462c2e4b0d86c803c74f0

[39] https://news.bitcoin.com/nobel-economic-winners-smart-contracts/

[40] https://en.bitcoin.it/wiki/Private_key

[41] https://en.bitcoin.it/wiki/Cold_storage

[42] https://www.independent.ie/business/world/banks-arent-markets-the-market-is-amoral-the-market-doesnt-care-who-you-are-youre-a-trade-34505714.html

[43] https://bitcoinmagazine.com/articles/the-blockchain-developer-shortage-emerging-trends-and-perspectives-1477930838/

[44] http://blogs.lse.ac.uk/businessreview/2016/04/14/blockchain-will-usher-in-the-era-of-decentralised-computing/

[45] https://www.stateofthedapps.com/whats-a-dapp

[46] https://www.mckinsey.com/industries/high-tech/our-insights/measuring-the-full-impact-of-digital-capital