Proof of Work as it relates to the theory of the firm.

Author: Craig Wright

Abstract

One of the little-known aspects of bitcoin is the nature of the proof of work system. There are many people, especially those who support a UASF or PoW change that believe a distributed system should be completed as a mesh. In this, they confuse centralised systems with centrality. The truth of the matter, no matter which proof of work system is implemented, they all follow a maximal growth curve that reflects the nature of the firm is detailed in 1937 by Ronald Coase. In this paper, we address the issues of using alternate proof of work systems with regards to either incorporating alternate functions in an extension of simply securing the network against the use of proof of work systems in an attempt to create a one person one vote scenario in place of economic incentivisation.

Keywords: Bitcoin, Proof of Work, Firm Theory, Condorcet's paradox

Introduction

One of the little-known aspects of bitcoin is the nature of the proof of work system. There are many people, especially those who support a UASF or PoW change that believe a distributed system should be completed as a mesh. In this, they confuse centralised systems with centrality. The truth of the matter, no matter which proof of work system is implemented, they all follow a maximal growth curve that reflects the nature of the firm as detailed in 1937 by Ronald Coase (1937).

The bitcoin White Paper was very specific. users of the system "vote with their CPU power" [1]. What this means, is that the system was never generated to give one vote per person. It is designed purely around economic incentives individuals with more hash power will have provided more investment into the system. These individuals who invest more in the system gain more say in the system. At the same time, no one or even two individuals can gain complete control of the system. We'll explore the nature of cartels in a separately, but these always fail without government intervention. The reason for cartels failing comes down to the simple incentivisation of the most efficient member. The strongest cartel member always ends up propping up the weakest. This leads to a strategy of defection.

No proof of work-based solution ever allows for a scenario where you have one vote to one person. The anti-sybiling functions of bitcoin and all other related systems based on proof of work or similar derivatives are derived from an investment based strategy. Solutions to the implementation of ASIC based systems are constantly proposed as a methodology of limiting the centralisation of proof of work systems as it is termed. The truth of the matter is that the mining function within any proof of work system naturally aligns to business interests. This leads to corporations running machines within data centres. On the way that democracies and republics have migrated away from small groups of people individually voting for an outcome towards a vote for a party, the transactional costs associated with individual choice naturally leads to corporate solutions. In this, the corporation mirrors a political party.

In this paper, we address the issues of using alternate approval work systems with regards to either incorporating alternate functions in an extension of simply securing the network against the use of proof of work systems to create a one person one vote scenario in place of economic incentivisation. We will demonstrate conclusively that all systems migrate to a state of economic efficiency. The consequence of this is that systems form into groups designed to maximise returns. The effect is that bitcoin is not only incentive compatible but is optimal. No system can efficiently collapse into an order of one vote one individual and remain secure. In the firm-based nature of bitcoin, we demonstrate that the inherent nature of the firm is reflected within mining pools. Multiple aggregation strategies exist. The strategies range from the creation of collective firms where members can easily join or leave (mining pools) through to more standard corporate structures.

Social choice, Bitcoin, and Arrow’s theorem

There are many alternative propositions to the bitcoin Blockchain. Some of these utilise alternative scenarios that have value or utility other than or in addition to the mere solution of problems that lead to the securing of the network. Some altcoins have proposed Seti-at-home style solutions for all types of problems including the search for cures to cancer.

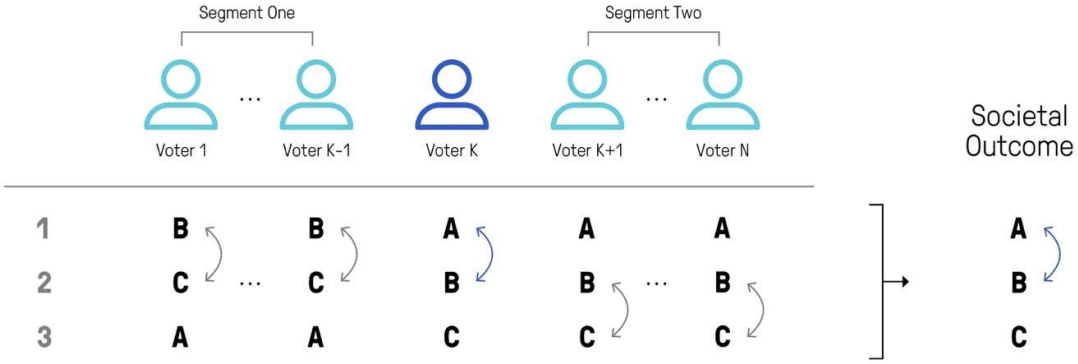
Whenever we add additional states into any system, these need to be taken in consideration of the overall utility and welfare that results. The initial system changes dynamically to vary significantly even on small changes. - The most important part of this consequence is that any additional inclusion is either of no utility and thus should not be incorporated or is of utility that can be expressed across a market in the form of profit. An additional inclusion is either (A) would be of no utility and thus should not be incorporated, or is (B) of utility that can be expressed across a market in the form of profit. Small variations in the initial states can result in large changes. This creates a social choice problem.

Bitcoin was simplified to only involve the solution of securing the network to ensure that no alternatives could diminish the security of the system. This is, it forms a simple two-good, two-person Edgeworth-box economy form of a distribution problem. At each point, there is a known solution representing the way of distributing goods between members. Each of these states is mutually exclusive. Although each agent will express his or her own preferences for alternative uses, it remains simple to determine the overall maximal returns.

Without alternatives, the mining solution becomes Pareto efficient.

The alternative of adding so-called "useful" puzzles to bitcoin leaves a scenario where there is an additional utility in the solution itself. This additional created utility varies between the users of the network. That is, no two individuals will have the same preference for this use. This is even assuming a single use alternative and precluding the addition of multiple competing solutions. In these extended scenarios we come up against problems such as Condorcet's paradox[1].

In this paper, we will only touch on is lightly on this topic, but for the dedicated reader we direct them to "Advanced Microeconomic Theory" (Jehele & Reny, 2000).



In chapter 6 of this book, the authors address Arrow's Impossibility Theorem[2] (Arrow, 1957).

The primary problem with the addition of alternate forms of utility is how to choose which one is included, how much and then who decides. In locking any alternative into the protocol, we start to incorporate possible debates over profitability and utility. The problem with this is that no two parties are going to see the same utility that results from the same expenditure.

The most important part of this consequence is that any additional inclusion is either of no utility and thus should not be incorporated or is of utility that can be expressed across a market in the form of profit. In the form of profit, the miner will benefit not only from the redistribution of bitcoin wealth in the allocation that comes from the discovery of a block solution, but also from the utility associated with the alternate use.

The result is that miners will still seek to maximise profit. This rational behaviour leads them to the optimal strategy seeking returns that are just over the risk-free rate as other miners enter the market. When the utility is divided between securing the network and alternative uses, the result that must

[1] https://ocw.mit.edu/courses/economics/14-75-political-economy-and-economic-development-fall-2012/lecture-notes/MIT14_75F12_Lec12.pdf
[2] https://en.wikipedia.org/wiki/Arrow%27s_impossibility_theorem

naturally flow is that the investment in securing the network in a mixed-use environment needs to be lower than that which will occur in a pure single use environment.

The overall consequences that bitcoin becomes less secure as the investment in mining infrastructure that would secure the network becomes divided between securing the network and other uses that have been tacked onto the network. This becomes an allocation problem with the efficient allocation of scarce goods no longer being optimised. In this instance, the primary good, the overall security of the system is mixed with alternatives that provide neither the optimisation of the primary security function or the alternative use. These alternative use scenarios are highly valued by the individuals proposing their incorporation into a proof of work solution, but they are less valued by most people using the system.

There are many "worthy causes" coupled with inherent scarcity. To the individual promoting each cause, the subjective value exceeds the cost of provision. However, the simple fact that these are not provided on market to the level desired by everyone demonstrates that they are not universally valued. To many, this concept seems to promote injustice or behaviour that is not fair. The tragic nature of scarcity is that there are always trade-offs and all value is subjective.

What we see from Condorcet's paradox is that the incorporation of multiple options reduces efficiency. In attempting to solve several problems outside the value of money, we create a scenario where no ideal valuation has been subjectively returned. The value of a pure money is in its ability to measure alternative values. A single maximised currency removes the ability to hide subjective preferences. The existing monetary system with the incorporation of inflation, fractional reserve banking, and government manipulation leads to a scenario where individual's value measurements cannot be individually obtained. Although each individual values each trade subjectively when compared to others, these are valued objectively based on the time and interceding factors that apply at that moment.

Simply put, the value of mining is not simply wasted, it is incorporated into the value that we gain in a new transactional medium. The value of mining is the security of the bitcoin network.

The Nature of the Firm

Ronald Coase (1937) demonstrated that transactional costs lead to firms optimising size. In his argument, he demonstrated that where all things are equal a firm will tend to be larger until a point of management inefficiency is reached. Where the cost of organisation increases at a lower rate than the increase in transactions organised, a firm will tend to grow. Additionally, in a system with more stability, entrepreneurial risk will be lowered. This leads to a scenario where the organisation is more aligned to market needs and less likely to make costly mistakes. In this scenario, an increase in the transactions organised results from the ability to plan more effectively.

As the increase in the supplier price factors of production lowers, firms will seek to maximise returns and grow to a point of maximal efficiency. This growth strategy has an overall limit. Once a threshold point has been exceeded, the gains associated with increases in organisation start to become balanced with the additional layers of management and control structures needed within the organisation. As hierarchical structures increase, the costs of providing services start to increase. The optimal size of any firm is maximised at the point where the greatest returns are achieved for each unit of cost.

Firm strategies

It is interesting when we start to note the reactions of many individuals to the formation of corporations. In an article in CoinDesk[3], they talk about the balance of power and how to return this to the "users". We have of course an extremely partisan view being aired. The reality is there are only a few strategies

[3] http://www.coindesk.com/bitcoin-scaling-give-everyone-control/

that are successful within any proof of work system. The system was determined to be based on one-vote per CPU (Satoshi, 2008) and not one vote per person or one vote per IP address.

The reasons for this is simple, there is no methodology available that can solve byzantine consensus on an individual basis. The solution developed within bitcoin solves this economically using investment. The parties signal their intent to remain bound to the protocol through a significant investment. Those parties that follow the protocol are rewarded. The alternative strategy takes us back to the former and failed systems such as e-cash that could not adequately solve Sybil attacks and decentralise the network. Bitcoin manages to maintain the decentralise nature of the network through a requirement that no individual party can ever achieve more than 50% of the network hash rate.

In all proof of work systems, there are requirements to inject a costly signal into the network that is designed as the security control. To many people, they believe that the cryptographic element, namely the hashing process is the security feature of bitcoin. This is a fallacy, it is the economic cost that is relevant to the overall system and not the individual element.

The benefits of a hash function are that they are difficult to solve in the nature of the proof of work algorithm but are easy to verify. This economic asymmetry is one of the key features of bitcoin. Once a user has found a solution, they know it can be quickly broadcast and verified by others. Additionally, the hash algorithm provides a fair distribution system based on the amount of invested hash rate. The distinction from proof of stake solution as has been proposed comes in the requirement to constantly reinvest. A proof of stake system requires a single investment. Once this investment is created, the system is incentivised towards the protection of the earlier investment. This leads to a scenario known as a strategic oligopoly game.

The solution using a proof of work algorithm is the introduction of an ongoing investment. This is different to an oligopoly game in that sunk cost cannot make up for continued investment. In a proof of stake system, prior investment is crystallised allowing continued control with little further investment. Proof of work differs in that it requires continuous investment. More than this, it requires innovation. As with all capitalist systems, they are subject to Schumpeterian dynamical change (Shumpeter, 1994). The system of creative destruction allows for cycles of innovation. Each innovation leads to waves of creation over the destruction of the old order.

This process creates continued growth. Proof of work-based systems continue to grow and continue to update and change. Any incumbent corporation or other entity needs to continue to invest knowing that their continued dominance is not assured. In bitcoin, we have seen innovative leaps as people moved from CPU-based mining into GPU-based systems. This initial innovation altered the software structure associated with the mining process in bitcoin. That change significantly altered the playing field leading to novel techniques associated with FPGAs and later ASICs dedicated to a specific part of the mining process.

The error held by many people is that this move from a CPU-based solution into more costly implementations could have been averted. A consequence of this has been the introduction of alternative proof of work systems into many of the alt-coins[4] . These systems have been implemented without the understanding that it is not the use of ASICs that is an issue. It is that the belief that individual users can individually mine in a mesh system will be able to be implemented as a successful proof of work.

In the unlikely event that a specialised algorithm was implemented that could only run once on any one machine CPU, it would still lead to the eventual creation of corporate data centres for mining. In the section above, we showed using Arrow's theorem how only a single use proof of work system can be effective. If we extend this and look at the Theory of the Firm (Coase, 1937) we note that in a system

[4] https://en.wikipedia.org/wiki/Scrypt in Litecoin and Dogecoin for example.

of prices, reduction could be carried out without any organisation. One issue against this arises from the cost of information. Interestingly, as we move into a world of increasingly more information, it becomes scarce information that is important. As the amount of information becomes more voluminous, the ability to uncover accurate and timely information becomes scarcer.

The ability to specialise in the coordination of the various factors of production and the distribution of information leads towards vertical integration within firms. We see this first voiced in Adam Smith's (Smith, 1776) postulation on the firm:

> "*It began to be seen that there was something more important than the relations inside each factory or unit contained by an undertaker; there were the relations of the undertaker with the rest of the economic world outside his immediate sphere … The undertaker busies itself with the division of labour inside each firm and he plans and organises consciously*"

The end of this specialisation as Coase (1937) demonstrated using Smith (1776) is that the capitalist:

> "*it is related to the much larger economic specialisation, of which he himself is merely one specialised unit. Here, he plays his part as a single cell in a larger organism, mainly unconscious of the wider role he fills.*"

Everyone can choose to either seek further information or act on the information that they already have. This information can be in the form of market knowledge, product knowledge, or expertise, but at some point, the individual needs to decide to act. There is a cost to obtaining information. The returns on obtaining more information hit a maximum level and start to decrease at a certain point. The entrepreneur acts as a guiding influence managing the risk associated with incomplete information compared to the risk of not acting but rather waiting to obtain more information.

In the instance of bitcoin mining, the firm can increase in size through the integration of multiple specialist roles. Even given the assumption that any one process can run on but a single CPU, we come to the scenario of high-end datacentre servers. The Intel Xeon Phi 7290f[5] implements 72 Atom CPU Cores. Each core runs two threads. Even taking the control system into account, this leaves 142 processes able to run per system. With four cards per RU[6] this allows for datacentre implementations of 5,964 mining processes to run on a pure CPU-based proof of work implementation.

One person can manage a small number of mining server implementations within a home or small business environment. In large data centre-based organisations such as Facebook, a single administrator can run 20,000 servers[7]. The effect of this would be one individual managing 2,840,000 individual CPU-based mining processes. This alone is outside the scaling capabilities of any individual. This can be further enhanced as cost savings through the creation of large data centres, management savings and integrating multiple network and systems administrators is considered. As we start to add additional layers we come to a maximum where it is no longer profitable to grow the firm in size. Right up until that point, the firm will grow.

The result is a longtail distribution[8] of firms. The most efficient and highly capitalised firms will grow to the point where they are no longer profitable. At each point in time, each organisation competes to maintain its market share and returns. If it seeks to grow its operations, it does this in competition with all the firms. Each block reward is a zero-sum game. To gain a larger percentage and return, the individual organisation needs to increase the amount of hash power supplied. Other strategies such as

---

[5] https://ark.intel.com/products/95831/Intel-Xeon-Phi-Processor-7290F-16GB-1_50-GHz-72-core
[6] Rack Unit
[7] http://www.datacenterknowledge.com/archives/2013/11/20/facebook-ops-staffer-manages-20000-servers/
[8] https://en.wikipedia.org/wiki/Long_tail

Selfish Mining[9] failed to understand this point. Any scheme that reduces the overall take reduces the revenue of the individual miner at the same time. Such a strategy leads to an overall loss.

At any point in time, in a proof of work-based system we also need to consider the looming threat of innovation. Any mining hardware would be expected to become obsolete within a short amount of time. Add to these increased efficiencies in energy use and cooling technology and we start to see that even foreseeable disruption can change the nature of the market. Each individual organisation can plan for the known risk factors but can never plan for unknown contingencies. The result is that organisations cycle as new innovators replace the incumbents.

For all proof of work systems, economic efficiencies naturally lead towards larger competing firms. There is no known system that allows for the fair distribution of resources in a distributed manner that does not lead to competing corporations managing the primary system.

Strategic Oligopoly Game

In modelling the outcomes of business strategies in models of incomplete information about the others intention, we can use game theory, and a subdiscipline on games of strategy. We can extend our analysis of proof of work when we model the decisions of firms on the pricing and levels of production coupled with decisions on how much to invest in research and development. As noted above, research projects are costly and represent a risk to business. Any firm that invests also should model the risk that a competitive firm may copy or otherwise follow the primary firms result. This risk needs to be balanced against that of losing competitive advantage. Such a loss can lead to a long-term decline in market share and profitability.

This leads as to oligopoly strategies. These would include price-fixing and market manipulation strategies. In a proof of work system, oligopoly strategies, or the formation of cartels fail due to the impact of the most profitable firm seeking to defect. In all cartels, the least profitable firm needs to be propped up by the other members. The scenario always leads to dissent and the eventual failure of the oligopoly.

Oligopoly grows when the individual parties in the system can set the rules in such a way that they can restrict entry to new players. In the case of a proof of Stake-based system, the ability to withhold funds for large entities leads to a high barrier to entry. In a situation such as that which has evolved in Ethereum, a single large player in a proof of stake system can set the rules. The aim of any oligopoly is to maximise profits. In general, oligopoly form businesses set barriers to entry using government licenses, economies of scale, patents, access to expensive and complex and highly capitalised systems and technology and predatory behaviours. Government regulation is also one of the major factors influencing this form of system.

Proof of stake allows players to form protective cartels. In competitive environments cartels breakdown naturally. Proof of stake can be created in a non-competitive manner. Even if the system starts off competitively, it is the nature of an oligopoly to seek abnormal profits and this can be achieved through the manipulation of the rules over time. Such manipulation can result in increasing levels of control as the incumbent firms ensure that innovation does not change or disrupt the status quo.

The system degrades into oligarchy. This is a power structure with rule by a small number of people. It is what the Greeks in the time of Aristotle called a tyranny. A more common name today would be a plutocracy. The proof of stake system is a form of oligarchy that represents societal control by a small number of wealthy individuals.

---

[9] http://fc14.ifca.ai/papers/fc14_submission_82.pdf

The introduction of control by wealth holdings (also known as proof of stake) leads to the creation of a Stackelberg leadership model (Stackelberg, 2011). The players of the game include the leader, the individual with the largest proof of stakeholding, and the followers. This is a game of competition based on quantity. In this, the Stackelberg leader is commonly referred to as the market leader. This former competition occurs when one member has an advantage that then allows it to move first. The requirement is commitment power. The equivalent is an incumbent monopoly and this is obtained through the holding of excess capacity. Proof of stake derives from this form of commitment scheme.

The introduction of a proof of stake form of commitment allows the dominant firm to make a move that directly contradicts Cournot's premise that each duopolist will produce the equivalent measures.

The biggest flaw with a proof of stake based system is the inability to account for present action. Past holdings lead to an ongoing scenario where the wealthy can hold their power without the need to innovate or continue to invest in the market. In a proof of work-based system, individuals need to reinvest consistently and constantly, research and develop, and evolve. It is this reason that these two systems are so different. As with many aspects of bitcoin and other crypto currencies, the defining factors are economic and not the implementation of cryptographic tools.

Mining pools

The first firm strategy to be discussed is that of Pool mining. Several pool mining strategies exist. In all mining pools, pool acts as a controlling function allowing each of the individual pool members to share in a block reward. There are various strategies involved with pool mining ranging from users providing their own hardware and solving on their own systems with an aim to receiving rewards and a more regular basis.

Joining a pool does change a miner's expected revenue, it provides a lowering of transaction costs to the business as any variation in revenue presents as a cost and a risk to the full miner. Another aspect of profitability is the time value to money. A small miner with infrequent returns requires capital to be tied up in larger quantities than would be needed in instances of variation being low. Uncertainty leads to higher levels of liquid assets to cover possible slow months.

Most pools are formed in groups of businesses. It is not true to say that miners in a pool behave as a single agent with a centralised coordinator. Some of the pools allow minors to vote individually, that is, they separate their voting on block policy based on the miner's individual hash power. The reason for this is rational, all operators who do not allow for members to make a choice quickly find that they are going to lose members. As noted above, members of a mining pool can move between pools relatively easily and only into long-term contracts when it is beneficial.

All rational organisations act strategically. This is not a function of bitcoin, it is the nature of the firm. The theory of the firm was hypothesised by Ronald Coase (1937). Just as Coase argued, "*economic theory has suffered in the past from a failure to clearly state its assumptions*", so has research into bitcoin suffered. The selfish mining paper is one of many that failed to analyse nature of the bitcoin network. As with all firms, the size of the organisation is a function of transactional costs. In mining pools, pool-based firms can consolidate the hash power associated with many individuals and small organisations. Each of the small organisations experience a combination of larger costs and higher risk when operating alone.

Risk is a form of transactional cost. There is a cost element associated with capital. When capital is scarcer it goes up in value. When an asset is less liquid it degrades in value. For the small organisation, bitcoin is a high-risk endeavour. Risk is partly associated with the inability to predict payment. Although an average, an individual will receive a return associated with their investment in hash rate, the inability to predict the frequency of such a return for a small party means that the cost of time needs to be considered into any profitability calculation.

For instance, a small organisation that would expect to win one block every week may gain one block in a week and then gain nothing for several months when they suddenly receive several block rewards in a row. During the period when they are not receiving any rewards the small operator would still need to pay for expenses including power and any property leases as well as staff costs and other incidentals. Most small organisations do not have capital available and may be leveraged. Any period where the organisation is not receiving a regular income results in additional charges from interest and even the loss of payment discounts to suppliers.

These are some of the many reasons why small organisations band together to form organisations and larger groups. Reducing the risk of operation reduces overall transactional charges within the firm. Rewards are distributed at infrequent, random intervals, miners form mining pools *in part* to decrease the variance of their income rate. In part as the transactional costs associated with running a firm are varied. It is not only the variance as we discussed above that other costs within the organisation. As Coase (1937) addressed, many aspects of an organisation are duplicated. A mining pool needs to secure their network. For a mining pool, operational costs can be distributed between pool members at a rate that is lower than any pool member can obtain themselves. These transactional costs increase the profitability of each member. Some of the reasons pools form include:

- Rather than many small providers duplicating services wastefully, pool mining consolidates the provision of these services to many parties.
- The fees associated with the mining pool are competitive and need to be offered at a rate lower than the participants can provide on their own through solo mining.
- Increased efficiency offers overall benefits to all participants.

The important thing to note in any pool mining system is that members of the pool are only loosely bound. There are pool mining services that offer binding contracts and as the mining pool is better able to manage their own revenue, the loss of freedom and being locked into a contract term generally comes at a lower cost to the consumer of the mining services. These long-term contracts offer pool members slightly higher profitability at the expense of lower freedom to choose and move pools. Members of the mining pool are either bound for a contractual term or can join it will and can move their combined hash power between organisations. To assert the mining pool controls the network is to misunderstand the nature of the firm. In this, the firm members, those people associated with the mining pool can choose to defect and leave the pool and join another.

Enjoining another pool, they are seeking either that the profitability offered by the pool or they are voting with their hash power for a proposal offered by that pool. It is a common miscomprehension that mining pools are centralised and do not reflect the will of the members.

The ease at which mining pool members can vote with their feet and change pools belies this. Mining pools are simply collections of individuals who can express their own opinions and choices by aligning with an organisation which supports similar goals. Hence mining pools mirror the creation of political parties in democratic political systems.

This again reflects the transactional costs of the firm.

The users political voice is amplified when they align with large groups. In society, we see this with the creation of worker's unions, political parties, industry associations, lobby groups and more.

The fallacy held by many in the bitcoin community is that bitcoin is somehow different or above society. It acts within it and as a conduit for financial transactions. It does not replace the nature of society nor the interactions of humans. We are a collection of self-interested individuals who act in a manner that some altruistically in extended kin groups. The reality of even these scenarios is that we act in our own self-interest but that the interests of the group we align with aid our own interests more. This mirrors

the transactional cost with a firm. Individuals act to minimise their own cost as well and sometimes this means forming groups.

Mining corporations

Corporations require less explanation than a distributed pool. As we noted above, the ability to consolidate can lower costs creating a more profitable solution. In any organisation, specialisation forms the key aspect of coming together to create a business. At the simplest example, we can take to individuals and investigate whether a strategic alliance would result in larger payouts for both.

First, we have Alice. Alice is an extremely proficient coder and can manage and control many systems. Her software allows her to create a platform that returns an average of £500 per hour for every hour she works.

Next, we have Bob. Bob can follow instructions and setup mining equipment and hardware, but he is very inefficient and the processes associated with managing this business leave him unable to patch servers in an efficient manner. Bob can create a return of £120 per hour for his equal investment to Alice's.

Although Alice's extremely technically proficient, she is also an excellent accountant. Alice can manage the systems, the purchasing and all the required statutory returns. Both Bob and Alice work 50 hours per week. Alice can work 10 hours a week completing all the supporting work leaving her 40 hours that directly adds to productive mining and the returns she gets overall. Bob can do the same.

The result is that Alice can earn £20,000 each week when working on her own. Bob can work to earn £4,800 per week. Together, the two individually work returning £24,800. If Bob and Alice form a partnership, Alice can now work 50 hours each week specialising on the mining farm. This returns £25,000. Bob now spends 20 hours doing the joint accounts. We are ignoring any savings this example that would accrue through the merger. Bob can also provide 30 hours' worth of work helping on the mining for a return of £3,600. In this example, we have the same cost base, but increased revenue for increased profitability.

Working in partnership, Alice, and Bob jointly and £28,600. In forming a business, Bob and Alice have increased their joint revenue by £3,800 for zero additional cost. Even though Alice is better than Bob and all activities, it is in her interest to form a partnership that increases their returns. If Alice can hire other developers that are more skilled than Bob allowing him to concentrate on the accounting, Bob can now specialise allowing the firm to grow even further.

We see in this simple example how bitcoin-based companies evolve. Many individuals operate rationally to produce the best outcome. This is the nature of the firm and therefore any proof of work system will always evolve into a corporate strategy. Even the me look at pool-based mining, the result is a collection of aggregation firms that collect results from pool miners and over time increasingly specialised pool members.

Merchant-based solutions

Merchants also coordinate and grow in scale to maximise returns. Eventually, we would expect to see groups of merchants making payments preferentially to different miners based on the level of service they expect. This does not require them to maintain full copy of the Blockchain. It is not receiving your transaction that is important, it is the ability to check that the majority of the hash power have accepted your transaction and included it into a block. It does not matter how many wallet nodes have received a transaction, it only matters that the majority hash power has received it. If there are 10,000 wallet nodes and 1,000 miners (nodes in the true definition) and the majority of the miners reject the transaction, it does not matter at all if every single wallet says that the transaction is valid. If a transaction does not get into a block, it is not a transaction in bitcoin.

The consequence is that merchants will end up working with miners to ensure the successful integration of their transactions. It is not users who care for the accuracy of protocol, it is merchants. When an individual walks into a store and makes a purchase, it is the merchant who was taking risk. It is the merchant who can be double spent not the person making the payment.

Bitcoin and centralisation

The bitcoin protocol is designed such that honesty is not required. The attacks against the existing protocol are limited in nature. A dishonest mining pool is unable to steal funds and would degrade their own profitability in seeking to attack the network. The system remains sound where 50% of the parties involved in the creation of blocks or less remain as separate parties.

> *I didn't really make that statement as strong as I could have. The requirement is that the good guys collectively have more CPU power than any single attacker.*
>
> *There would be many smaller zombie farms that are not big enough to overpower the network, and they could still make money by generating bitcoins. The smaller farms are then the "honest nodes". (I need a better term than "honest") The more smaller farms resort to generating bitcoins, the higher the bar gets to overpower the network, making larger farms also too small to overpower it so that they may as well generate bitcoins too. According to the "long tail" theory, the small, medium and merely large farms put together should add up to a lot more than the biggest zombie farm.*
>
> *Even if a bad guy does overpower the network, it's not like he's instantly rich. All he can accomplish is to take back money he himself spent, like bouncing a check. To exploit it, he would have to buy something from a merchant, wait till it ships, then overpower the network and try to take his money back. I don't think he could make as much money trying to pull a carding scheme like that as he could by generating bitcoins. With a zombie farm that big, he could generate more bitcoins than everyone else combined.*[10]

Bitcoin is formed as a NSW Random graph with a distance of approximately d=1.32. At its heart, the centre of the bitcoin mining network is nearly a complete graph. In the paper, "*On red balloons and bitcoin*"[11] the researchers note that Sybil resistance cannot be achieved at a distance greater than d>4.

The proposed changes to the system trying to be introduced in segregated witness and the UASF are based on a concept of transactions and blocks hopping across the mesh. This is inapplicable as it would be a power law network different to bitcoin. In the default bitcoin in limitation, it does not matter if 10,000 wallets decide they want to block transactions or blocks within bitcoin. The mining network forms what is termed a giant node. There is no such thing as a full validating node. At best, each of these nodes stops broadcasting. As it prunes itself from the network, the rest of the network acts to broadcast more efficiently.

All that matters in bitcoin is mining. As more fully validating Sybils are added to the network, the more you get attackers to waste their money. The changes to the network, as are proposed as a part of segregated witness change this leading to an incentivising of attacks. This problem with a defence by wallets comes because of a lack of understanding of network graph theory.

The introduction of a wallet defence changes the structure of the giant node within bitcoin from a Newman Strogatz Watts (NSW) random graph into a power law system. In computer science, this is more generally known as a mesh network. That sounds great and looks really distributed when you

---

[10] http://www.mail-archive.com/cryptography@metzdowd.com/msg09967.html
[11] *https://arxiv.org/abs/1111.2626*

draw a picture, the issue is that the lower we have our distance the less likely we are to have an attack. The introduction of the sibyls which is what in effect we are doing with wallets creates the scenario that bitcoin was trying to stop

The argument is that verification nodes will stop propagation. The reality is they self-prune. As they do not send alerts stating that the connecting node has violated any conditions, all that occurs is that they are bypassed.

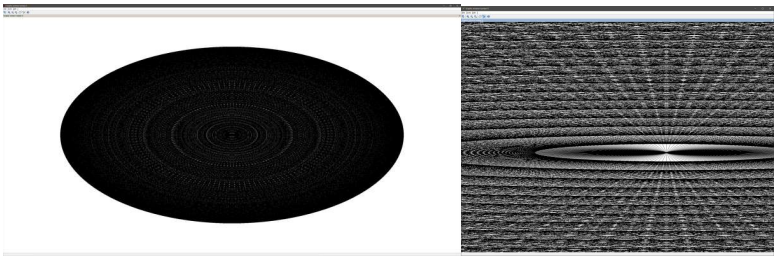


Figure 1: The Bitcoin Network.

The interconnection of nodes within bitcoin forms what is described as a near complete ring network.

The authors of On Red Balloons and Bitcoin state[12]:

- "Theorem: Suppose that $H \geq 3$. There is no Sybil-proof reward scheme in which information propagation and no duplication are dominant strategy for all nodes at depth 3 or less."

Here, the authors define this using:

- "We assume that the network consists of a forest of d-ary directed trees, each of them of height H."

The assumption of a mesh network moves away from the completely connected ring network that is formed in the majority of hash power within bitcoin into an easily compromised mesh. This is what you have when you alter Bitcoin. Making a UASF chain would enable this. Bitcoin only works with miners controlling it.

Segregated witness

The reason for the introduction of segregated witness is an attempt to return power away from the miners and to give this back to the developers. The argument is that users are the ones who benefit. The reality is that users have no say unless they mine. This does not change with segregated witness. The best that is achieved is the introduction of security flaws.

Conclusion

We can see that in all possible instances, any proof of work system, it is incentivised towards corporate consolidation. The frequently promoted idea of many individuals voting through individualised wallets within bitcoin does not stand scrutiny. Proof of work systems derived from continuous and updated investment. It is not past investment or current holdings that matter, it is the amount that a party is willing to spend at the time the vote is occurring. In this way, we see that the introduction of a low-cost voting mechanism such as that proposed in a UASF acts to lower the overall security of the network and allows for the introduction of Sybil attacks. In a proof of work system, it is the party's willingness to continue investing that provides their ability to vote for the system. To mine blocks, it is not just the prior investment, but rather, the overall investment at a point in time. When a proposal for change

[12] *https://arxiv.org/abs/1111.2626*

occurs, it is a requirement of the system that energy is expended in the solution of a block that both secures a network and allows the individual miner to choose.

The rational decision for any mining firm is to choose the most profitable strategy. The impact of transactional costs naturally leads to the growth of consolidated entities. Any time where there is a differential of any type between two individuals, it starts to become profitable for everyone to specialise. Even in the event where one individual is more skilled with regards to all areas than any other party, they will still find that they have differentials between their own skill sets. The marginal differences between their own skills always lead to a scenario where it is more profitable for that individual to concentrate on their specialties allowing others to increase the overall profitability of the firm. In the worst-case scenario, even where the introduction of additional people and the merger of mining entities leads to no more hash rate being obtained, it does lead to the reduction of time. The same amount of money earnt in a lower amount of time is an increased level of profit. Both parties can choose to either work on other tasks, engage in more leisure, or find other profit producing activities.

Consequently, all proof of work systems always consolidates into corporate entities. This is the nature of the system. It was not and cannot be designed for individualised control.

References

1. Arrow, K.J. (1950). "A Difficulty in the Concept of Social Welfare". *Journal of Political Economy* **58** (4): Pp 328–346. Archived.
2. Coase, Ronald (1937). "The Nature of the Firm". Economica. Blackwell Publishing. 4 (16): 386–405. JSTOR 2626876.
3. Jehle, Geoffry A. and Reny, Phillip J. (2000) “Advanced MicroEconomic Theory” Second Ed. Addison Wesley Longman, USA
4. Satoshi Nakamoto (2008), “” https://bitcoin.org/bitcoin.pdf
5. Schumpeter, Joseph A. (1994) [1942]. Capitalism, Socialism and Democracy. London: Routledge. pp. 82–83. ISBN 978-0-415-10762-4. Retrieved 23 November 2011.
6. Smith, Adam (1776). An Inquiry into the Nature and Causes of the Wealth of Nations. 1 (1 ed.). London: W. Strahan. Retrieved 2012-12-07., volume 2 via Google Books
7. von Stackelberg, H. (2011) “Market Structure and Equilibrium: 1st Edition Translation into English”, Bazin, Urch & Hill, Springer, XIV, 134 p., ISBN 978-3-642-12585-0