ACHAIN WHITEPAPER

ACHAIN

AUGUST 21, 2020

Contents

1. Background

The philosophy of blockchain is decentralization and disintermediation: multiple untrusted or semi-trusted parties can directly and transparently interact with each other without the presence of a trusted intermediary. This property makes blockchain particularly appealing to financial institutions suffering from huge middleman costs in settlements and other back office operations. So far, despite many breakthroughs and improvements, blockchain, compared to its traditional counterparts, still faces major hurdles before widespread adoption including but not limited to stability, performance and scalability. As per these properties, consensus protocols are the corner stone and are closely linked to them. Based on the same consensus protocol, all nodes will agree on the same criteria to pack, verify and mine a block. A consensus protocol is the vital safeguard to guarantee the blockchain's health and legality: only legal blocks (meeting the criteria of consensus protocol) can be added to the blockchain while illegal ones will be rejected. Two key properties that a consensus protocol should have:
(i) completeness, legal requests from correct clients are eventually processed, and
(ii) consistency, if an honest node accepts (or rejects) a value then all other honest nodes make the same decision.

Consensus is not a new topic: the distributed systems community has extensively studied it for decades, and developed robust and practical protocols that can tolerate faulty and malicious nodes. In this paper, we will present a new PoW consensus algorithm AChain, based on MPoW.

2. Cryptocurrency

Cryptocurrency is an internet-based medium of exchange which uses cryptographical functions to conduct financial transactions. Cryptocurrencies leverage blockchain technology to gain decentralization, transparency, and immutability. The most important feature of a cryptocurrency is that it is not controlled by any central authority: the decentralized nature of the blockchain makes cryptocurrencies theoretically immune to the old ways of government control and interference. Cryptocurrencies can be sent directly between two parties via the use of private and public keys. These transfers can be done with minimal processing fees, allowing users to avoid the steep fees charged by traditional financial institutions. In a cryptocurrency network, all transactions are stored as blocks that are linked internally creating a chain called a blockchain. These blocks have to be analyzed and authenticated to ensure seamless transactions across the network. But, the parties involved in issuing such currencies are not always equipped with the processing power of technology to ensure smooth transactions. This is where miners come in. Mining is the process of participating in a cryptocurrency network and solving mathematical problems. A miner is rewarded for his/her solutions. They also help the issuers of currencies to handle transaction blocks. Miners provide issuers with solutions that are used for the verification of transactions. After successful verification, issuers reward miners. Rewards are the portions of transactions verified by using solutions. Digital coins are also offered to miners. Cryptocurrency mining is the process in which transactions between users are verified and added into the blockchain public ledger. The process of mining is also responsible for introducing new coins into the existing circulating supply and is one of the key elements that allow cryptocurrencies to work as a peer-to-peer decentralized network, without the need for a third party central authority.

2.1 Cryptocurrency Feature

Decentralized

Unlike centralized banking systems, A major pro of cryptocurrency is that most are decentralized on distributed networks of computers that are spread around the world, also known as nodes. Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain. The transaction is propagated across the peer-to-peer network and is replicated by every node, reaching a large percentage of the nodes within a few seconds.

“Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and the system behaves like a single computer).” — Vitalik Buterin

Decentralization is the feature of most of the cryptocurrency including Bitcoin which increases the attack resistance power, collusion resistance capacity and decrease the fault tolerance level.

- Fault tolerance: decentralized systems are less likely to fail accidentally because they rely on networks of separate components.
- Attack resistance: decentralized systems are more expensive to attack and destroy or manipulate because they don’t have vulnerable central points that can be attacked at much lower cost than the surrounding system.
- Collusion resistance : it‘s harder for members of decentralized systems to act in ways that benefit them at the expense of others. On the other hand, corporations and governments collude in ways that benefit themselves but hurt others all the time.

Limited

Most cryptocurrencies limit the supply of the tokens. In Bitcoin, the supply decreases in time and will reach its final number sometime around the year 2140. All cryptocurrencies control the supply of the token by a schedule written in the code. This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today. There is no surprise.

Fiat currencies (e.g. dollars, euros) have an unlimited supply, as the central banks can issue as much fiat currencies as they want. Central banks often manipulate the value of the countries' currencies as part of its economic policies. Most countries often manipulate their currency to be inflationary over a period of time. The inflationary nature of fiat currencies would mean a decrease in the value of the currency over time. Therefore, fiat currency holders might bear the cost of the decrease in value and also face the uncertainty of currency manipulation. On the other hand, most cryptocurrencies have a limited and pre-determined supply of the cryptocurrency that is coded into its underlying algorithm when it is created. For example, Bitcoin has a maximum supply of 21 million, and once this limit is reached, no new Bitcoin can be mined. Cryptocurrency intentionally creates scarcity to prevent currency manipulation and the decrease of value over time.

International

These currencies don't care about the specific location: Cryptocurrencies don't care at all about the owner's physical location. You can send cryptocurrency to your relative down the street or you can send the same to a friend living in another part of the world. And the transactions would take the same time and would be treated similarly.

3. About Mining

Cryptocurrency mining, or cryptomining, is a process in which transactions for various forms of cryptocurrency are verified and added to the blockchain digital ledger. Also known as cryptocoin mining, altcoin mining, or Bitcoin mining (for the most popular form of cryptocurrency, Bitcoin), cryptocurrency mining has increased both as a topic and activity as cryptocurrency usage itself has grown exponentially in the last few years. Each time a cryptocurrency transaction is made, a cryptocurrency miner is responsible for ensuring the authenticity of information and updating the blockchain with the transaction. The mining process itself involves competing with other cryptominers to solve complicated mathematical problems with cryptographic hash functions that are associated with a block containing the transaction data. The first cryptocurrency miner to crack the code is rewarded by being able to authorize the transaction, and in return for the service provided, cryptominers earn small amounts of cryptocurrency of their own. In order to be competitive with other cryptominers, though, a cryptocurrency miner needs a computer with specialized hardware.

Mining is defined in the protocol, implemented in software, and is an essential function in managing the cryptocoin network. Mining verifies transactions, prevents double-spending, collects transaction fees and creates the money supply. Mining also protects the network by piling tons of processing power on top of past transactions. Mining verifies transactions by evaluating them against the transactions that happened before.

Just like mining gold or precious metals is performed to increase the number of metals in the market, digital mining is done to increase the number of digital currencies. Similarly, Ethereum mining is done to maximize the quantity of Ether in the market.

3.1 Proof of Work Mining

A proof of work is a consensus algorithm in which it’s costly and time-consuming to produce a piece of data, but it’s easy for others to verify that the data is correct. The most popular cryptocurrency Bitcoin is using Hashcash proof of work system. Although initial Hashcash idea was to fight against email spammers, Satoshi applied this idea to bitcoin transactions.

For a block to be accepted by the network, miners have to complete a proof of work to verify all transactions in the block. The difficulty of this work is not always the same, it keeps adjusting so new blocks can be generated every 10 minutes. There's a very low probability of successful generation, so its unpredictable which worker in the network will produce the next block.

In a network users send each other coins and ledger gathers transactions into blocks, but someone should take care of all transactions and validate them. In every blockchain some nodes are doing validation In the example of Bitcoin miners are nods. The way those nods authorize transactions depends on consensus algorithm, it doesn't need to be proof of work, but in Bitcoin example it is. Long story short, proof of work is a system which ensures security and consensus throughout blockchain network. It's evident that participant which validates block have invested significant computing power to do so.

PoW is adopted by Bitcoin,Ethereum, etc. PoW selects one node to create a new block in each round of consensus by computational power competition. In the competition, the participating nodes need to solve a cryptographic puzzle. The node who first addresses the puzzle can have a right to create a new block. It is very difficult to solve a PoW puzzle. Nodes need to keep adjusting the value of nonce to get the correct answer, which requires much computational power. It is feasible for a malicious attacker to overthrow one block in a chain, but as the valid blocks in the chain increase, the workload is also accumulated, therefore overthrowing a long chain requires a huge amount of computational power. PoW belongs to the probabilistic-finality consensus protocols since it guarantees eventual consistency.

3.2 PoS (Proof of Stake) Mining

In PoS, selecting each round of node who creates a new block depends on the held stake rather than the computational power. Although nodes still need to solve a SHA256 puzzle:SHA256(timestamp,previoushash…)<target×coin.The different from PoW is that nodes do not need to adjust nonce for many times, instead, the key to solve this puzzle is the amount of stake (coins). Hence, PoS is an energy-saving consensus protocol, which leverages a way of the internal currency incentive instead of consuming lots of computational power to reach a consensus. Like PoW, PoS is also a probabilistic-finality consensus protocol. PPcoin was the first cryptocurrency to apply PoS to the blockchain. In PPcoin, in addition to the size of the stake, the coin age is also introduced in solving a

PoS puzzle . For instance, if you hold 10 coins for a total of 20 days, then your coin age is 200. Once a node creates a new block, his coin age will be cleared to 0. In addition to PPcoin, many cryptocurrencies adopt PoS, e.g., Nxt, Ouroboros. Note that Ethereum plans to transition from PoW to PoS.

4. Problems with traditional mining

4.1 Hash power monopoly

When a successful majority attack allow the attacker to prevent some or all transactions from being confirmed (transaction denial of service) or to prevent some or all other miners from mining, resulting in what is known as mining monopoly.

4.2 Involuntary attack on the market

51% Attack

The best-known type of attack on public PoW blockchains is the 51% attack. The goal of a 51% attack is to perform a double spend, which means spending the same UTXO twice. To perform a 51% attack on a blockchain, you need to control a majority of the hash rate, hence the name. A malicious miner wanting to perform a double spend will first create a regular transaction spending their coins for either a good or for a different currency on an exchange. At the same time, they will begin mining a private chain. This means they will follow the usual mining protocol, but with two exceptions.

First, they will not include their own transaction spending their coins in their privately mined chain.

Second, they will not broadcast the blocks they find to the network, therefore we call it the private chain.

If they control a majority of the computing power, their chain will grow faster than the honest chain. The Longest Chain Rule in PoW blockchains governs what happens in case of such a fork. The branch, that has more blocks to it and accordingly represents the chain created with a larger amount of computing power is considered the valid chain.

Once the attacker has received the good or other currency bought with their coins, they will broadcast the private branch to the entire network. All honest miners will drop the honest branch and start mining on top of the malicious chain. The network treats the

attacker's transaction as if it never happened because the attacker did not include it in his malicious chain. The attacker is still in control of their funds and can now spend them again.

DDOS Attack

A Distributed Denial-of-Service (DDOS) attack in computing is an attack, where a perpetrator seeks to make a network resource unavailable to its users, by flooding the network with a large number of requests in an attempt to overload the system. It is an attack that not only blockchains but any online service can suffer from. In a simple form, the DOS (Denial-of-Service) attack, all these requests originate from the same source. This makes it somewhat easy to prevent. If a single IP-address sends a huge amount of requests that cannot be justified by legitimate reasons, you can have a measure in place that automatically blocks this IP-address. In the case of a DDOS attack, the distributed part refers to a large number of different sources that the malicious requests originate from.

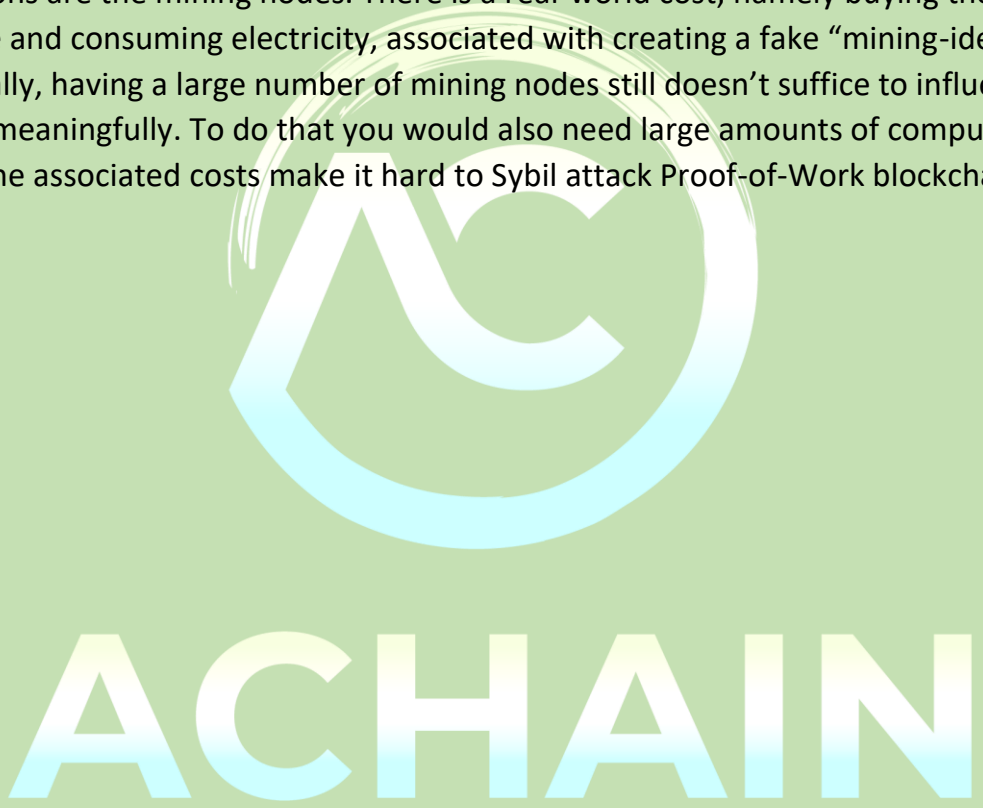
A DDOS attack is much harder to tackle because to do so you need to differentiate between legitimate and malicious requests. This is a very hard problem. In the context of blockchains, this comes down to an almost ideological question. The motivation to introduce transaction fees was to eliminate spam. Some people argue that as long as the requests have a transaction fee attached they cannot be considered spam by definition. While there are certainly situations where you could consider transactions to be spammy, it would be a slippery slope to start blocking them. One of the greatest value propositions of public blockchains is their censorship resistance. Starting to pick transactions that are not included - no matter of what criteria this censorship is based on - would be a dangerous precedent for any blockchain.

Sybil Attack

A Sybil Attack is an attempt to manipulate a P2P network by creating multiple fake identities. To the observer, these different identities look like regular users, but behind the scenes, a single entity controls all these fake entities at once. This type of attack is important to consider especially when you think about online voting. Another area where we are seeing Sybil attacks is in social networks where fake accounts can influence the public discussion.

Another possible use for Sybil attacks is to censor certain participants. A number of Sybil nodes can surround your node and prevent it from connecting to other, honest nodes on the network. This way one could try to prevent you from either sending or receiving information to the network. This “use case” of a Sybil attack is also called Eclipse Attack.

One way to mitigate Sybil Attacks is to introduce or raise the cost to create an identity. This cost must be carefully balanced. It has to be low enough so that new participants aren’t restricted from joining the network and creating legitimate identities. It must also be high enough that creating a large number of identities in a short period of time becomes very expensive. In PoW blockchains, the nodes that actually make decisions on transactions are the mining nodes. There is a real-world cost, namely buying the mining hardware and consuming electricity, associated with creating a fake “mining-identity”. Additionally, having a large number of mining nodes still doesn’t suffice to influence the network meaningfully. To do that you would also need large amounts of computational power. The associated costs make it hard to Sybil attack Proof-of-Work blockchains.



5. Overview of AC

AC is a new cryptocurrency based on AChain, which can effectively resist ASIC and avoid concentration of computing power. AC also adopts MPoW mining mechanism innovatively, which limits the mining participation entry. Through this mechanism, it could effectively avoid the power monopoly, reduce the amount of digital currency flowing into the market and increase the income of miners. There is no longer competition between minors, but cooperation, which makes AChain more secure and trustworthy to stimulate the sustained growth in quotation.

5.1 Problems solved by AC

AC is not only a new type of cryptocurrency, but also are shuffle of the traditional mining industry. It subverts the concept of traditional mining and can effectively solve the following problems:

Hash power monopoly

AChain using an improved AChain algorithm that can effectively resist the ASIC mining machine and prevent the power monopoly from the large miners which cause it is too difficult for retail investors to obtain profits.

Malicious attack on the market

The MPoW mining mechanism adopted by AChain can reduce the number of market circulation, increase the miner's coin- holding period, prevent miners from digging with selling which invisibly lead to malicious smash.

Over Increase of Computing Power

The MPoW mechanism can effectively control the number of mining machines to grow too fast. To increase the number of mining machines, there must be enough AC to be pre- stored in the wallet, which can inhibit the quantity increase of mining machines to avoid the loss of miners' interests.

Increase the Right of Miner

AChain mining must be held in AC and pre-stored in the wallet to mine for higher interest, AChain is more like a miner's rights protection. Only holderscan enjoy high returns, and not holding AC will not be able to obtain high profits.

Tamper-Resistance

Tamper-resistance refers to the resistance to any type of intentional tampering to an entity byeither the users or the adversaries with access to the entity, be it a system, a product, or otherlogical/physical object. Tamper-resistance of blockchain means that any transaction information stored in the blockchain cannot be tampered during and after the process of block generation

5.2 Principle of Achain

The design behind Achain is intended to follow the following principles:

Simplicity

The Achain protocol should be as simple as possible, even at the cost of some data storage or time inefficiency. An average programmer should ideally be able to follow and implement the entire specification so as to fully realize the unprecedented democratizing potential that cryptocurrency brings and further the vision of Achain as a protocol that is open to all. Any optimization which adds complexity should not be included unless that optimization provides very substantial benefit.

Universality:

A fundamental part of Achain design philosophy is that Achain does not have "features"Instead, Achain provides an internal Turing-complete scripting language, which a programmer can use to construct any smart contract or transaction type that can be mathematically defined.

Modularity:

The parts of the Achain protocol is designed to be as modular and separable as possible. Over the course of development, our goal is to create a program where if one

was to make a small protocol modification in one place, the application stack would continue to function without any further modification. This is so that even though they are used in AChain, even if Achain does not require certain features, such features are still usable in other protocols as well.

Agility:

Details of the Achain protocol are not set in stone. Although we will be extremely judicious about making modifications to high-level constructs, for instance with the sharding roadmap, abstracting execution, with only data availability enshrined in consensus. Computational tests later on in the development process may lead us to discover that certain modifications if any such opportunities are found, we will exploit them.

Non-discrimination and non-censorship:

the protocol will not attempt to actively restrict or prevent specific categories of usage. All regulatory mechanisms in the protocol should be designed to directly regulate the harm and not attempt to oppose specific undesirable applications. A programmer can even run an infinite loop script on top of Achain for as long as they are willing to keep paying the per-computational-step transaction fee.

6. Whai is the MPOW Mining?

In this paper, we introduce a new PoW consensus algorithm (MPoW) which requires miner to use SHA function to get specific number, n hashes and then use these hashes to construct a matrix($n \times 256$) that satisfies two criteria: the determinant of first $n \times n$ submatrix should be not less than a target which can be dynamically adjusted based on the block time; Also, the number of submatrices with non-negative determinants should be larger than another given value. This MPoW consensus algorithm can efficiently eliminate the dominant advantage of machines whose hashrates are hundreds or thousand of times larger than personal computers. This consensus algorithm may pave the way to a real decentralizated blockchain. Furthermore, our new PoW (MPoW) consensus algorithm provides a new way to utilize the properties of a matrix to implement an efficient and secure blockchain’s consensus algorithm.

6.1 MPOW Mining Interpretation

In this section, we will discuss the performance of our new MPoW consensus algorithm from the perspectives of blocktime, difficulty adjustment and its efficiency in preventing machines with hashrate advantage, such as ASICs or GPUs, from dominating all mining rewards. A. Mining First of all, we will discuss the difficulty adjustment for our MPoW consensus algorithm. As more and more nodes (miners) join into the peer-to-peer network, stabilization of the network's mining process require a stale block time to guarantee safety and decentralization. On the other hand, the block difficulty adjustment of MPoW algorithm needs to be gradual and smooth to achieve a stable block time (for Seele's main-net, the goal of block time is 10 seconds). there is a well-defined probability distribution for determinants of submatrices and for the number of "large submatrices". The difficulty adjustment formula is defined as follows:

$d = dp + dp\, f \times \max\ 1 - t - tp\ 10\ , -99$ (12)

Where: d is the current block difficulty,

dp is the previous block difficulty,

t is the current block time,

tp is the previous Block time distribution with dynamically adjusted difficulty.

The block mining process will try to find a target matrix which meets two criteria:

(i) The determinant s of the submatrix constructed by first 30 columns and 30 rows meets: $s \geq d \times 65$ (13) If the matrix meets the first criterion, in order to increase the calculation time percentage of mining a block, our MPoW consensus algorithm further requires the miner to calculate determinants of all submatrices and the number of the "large submatrices" to be as large as count.

(ii) (ii) count is defined as: $count \geq 256 - n\ 2 + n\ 5$ (14) where n is the row size of target matrix, here we use n = 30. In Fig.3, we present the difficulty and block time curves over block index. In order to better see the correlation between difficulty and block time, we intentionally set the smooth factor f in Equation(12) to 1. Generally, there is a strong correlation between the difficulty (red curve) and block time (blue curve). The difficulty is subsequently adjusted to be smaller if the block time increases, vice versa. This indicates our difficulty function works quite well in dynamically adjusting the difficulty.

The target matrix finding process is feasible and within a reasonable block time. For a better look, we also fit the block time with a sinusoidal function as in Fig.3. The coefficient values from the fitting curve roughly give us an average block time of 14 seconds which well matches our 10 seconds block time goal considering other processes, such as packing a block, takes some extra time. Finally, note that if we set smooth factor f to 2048 other than 1 (as we use in our Seele's main-net), the curves of difficulty and block time will be smoother with smaller deviations. B. Time Distribution Second, in the Fig.4, we show the results of hash time percentage within mining a block. The hash time percentage in the inset diagram of Fig.4 shows a clear regression to 30% with some random fluctuations. The histogram further confirms that the hash time percentage during mining a block is around 30%. By comparison, traditional PoW consensus algorithms, requiring miner to solve a hash puzzle, will take up almost 100% of hash time when mining a block. However, hash time percentage is balanced out by our new MPoW consensus algorithms requirement: miner should further construct a matrix and calculate the determinants of its submatrices instead of just hashing. In this case, we can not only keep the blockchain safe and feasible with one-way data conversion using SHA function but also eliminate the advantage of machines with high hashrates.

7. Smart Contract

Achain allows its users to build and execute smart contracts and distribute autonomous applications all without third-party censorship making it extremely easy to set up and complete transactions. Achain provides developers with a comprehensive set of tools to build decentralized applications. There are no third-party interferences, which makes using this blockchain extremely empowering. The team behind Achain are focused wholly on continually improving the underlying blockchain infrastructure as the recent Constantinople upgrade demonstrated. This is a company that is in it for the long-term rather than 'just cashing in the chips.' This commitment is very reassuring and allows Achain developers to operate with unparalleled freedom which cannot be matched by any centralized company.

7.1 Commercial application of smart contracts

Blockchain and the potential to help notoriously difficult industries.

Whether you're starting a new job or buying a new phone, contracts are integral to any official agreement. The sheer volume and complexity of traditional contracts can be overwhelming, involving high administrative costs, dependence on a third party system and often outright confusion. As processes are increasingly digitalised, it's become necessary to find a way to make reliable, digital business agreements. Enter the smart contract, a computerised protocol which stores and carries out contractual clauses via blockchain. The point is to avoid relying on third party systems, and allow visibility and access for all relevant parties. But what exactly can they be used for?

Insurance

Due to a lack of automated administration, it can take months for an insurance claim to be processed and paid. This is as problematic for insurance companies as it is for their customers, leading to admin costs, gluts, and inefficiency. Smart contracts can simplify and streamline the process by automatically triggering a claim when certain events occur. For example, if you lived in an area that was hit by a natural disaster and your house sustained damage, the smart contract would recognise this and begin the claim. Specific details (such as the extent of damage) could be recorded on the blockchain in order to determine the exact amount of compensation. The same series of events would happen following a car accident, or if somebody reported an insured personal device as stolen.

Supply chain management

Supply chain management involves the flow of goods from raw material to finished product. Smart contracts can record ownership rights as items move through the supply chain, confirming who is responsible for the product at any given time. This has become far easier using Internet of Things sensors, which track goods from producers to warehouses, from warehouses to manufacturers, and from manufacturers to suppliers. The finished product can be verified at each stage of the delivery process until it reaches the customer. If an item is delayed or lost, the smart contract can be consulted to find out exactly where it should be. If any stakeholder fails to meet the terms of the contract, for instance if a supplier did not send a shipment on time, it would be clear for every party to see. Making supply chains more transparent via smart contracts is helping to smooth out the movement of goods and restore trust in trade.

Mortgage loans

The mortgage process is far from simple. The terms of a mortgage agreement, for example, are based on an assessment of the mortgagee's income, outgoings, credit score and other circumstances. The need to carry out these checks, often through third parties, can make the process lengthy and complicated for both the lender and the mortgagee. Cut out the middle men, however, and parties could deal directly with each other (as well as access all the relevant details in one location). As a general rule, the simpler something is, the cheaper it will be – and through smart contracts, US lenders alone could reportedly save a minimum of $1.5bn.

Employment contracts

The relationship between an employee and their employer can be tempestuous, especially if either party fails to meet expectations. By entering into a smart contract, an employee would know exactly what was expected of them, as would the employer. Recording interactions in this way could help to improve fairness in wages or conditions, as any changes to contracts would be recorded. This openness could greatly improve the relationship between employers and their employees. Smart contracts could additionally be used to facilitate wage payments, according to the agreed amount and within a specific time period. Smart contracts could also help to regulate the use of temporary labour, which involves an employer, an agency and a worker. The worker joins the agency and is then hired by an employer. Unfortunately, a lack of transparency has meant that agencies can alter the contract's terms after workers have already started the job. This could mean shortening or lengthening the contract, changing wage rates or other worker's rights. It can be difficult for the authorities to detect these changes, but not if a smart contract system is applied.

Protecting copyrighted content

Every time that a piece of content is used for commercial purposes, for example a song, the owner of the rights to that song receives a royalty fee in theory. Of course, there are multiple parties involved in creating a song, and it can be hard to work out who owns these rights and who is therefore entitled to payment, plus existing systems do not work well. This has led to confusion over entitlement, no doubt giving some contributors more than they are due to the detriment of others while some receive nothing at all. Smart contracts can ensure that royalties go to the intended recipients by recording ownership rights in a decentralised blockchain system. This could theoretically be applied to any piece of content with a team of contributors.

Smart contracts have many benefits for a wide range of industries, reducing unnecessary costs and time expenditure while enhancing transparency. In theory, they are more efficient and trustworthy than traditional contract law, and are also thought to offer better security as all actions are recorded and verified. However, like paper contracts, they could still experience fraud. Code is not infallible and can be delayed, intercepted and corrupted. As businesses move forward into digital negotiations, an awareness of these risks is integral.

The traditional corporate hierarchy developed in the industrial age. Its system of executives, managers, middle-managers, supervisors and employees worked well when companies operated in relative isolation from the rest of the world and manufactured physical products. Today's global companies that sell ideas as often as they sell products encounter disadvantages when they use a traditional organizational structure.

8. Problem with Traditional Business

Long Decision-Making Time

If your small business has many layers of management, you may find that it can take a long time for the decisions to work their way through all the people that need to weigh in on an issue. Coordinating the input of multiple managers can require a level of compromise that waters down the decision-making process. In addition, you have to be adept at handling the politics of decision making with many managers so that no one feels their opinion is being ignored.

Message Distortion

As directives move through a traditional hierarchy, the message can get distorted. Each supervisor or manager may interpret your words differently until the message that reaches employees has little resemblance to what you intended. Even written instructions require interpretation. The same is true in reverse. If employees raise issues by reporting them to their immediate supervisors, complaints and suggestions may reach you after several levels of management. You may get an entirely different picture of what employees were trying to say.

Lack of Individual Authority

A traditional structure assigns authority to the position rather than to the individual. This means individual managers do not earn respect. They inherit it. This requires you to

constantly check the effectiveness of individuals in various positions to see if they have the actual skills for the job, or if they are counting on the authority of the position to maintain their status.

Inability to Adapt Globally

The traditional organization has a headquarters. Decisions that affect the entire company are made at headquarters. This can be a disadvantage in a global economy where people on the ground in specific locales need the authority to make decisions to adapt a company's strategy to the local population. The one-size-fits-all decision making of the traditional organization may cause the company to lose global customers.

Over-specialization

If your company has the rigid job descriptions that go with a traditional style of organization, you may find that employees limit their sense of responsibilities and their skills to just what the job requires. This can kill spontaneity and problem solving as employees increasingly declare "it's not my job" when confronted with issues. Employees who are anxious to get good performance reviews may focus exclusively on the requirements of their current positions and be reluctant to take on responsibilities outside of their positions.

9. AC Mining

The architecture focuses on decentralization and security, but also allows the maximum transaction speed that hardware and telecommunication technology allows today. Before designing architecture , analysis based on mathematics was considered and concepts got proved, under some assumptions, to be certain that the final product will be solid. All ecosystem is based on the core, and this is true for every blockchain. A weak architecture can attract attackers and decrease trust. A technological solid product based on sound financial fundamentals is the best option for real world uses cases and applications. That's why in our analysis we consider the cost factor for both dApps, users and network preserves (people running a node).

To better understand how concentration in a blockchain affects double spending attacks we consider pools and miners in an industrial organization framework. We find that concentration in mining power is harmless for the networks resilience against double spending attacks. The findings stem from the fact that, the larger a pool is, the more it loses if the network value collapses. Hence, even if a large pool is more able to conduct mischief, it should be less willing to do so. Our model is stylized, yet its intuition carries over to other settings where large miners, pools or coalitions receive economic profits.

Model Setup

Consider a world in which time is infinite and discrete and is indexed by t, t = 0, 1, 2, . . . There are two types of agents – miners and pools – having a discount factor $\beta \in (0, 1)$. Miners are homogeneous, risk averse and atomistic, whereas pools are risk neutral. In every period $t \geq 0$, miners choose their hashing power at a unit cost C, and hashing power allocation hm for each pool $m \in \{1, 2, ..., M\}$ and ho for solo mining.

Mining Pools

Mining pools offer different fee and reward contracts; the simplest mechanisms being proportional payment and pay- per-share . In a proportional reward system , whenever a pool wins a mining competition a miner receives

$$(1 - f^m)R\frac{h_i}{H_m} \qquad (1)$$

where h_i is the miner's hash rate contributed to the pool m, R is block reward, H_m is the total hashing power in that pool and

$f^m$is a fee collected by pool m. In a pay-per-share reward mechanism a pool effectively rents miner's hashing power and pays a rent regardless of whether the pool wins block rewards or not, fully insuring participating miners. However, pay-per-share is uncommon and usually associated with significantly higher fees. In addition, diversification of miner's hashing power to different pools would effectively insure miners against idiosyncratic risk. Hence, in our model we choose to concentrate on proportional reward mechanisms.

Collusive Equilibria

We restrict each pool's strategy to the standard super game grim trigger strategy. Specifically, consider the following strategy for M incumbent pools to collude:
1. Collusion: In every period, pools agree upon a fee $f\ c$. Miners allocate their hashing power to pools.

2. Punishment phase: once one of the incumbent pools does not have any participants, punishment phase is triggered and the pools enter into a Bertrand competition. In absence of marginal costs, and because the pools are homogeneous, the pools will receive zero profits. In a collusive phase the pools discounted future profits are

$$\sum_{t=0}^{\infty}\beta^t\frac{H_m}{h}f_cR = \frac{f^cR}{1-\beta}\frac{H_m}{h} \qquad (2)$$

where H is network's total hashing power and β is the time discount factor.

Corollary 1, ***A collusive strategy is an equilibrium if***

$$\sum_{t=0}^{\infty}\beta^t\frac{H_m}{h}f_cR = \frac{f^cR}{1-\beta}\frac{H_m}{h} > f^cR \qquad \forall\frac{H_m}{h} \qquad (3)$$

Corollary 1, states that the profit from lowering the fee, and hence capturing the whole market, should be less than the value of discounted future profits in collusion phase. From this naturally follows:

Proposition 1 If

$$\exists \frac{H_m}{h} \quad for\ which\ \frac{H_m}{h} < 1 - \beta \qquad (4)$$

no collusion equilibrium exists.

Proposition 1 states that – given the discount factor – there should not exist extremely small pools for collusion equilibrium to exist. E.g. for annual β of 0.9, there should exist pools vesting less than 0.0002 percent of hashing power for collusion strategy not to be a Nash Equilibrium. For the remaining part of the analysis we will assume that such pools don't exist in the market, thus a collusion equilibrium can be sustained. Above, we have assumed that R is constant. In reality, because rewards are paid in a cryptocurrency, they are highly volatile. In our model this would yield the same result, because pools are assumed to be risk neutral. In addition, (some) crypto-currencies 8 Electronic copy available at:

https://ssrn.com/abstract=3506748 have expected declines in rewards (e.g. BTC reward is halved every 210,000 blocks, which occurs approximately every four years). It is a standard result that in these cases the benefit from deviating would be highest just prior to the expected decrease in reward [Rotemberg and Saloner, 1986]. For parsimony we have restricted our analysis from considering such cases.

Entry and Collusive Fee Setting

Every period t ≥ 0 there exists a possible entrant pool without miners. Therefore, an entrant would set a fee $f^e < f^c$ to obtain miners. Prior to an entry the entrant pays a positive entry fee ζ. An entry will trigger the price competition phase and, hence, each pool makes zero profits post entry. Therefore, a condition for a feasible entry is given by

$$f^e R - \zeta > 0 \qquad \text{where } f^e < f^c \quad (5)$$

Corollary 2 It follows from feasible entry condition (Equation 5) that in order to deter entry colluding pools set a fee f^c

$$f^c \leq \frac{\zeta}{R} \qquad (6)$$

To keep the model parsimonious we have chosen a very simple barrier of entry as is manifested by Corollary 2.

However, one could equivalently assume that, once an entry occurs only an active fraction of miners observes it. Hence the active miners would face a trade-off between lower fees and smaller diversification benefits. In this case, to deter entry incumbent pools' fee setting strategy should make active miners indifferent between choosing an entrant pool or staying in incumbent pools. In addition, incumbent pools have likely established credibility for not siphoning rewards, having a reliable infrastructure etc. all attributes that an entrant might easily lack.

Miners

In every period t, a reward R is randomly assigned to a solo miner or a pool . The probability of winning the reward in every period t is $\frac{h_i}{H_m}$ for a solo miner and $\frac{H_m}{H}$for a pool, where H is network's total hash power and H_m is pool m's hashing power. Whenever a pool wins the mining competition it collects a fee $f^m \in (0, 1)$ and distributes the remaining reward to participants according to their contribution to the pool's total hashing power $\frac{h_i}{H_m}$. The miner j' s expected utility at t for t + 1 is hence given by the von-Neumann-Morgenstern Utility Function

$$U(H_J) = \frac{h_0}{H} u\left(R - C\sum_{i-0}^{m} H_i\right) + \sum_{i-0}^{m} \frac{H_m}{H} u((1-f^m)R\frac{h_i}{H_m} - C\sum_{i-0}^{M} h_i \qquad (7)$$

where, $U(\quad)$ is a continuous, monotonic and concave utility function and h0 is the allocation to solo mining and hm m ∈ [1, 2, 3, . . . , M] are the allocations to M

different pools. Each pool sets a fee f m to maximize its profit.

Equilibrium Hashing Power and Allocation

Proposition 2 Given fees and total hashing power, all miners' symmetric allocations among pools offering the lowest fee are Subgame Perfect Equilibria. Proposition 2 was initially discussed by Cong et al [Cong et al., 2018]. Following intuition of Modigliani-Miller [Modigliani and Miller, 1958] the initial pool size does not matter whenever miner's are able to diversify by allocating their hashing power to multiple pools. Hence, any 13

observed in most crypto-currencies, namely that small scale mining is not profitable.

As proposed above, all miners symmetric allocations are Nash Equilibria. Miners, however, would need to coordinate to reach this allocation. Hence, to simplify our analysis we make the following assumption:

Assumption 1

Miners coordinate their allocation amongst pools offering lowest fees at t by employing aggregate allocation at $t - 1$ as a focal point in every period $t > 0$. Miners' allocation at $t = 0$ is exogenously given. In the absence of a definite coordination device, a focal point may function as such [Schelling, 1960][Mehta et al., 1994][Bacharach and Bernasconi, 1997]. We argue that if a set of pools is homogeneous and provides the same service for the same price, previous aggregate allocation is a natural focal point for miners to allocate hashing power. This is accentuated, when there exists a large number of miners causing coordination to be unfeasible. An allocation determined by a focal point is an allocation in the set of possible Nash Equilibria allocations given by Proposition 2. The assumption implies that, ceteris paribus, pool sizes are stable.

Proposition 4 In equilibrium total hashing power H is a function of f, R and C

$$H = \frac{(1-f^C)R}{C} \qquad (9)$$

Proposition 4 follows from Proposition 3 by summing over all miners and it states that in equilibrium, because miners are fully insured against idiosyncratic shocks and make zero profits, total cost of hashing power equals the net reward.

Conclusion

Our aim while implementing a proof-of-work based blockchain consensus was to gain a better understanding of the protocol. While building the visualization tool, our aim was to provide a simple interface for a user to keep track of the system and further supplement the understanding of the protocol. Demonstrating robustness in the presence of failure is critical to any viable system, and we hope that in the future we can analyze the different vulnerabilities of the protocol Blockchain technology is in its early stages and there are many technical challenges that need to be overcome before it become part of mainstream commercial technology.

In conclusion, AC Network provides significant advances over existing approaches in scalable public blockchain. It provides unparalleled increases in PoW throughput while keeping the global hashrate, and thus energy required, constant. The confirmation latency of AC Network is also significantly decreased from traditional PoW and is potentially even 18 lower than that of PoS systems. AC Network achieves these advances while maintaining the core trustless, decentralized nature of PoW. This protocol enables greater practical decentralization and enables the creation of an ecosystem where enterprises, individual users, and large mining pools can co-exist peacefully by acting selfishly. AC Network avoids liquidity and centralization problems associated with using staked channels for scaling while also staying in the existing global regulatory context. We present in AC Network as a solution by which PoW can be scaled such that it support true decentralized economy.