COOPERATIVE APPROACH TO BLOCK CONFIRMATION

[Document subtitle]

CARSON ROSCOE
DECEMBER 7TH, 2017

Abstract

The proposed study aims at exploring how a cooperative approach to blockchain confirmation mechanisms compares to the standard competitive approach. This exploration spawns from a desire to solve the scalability problem of cryptocurrencies, as well as to determine how to create a blockchain system that can support applications with heavy networking requirements, such as videogames. The research question being asked by the proposed study is “How would one replace competitive proof-of-work with cooperative proof-of-gameplay for decentralized blockchain game servers”. The proposed study will be conducted by creating a blockchain system with three separate confirmation mechanisms. It will implement the standard method, proof-of-work, the second most frequent method, proof-of-stake, and a theorized cooperative take on proof-of-stake, which is referred to as proof-of-gameplay. Benchmarking will be run on the performance of the system using the three implementations in various test scenarios, and then the data will be analyzed. A conclusion then will be pulled regarding how the differing cooperative mechanism compared in scalability to the traditional competitive mechanisms.

Table of Contents

Introduction

Background

As the blockchain field matures from infancy to adolescence, the Bitcoin protocol faces more scrutiny and criticisms. Concerns regarding scaling have been addressed, with the Bitcoin network itself forking twice in 2017 over scaling solution disputes.

However, Bitcoin's flaws have not been a hidden problem. Hundreds of altcoins, alternative cryptocurrencies to Bitcoin, have been developed over the last few years, many of which attempting to solve issues with the underlying Bitcoin protocol. Some altcoins have succeeded in some ways but failed to attract a big enough following to prove their success, while others have proven to be successful while finding other flaws in the mean-time. No cryptocurrency has yet proven to be scalable enough, nor fast enough, to power a real-time server with adequate performance. The cryptocurrency scaling problem is an estimated multibillion dollar problem, who's solution has not yet been proven.

There are many claims as to which parts of the protocol present the biggest bottleneck. Many believe it is not a protocol issue at all, simply an implementation issue, where Bitcoin's implementation simply defined a block size that's too small. They believe the solution is to simply increase the block size so blocks never fill up, and therefore the network never gets delayed. A similar group believes it is also an implementation issue, where the issue is the ten-minute delay between Bitcoin blocks in creation time, believing reducing this time is all that's required.

On the other side of the debate, some believe the protocol itself to be flawed specifically. A common section of the protocol that is believed to be both a artificial bottleneck, as well as a generally inefficient piece computationally, is the proof-of-work mechanism. The proof-of-work mechanism requires multiple miners on the system to expend energy solving the same problem as one other, with the first one to solve it being the only user rewarded. Alternatives have been proposed, such as proof-of-stake and proof-of-activity.

Another section of the Bitcoin protocol that has been under debate is if it should include the ability to atomic swap. Atomic swapping is a mechanism certain blockchains implement that allows for cross-communication of blockchains. This would allow work to be done on temporary blockchains following rules that are understandable by Bitcoin, and then submitting the results to the Bitcoin blockchain for permanent storage. This is known as a second layer solution, as it suggests putting a

compatible layer on top that is used directly, with that layer being the portion that communicates with Bitcoin.

These solutions, both for and against modifying the underlying protocol, all face heavy scrutiny. Many believe raising the block size or reducing the block time will increase the overall size of the blockchain excessively. Many also believe replacing proof-of-work with an alternative may present security risks that have not been fully addressed. Second layer solutions are also under heavy scrutiny, as users fear layers may become centralized. These concerns, and more, arise when solutions are proposed.

The solutions that has seen the most success, as well as has been explored the most academically, has been those that try to replace the proof-of-work mechanism. The proof-of-work mechanism has successfully been replaced by proof-of-stake in many cryptocurrencies, often showing tremendous improvements in energy consumption. This removes a artificial bottleneck that is the mining process, which also reduces the energy usages to secure the network tremendously, however the system is still constrained by the rate blocks are created and the size of a block. This means other bottlenecks still must be addressed for a proof-of-stake system to scale adequately.

The similarity between proof-of-stake and proof-of-work is the competitive nature in the mechanisms. Proof-of-stake simply bases the value of a users vote on their stake in the network, while proof-of-work bases the value of a miner's block on the work put into its creation. Each have users competing against one another, proof-of-stake simply competes more efficiently. The competitive nature appears to cause the scenarios that require validation, opening a new avenue for discovery; What if a mechanism was cooperative, rather than competitive?

Problem statement

It is unknown how a cooperative mechanism affects a cryptocurrencies efficiency, nor how a blockchain protocol meet real-time server requirements.

Sub-problem 1

To analyze and compare the competitive proof-of-stake mechanism to competitive proof-of-work, validating that proof-of-stake is a valid alternative from a security standpoint.

Sub-problem 2

It is unknown how a cooperative confirmation mechanism would affect the security compared to its competitive implementation.

Sub-problem 3

To analyze the throughput, scalability and bottlenecks of a proof-of-work mechanism, as well as a proof-of-stake mechanism.

Sub-problem 4

To analyze the throughput, scalability and bottlenecks of a cooperative proof-of-stake mechanism.

Sub-problem 5

To determine what an analysis of sub-problem 3's and sub-problem 4's results show about what can be revealed comparing proof-of-work with proof-of-stake, as well as what can be revealed regarding comparing competitive mechanism with a cooperative alternative.

Research Question

Following the problem statements driving this research, the research question is "How would one replace competitive proof-of-work with cooperative proof-of-stake for decentralized blockchain game servers".

Hypothesis

A cooperative approach may increase the scalability of blockchain technologies by a significant margin. This would be

Terms and definitions

Blockchain: A structure of data which contains multiple blocks of data linked together. Each block contains information about all the transactions or changes of data that occurred to recreate its current state. Blockchains utilize hashing to prove the order of blocks and validate if a block truly fits in it's blockchain.

Cryptocurrency: A digital currency that traditionally is built using blockchain technology as it's core data structure, as well as traditionally using a mechanism known as proof-of-work to decentralize the validation process.

Bitcoin: The first digital currency to solve the double-spending problem, which it accomplished by inventing and incorporating the proof-of-work mechanism.

Proof-of-work: A mechanism used by Bitcoin and many other cryptocurrencies to distribute block creation and transaction validation. It requires every miner to expend computing power creating

validation work for the created block, with the first miner to succeed being the one rewarded for their efforts.

Miner: A user in a proof-of-work system who gathers transactions, builds a block out of them, finds work for their block then propagates their block to the network.

Proof-of-stake: A alternative to proof-of-work where financial stake in the network is used to determine which blocks to add to the blockchain, rather than expended work.

Delimitations and limitations

The proposed study's scope will be limited to gathering and analyzing data comparing competitive proof-of-work, competitive proof-of-stake and a theorized cooperative proof-of-stake which will be referred to as proof-of-gameplay.

The proposed study will not explore frontend programming for these systems, nor will a program be developed that inherently utilizes the proposed software. A system will simply be developed that can run in either proof-of-work mode, proof-of-stake mode and proof-of-gameplay mode, which will then be stress tested and analyzed in artificial situations for each mode.

Assumptions

Network Scalability

It is assumed that the scalability of a confirmation mechanism is unaffected by propagation time, and instead only affected by the amount of transactions sent. The testing environment will not fully simulate propagation time.

Hardware Performance

All computers used during the experiment for testing will run on the same hardware as one other. It is assumed that the performance difference from one computer to another is therefore insignificant. It is also assumed that even if there is a significant performance difference present, it would not skew the results as every test for every mechanism would include the faulty computer equally.

Importance of the study

Cryptocurrencies are becoming a popular digital cash, and their underlying technology is beginning to see uses outside of the digital cash ecosystem. Some of these new uses include servers for

decentralized applications, yet none yet have been able to support a real-time videogame or equal payload application. With the popularity of cryptocurrencies exploding recently, and being such a recent technology, the technology's scaling potentials are being tested and scrutinized. Solutions have been proposed, but to date, there has been no solution that scales well or uniformly. The most promising solution at present appears to be developing an alternative to proof-of-work, such as proof-of-stake. One aspect of these mechanisms that has not been explored is changing how they function from a socioeconomic perspective. Currently, these mechanisms are competitive, where miners fight over being the miner who validated the block first and receives the award. This is a capitalistic behaviour that results in a disproportion of wealth distribution, disproportion in work distribution, and an artificial bottlecap for the competition to occur. A cooperative approach, where users validate each other, has not yet been explored. The benefits of this approach are not yet known, however could result in a network speedup as it simplifies the structure significantly. The benefits of conducting this research are that developers of existing and future cryptocurrencies will have another alternative to proof-of-work like competitive mechanisms when developing their blockchains, that could potentially scale to support live videogame servers with high payloads.

Literature Review

This literature review will focus on the flaws surrounding proof-of-work, how it causes a misalignment of interests in users, the inefficiencies of the mechanism, and explored alternative mechanisms.

A Literature Review of Blockchain's Proof-of-Work, Flaws and Alternatives

Blockchain technology has been a rapidly growing interest over the last few years in technology focused communities, as well as in investment focused communities. From blockchain technology grew Bitcoin, the first blockchain based digital cash to solve the double spending problem. Bitcoin paved the way for a new genre of digital currencies known as cryptocurrencies, most of which rely on the proof-of-work mechanism developed by Satoshi Nakamoto during the development of Bitcoin. Proof-of-work is a mechanism used for determining the order in which transactions took place. In the system a type of user referred to as a miner utilizes their GPU time to compete in a race over hashing and validating a block of transactions. The first miner to verify all the recent transactions were legitimate, and to show the appropriate work as proof to other miners, earns a payment in Bitcoin for their efforts [1][2]. This system secures the Bitcoin network and allows for alternating independent individuals to contribute to

the decentralization of the blockchain, without any centralized servers or governing bodies. Proof-of-work has been successful in providing security to a decentralized network, however it isn't without consequence. It results in a misalignment of interests between general users, who want a fast, low-fee network, and miners, who are motivated by returns on their investment. Proof-of-work is also purposely inefficient in it's processing usage, as it requires multiple miners to each spend processing time verifying the same transactions, with each miner expending energy trying to find valid work. My research question, "How would one replace competitive proof-of-work with cooperative proof-of-gameplay for decentralized blockchain game servers", is aimed at addressing the issues with proof-of-work and layout an alternative tailored for a decentralized videogame server.

Misalignment of Interests

The first consequence of proof-of-work to address is the misalignment of interests between general users and miners. A user in a cryptocurrency network has a variety of interests, including the security of their assets, security of transactions, cost of transacting, ease of transacting and transaction confirmation times. The interest of miners, however, is one of profit. Miners are in competition with one other to be the first miner to mine a block. Miners pick and choose which transactions make it into their blocks, allowing them the freedom to prioritize transactions based on which would pay them the greatest in fees. Miners prefer less competition to gain a higher portion of the total hashing power, despite this desire conflicting with the desire of a secured decentralized system [4]. Miners may also resist future changes that benefit users, if those same changes do not benefit the miners. This phenomenon has occurred multiple times on the Bitcoin network, with the most recent example occurring on August 1st of 2017. A fork occurred, which is a split in a blockchains network, where one part of the Bitcoin ecosystem chose to move forward with changes to Bitcoin which would solely benefit users while hurting miners, and the rest stayed back, refusing to upgrade. This upgrade caused a change in the mining algorithm which would break certain existing mining hardware, however heavily benefit users in terms of transaction speeds, transaction fees, confirmation times and would also heavily benefit the decentralization of the network. The current miners, having sunk costs into such hardware and desiring to keep the system centralized to just those who have such hardware, refused to upgrade. On the other side of the debate, the clear majority of users accepted the upgrade. This conflict resulted in a split of the Bitcoin network, creating a new coin known as Bitcoin Cash, which is effectively the legacy Bitcoin version from the miners who refused the upgrade. Human nature has shown to be the cause of virtually every cryptocurrency split, with proof-of-work being one of the frequent mechanisms causing the lack of unity in these cryptocurrency ecosystems. Creating an alternative where different users do

not have separate roles in the system is crucial in aligning these interests to better avoid these issues in the future.

Inefficiencies in Proof-of-Work

The next consequences to address are those that stem from the proof-o f-work mechanism's inefficiencies. Proof-of-work forces miners to do duplicate work in a race with each other, each attempting to be the first miner to solve their block. This means multiple miners are validating the same transactions, and then discarding their work once they see a new completed block to mine. Once all the transactions have been validated, but a finished block is still not received from other miners, the mining system has miners keep trying to find a hash for their block that starts with a set amount of zero bits [1][2]. This artificial work both throttles the system, as well as wastes processing power doing work whose whole purpose is to simply determine which miner gets the right to determine the current block. The proof-of-work mechanism boils down to simply being a solution to a synchronization problem. The equivalent problem, if written in a threaded software program, would be one where multiple threads want to write to the same buffer while validating what the other threads wrote. The proof-of-work solution is to keep randomly guessing a number, and have the first thread who guesses the correct number being allowed to write to the buffer. The system is secure and reliable at decentralizing block creation, however inefficient in how it goes about these goals.

Alternative Mechanisms

Alternatives to proof-of-work currently exist, which various other papers have discussed in the past. The most common alternative mechanism seen in cryptocurrencies is the proof-of-stake mechanism, which allows users to view their cryptocurrency holdings as their stake in the network, and get voting rights based on that stake [3][4][5]. Another alternative mechanism is a hybrid approach of proof-of-work and proof-of-stake known as proof-of-activity. These existing solutions succeed in being alternative mechanisms for a blockchain based cryptocurrency, however they do not work perfectly, in their raw form, for blockchain products that do not have the same technical requirements as a currency. Proof-of-stake relies on having a form of cryptocurrency to act as your holdings, whereas not all blockchain products necessarily possess a dedicated token or cryptocurrency in their implementations. Products may have different requirements that currencies do not have, such as requiring near-instant transactions, or near-instant confirmations. One example of such systems would be a videogame server, which uses blockchain technology to run a decentralized online video game while maintaining a consensus on the games state across every player. Such a system would not have a dedicated currency

for users to own a stake in without relying on that stake being a videogame currency, which would be ineffective due to the lack of wealth equality in video games when comparing inexperienced players to veterans. A system would be required where the top ranked players could not simply pool their power together to break the system, which is what would most likely occur in a proof-of-stake implementation. Proof-of-activity is an effective alternative in theory, however it relies on two rounds of communication to establish a block, whereas proof-of-work, proof-of-stake and proof-of-burn do this in one round of communication [6]. This results in proof-of-activity having to deal with double the latency, which is not a constraint that most online games can accept.

Filling the Niche

The lack of alternatives that fit this niche use of blockchains leads to the question, "How would one replace competitive proof-of-work with cooperative proof-of-gameplay for decentralized blockchain game servers". The previous papers I've referenced on proof-of-stake, and proof-of-activity all attempted to fix various parts of proof-of-work, each under their own constraints. Other papers I've read, specifically on Smart Contracts [7][8] but also on transaction channels [9][10], have shown how one can execute useful work on the blockchain in a timely manner, with transaction channels doing so utilization a second layer solution. My research question is effectively intending on creating an alternative mechanism to proof-of-work which treats all users as equals, does not inherently require a underlying currency, and allows for gameplay to execute across the blockchain in near real-time conditions.

Methodology

Required data & test scenarios

The data required for this research is data pertaining to the efficiency of each mechanism while successfully validating the network. Over multiple test scenarios, data will be gathered. The independent variable that changes between tests is the confirmation mechanism implemented. A grouping of pass-or-fail security test scenarios will also be run, gathering data proving that security is not compromised when using alternative mechanisms to proof-of-work.

For each performance test scenario, various pieces of data must be gathered. These pieces include the end blockchain data structure size in megabytes after the test scenario has completed, the average transaction time over a simulated network, average confirmation time, theoretical transactions per second throughput as well as recorded transactions per second throughput.

For each of the security test scenario, a simple pass or fail test recorded. These scenarios will all attempted double-spend attacks. We check for double-spend attacks as that is the problem that was solved by the creation of proof-of-work, so alternatives must also prevent against such an attack.

Research Methodology

The proposed study is designed to explore a cooperative approach to transaction validation rather than a competitive one, while also comparing the performance of both proof-of-work with proof-of-stake mechanisms. The proposed study also wishes to explore if such an approach can achieve real-time networking speed requirements that a game may require. The study will follow Quasi-Experimental Design due to the non-equivalent groups being tested. Each mechanism is it's own entity being compared, and therefore is it's own non-equivalent group.

Sampling

The test scenarios will resolve taking various samples of data. For each test, a stress test occurs where data is sampled every fifteen minutes for twenty-four hours. Tests will be run, modifying the number of simulated users on the system, as well as the amount of transactions per second sent for each simulated user. In total, the testing will range from a minimum of fifty users sending a transaction every ten seconds, up to a hundred thousand users sending two transactions a second. The users will be simulated over ten computers.

Instrumentation

As no similar research studies could be followed, this proposed study will include the creation of its own instrument. The measuring instrument will be built into the blockchain system being created for the study, therefore the software will benchmark its own performance. For this study, all the computers the software is being run on will possess the same hardware.

Data Collection

As explained above in the Required Data & test scenarios section, various tests will be run, gathering data regarding the performance benchmarks and security confirmation.

The data gathered regarding measured blockchain size, transactions per second, transaction backlog and orphan blocks are all required for benchmarking comparisons. This information is ratio scale.

The data gathered regarding security confirmation includes running sample scenarios in which proof-of-work will, by design, solve the security flaw. These tests are pass-or-fail, where a mechanism is only a valid alternative if it passes every test. Therefore, this testing delivers nominal scale data regarding whether the mechanism passed or failed the scenario.

Data usage

Memory Size

For each test scenario and mechanism, the end blockchain size is benchmarked. From this we can compare the differences in memory usage for each mechanism, determining which is the most memory efficient. Significances testing will be done, as well, to check whether the differences in memory usage between mechanisms is significant or not.

The differences between test scenarios is determined by the number of simulated users and the amount of transactions per second a user produces. Therefore, the difference between each test comes down to the amount of transactions being attempted on the network per second. As these comparisons will be drawn for each scenario, it is impossible to run the test for every transactions-per-second parameter, therefore we will compare the significance values between each scenario, using confidence intervals, to determine how confident the results are that a mechanism outperforms another for any scenario by any significant margin.

Transaction Time vs Transaction Throughput

For each test scenario and mechanism, the amount of transactions successfully run through the blockchain and the amount of transactions backlogged, are both benchmarked. From this, similar analysis will be run on these pieces of data to that of the memory size. Significance testing will be done to showcase the significances of the differences in transaction throughput and transaction times. Afterwards, using confidence intervals, it will be determined the confidence of these results.

Orphan Blocks and History Uncertainty

Orphan blocks are excess blocks that are the result of error resolution on the blockchain. When conflicts occur, where two miners both create a block at roughly the same time that are both valid, one of the two blocks will not be used and therefore orphaned. It increases the blockchain size by containing duplicate transactions that are already stored. The length of a chain of orphan blocks determines the duration of uncertainty within a system, where each block represents uncertainty for the duration it took from creation until the blockchain appends the block which follows it.

After each test, a tally will occur on the number of orphaned blocks on the blockchain. Instead of the statistics being done on the number of orphaned blocks, however, it will be done on the amount of orphaned transactions inside those blocks, as well as on the total amount of time the blockchain spent uncertain. This reinterpretation of data before statistical analysis is due to the fact that the cooperative mechanism approach may result in zero orphaned blocks appearing if it redefines the validation process, however it still may result in uncertainty with specific individual transactions.

Using the data regarding orphaned transactions and uncertainty time, significance testing and then confidence intervals will be used to determine the significance of the differences in the data, and then the confidence that such a similar performance results would occur for other scenarios.

Security

Pass or fail security tests will be run on each of the three implementations. These tests are to validate the implementations are implemented correctly, as well as to confirm that any proof-of-work alternative tested also functions as a valid alternative from a security standpoint.

The expected outcome is that all tests pass for both competitive mechanisms, however may pass or fail for the cooperative mechanism. If the cooperative mechanism does not pass the security tests, it then does not fulfill the role adequately that proof-of-work solves in blockchain technologies

and is therefore not a valid alternative. If the cooperative mechanism does pass, it then fulfills the goal of proof-of-work equally from a security standpoint and is a valid alternative.

Any other result from these tests would indicate a failure in the developed software implementation built for the study.

Proposed Study Outline

Outline

The study plans on comparing the performance between proof-of-work, proof-of-stake and a modified version of proof-of-stake that is cooperative in nature rather than competitive. The study wishes to know if a significant difference in scalability of speed can be achieved through implementing a confirmation mechanism, such a proof-of-stake, in a cooperative fashion rather than a competitive fashion.

Qualifications of the Researcher

The qualifications of the researcher who can accomplish the proposed study is one who has either extensive knowledge of blockchain technology and programming, or must be assisted by a professional who does. It is assumed that the researcher has access to a computer lab with at least ten computers.

Steps

The following steps will be taken:

Step 1: Develop a blockchain system that can run either using proof-of-work or proof-of-stake.

Step 2: Design and implement into the developed system an alternative mechanism, based on proof-of-stake, who's function is cooperative in nature rather than competitive. What this means exactly is that transactions of users would validate other user's transactions, cooperatively securing the network as it's shared, rather than having users compete over creating and propagating blocks of validated transaction every set interval.

Step 3: Monitor and gather data regarding the performance of the blockchains in various test scenarios. This data gathering procedure will be repeated for the blockchain system in all three modes independently.

Step 4: Analyze the data gathered, comparing the performances of each mechanism.

Timeline

The research will be conducted over approximately two months. The first month is designated for Step 1, building the simple blockchain system with proof-of-work and proof-of-stake implementations. The following two weeks would be used for designing and implementing the

alternative system required for Step 2. The last two weeks are for Step 3 and 4, where the testing will be carried out and analyzed.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2] Decker, C., & Wattenhofer, R. (2013, September). Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on (pp. 1-10). IEEE.

[3] Bentov, I., Gabizon, A., & Mizrahi, A. (2016, February). Cryptocurrencies without proof of work. In International Conference on Financial Cryptography and Data Security (pp. 142-157). Springer Berlin Heidelberg.

[4] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19.

[5] Vasin, P. (2014). Blackcoin's proof-of-stake protocol v2.

[6] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract] y. ACM SIGMETRICS Performance Evaluation Review, 42(3), 34-37.

[7] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper.

[8] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Security and Privacy (SP), 2016 IEEE Symposium on (pp. 839-858). IEEE.

[9] Decker, C., & Wattenhofer, R. (2015, August). A fast and scalable payment network with bitcoin duplex micropayment channels. In Symposium on Self-Stabilizing Systems (pp. 3-18). Springer International Publishing.

[10] Kraft, D. (2016). Game Channels for Trustless Off-Chain Interactions in Decentralized Virtual Worlds. Ledger, 1, 84-98.