Proof-of-Play: A Novel Consensus Model for Blockchain-based Peer-to-Peer Gaming System

Ho Yin Yuen
The Hong Kong Polytechnic University
Hong Kong, China
andy.aa.yuen@connect.polyu.hk

Feijie Wu
The Hong Kong Polytechnic University
Hong Kong, China
harli.wu@connect.polyu.hk

Wei Cai*
The Chinese University of Hong Kong, Shenzhen
Shenzhen, China
caiwei@cuhk.edu.cn

Henry C.B. Chan
The Hong Kong Polytechnic University
Hong Kong, China
henry.chan.comp@polyu.edu.hk

Qiao Yan
Shenzhen University
Shenzhen, China
yanq@szu.edu.cn

Victor C.M. Leung
Shenzhen University
Shenzhen, China
vleung@ieee.org

ABSTRACT

Data storage in peer-to-peer (P2P) games in a perfect applications scenario for blockchain. However, suffering from high transaction cost and latency, proof-of-work (PoW) becomes the bottleneck of blockchain games. Many attempts have been made to overcome various limitations of blockchain for P2P games, but many of them require modifying the game itself to be compatible with a blockchain solution. These overheads often bring new undesirable results to deal with. In this paper, we propose Proof-of-Play, a novel consensus model, to address these issues with a blockchain naturally integrated with P2P games, with minimum intervene to the game. The ultimate goal is to create a secure and fully decentralized architecture to transform a game being community-sustainable.

KEYWORDS

Blockchain; Security; Consensus Model; P2P; Games

ACM Reference Format:
Ho Yin Yuen, Feijie Wu, Wei Cai, Henry C.B. Chan, Qiao Yan, and Victor C.M. Leung. 2019. Proof-of-Play: A Novel Consensus Model for Blockchain-based Peer-to-Peer Gaming System. In *2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI '19), July 8, 2019, Auckland, New Zealand.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3327960.3332386

1 INTRODUCTION

Peer-to-peer (P2P) games are among the most popular categories of multiplayer games, especially when multiplayer online battle arena (MOBA) games, such as Dota[1] and League of Legends[2], dominate recent video gaming market. P2P gaming architecture decentralizes a game network by having every player acts as the client and the server at the same time, such that all the game server hosting effort is distributed among players. P2P architecture receives a great deal of research attention [1][16] due to its high scalability, especially in a network intensive game genre like Massively Multiplayer Online game. However, pure P2P gaming architecture with distributed data storage is rare, due to the vulnerability to cheating behaviors in decentralized P2P data storage, in which every player is in control of some piece of game objects. Therefore, a centralized server is still required to save the data for the participating players, including account balance, battle records, etc.

On the other hand, the blockchain system [12] has introduced a decentralized, transparent and trustworthy platform, which is resistant to data modifications. Apparently, it is a natural fit for P2P games. The immutability of blockchain data makes it a perfect solution to the distributed data storage issue in P2P gaming, such to avoid various tampering issues like distorting player's combat historical records. In fact, the adoption of blockchain for data storage can also remove the single point of failure problem in P2P games, which means the whole gaming ecosystem can be sustained by the players' community rather than the game operator. In addition, by leveraging cryptocurrency driven by the blockchain, the participating players are able to use a unified, fine-granularity, and transparent token to stimulate the gaming ecosystem, including the incentives for data storage and in-game economics.

Nevertheless, the blockchain integration model for the P2P gaming system is yet to be investigated. A straight forward idea is to adopt a conventional public blockchain system, e.g. Ethereum[3] [4], as an external data storage. These blockchains are commercial platforms enabling immutable data writing and reading services. For example, CryptoKitties[4] [3], a web-based kitty collection game, utilizes Ethereum to store its gaming data. In particular, the virtual kitties can be purchased and traded through smart contracts [10] by the players, while all gaming data are synchronized in the

[*] corresponding author

BSCI '19, July 8, 2019, Auckland, New Zealand
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6786-8/19/07…$15.00
https://doi.org/10.1145/3327960.3332386

[1] http://www.dota2.com/
[2] https://na.leagueoflegends.com/
[3] https://www.ethereum.org/
[4] https://www.cryptokitties.co/

blockchain after each operation performed by the players. However, the bottleneck of system performance is the cost and delay overhead for the data synchronization to the blockchain, which is introduced by the proof of work (PoW) [2] consensus model proposed in Satoshi Nakamoto's classic Bitcoin whitepaper[11].

The consensus model [14] is the key technique to keep independent parties in a blockchain to agree on the data that should be stored in the network. The purpose of the consensus model is to solve one of the major problem in a decentralized system, the Byzantine Generals' Problem [8]. The Byzantine Generals' Problem stated that a decentralized system must require a certain number of honest users, otherwise certain type of algorithm has to be implemented to guarantee a majority consensus on the decisions of the decentralized system. Satoshi's PoW approach requires participating nodes to compete for the privilege of writing blocks with each other in solving a puzzle, which is a mathematical calculation to scan for a numeric value whose hash value is smaller than a specific threshold. The computational difficulty of PoW reduces the collision of puzzle solver, thus, enforces a public consensus over the PoW winner to secure the majority consensus. Apparently, PoW is the primary cause of monetary cost and delay in a blockchain. So, many attempts on building a consensus model have been made.

In this work, we explore the similarity of the nature of P2P gaming system and blockchain, and investigate the possibility to leverage the gaming behavior as part of the consensus model in a blockchain. We dive deep into this idea to proposes Proof-of-Play (PoP), a consensus model for the blockchain-based P2P gaming system and evaluate its ability in keeping data integrity as a consensus model in comparison to other major consensus models.

The rest of this paper is organized as follows. We reviewed the related work of the gaming system with blockchain in Section 2 and presented the overview of the proposed PoP consensus model in Section 3. We then present the technical design and test-bed implementation in Section 4, and Section 5.1, respectively. Then, ao experiments are conducted to validate our system in Sections 5.2. A short case study of PoP is conducted against other major consensus models in Section 6. Finally, Section 7 concludes this paper.

2 RELATED WORK

2.1 Blockchain Systems

A blockchain system consists of blockchain data structure, consensus model and P2P network. The blockchain data structure, by definition, is a continuously growing chain of blocks, each of which contains a cryptographic hash of the previous block, a time-stamp, and its conveyed data [12]. The blockchain data structure is designed to resist modifications. With the help of P2P system and proof-of-work (PoW) [2] consensus model proposed in Bitcoin [11], the blockchain system can be utilized to support decentralized data synchronization, which becomes the foundation of decentralized ledgers. In order to add more values to the blockchain ecosystem, Ethereum [4] was implemented to facilitate decentralized smart contracts, which are immutable and transparent executable programs hosted by the blockchain. Nowadays, the blockchain-based decentralized applications (dApps) [13] have been extended to various areas, including initial coin offerings (ICO), social networks, networked games, and IoT.

2.2 General Consensus Models

As discussed in Section 1, PoW requires participating nodes to do useless mathematical works for the privilege of writing blocks, which brings the energy and time inefficiency issue to the blockchain systems. Therefore, a number of novel consensus models have been proposed as alternatives for general purpose blockchains.

Proof-of-Stake (PoS) [15] chooses the producer of the new block based on their stake on the network. For example, coin age is defined as the time of the coin left unspent, the higher the coin age of an individual, the more likely the individual will mine a new block. In other words, the richer an individual is, the more blocks the individual will mine in the blockchain. However, since holding tokens in different forks introduce no extra overhead for the stakeholders, PoS blockchains will spawn a large number of forks that reduce the value of the network. This is known as the nothing-at-stake problem.

Proof-of-Excellence [15] is a conceptual model mentioned in the PoS whitepaper. It stated that "a tournament is held periodically to mint coins based on the performance of the tournament participants, mimicking the prizes of real-life tournaments". Essentially, the node for the blockchain to hold consensus with is chosen via a game. However, in this model, good players will be more likely to win a game, this creates an unfair situation where good players will be able to write blocks repeatedly. So, the blockchain will become a partially centralized platform controlled by elite players.

Delegated Proof of Stake (DPoS) consensus model[5] solves the PoW overhead issue from another aspect: network participants delegate their rights of producing blocks to a small group of supernodes, which write blocks in turns for all users in the blockchain network. High throughput and low latency have been achieved in such a model. However, the public is still criticizing that DPoS being a partially centralized platform since it is impossible to prevent the supernodes from colluding with each other. A similar idea has been adopted by Proof of Vote (PoV) [9], which is coordinated by the distributed nodes controlled by consortium partners who come to a decentralized arbitration by voting. The key idea is to establish different security identity for network participants so that the submission and verification of the blocks are decided by the agencies' voting in the league without the depending on a third-party intermediary or uncontrollable public awareness.

2.3 Game-Specific Consensus Model

Since novel consensus models for general purpose blockchains are not yet accepted by the public, consensus models for specific verticals may leverage application features to improve the blockchain data synchronization. In this section, we summarize the approaches in the gaming domain.

Huntercoin[6] claims that around 80% of their coins are obtainable by collecting coins in a virtual universe which resides inside the blockchain. The platform provides a multiplayer game for the players to combat with each other in the map to collect coins. Huntercoin proposes the concept of Human (or AI) mining, and they can adjust the mining speed by increasing/decreasing the game

[5] https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[6] https://huntercoin.org/

difficulty over time. Similarly, Motocoin[7] has players to play a coin-collecting (the motocoin) game by driving a virtual motorbike. If a player finished the game before a targeted time, the player can write a new block on the blockchain along with the coin collection. The targeted time will be adjusted dynamically to maintain a consistent mining rate. These two consensus models rely on the players' effort in playing the games. However, the gaming progress is lack of entertainment but incentive driven only.

BUFF[8] proposed a Proof-of-Play consensus with another approach, where players earn token from playing games. The mining process is performed in the background, it does not interfere with the gameplay nor requires any expenses. From their whitepaper, the BUFF PoP has the player-base elect 21 players to vote for the consensus of the next block. The elected players are motivated to produce block since there are rewards. Also, their best interest is not to collude, since that harms the reputation of the blockchain and thus their stake on the blockchain (e.g. the value of their rewards). This type of consensus model is intrinsically a DPoS consensus, and so their design is to have the consensus drove mainly by some specific players.

Motivated by these approaches, we propose another Proof-of-Play (PoP) consensus model. The PoP model acts as a data storage solution in P2P gaming and aims to interfere with the gameplay at a minimum. By simply playing in a P2P game, the blockchain runs and form consensus automatically, and players will naturally receive incentives to participate in the distributed data storage service of the game.

2.4 Blockchain Security

Decentralization security is important in blockchain systems. This section features attacks that consensus models aim to solve.

2.4.1 Byzantine Generals Problem. In a decentralized system, there is a problem of forming consensus over the system, as no node knows which is the agreed the system. This is the Byzantine Generals Problem [8]: There is a Byzantine army with generals that requires consensus on whether to attack or retreat. How may an algorithm be designed to assure consensus can be made with if there are traitors within the generals? Several solutions have been made in the paper[8]. The solutions either use a signature on consensus, or rely on majority consensus. In blockchain, the solution is to implement a consensus model.

2.4.2 Sybil Attack. Sybil Attack [5] is an attack related to dishonest nodes in a decentralized network: a single faulty entity can present multiple identities, thus is able to control a substantial fraction of the system and undermine the integrity of the system. However, the malicious party requires the time and energy to disguise as multiple identities in the network. Techniques like PoW is known as economically secure since it requires a node to have the tremendous computational power to become an effective miner. Other technical techniques are also introduced, in Bitcoin, the number of outbound connection per IP address is regulated[9]. There are variations of this attack, e.g. Eclipse Attack [6].

3 SYSTEM OVERVIEW

The following section discusses the properties of the Proof-of-Play(PoP) consensus model and summarized as a list of rules.

3.1 The Need of the PoP

As mentioned in Section 1, blockchain is a perfect solution for data storage issues in P2P gaming. So, by having a game database powered by blockchain, data integrity in the P2P gaming system is enforced. Yet, many designs of the game may need to be changed to integrate into a blockchain naturally. For example, adding cryptocurrency to the game such that players are economically motivated to write blocks. However, any modification upon the game content is not an optimal solution. For example, the act of play in both Huntercoin and Motocoin (Section 2.3) becomes incentive-driven due to the blockchain, making the game progress lack entertainment. The Proof-of-Play aims to avoid these problems by having the consensus comes from playing naturally.

3.2 The Properties of the PoP

The PoP consensus model is proposed to integrate a P2P gaming system with a blockchain seamlessly. PoP by definition, is the act of play enables players to write blocks (data) to the blockchain. Then, by simply playing, new blocks will be written into the blockchain.

Also, the concept of PoP fit nicely with the trustless aspect of a blockchain design. The following properties can be secured by PoP:

(1) Users tend to be honest (Since gaming is time-consuming)
(2) Users are motivated to keep the blockchain reputable (Since users are the stakeholder of the blockchain)

With this design, blockchain can be integrated into a P2P gaming system seamlessly without modifying the game for the use of a blockchain. Also, without the separation of miners and users, the intention of the users of the system remains simple: they play the game and run the blockchain because they want to, not because of external motivation e.g. cryptocurrency.

3.3 Breakdown of PoP System Design

There are two system components to realize the properties of PoP:

(1) The integrity of the data representing the act of play
(2) The block writing process is an act of play

The first property corresponds to the data integrity of the P2P gaming architecture, and the second property corresponds to the PoP blockchain. This system flow is designed as in figure 1.

To elaborate figure 1, assume a game of chess for player group A and player group B. The players finished their game and form a consensus on their game result as game data. Then one of the players of each group broadcasts the game data to the blockchain. The PoP will validate the game data integrity and rate the game for each game. The rating process then determines if any player can be a candidate block's writer. In this figure, a player in Group B will be a candidate block's writer, then the player successfully write the next block to the blockchain.

Note that the game data need not be a game result, but could be a state of a game at any point of time.

[7] https://motocoin-dev.github.io/motocoin-site/
[8] https://buff.game
[9] Bitcoin community on Sybil Attack: https://en.bitcoin.it/wiki/Weaknesses#Sybil_attack

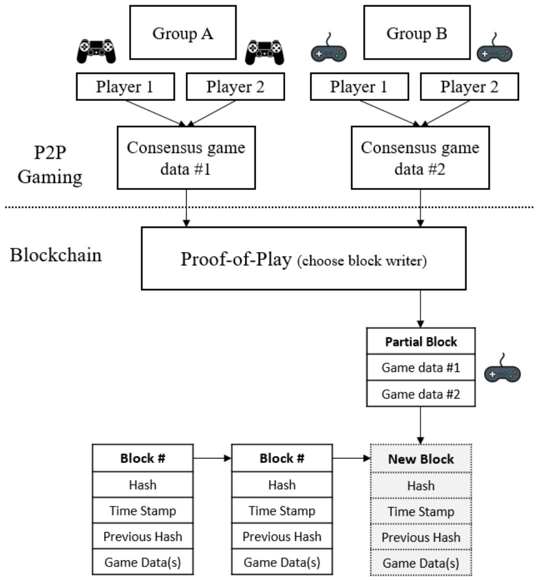

Figure 1: Proof-of-Play overview

4 SYSTEM DESIGN

The following section is to realize the design in Section 3.3.

4.1 Game Data Integrity

By keeping the integrity of the game data, the act of play is then a valid representation as PoP (section 3.2). In this section, we will focus on assuring the data integrity from players' collusion. Other problem will be discussed in section 4.3.3

As shown in figure 1, the consensus game data is formed based on an agreement of the players in a game. However, a malicious party can forge a game result that is beneficial for everyone to agree with, then the game result will simply be an outcome of players' collusion instead of an act of play. Thus, the game data integrity of the blockchain is compromised. Although this is not the best interest of a node in a PoP blockchain (section 3.2), the following technique is proposed to reduce the risk of such collusion.

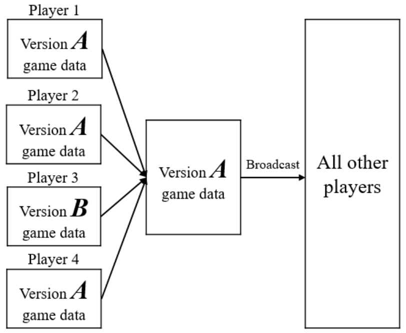

Figure 2: Proof-of-Play Shared Turns

The idea of Shared Turns[7] is discussed to have two players reveal their move simultaneously, without knowing opponent's move in advance. This is a Commitment scheme and can enable consensus of the majority players shown in figure 2, corresponds to the consensus game data in figure 1. The flow is as follows:

(1) obtain everyone's public key
(2) players hash the game result (becomes a game hash)
(3) players create a signature with the copy of game hash using their private key
(4) players broadcast the game hash and the signed game hash
(5) after players has received everyone's broadcast, broadcast own's game result
(6) players verify the game result by the corresponding public key and game hash
(7) determine the most competitive player by the consensus game result
(8) the most competitive player is responsible to broadcast the game result along with the signatures

After the process, the final game result is agreed by the majority of players to broadcast a truthful act of play by step 3 and 4: In step 3, the game hash is signed, so the received game hash in step 5 is authenticated by the signature's owner. In step 4, players broadcast their game result. Malicious players may broadcast their game result based on others' game result. This opens up an opportunity to collude. However, since the game result is hashed, raw game result from other players is not known until step 6, so to avoid the aforementioned cheating behavior. If a player still decides to broadcast a raw game result different than the hashed game result after the first broadcast, other players will know immediately that the player is telling lie by comparing the hash value of both received game result.

At step 7 and 8, the most competitive player (the MVP) will broadcast the game. This step is to facilitate the design of the next section 4.2. The design in the next section ensures the PoP process is an act of play. Only the competitive player will be a block writer, this enforces the PoP since players compete for block writing.

4.2 Block Writing Procedure

With the process above, the integrity of the game data is secured and the act of the play is presented. Then, the last step is to ensure the block writing procedure is an act of play (section 3.3), so that the blockchain integrates into a P2P game naturally (section 3.2).

The design of the block writing procedure is shown in figure 3, and is corresponding to the "Proof-of-Play" block in figure 1. Firstly, to realize the block writing process as an act of the play, one has to evaluate if the player of the game is paying enough effort. So, for a player to become a candidate block's writer, the player must have paid enough effort in the game data the player is presented in. Then, after the list of candidate blocks' writer are established, one candidate block's writer has to be selected as the final block writer for the next block. (Note that the term "competitive player" in figure 3 indicates the player is the representative of the game. This is to enforce the rule "the act of play" being the consensus of the blockchain as mentioned in section 4.1)

The final block writing process is designed to be probabilistic to reduce collision in the blockchain network, known as a fork. Fork stated that some of the nodes of the blockchain recognize a node as the next block writer, while other nodes recognize another node as

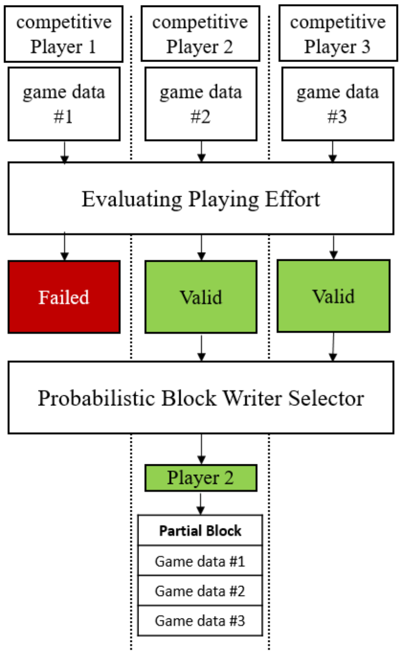

Figure 3: Block Writing Procedure in Proof-of-Play

the next block writer. If the block writing process is deterministic, it will function the same as "Evaluating Playing Effort" in figure 3 due to the nature of PoP. Then:

(1) if average (majority of) players can normally pass the evaluation, there will be too many valid block writers
(2) if only good players can normally pass the evaluation, this is an unfair advantage to lower-skilled players

Even if the evaluation is dynamically adjusted according to the individual's ability, the result of the adjustment will be classified between one of the two cases above (too easy / hard to pass), thus a deterministic approach is not feasible.

Note that the probabilistic selection process is not part of the mining. The mining has already happened at the process of "Evaluating Playing Effort", and the probabilistic selection works similarly to a random access protocol in the Data Link Layer of the OSI model. It is to avoid a burst in a number of candidate blocks' writer that massively forking the blockchain network. So, the act of play of the players is still where the blockchain nodes agree to form a consensus with.

In the current PoP design, the evaluation is adjusted according to the player's ability. This provides a fair chance for everyone to pass through the evaluation stage with enough effort of their ability.

With the proposed PoP process, a block writing procedure with minimum intervene to the P2P gaming system is designed.

4.3 Security Concerns

The main idea of the PoP system is to have human cognitive work in the block mining process, such that a user is both a miner (section 3.2) and a human. The following section discusses some major security problems in the blockchain based on PoP.

4.3.1 *Byzantine Generals Problem and PoP.*

In PoW, Byzantine Generals Problem is solved[10] by having generals agree to hold consensus on the single PoW winner. PoP also has a single winner and analog is given as follows: Suppose there are n generals decided that whoever wins a game of chess against any general may be a PoP winner. For each winner, PoP will rate if sufficient effort has put into the game. Then, PoP will be randomly select a winning general as the PoP winner. The game loop starts over if no winner or multiple winners are selected. Note that the expected number of games to get a PoP winner is $\frac{1}{n}$, so every general just have to finish one game to form consensus for the blockchain.

4.3.2 *General Anonymity Concerns.*

Anonymity is a properties of blockchain and it causes problem of an entity disguised as multiple identities, a Sybil Attack[5]. PoW solves this problem by having a node to invest in huge computational resources to mine, making a PoW blockchain "economically secured".

In PoP, rather than economical approach, anonymity is assured by assume playing is a human-exclusive cognitive work. It is achieved by a game complex enough and is competitive, such that it is hard to have computational resources substituting humans. So, PoP has a one-to-one relationship of a miner and a human, limiting the ability for an anonymous entity to present as multiple miners.

4.3.3 *General Data Integrity Concerns.*

A blockchain is designed to resist against modification[12]. Also, the source of the data should be correct to being with to have a complete data integrity.

Part of the PoP (section 4.1) is to avoid data integrity problem by collusion. However, there are other problems. For example, if the game allows players to connect to other players directly, a colluding party can be formed to broadcast game data without playing. Yet most of the problems depends on the implementation of the game. For example, including an anti-cheating mechanism in the genesis of the PoP blockchain can resolve above problem.

For the property of irreversible modification, same as other consensus models, the mechanism is to make rewriting the data very costly. In PoW, attackers need to possess 51% of the network computational resources to outrun other computers in solving the puzzle to write a new block. It is economically very difficult to compete against the computational resources of all other users combined. In PoP, computational resources are replaced by the efforts of playing, which requires cognitive efforts and is difficult to outrun.

5 SYSTEM IMPLEMENTATION

The following section introduces the implemented system and the experiment on PoP: A demo for the PoP architecture flow (figure 1) to demonstrate the flow of the system, and the PoP mining simulation to test the system stability.

5.1 Architecture Flow Demo

The flow demo consists of the Shared Turns implementation (figure 2) and the PoP implementation (figure 3). For the PoP implementation, the "Probabilistic Block Writer Selector" part is implemented separately in the next section (section 5.2) as a simulation.

[10] the original Bitcoin mailing list on Byzantine general's problem: http://www.metzdowd.com/pipermail/cryptography/2008-November/014849.html

The repository contains the library with example scripts on the blockchain usage. The demo is to let interested developers understand roughly the implementation of PoP. The repository has a comprehensive README to explain the repository structure.

5.2 PoP Mining Experiment

In section 4.2, a probabilistic approach to select the block writer is described to ensure the robustness of the PoP system. This section will discuss the importance of the mining process, perform experiments on the system's stability, and explain the result.

5.2.1 *The details of probabilistic mining.*

As explained in section 4.2, the probabilistic approach for PoP mining is to reduce the probability of forking in the blockchain. However, several parameters need to be defined for a complete probabilistic approach.

To begin with, the implementation of the guessing puzzle in Bitcoin PoW[11] is explained as an idea of probabilistic technique in a decentralized system. Bitcoin PoW has users to guess a number below the "Target value". For example, if the "Target value" is 10, then miners have to guess a number lower than 10. With this concept, "Difficulty" can be defined. There is a "maximum target value" for Bitcoin (i.e. 2^{224}). So, the "Difficulty" is defined as:

$$\text{Difficulty} = \frac{\text{Maximum target}}{\text{Target value}} \tag{1}$$

where Difficulty = 1 is the easiest Difficulty, the higher the Difficulty value, the harder the number to guess.

Then, to generate random number, Bitcoin's PoW use hashing (i.e. SHA-256 algorithm). By having miners input values into the SHA-256 algorithm, a hash value will be generated. A good hash is a random value, so the hashed value can be used to guess a valid "Target value". In Bitcoin PoW, the possible combination of hexadecimal number output is 2^{256} using SHA-256. So, the probability of finding a valid number (below the "Target value") is as follows:

$$P[\text{Getting a valid number}] = \frac{\text{Target value}}{\text{Range of hash value}} \tag{2}$$

where "Range of hash value" is 2^{256}. Then, by substituting the Equation (1) to Equation (2), the P[Getting a valid number] in Bitcoin PoW can be alternatively expressed as:

$$P[\text{Getting a valid number}] = \frac{\text{Maximum target}}{\text{Difficulty} \cdot \text{Range of hash value}}$$

Since "Maximum target value" is 2^{224}, and "Range of hash value" is 2^{256}, this can be rewritten as:

$$P[\text{Getting a valid number}] = \frac{1}{\text{Difficulty} \cdot 2^{32}}$$

Then, by definition, the "Expected number of hashing to get a valid number" is:

$$\text{Difficulty} \cdot 2^{32} \tag{3}$$

Since the "Expected time between mining each block" (i.e. Confirmation Time) in Bitcoin is 10 minutes, suppose we know the "History number of hashing per block" and the "History confirmation time", By Equation (4)

$$\text{Hash rate} = \frac{\text{Number of hashing per block}}{\text{Confirmation time}} \tag{4}$$

where the term "History confirmation time" means "the average of n previous actual confirmation time", the same applies for "History number of hashing per block". It can be written in such way to calculate the "Expected number of hashing of a block":

$$\frac{\text{Expected number of hashing}}{\text{Expected confirmation time}} = \frac{\text{History number of hashing}}{\text{History confirmation time}} \tag{5}$$

thus, the "Expected number of hashing" of a block can calculated using equations 5, and a mathematically sensible "Target value" can be derived by backtracking from equation 3.

5.2.2 *PoP Probabilistic Mining.*

In PoP, the same mathematical approach has implemented as a probabilistic selector (figure 3). Since the hashing operation happens much less frequently than PoW, the confirmation time is also different than the one in Bitcoin (i.e. 10 minutes). So, the following experiment is conducted to observe how changes in different variables in the calculation brings impact to the stability of the system.

A simulation program has been written to simulate the mining process. A few adjustments have been made to the calculation in section 5.2.1, customized for the mining process in PoP:

PoP should have an average confirmation time dependent on the time length of a game match (For a non-match-based game, the time can be arbitrarily defined). For example, when a player has played n matches, a block will be mined. so the "Play Effort" in the "Evaluating Playing Effort" block (3) is the scores of a player winning n matches. Assume all players win a match simultaneously, the desired probability of getting a valid number of any time is:

$$P[\text{Getting a valid number}] = \frac{1}{\text{Number of players} \cdot n} \tag{6}$$

Since the number of players is defined for a simulation, using equation (2), the initial target can be calculated as follows:

$$\frac{1}{\text{Number of players} \cdot n} = \frac{\text{Maximum target}}{\text{Difficulty} \cdot \text{Range of hash value}}$$

$$\text{Target value} = \frac{\text{Range of hash value}}{\text{Number of players} \cdot n} \tag{7}$$

For the actual implementation, n is $\frac{\text{Expected confirmation time}}{\text{Average match time}}$. n is not fixed since n is dependent to the experiments i.e. experiment on change of confirmation time will be conducted.

After the initial target, the first block will be mined. Then, the hash rate of the first block can be known. So, after the first block, the adjustment of the target is made by m previous hash rate using equation (5). The mean of m previous hash rate is taken to represent the blockchain network history hash rate.

For the maximum target, we assume that it is dependent on the confirmation time, since the function of target value is to govern the confirmation time when the blockchain scales. As a lower confirmation time means a lower difficulty, we assume a negative linear relationship between the target and the confirmation time (i.e. the lower the confirmation time, the higher the target value). Then, by using Bitcoin average confirmation time (600 seconds) and the base-2 exponent of its maximum target (224), the maximum target of any confirmation time is defined as:

$$\log_2(\text{Maximum target}) = 256 - \frac{\text{Confirmation time} \cdot (256 - 224)}{600} \tag{8}$$

[11] Bitcoin Difficulty: https://en.bitcoin.it/wiki/Difficulty

5.2.3 *Experiment Implementation.*

1. create a manager process with n players' process
2. manager process defines and calculates the parameters of the blockchain. (initial block index = 0, number of players, expected confirmation time, maximum target value, initial target value, number of blocks to mine)
3. manager process tells players' process to start mining
4. players wait average 5 seconds to simulate playing a match. (100 samples of match time are generated with a normal distribution of 5 seconds μ and 1 seconds σ)
5. if no longer chain was received from the manager process, the player will continue hashing values, including the string of his game score, a random number, and a nonce
6. if the hashed value is lower than the target, broadcast to the manager, otherwise do nothing, then go to step 4

By the flow above, the manager will keep waiting for a valid new block, calculate new target, store the history blockchain states, and broadcast the new blockchain.

Manager process exists to handle inter-process communication. This is to simplify the workload of players' process purely to mining. So, measurement on player's process is less affected by other undesirable variables (e.g. time of a process in communicating).

5.2.4 *Experiment Variables.*

The variables below are the experiment's subject. By changing the value, we would like to observe its impact on the stability of the PoP system.

1. expected confirmation time
2. the number of miners (players)
3. number of history blocks, parameter of history hash rate

For the third variable, let number m. The mean of m previous block's hash rate will be obtained as the history hash rate for the calculation of the current block.

The 3 variables are the experiment input, they determine the adjustment of the "target value". The first and the third variable are parameters to calculate the target, while the second variable derive the history hash rate to calculate the target. Via the variables change corresponds to the actual confirmation time, it shows the stability of the blockchain. We can then conclude the practicality of the methodology on deriving the calculation for the PoP mining.

5.3 Experiment Results

The following three experiments have been conducted. It is to observer and interpret the performance and the side effect on variable changes corresponds to the target value.

The mining in the experiments are conducted using a single AMD Ryzen 1400 CPU, GPU is not used for the experiments. So, the values to be experimented are chosen based on the CPU performance. The details will be explained prior discussing the experiment results.

5.3.1 *Expected Confirmation Time.*

The experiment parameters are:

- number of blocks = 100
- number of players = 10
- number of reference history blocks = 10
- confirmation time: experiment subject

The number of adjustments is chosen to be 7 according to the number of processes the CPU can handle simultaneously under maximum usage, by the simulation.

This experiment is to evaluate if a target value produces an intended confirmation time. So, a range of short and realistic confirmation time is picked as parameters, they are 10, 30, 60, 90, 150, 180 seconds. It is expected that other experiment values scale the same way the experiment values do.

The result of the experiment shows roughly an exponential distribution, where the "percentage of a block being mined" decrease exponentially as the "confirmation time" increases.

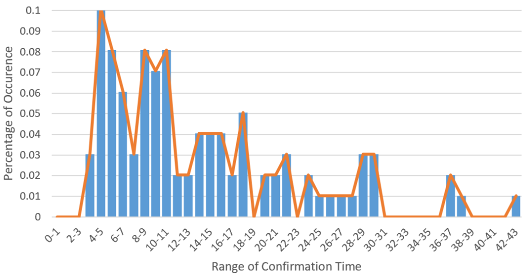

Figure 4: Occurrence of actual confirmation time under 10 seconds expected confirmation time

Figure 4 depicts the experiment result with a parameter of 10 seconds expected confirmation time. Similar to Bitcoin[12], it roughly shows an exponential distribution. It is expected that the variance of the confirmation time will be normalized as the number of trials increase (as shown in later experiments), then the exponential distribution will be more apparent. So, the hashing operations in the mining process are properly implemented.

Parameter	μ	Range	$\tilde{\mu}$	σ
10	13.85591	40.92175	10.60783	9.272552
30	29.24059	131.9419	22.5276	23.24391
60	57.19258	222.9035	49.98521	45.61157
90	113.7163	532.5268	85.62569	107.2782
120	123.6353	765.8719	78.50864	134.1295
150	146.9611	784.2096	98.08061	147.5669
180	164.2757	958.4286	102.3475	164.5644

Table 1: Section 5.3.1 Experiment Result

Table 1 shows the experiment result of the 7 different expected confirmation time with figure 5 showing the distribution of actual confirmation time in the experiment.

The notation of the table is defined as follows: Parameter is the expected confirmation time, Range is the "maximum confirmation time from the sample" minus the "minimum confirmation time from the sample", σ is the standard deviation of the sample, the μ is the Mean and the $\tilde{\mu}$ is the Median, both calculated from the result of actual confirmation times.

It is expected that an increase of the parameter results in the increase of the μ of the sample confirmation time. It is clear that the μ is close to the parameter. Also, the μ and the σ is similar, since

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

an exponential distribution has the same value for both mean and σ. Thus, the calculation in section 5.2.2 is efficient.

Also, there exists an increase of value for $\mu - \tilde{\mu}$ as the Parameter increases. This effect is explained by increase of Range: Since the difficulty increases as the parameter increases, some blocks take much longer time to hash a valid target. These small cases of very large confirmation time increases the Range and also affect the μ, so the mean moves further away from the $\tilde{\mu}$ as the parameter increases. In other words, the λ (rate parameter) in the exponential distribution increases as the Parameter increases.

Developer can increase the Parameter to have better blockchain stability, since more percentage of the blocks will have an actual confirmation time before the μ. This is shown by the Peak Frequency of each expected confirmation time at Figure 5: both 10 and 30 seconds of expected confirmation time has its peak frequency at sample portion 0.1<n<0.2, the rest of the expected confirmation time has its peak frequency at sample portion of 0.0<n<0.1.

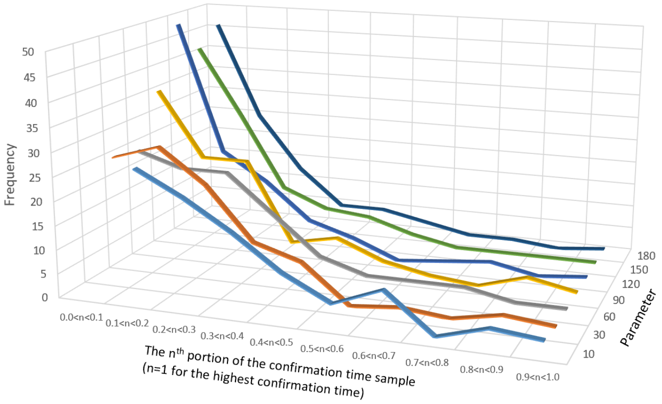

Figure 5: Frequency distribution of the sample confirmation time (Experiment Section 5.3.1)

5.3.2 *Number of reference history blocks.*

The experiment parameters are:

- number of blocks = 1000
- number of players = 10
- number of reference history blocks = experiment subject
- confirmation time: 10

This experiment is to evaluate the variance of the target value. A sudden change in history hash rate will easily affect the target value by making the blockchain very difficult or very easy to mine all the sudden. Increasing the number of reference blocks for the history hash rate neutralize the effect of the sudden change in history hash rate to the target value (i.e. concept of moving average).

The number of blocks has been set to 1000 to allow an adjustment to a larger value of the experiment subjects. The number of 1000 blocks is picked to normalize the variance as an exponential distribution in figure 4. Since a good exponential distribution assure an improvement in target value, evaluation can be made.

The adjustment function of the experiment subject is:

$$n = \begin{cases} 2(n-1), & \text{if } x \geq 1 \\ 10, & \text{otherwise} \end{cases}$$

The number of adjustments is chosen to be 7 according to the number of processes the CPU can handle simultaneously under maximum usage, by the simulation. This adjustment is defined so that there is a sufficient range of experiment subject while having a reasonable experiment duration length, average 2.7 hours per process, to introduce enough variance of the data.

Similar to section 5.3.1, it is expected that other experiment values scale the same way the experiment values do.

Parameter	μ	Range	$\tilde{\mu}$	$\tilde{\mu}_{loc}$	σ	α
10	14.55	114.42	11.56	0.10	10.45	166
20	14.74	93.52	11.44	0.12	10.61	-66
40	14.77	63.50	11.77	0.18	10.24	-142
80	14.14	80.14	11.38	0.14	9.75	-154
160	14.14	80.14	11.38	0.14	9.75	-154
320	13.92	64.75	11.17	0.17	9.21	-178
640	14.34	54.33	11.35	0.20	9.32	-175
1000	14.22	71.24	11.49	0.16	9.66	-193

Table 2: Section 5.3.2 Experiment Result

Part of the table 2 evaluates the same notation of the experiment result as table 2 does. The rest of the notation is defined as follows: "Parameter" means "Number of reference history blocks" instead, $\mu_{\tilde{loc}}$ means the location n of the $\tilde{\mu}$ of the Parameter (shown in figure 6), and α means the difference of y (Y-axis) between n = 0.0<n<0.1 and n = 0.1<n<0.2 (X-axis) in figure 6.

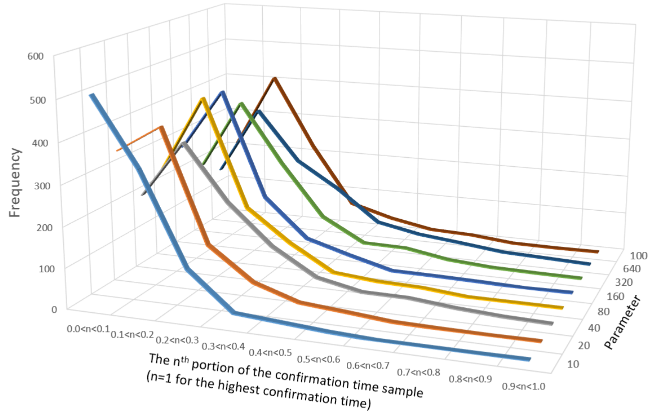

Figure 6: Frequency distribution of the sample confirmation time (Experiment Section 5.3.2)

Figure 6 in this section has the same X-axis and Y-axis as figure 5. So, both figures can be interpreted similarly.

It is expected that an increase of the Parameter results a decrease of the Range, since the history hash rate used in Equation (5) is now based on a larger portion of the full history hash rate. The decrease in the Range of the experiment result shows the mining is effective. The μ is also consistent as expected, by calculations in section 5.2.2.

From figure 6, a shift of the distribution (by observing the x with peak y) with the increase of parameter is shown. This shift is expressed in α in table 2. To interpret, since the Range decreases, outlier values are not present anymore. That makes the $\tilde{\mu}$ shifts towards the right. Thus the increasing value of $\tilde{\mu}_{loc}$.

Thus, the higher the number of reference history blocks, the more reliable the target value is. This makes the blockchain resists to a sudden burst or cut in hash rate, thus to stablize a blockchain.

5.3.3 Number of Players. The experiment parameters are:

- number of blocks = 100
- number of players = experiment subject
- number of reference history blocks = 10
- confirmation time: 10

This is to evaluate the effect of the number of players to the target value. The adjustment function of the experiment subject is:

$$n = \begin{cases} 2(n-1), & \text{if } x \geq 1 \\ 10, & \text{otherwise} \end{cases}$$

There are 6 adjustments in total, it is decided by the CPU capability. Running 320 python multiprocessing process takes full processing power of the CPU, so it is the highest Parameter allowed. Also, similar to section 5.3.1, it is expected that other experiment values scale the same way the experiment values do.

Parameter	μ	Range	$\tilde{\mu}$	σ
10	13.85591	40.92175	10.60783	9.272552
20	15.39057	57.12786	11.3413	11.19832
40	16.12811	65.08809	13.89211	10.4721
80	16.1453	68.46416	12.51086	12.20591
160	15.1577	58.9716	11.52297	9.714505
320	17.565	79.87559	12.82916	14.37079

Table 3: Section 5.3.3 Experiment Result

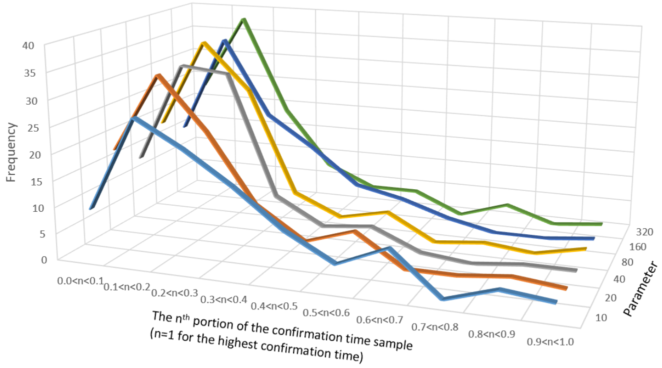

Figure 7: Frequency distribution of the sample confirmation time (Experiment Section 5.3.3)

Part of the table 3 evaluates the same notation as table 1 does. Here, the notation "Parameter" means "Number of Players" instead.

Figure 7 in this section has the same X-axis and Y-axis as figure 5 and figure 6. So, all three figures can be interpreted similarly.

It is expected that an increase in "Number of Players" results the decrease in target value. The target value affects the Range as in table 1, yet the increase of Range is of a smaller degree. This concludes the indirect relationship of the "number of players" affecting the target value via the history hash rate.

The μ has an increase as the parameter increases, divergent with the $\tilde{\mu}$. It is concluded to be due to the increase of λ parameters in the exponential distribution (section 5.3.1). However, in figure 7, we can observe that the central tendency does not shift.

The slight increase in μ is the effect of block propagation time: the delay in receiving the latest data of the blockchain. Since the broadcast to the players is queued by a manager process, some processes have a delay in receiving the new block. Assume node x is the current block producer and has a delay in receiving the latest block. Since the history confirmation time comes from the mining time of node x, it does not account for nodes with a headstart in mining . So, by Equation (4), the history hash rate is overestimated. The severity of the problem is ranked by the Parameter: 320, 80, 40, 20, 160, 10.

When the blockchain scale, it is inevitable for an increasing block propagation time. Bitcoin has defined a confirmation time of 10 minutes, and is accepted by the community as a countermeasure for the problem of block propagation[13], so that nodes with high receiving delay will not be wasted too much of a mining effort.

In our experiment, although the block propagation time is artificial, in reality the situation is similar. There will be a chain of broadcast before every node is synchronized to the latest blockchain that creates a huge delay. Developers have to consider the ideal expected confirmation time according to the scale of the blockchain.

5.3.4 Experiment Conclusion. This experiment concludes that the adjustments of the three variables: "Expected Confirmation Time", "Number of reference history blocks", and "Number of players" can effectively change the target value of the PoP mining algorithm. Both "Expected Confirmation Time" and "Number of players" have side effects on the system in adjusting.

The increase of "Expected Confirmation Time" increases the Range of the sample confirmation time, and the increase of "Number of players" introduce the block propagation time. "Number of reference history blocks" stabilize the target value, resists to sudden burst or cut in blockchain hash rate, this may act as a countermeasure of the side effects in the increase of the "Expected Confirmation Time". However, for the side effect on the increase of "Number of players", it is up to the developers to compensate between an ideal expected confirmation time in a cost of the blockchain stability.

The experiment can generally apply to any probabilistic mining approach similar to PoW, developers can make decisions on a blockchain system design based on the parameters' effect above.

6 DISCUSSION

In this section, we discuss the nature of this consensus model, with comparison of other major consensus models in Section 2.2.

6.1 Nature of the PoP

The design of the PoP aims to decentralize a P2P gaming system without data storage issues (section 1). This model is not limited to the act of gaming, any the use of the blockchain can achieve consensus. Generally it is defined as follows:

- The act of using the blockchain fulfills the consensus
- The representation of this act is not exploitable

Both of this rule is fulfilled by the block writing process (section 4.2) and the shared turn process (section 4.1) respectively. To apply

[13] https://medium.facilelogin.com/the-mystery-behind-block-time-63351e35603a

this rule into other application, a metaphor of a cryptocurrency based on PoP is given:

- The money spent/received of an individual is the rating
- By spending / receiving money, the rating of an individual goes up, to a point of becoming a candidate block's writer
- The money spent/received by an individual must be productive e.g. Gross Domestic Product (GDP) factor

6.2 PoP and other consensus model

Model	Consensus Mechanism	Efficiency	Fairness
Proof-of-Work	Computational Power	Low	Medium
Proof-of-Stake	Stake	High	Low
Proof-of-Play	Use of blockchain	High	High

Table 4: Section 6.2 Summary of Proof-of-Play comparison

This consensus model is similar to the conceptual model Proof-of-Excellence. However, the player in PoP need not be excellent, the player simply has to present its act of play to mine. This avoids the issues of better players having an unfair advantage in mining.

PoP adopts some of the ideas in PoS and PoW with the disadvantages of them being eliminated. A summary of the comparison of Proof-of-Play to other models is shown in table 4 for further discussion based on their consensus mechanism.

6.2.1 PoW. The main cost of the PoW is the energy and time inefficiency(Section 2.2). Also, for a basic PoW system, nodes with better computational power (i.e. CPU performance) will hash the valid number faster to other nodes. So unfairness exists in PoW.

In PoP, the probabilistic mining function acts as a random access protocol (section 4.2). It also has an overhead of n game matches before the mining occurs. Developer can derive (equation (8)) a low expected hash rate for a PoP blockchain, making it power-efficient.

Also, the evaluation of the playing effort of a player (section 4.2) is adjusted dynamically according to the player's ability. Different skilled players have the same chance in mining a PoP block.

6.2.2 PoS. The biggest problem in PoS is the nothing-at-stake problem (section 2.2). It opens up opportunities to launch security attacks. PoW does not have the nothing-at-stake problem, since the intrinsic cost of mining on multiple chains is the decrease in the chance of mining successfully. So, In a PoW system, miners are encouraged to mine on the same chain.

Also, PoS is not fair, since the more stake a node holds, the more likely the node will mine a block. A new node joins the network will never have a hash rate higher than older nodes in the network.

In PoP, the rule is the use of the blockchain fulfills the consensus, there is no reason a community wants multiple version of game data. This is a weak assumption. To strengthen the security, similar to PoW, in-game rewards on successful mining can be implemented, such that the intrinsic cost of mining on multiple chains is the decrease in value of the player's in-game rewards (some chain do not acknowledge the player's rewards).

Also, as mentioned in Section 6.2.1, the chance of mining is designed to be more fair compare to PoW/PoS due to the dynamic adjustment of the "evaluation of the playing effort".

7 CONCLUSION

This paper introduces a consensus model P2P gaming system using blockchain as a solution to data storage issues. The consensus model aims to create a blockchain system that forms a consensus by the use of the blockchain itself, while not compromising the general properties of a blockchain. Then, the system is implemented to demonstrate the flow of the PoP, experiments have conducted to show how different parameters affect the stability of the PoP system or probabilistic mining system in general. Finally, this paper generalizes the consensus model and discuss the differences between PoP and other major consensus models.

We believe this design would bring more attention on blockchain system related to the P2P gaming system. This also acts as a design reference on blockchain in interactive system, eventually decentralize any interactive system reliably with a simple design nature like PoP: the use of a blockchain form consensus for the blockchain.

REFERENCES

[1] BETTINA Kemme AMIR Yahyavi. 2013. Peer-to-Peer Architectures for Massively Multiplayer Online Games: A Survey. *Comput. Surveys* 46, 1 (October 2013). https://doi.org/10.1145/2522968.2522977

[2] Adam Back. 2002. Hashcash - A Denial of Service Counter-Measure. (09 2002).

[3] Blockchain Technology 2018. BLOCKCHAIN GAMES: A SURPRISING NEW PLAYER IN THE INDUSTRY. http://bitcoinist.com/blockchain-games-a-surprising-new-player-in-the-industry/.

[4] Vitalik Buterin. 2013. Ethereum white paper: a next generation smart contract & decentralized application platform. *https://github.com/ethereum/wiki/wiki/White-Paper* (2013).

[5] John R. Douceur. 2002. The Sybil Attack. In *Peer-to-Peer Systems*. Springer Berlin Heidelberg, Berlin, Heidelberg, 251–260.

[6] Aviv Zohar Sharon Goldberg Ethan Heilman, Alison Kendler. 2015. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In *Proceedings of the 24th USENIX Conference on Security Symposium*. USENIX Association Berkeley, CA, USA, 129–144.

[7] Daniel Kraft. 2016. Game Channels for Trustless Off-Chain Interactions in Decentralized Virtual Worlds. *http://ledger.pitt.edu/ojs/index.php/ledger/article/view/15* (2016).

[8] Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* 4, 3 (July 1982), 382–401. https://doi.org/10.1145/357172.357176

[9] K. Li, H. Li, H. Hou, K. Li, and Y. Chen. 2017. Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism amp;amp; Consortium Blockchain. In *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. 466–473. https://doi.org/10.1109/HPCC-SmartCity-DSS.2017.61

[10] B. K. Mohanta, S. S. Panda, and D. Jena. 2018. An Overview of Smart Contract and Use Cases in Blockchain Technology. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 1–4. https://doi.org/10.1109/ICCCNT.2018.8494045

[11] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *White Paper: https://bitcoin.org/bitcoin.pdf* (2008).

[12] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. 2017. Blockchain. *Business & Information Systems Engineering* 59, 3 (01 Jun 2017), 183–187. https://doi.org/10.1007/s12599-017-0467-3

[13] Siraj Raval. 2016. *Decentralized applications : harnessing Bitcoin's blockchain technology* (1 ed.). O'Reilly Media.

[14] L. S. Sankar, M. Sindhu, and M. Sethumadhavan. 2017. Survey of consensus protocols on blockchain applications. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. 1–5. https://doi.org/10.1109/ICACCS.2017.8014672

[15] Scott Nadal Sunny King. 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. (August 2012).

[16] Youki Kadobayashi Takuji Iimura, Hiroaki Hazeyama. 2004. Zoned Federation of Game Servers: a Peer-to-peer Approach to Scalable Multi-player Online Games. In *3rd ACM SIGCOMM workshop on network and system support for games*. 116–120. https://dl-acm-org.ezproxy.lb.polyu.edu.hk/citation.cfm?doid=1016540.1016549