A Scalable Proof of Play Consensus

Kosuke Minoru
kosukem@insight.dev
www.insight.dev

June 22, 2022

Abstract

In this paper, we propose a novel consensus algorithm that yields a secure and sustainable cryptocurrency utilizing human input. Work on blocks is retained in the form of "logic" instead of computation, while validation remains objective and unforgeable. Proof of Play, which requires human participation, is a truly accessible and secure remedy to the negative environmental effects of Proof of Work.

1 Introduction

The rise of Bitcoin has spurred the emergence of a new technological revolution: Blockchain and decentralization. Bitcoin introduced the ability for members of a decentralized network to agree on a set of transactions in a secure and trustless manner. This in turn facilitated the inception of countless new blockchains — the most innovative being, arguably, Ethereum. With its concept of a smart contract, Ethereum successfully incorporated an application layer to blockchain, revolutionizing how decentralization can function. However, despite the considerable advancements in blockchain technology, major issues still remain. The most notable obstacle is scalability. The Bitcoin network uses on average 200 TwH per year [2]. This energy consumption is on par with the 22nd most energy intensive country [3]. As miners with more computing power enter the network, energy expenditure increases further, meaning that Bitcoin can never scale to wide adoption without causing irreversible harm to the environment. There are attempts to replace Proof of Work with algorithms that require less computational expenditure, but these consensus mechanisms sacrifice security. In this paper we will outline issues with Proof of Work and Proof of Stake, and propose our new consensus algorithm, which remedies the issues of existing consensus mechanisms.

2 Consensus

2.1 Proof of Work

Proof of Work is the original consensus algorithm. While it is quite secure, it uses computational power to achieve consensus. The miners that have the most computational power will have the highest likelihood of winning the mining reward. As computational power is positively causally related to energy consumption, Proof of Work results in an arms race that accelerates carbon

emissions. Additionally, computational power is a resource that can be purchased monetarily. Proof of Work networks thus lead to centralized mining, as those with more wealth, and consequently more computing power, accumulate rewards which in turn yields more computing power. This cyclical process of power accumulation endangers the cryptocurrency as it is susceptible to a 51% attack. This is where a malicious party has over 51% of the mining power and can outpace the rest of the network, resulting in the takeover of the blockchain. Although potentially difficult, a government or powerful enough entity could overpower the network.

2.2 Proof of Stake

Proof of Stake is a consensus algorithm that selects validators in probabilities proportional to the quantity of their holdings staked in the associated cryptocurrency. In both Proof of Stake and Proof of Work, miners with more resources have an advantage, meaning Proof of Stake follows the same cyclical process of power accumulation as Proof of Work. While Proof of Stake resolves the environmental issue by not leveraging computing power, it sacrifices its security. Distributed systems traditionally have a 33% fault tolerance. Proof of Stake, by removing Proof of Work, remains at a 33% fault tolerance [5]. Proof of Stake also removes the cost involved with creating a block, which has several negative consequences. To guarantee a currency is unforgeable, it must be costly to produce [5]. This costliness also serves as a proxy for value, meaning that Proof of Work tokens have inherent value in their costliness. In Proof of Stake systems, this feature is not present. Additionally, as work accumulates in Proof of Work, it is nearly impossible to forge the entire blockchain, whereas in Proof of Stake, the total amount of computational work required is minimal [5]. In Proof of Stake, whenever a fork occurs, it is in the self-interest of all validators to stake on both chains since there is no cost involved [4]. This means that there is no longer objectivity in fork choice [5]. Finally, social scalability is determined by the objectivity of the system: Objective systems are socially scalable since no one can be excluded from participating. In practice, Proof of Stake systems are subjective and controlled by few stakers, making it not socially scalable.

2.3 Proof of Play

The novel Proof of Play consensus algorithm implemented in Insight's blockchain eliminates the negative environmental effects of Proof of Work while also maintaining security. Proof of Play is a competition amongst miners that cannot be solved with computing power. The competition holds similar properties to a CAPTCHA in the sense that humans can easily solve it, but computers cannot. To incentivize mining, participation is entertaining (unlike a CAPTCHA) and the winner profits from mining rewards. A Proof of Play miner cannot leverage computing power to substantially improve their chances of winning. This also means that unlike Proof of Work and Proof of Stake cryptocurrencies, Insight requires no upfront investment to mine the coin. Thus as smaller miners

do not get beaten out, new miners will be incentivized to join as the network scales. Moreover, as Insight's consensus mechanism is similar to Proof of Work without significant energy consumption, the security of the cryptocurrency is maintained. Finally, a 51% attack is infeasible as one would need to outpace the entire network and would need an equivalent of 51% of the active people instead of 51% of the resources to take over the blockchain. This would not be viable for a single party to coordinate. The Proof of Play algorithm remains secure and retains a cost involved in producing a coin. As the cost of producing a block is not computational, Proof of Play remains environmentally sustainable. Figure 1 shows the comparison of Proof of Play to Proof of Work and Proof of Stake.

Features	Proof of Work	Proof of Stake	Proof of Play
Fault Tolerance	50%	33%	50%
Fork Choice	Objective	Subjective	Objective
Unforgeable Costliness	Yes	No	Yes
Proxy for Value	Yes	No	Yes
Accumulated Work	Yes	No	Yes
Block Creator Location	External	Internal	External
Division of Power	Yes	No	Yes
Sunk Investment	Yes	No	Yes
Socially Scalable	Yes	No	Yes
Computationally Scalable	No	Yes	Yes

Figure 1: Comparison of the consensus algorithms: Proof of Work, Proof of Stake and the newly proposed Proof of Play.

3 A Suitable Proof of Play Example

3.1 Overview

A suitable Proof of Play mechanism is np-complete, requiring non-deterministic polynomial time to solve and polynomial time to verify. One such example is a physics simulation. Traditional games involving physics simulations are notoriously difficult for computers to solve [1], but easy to verify. A physics simulation such as Angry Birds has an immense set of possible moves, making brute force infeasible.

3.2 Level Generation

In this model, there is a unique level for each unique hash and difficulty. The hash is used as the seed value which determines a pseudo-random level output. The hash also determines the starting location of the player, the gravitational

constant of the level, and the amount of power the player can apply to launch the object. This yields a unique, deterministic level based on the hash. The difficulty affects the number of shots the player has, the number of enemies and the ratio of the different materials of objects. Stone objects are much more difficult to break and are more abundant at higher difficulty. Conversely, the more brittle glass objects are less abundant at a higher difficulty. To generate a level, the level generating algorithm heuristically creates a stable structure and maximizes the following fitness function:

$$F = 3\frac{1-d}{1+|e|} + 0.002\frac{n}{n+v} + 5\left(1 - \frac{r}{18}\right) \tag{1}$$

$|e|$ is the total number of possible enemy locations, d is the dispersion value of the enemies within the structure, v is the number of different block types within the structure, n is the number of rows within the structure and r is the number of angles at which the structure was deemed stable. The constants in Eq. 1. were chosen to maximize stability.

The global stability is evaluated by rotating the structure clockwise and anticlockwise with angle intervals of five degrees until the structure hits 45° rotation in each direction or becomes unstable. This yields a total of 18 possible angles at which the structure could be stable. Figure 2. shows a level generated by the proposed algorithm.

Figure 2: A level generated using parameters: difficulty = 70 and hash = 0x9f84d084884c7d65aaa2aa0c55ad315a3bf4f1b2b0b822cd15d6c15b0f00a08

3.3 Network

Similar to Bitcoin, Insight's p2p network has various different types of nodes. The reference node functions as a miner and wallet, performs network routing, and stores the full blockchain database. Inspired by the pool mining protocols

for Bitcoin, we propose a lightweight mining client that contains the Proof of Play mining functionality. The lightweight mining clients receive the blocks to be mined from the pool protocol servers that act as gateway routers connecting the mining clients to the Insight p2p network. A block includes a coinbase transaction with two outputs, one to the pool operator and one to the lightweight client. The client validates the coinbase transaction. Sending an invalid block is not in the interest of the pool operators, as they would only be decreasing their potential return and the lightweight mining client will switch to a different pool operator.

3.4 Mining

Figure 3. shows the structure of the block header for the Proof of Play protocol.

Size	Field	Description
4 bytes	Version	Block version number
32 bytes	Previous Block Hash	Hash of parent block
32 bytes	Merkle Root Hash	Hash of Merkle Root
4 bytes	Timestamp	Unix timestamp
1 byte	Diffculty	Proof of Play level difficulty for this block (in the future we might be able to do more)
64 bytes	Winning Moves	The winning moves for the Proof of Play algorithm

Figure 3: Structure of block header for Proof of Play protocol.

When the player receives the block to be mined, they validate the coinbase transaction. To start mining they hash the first five serialized fields of the block header to obtain the hash, H_L. They then run the level generating algorithm with H_L and the difficulty as arguments. Since the coinbase transaction output points to their address, each level generated is unique to the player. Once the player wins, they include the winning moves inside the block header and send the completed block to the pool operator. The winning moves are the initial horizontal and vertical impulses given to each of the projectiles fired. We refer to these as x and y values respectively. Figure 4. shows the flow for mining in Proof of Play.

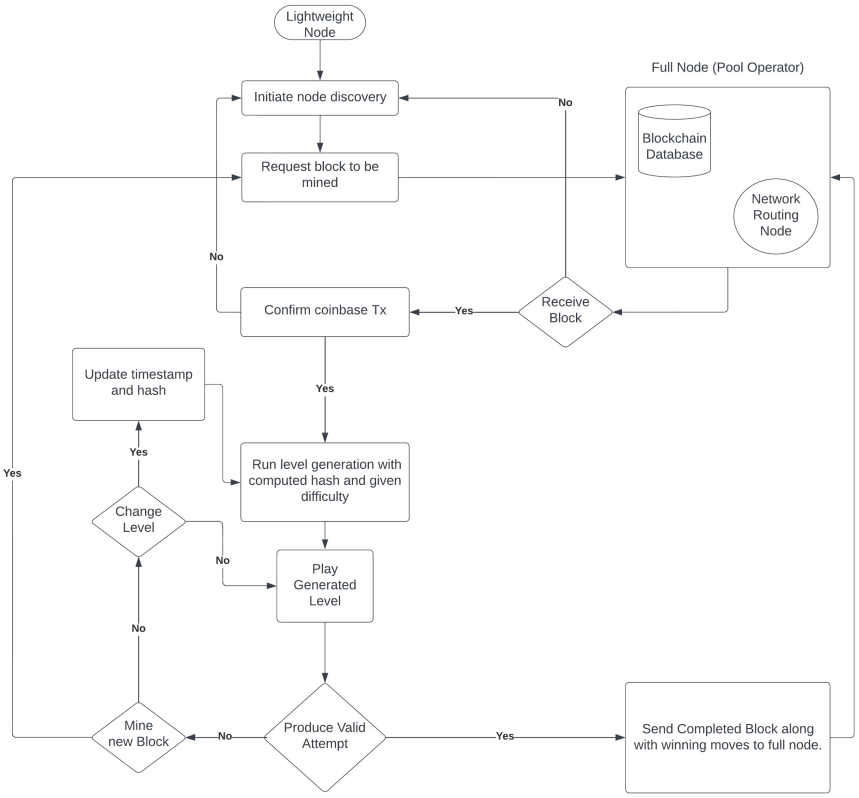

Figure 4: Mining in Proof of Play.

3.5 Validation

As level generation is deterministic, validators can generate the same level solved by a miner based on the block header hash, H_L and difficulty. Any validator can then validate by simulating the play-through using the attempt that the miner includes in the block. The validation function takes the winning moves as its argument. The function then simulates an attempt for a given level with the x and y values, which are used to calculate velocities and positions of the projectile. If all enemies in the level are destroyed, then the attempt is successful.

3.6 Deterring Machine Learning

AI and machine learning algorithms currently cannot outperform humans in Angry Birds [1]. This is for a plethora of reasons, but, simply speaking, algorithms can only determine the best move for one shot. When given more shots, computers cannot strategize and plan using every shot. Additionally, the high number of possible total attempts makes heuristic approaches flawed.

Additional factors can also thwart machine learning algorithms. Each level has different physics parameters; while humans can easily and quickly adapt to these changes, a machine learning algorithm would need to re-train on each level. Furthermore, since there is a small computational cost to simulate, if a machine learning algorithm were to train on a level by simulating thousands of times, it would be too computationally expensive to be economically feasible.

4 Conclusion

Proof of Play is a secure, eco-friendly, and decentralized mining mechanism that remedies the detrimental environmental effects of Proof of Work. Insight is the first cryptocurrency that can be mined without an upfront monetary cost, whereas in both Proof of Work and Proof of Stake, an initial investment is required. All miners participate on a level playing field, since mining on the network requires only playing a game. This makes Insight an accessible currency.

References

[1] Cheng Xue Chathura Gamage et al. Ai birds.org angry birds ai competition. http://aibirds.org/, 2022. [Online, accessed 17-May-2022].

[2] Digiconomist. Bitcoin energy consumption index. https://digiconomist.net/bitcoin-energy-consumption/, 2022. [Online, accessed 17-May-2022].

[3] International U.S. Energy Information Administration (EIA). U.s. energy information administration - eia - independent statistics and analysis. https://www.eia.gov/international/data/world/electricity/electricity-consumption, 2021. [Online, accessed 17-May-2022].

[4] Daniel Frumkin. Nothing-at-stake problem. https://golden.com/wiki/Nothing-at-stake_problem, 2018. [Online, accessed 17-May-2022].

[5] Author Donald McIntyre. Why proof of stake is less secure than proof of work. https://etherplan.com/2019/10/07/why-proof-of-stake-is-less-secure-than-proof-of-work/9077/, 2021. [Online, accessed 17-May-2022].