Proof of Phone: A Low-cost Blockchain Platform

Jae Min Kim, Jae Won Lee, Kyungsoo Lee and Junho Huh
S.LSI, Samsung Electronics, Hwaseong-si, Republic of Korea
Email: {jmy.kim, jw1223.lee, ks.sys.lee, huhjunho}@samsung.com

***Abstract*—Blockchain which enables decentralization of data based on various consensus mechanisms is considered the leading technology of the next generation. Numerous applications are being proposed to benefit from its immunity against modification and manipulation. However, not many appears as a successful business up to now, except for crypto currencies. High operation cost which is essential for the conventional consensus, is acting as an obstacle to the wide adoption of blockchain applications. In this paper, we introduce a novel blockchain platform based on PoP (Proof of Phone), which lowers the operating cost by imposing high entry cost. We conduct theoretical analysis to show that our proposed platform reduces total cost by up to 98.2% compared to that of conventional blockchain. Our new platform will turn various blockchain applications from theory to practice.**

I. Introduction

Blockchain is definitely among the hottest topic of the year, with explosive growth of crypto currencies including Bitcoin [1], Ethereum [2], etc. The concept of distributed ledger that cannot be manipulated seems to be a perfect alternative to the formal centralized system where a single point of attack breaks down the entire system. Startup companies with blockchain applications have raised 5 billion dollars in 2017, just counting the initial coin offering [3]. Enthusiasts insist that blockchain will drive the industry of the next generation.

However, regardless of the rosy expectations, most of the blockchain applications remain on-the-shelf as the artificial intelligence applications did in the 20th century. The situation is also similar. It is not the effectiveness but the efficiency that is being doubted and challenged. Due to PoW (Proof of Work) based consensus mechanism, major blockchain techniques require enormous amount of power consumption in exchange for its integrity. A study on Bitcoin analyzes the annual electricity consumption on its mining to be 70.8 trillion watts, which is estimated to be 3.5 billion US dollars [4]. Due to the enormous cost, top four mining companies are operating 60.7% of total mining pool with their powerful hashing machines [5]. Vitalik introduced a new blockchain platform, Ethereum to overcome this problem by tweaking the consensus mechanism to prohibit the use of ASIC (application specific integrated circuit) and put high dependency on the memory performance rather than computation performance. However, it only introduced a shift in the type of machine used in mining pools, still consuming 2.4 billion US dollar, annually [6].

There are still on-going studies to use different consensus mechanisms such as PoS (Proof of Stake) or PoET (Proof of Elapsed Time) [7]. In addition, a study from Berkeley utilizes trusted execution environment based consensus mechanism to reduce the mining cost for individual nodes [8]. Nevertheless, the fundamental problem remains: the high cost put into the network ensures the high integrity of the network.

To overcome this dilemma and enable blockchain applications with relatively low cost, we introduce HELO (High Entry cost and Low Operation cost) concept. The main idea of HELO is to lower the operation cost based on customized hardware accelerator, while imposing high entry cost, which preserves the integrity of the platform. In the meanwhile, the high entry cost is mostly paid for an existent value. As a result, the actual cost to enable the inherent blockchain is just a small overhead.

We describe the details of the HELO concept and propose a novel blockchain platform in Section 2. We present the implementation details in Section 3, and conduct theoretical analysis on Section 4. Finally, we conclude the paper in Section 5.

II. A Novel Blockchain Platform

There are typically two types of people engaged to the blockchain platform: blockchain service providers (miners) and blockchain service users. From the user's view, they benefit from whatever the blockchain application does for them and pay for the service in form of commission; it could either be direct commission or indirect commission. Then, the commission is distributed to the providers as a reward to compensate with their mining cost based on the platform policy. Fig. 1 describes a brief example of this process. In the figure, a user wants to store his asset safely in the blockchain and miners attempt to create the block that holds the asset. When one of the miners succeeds in creating the proper block,

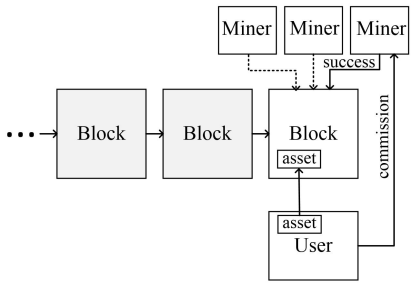

Fig. 1. Cost and rewards in a typical blockchain platform

the miner receives reward. In this figure, the reward comes directly from the user as a form of direct commission.

The problem in the described system is that the overall cost is not technically controllable. Modification of the consensus mechanism or invention of new hardware that reduces the mining cost is not a solution. At first, it will reduce the overall cost. However, more miners enter the competition due to the improved payability; payability is the percentage of gain over your investment. Eventually, the overall cost increases until the payability meets some specific point, which we define as the minimum payability.

To resolve this problem, we propose HELO where high entry cost prevents indiscriminate increase of mining nodes, and gives control on the mining cost. In HELO, a mining module is a part of a larger base system which acts as the entry cost to become a new mining node. The base system must satisfy the following characteristics:

- It should be widely used regardless of the mining feature
- It should be resistant to modification by end user
- It should give extremely lower value to a person who owns more than one of it

Smartphone is among the best candidates that satisfies all three conditions. The hardware architecture of a Smartphone is hardly modifiable after assemble, and a person cannot not benefit much from having hundreds of them. Nevertheless, it is hard to find a person not using a smartphone, and billions of them are actively used. Thus, in this paper we apply HELO concept on Smartphone and propose the blockchain platform with novel consensus mechanism: PoP (Proof of Phone).

Fig. 2 briefly presents the basic concept of PoP and the conventional consensus mechanisms. When Bitcoin was first invented, the ideal state of mining was millions, if not billions, of general miners with their desktop participating to construct a high-integrity blockchain platform. In this model, users share the spare computation power of their existing machines and receive relatively small incentive. However, as the platform become reliable and began generating higher incentives, the miners wanted to take more share. This raised excessive competition, which led to the increase of computation cost as well as centralized mining. Transition to PoS system partially slows down the competition and lowers the cost. However, in the long term it only changes the means of competition from computation power to capital power, which indicates high capital cost. Different from the two most popular consensus mechanisms, PoP imposes high entry cost, which prevents the excessive competition and enables the low cost blockchain platform.

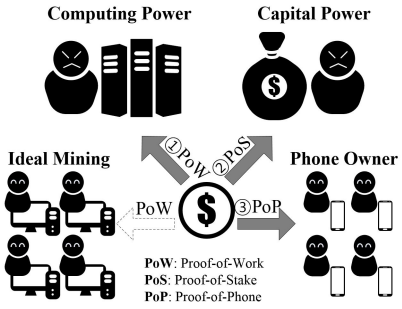

Fig. 2. Conceptual view of PoP compared to the conventional consensus mechanisms

III. Implementation

A. Hardware Architecture

Basically, PoP is a type of PoW which uses a special hardware to add constraints on indiscriminate increase of competition and cost. For this we implement AMU (Authenticated Mining Unit). AMU is integrated in a smartphone system to check the integrity of the system and execute hash operations for mining new block. AMU consists of 4 functional sub-blocks: BCU (Block Control Unit), MMA (Micro Mining Accelerator), data transceiver, and KAU (Key Authentication Unit). Fig. 3 shows the simplified block diagram of AMU.

BCU is mainly used for verifying the integrity of new blocks as well as transaction data. It communicates with the transceiver to receive data and verifies blocks as well as transactions based on the previous transaction history. It notifies the verification result to the transceiver. In addition, it also adds verified block to the transaction history.

MMA is a simple low-power accelerator designed to find a nonce for the next block. It receives the authenticated transaction data from KAU and repeats hash operations to find a proper nonce. On a success, it sends the mining block to the data transceiver. When it receives new transaction data from KAU during the mining process, it discards the previous data and starts over with the new data.

Data transceiver is used to communicate with the external peer nodes. When it receives a valid transaction data from the network, it stores the data in its transmission buffer, which is used for generating the next block. When it receives a valid block, valid block is re-sent out to the network. In the meanwhile, the transaction data stored in its buffer is compared to the data in the block to remove overlapping data from the buffer. Then, any remaining data in the buffer is sent to KAU to be used for the next mining block.

Finally, KAU is used to authenticate the mining procedure. It consists of a one-time programmable memory used to store the system identifiers. At the initiation, manufacturer must

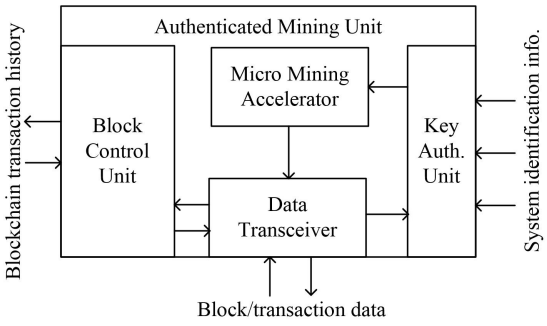

Fig. 3. Simplified block diagram of AMU and its submodules

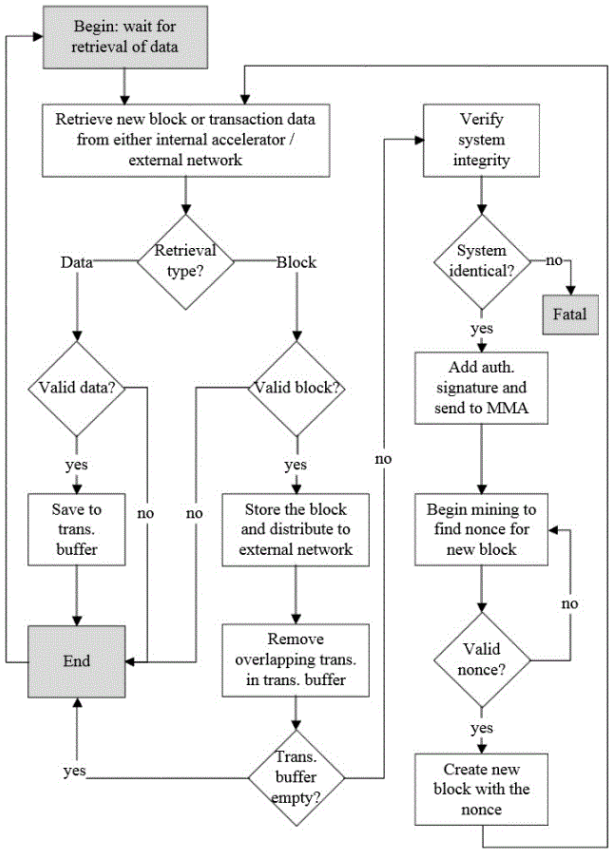

Fig. 4. Flowchart of AMU mining procedure

integrate AMU in a place to receive several device specific identifiers (e.g. IMEI as well as hardware IDs of key modules of the system) and power-up KAU which is self-programmed to store retrieved identifiers. After initiation, it authenticates incoming transaction data with private signature, only if the identical system has not been modified. This prevents a person or a group to use a large number of AMUs, and dominate the consensus without paying the proper entry cost (1 smartphone per 1 AMU).

B. Mining Flowchart

The details of the mining procedure are described in Fig. 4. The initial sequence begins when the data transceiver receives a new transaction data or a new block. When AMU receives a transaction data, it checks the integrity based on transaction history. If the transaction is valid, it is stored in the transaction buffer, and AMU returns to the initial state. When AMU receives a new block from either the internal MMA or from the external network, AMU checks the integrity of the block. When the block and all of its consisting transactions are valid, AMU stores it to the transaction history and also sends out to the network to be shared with peer nodes. Then, it compares the block data to its transmission buffer and removes any overlapping data.

If the transaction buffer is empty after removing the overlapping data, AMU returns to the initial state waiting for the next incoming data. Otherwise, AMU utilizes KAU to check the system integrity to begin mining procedure of the new block. If the system integrity is verified, a candidate for the new block is generated with the transaction data in transaction buffer, and signed by KAU. Then, MMA begins to find the proper nonce value to complete mining of the new block. In case MMA is busy, AMU forces MMA to reset and start mining with the new data. When MMA succeeds in finding a valid nonce, AMU completes the mining procedure and restarts from initial state with the mined block.

IV. Theoretical Analysis

A. Cost in the conventional blockchain

In the conventional blockchain platform, the total cost includes electricity and capital cost as well as depreciation of mining devices. However, instead of estimating each of them the total cost is simply derived from the payability of the blockchain platform:

$$Cost(conventional) = Reward/(1 + P_{min}) \qquad (1)$$

where $Cost(conventional)$ is the total cost used for mining in the conventional blockchain platform per year, $Reward$ is the total reward generated by the platform per year, and P_{min} is the minimum payability for the miners to keep working.

This formula is derived based on the Nash equilibrium [9], where each miner attempts to maximize his own profit. P_{min} is added in the formula to reflect inflation and compensate for the risk. When the total reward increases, additional investments are made to get more rewards. On the other hand, if the reward decreases and payability does not satisfy the P_{min}, some of the miners will stop running their device. As a result, the cost converges to a proportional value to the reward, as shown in Table I.

TABLE I
Correlation between cost and reward

P_{min}	0	0.1	0.2	0.3
$\frac{Cost(conventional)}{Reward}$	1.00	0.91	0.83	0.77

B. Cost in the PoP blockchain

In case of PoP, there are several methods to minimize the operation cost, based on the dedicated hardware. Thus, the total cost is mostly derived from the entry cost, which is applied differently depending on the type of miners. For general smartphone users (will be denoted as general miners), the only overhead is AMU module price. On the other hand, for a dedicated miner who buys more smartphone just for mining, the cost includes not only the AMU module price but also the depreciation price of smartphone. In order to formularize the cost, we first make following assumptions. Firstly, we assume the maximum lifetime of AMU as one year to prevent excessive increase of the mining devices and impose proper entry cost for new dedicated miners. Note that major smartphone vendors release their new premium

products annually. Secondly, we assume the depreciation rate of a smartphone as 50% of original price after a year, based on several p2p web markets. With the assumption, the total cost of PoP platform for dedicated miners and general miners are derived as follows:

$$Cost(PoP_{dedicated}) = Cost(AMU) + Cost(Phone) \times 50\% \quad (2)$$

$$Cost(PoP_{general}) = Cost(AMU) \quad (3)$$

where $Cost(PoP_{dedicated})$ is the annual cost in dedicated miner's view, $Cost(PoP_{general})$ is the annual cost in general miner's view, $Cost(AMU)$ is annual sales of AMU module, $Cost(Phone)$ is annual sales of smartphones that have AMU (excluding the AMU price), and 50% is the depreciation rate.

In the equations, the cost is reasonably much higher for the dedicated miner. This indicates that if more dedicated miners begin mining, the total cost will increase. Dedicated miners will do so when the cost derived from (2) is still lower than that derived from (1), since the same rule of Nash equilibrium applies to the dedicated miners. However, considering the high expectation of $Cost(Phone)$, increase of dedicated miners are likely to be minimized.

C. Comparison of PoP and conventional blockchain

Fig. 5 compares the cost of PoP to that of conventional blockchain, in respect to the varying $Reward$. $Reward$ is shown as a relative value to the $Cost(Phone_{general})$, which is the annual smartphone sales to normal users. We assume P_{min} is 0.1 in this analysis. Three different conditions are shown in the figure, where the $Cost(AMU)$ is 1%, 2%, and 3% compared to $Cost(Phone)$.

The ideal case is observed where the reward is between 56.1% and 58.3%. On that case, $Cost(PoP)$ is only 1.8%, 3.5%, and 5.1% of $Cost(conventional)$, where $Cost(AMU)$ is 1%, 2%, and 3% of $Cost(Phone)$, respectively. On the other hand, the worst case is where the reward is too small. In such case, $Cost(AMU)$ becomes an overhead. However, if the reward is just over 3.3%, the cost for PoP becomes lower than that for conventional blockchain, for all case. In addition, when blockchain platform does not create enough reward, we may limit the sales of AMUs to prevent overhead.

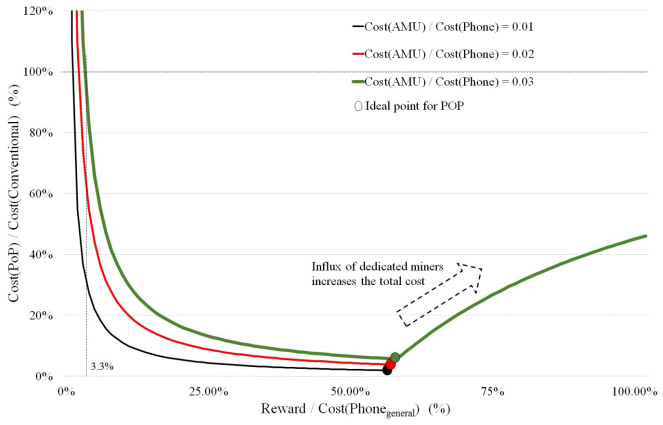

Fig. 5. Cost comparison of our proposed blockchain and the conventional blockchain

We also observe that the ratio keeps on growing when reward exceeds the ideal point. In such case, dedicated miners find it attractive to buy new smartphones just for mining, as explained in the previous subsection. This causes increase of the cost same as in the conventional blockchain. However, since there are still a portion of general miners, $Cost(PoP)$ will not increase any higher than the $Cost(conventional)$. In addition, the precondition of very high reward paradoxically indicates a success of our platform, when considering the annual sales of smartphone.

V. Conclusion

In this paper, we explain the dilemma of ever increasing cost of the conventional blockchain platform. To overcome the problem, we introduce novel PoP (Proof of Phone) blockchain platform based on HELO (High Entry cost and Low Operation cost) concept. Our analysis indicates that cost of PoP reduces the cost by up to 98.2% compared to that of the conventional blockchain. Nevertheless, PoP still ensures high integrity by enforcing high entry cost. Considering the annual smartphone sales which is easily over billions of dollars, it is impossible, or at least inefficient, for a person or group to dominate the consensus. Numerous blockchain services on-the-shelf will become a real-world application on our platform, without concerns of the cost.

Along with the contributions, we believe the following extensions to our work will add more value to our study: 1) a quantitative analysis of the price of AMU as well as the power and network overheads, 2) methods to further optimize the cost, and 3) further evaluation of our platform in terms of blockchain integrity. We leave these as our future works.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin project white paper, pp. 1-9, 2008.

[2] G. Wood, Gavin, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, pp. 1-32, 2014.

[3] S. Lee, "AI will take over blockchain in 2018, but it won't happen without these 3 key areas," Forbes article, available at: https://www.forbes.com/sites/shermanlee/2018/03/19/ai-will-take-over-blockchain-in-2018-but-it-wont-happen-without-these-3-key-areas, 2018

[4] "Bitcoin Energy Consumption Index", Digiconomist, available at: https://digiconomist.net/bitcoin-energy-consumption, 2018.

[5] "An estimation of hashrate distribution amongst the largest mining pools," Blockchain Info, available at: https://blockchain.info/en/pools, 2018.

[6] "Ethereum Energy Consumption Index," Digiconomist, available at: https://digiconomist.net/ethereum-energy-consumption, 2018.

[7] A. Baliga, "Understanding blockchain sss models," White paper, Persistent Systems Ltd, 2017.

[8] M. Milutinovic, W. He, H. Wu and M. Kanwal, "Proof of luck: an efficient blockchain consensus protocol," in proceedings of the 1st Workshop on System Software for Trusted Execution pp. 2-7, ACM, 2016.

[9] J.F. Nash Jr, "The bargaining problem," Econometrica: Journal of the Econometric Society, pp. 155-162, 1950.