Blockchain Contract: Securing a Blockchain Applied to Smart Contracts

Hiroki Watanabe[1], Shigeru Fujimura[1], Atsushi Nakadaira[1], Yasuhiko Miyazaki[1], Akihito Akutsu[1], and Jay Kishigami[2]
[1]NTT Service Evolution Laboratories, Yokosuka-City, Kanagawa, Japan
[2]Muroran Institute of Technology, Muroran-City, Hokkaido, Japan
Email: watanabe.hiroki@lab.ntt.co.jp

***Abstract*-- A new mechanism is proposed for securing a blockchain applied to contracts management such as digital rights management. This mechanism includes a new consensus method using a credibility score and creates a hybrid blockchain by alternately using this new method and proof-of-stake. This makes it possible to prevent an attacker from monopolizing resources and to keep securing blockchains.**

I. INTRODUCTION

The Bitcoin [1], which is the first and most popular cryptocurrency, has been receiving a lot of attention and the importance of academic research on Bitcoin is continuing to grow [2]. One of its technical features is that it enables reliable transactions without a centralized management mechanism even if there are unreliable participants in the network, and this feature is obtained by the invention of blockchain technology. The structure of a blockchain is that a block that consists of multiple transactions is connected with a previous block in chain-like form. To ensure reliability, when a new block is generated and added to the previous block, a little special process of solving a computationally heavy puzzle, called a proof-of-work puzzle, is needed and this puzzle is solved competitively by the participants. (The generating of blocks is called mining and the participants are called miners.)

However, solving proof-of-work puzzles wastes a significant amount of electricity, i.e., the computing power used to solve the puzzle is wasted unproductively. To save energy, therefore, an alternative method of securing a blockchain called the proof-of-stake method was proposed within the Bitcoin community as early as 2011 and was first implemented in the Peercoin [3], another type of cryptocurrency. With proof-of-work, the probability of mining a block depends on the work done by the miner. On the other hand, the resource of the proof-of-stake is the amount of coins that are held. In order to successfully complete an attack on the blockchain, an attacker has to control more than 50 percent of the resources of the entire network (known as a 51% attack). With proof-of-stake, if an attacker tries to monopolize coins the network participants will detect it, and the value of the coins held will be significantly reduced. This works as a deterrence against attacks.

Meanwhile, blockchain technology applications for things other than currency have started surfacing. We believe that blockchain technology has great potential for managing contracts such as digital rights management because the blockchain is strong against attacks and is difficult to change its history, and the system works without a central authority. This creates the possibility of lowering users' fees.

The next section describes the most serious issue for the proof-of-stake method in applying blockchain to managing contracts. The method we propose to address this issue is described in Section 3 and a theoretical evaluation of it is shown in Section 4. The paper is concluded in Section 5 with a summary of important points and a mention of future work.

II. THE ISSUE FACING PROOF-OF-STAKE IN CONTRACTS MANAGEMENT

Our assumption is that blockchain-based applications for contracts management should be realized by expanding the existing framework of the blockchain. In other words, scripts included in transactions should be expanded so that the fact that a contract has been made can be made clear. One simple way of doing so, for example, is to have the hash value of the contractual document recorded in the script as metadata.

As has been mentioned, the proof-of-stake method was proposed as a means of saving energy in comparison with the proof-of-work method. We believe that choosing it is a good solution for many types of blockchain applications. However, there is a serious issue involved when using it in contracts management. Specifically, the deterrence based on the exclusive holding of coins it provides against attacks on the blockchain may not function because participants in contracts management probably don't care about the value of the coins. That is, their main purpose is to use the coins to record their contracts in the blockchain. In such a situation, the value of the coins is not so important and the purpose of the attack is not the unfair use of coins but the illegal renewal or vitiation of contracts in the blockchain. Taking these things into consideration, attackers will probably try to attack if they are more likely to gain than to lose by forging contract contents, even if the attack completely destroys the value of the coins.

III. PROPOSED METHOD

In the following we describe a new method of securing a blockchain network, which addresses the issue described in the previous section.

A. Deterrence by collapse of credibility

An alternative way to deter attacks via the collapse of coin prices is required to solve the issue. The alternative we propose is the collapse of credibility. Credibility is an absolutely essential factor in any contract and contractors must know each other well to build up credibility and trust. The more contracts a contractor has with different people, the more credibility he gains. Consequently, he comes to gain many people's trust and be well known to many other parties. If he attacks a blockchain, he loses trust not only in the blockchain

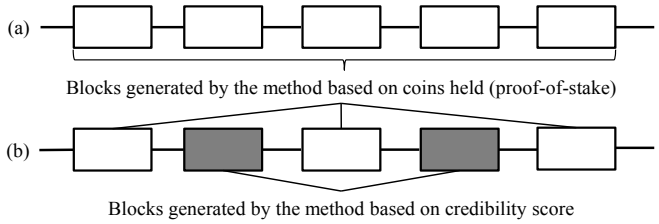

Fig. 1. (a) Conventional simplex blockchain (b) Proposed hybrid blockchain

network but also in society as a whole. Therefore, having substantial credibility works as a deterrence factor in place of having a great number of coins.

Our approach to measuring credibility is to calculate the number of parties the contractor enters into contracts with. We define this number as a credibility score. Instead of using proof-of-stake, we propose to achieve consensus in the blockchain network by having a miner who generates a block provide proof that he has a high enough credibility score.

B. A proposal for a hybrid blockchain

Using a credibility score instead of a stake, however, creates a problem in the case where an illusory contract is involved. A credibility score is added whether a contract is fake or true. If an attacker makes fake contracts with fictitious parties' addresses, the attacker can easily increase his credibility score. Therefore, an attacker who has a high fake credibility score can possibly succeed in a 51% attack, and if he joins hands with a node that has true contracts they can renew illegally the contracts.

One of the ways to address the problem is to make a 51% attack cost more than before. We therefore propose a new mechanism to create a blockchain, which is based on two types of consensus methods: the proof-of-stake method and the aforementioned method based on credibility score. While the proof-of-stake method needs to store enough coins, the consensus method using credibility score needs to use enough coins in order to make contracts. Since storing and using coins are opposite ideas, it is harder to increase both of them. The mechanism we propose creates a hybrid blockchain based on the proof of stake and credibility score methods. The hybrid blockchain is created when the proof of stake and credibility score methods are executed alternately. As shown in Fig. 1, if some miner generates a block using stakes, the next miner has to generate the next block using a credibility score, and the next block after that has to be generated using stakes. In the next section, we model an attack on this hybrid blockchain.

IV. CALCULATIONS

To complete an attack, the attacker has to generate an alternate chain that is faster than the honest chain. To model an attack mathematically, we consider the success probability of an attacker trying to use a dishonest chain. According to Nakamoto [1], the probability of an attacker catching up from a given deficit, in which there is a z block difference between the honest blockchain and his dishonest blockchain, is analogous to a Gambler's Ruin problem. If we assume the attacker's potential progress will be a Poisson distribution with an expected value, the probability that P_z will succeed is:

$$P_z = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left\{ 1 - \left(\frac{q}{p} \right)^{z-k} \right\}, \quad \lambda = z \frac{q}{p} \tag{1}$$

The variable q equals the fraction of the resources (e.g., computing power, holding coins and credibility score) owned by the attacker, and p equals the fraction of the rest of the network resources (therefore, p=1-q). With our proposed hybrid blockchain, equation (1) for a conventional simplex blockchain converts to the following equations.

$$P_z = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left\{ 1 - \prod_{n=1}^{z-k} \left(\frac{q}{p} \right) \right\}, \quad \lambda = \sum_{n=1}^{z} \frac{q}{p} \tag{2}$$

$$q / p = \begin{cases} q_1 / p_1 & \text{if } n = 2m-1 \quad (odd) \\ q_2 / p_2 & \text{if } n = 2m \quad (even) \end{cases} \tag{3}$$

In equation (2), q_1/p_1 shows the ratio of one resource and q_2/p_2 shows the ratio of the other resource, where both ratios may refer to either the coins held or the credibility score. The parameter z shows how many blocks the recipient of a new transaction needs to wait for in order to prevent the attacker from succeeding. The Bitcoin's z parameter is set to 6 blocks as confirmation. Table I summarizes the probabilities of completing an attack on the simplex blockchain and on the hybrid blockchain when z=6. The result confirms that proposed hybrid chain is stronger against a 51% attack than conventional simplex chain.

TABLE I: PROBABILITIES OF COMPLETING AN ATTACK ON EACH CHAIN

Attacker's fraction q, q_1	Simplex chain	Hybrid chain (proposed)				
		$q_2 = 0.1$	0.2	0.3	0.4	0.5
0.1	2.4×10^{-4}	2.4×10^{-4}	2.3×10^{-3}	1.3×10^{-2}	5.0×10^{-2}	0.16
0.2	1.4×10^{-2}	3.2×10^{-3}	1.4×10^{-2}	4.6×10^{-2}	0.12	0.29
0.3	0.13	2.1×10^{-2}	5.7×10^{-2}	0.13	0.27	0.48
0.4	0.50	9.0×10^{-2}	0.18	0.31	0.50	0.73
0.5	1	0.29	0.44	0.62	0.82	1

V. CONCLUSION

We have proposed a new mechanism for securing a blockchain applied to contracts management. A serious issue in contracts management is that a collapse in coin prices will not work as deterrence against attacks when using the proof-of-stake method. To solve this, we devised a new consensus method using credibility score and described a hybrid blockchain created by alternately using this new method and proof-of-stake. We also modeled an attack on the hybrid blockchain and revealed the probability of its being completed. Subjects for our future work include elaborating the mechanism in order to implement it on an actual cryptocurrency.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, 2008.

[2] J. Bonneau et al, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in 36th IEEE Symposium on Security and Privacy, May 18-20, 2015.

[3] S. King, S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake", http://peercoin.net/assets/paper/peercoin-paper.pdf, 2012.