Blockchain-based Trusted Computing in Social Network

Dongqi Fu
International School
Beijing University of Posts and Telecommunications
Beijing, China
e-mail: fudongqi@bupt.edu.cn

Liri Fang
School of Environment and Natural Resources
Renmin University of China
Beijing, China
e-mail: fangliri@ruc.edu.cn

***Abstract*—MIT Media Lab employed blockchain to describe a decentralized personal data management system (i.e. Decentralizing Privacy) that ensures users own and control their data without authentication from a third party. In this paper, we employ a better encryption algorithm from NTT Service Evolution Laboratory to enforce the "Decentralizing Privacy". Instead of using Proof-of-Work (PoW) for protection, we employ Proof-of-Credibility Score to improve the pervious system and analyzed attack situations.**

Keywords-Blockchain; Trusted Computing; Decentralized; Privacy Production; Proof-of-Credibility score

I. INTRODUCTION

The amount of data in our world is rapidly increasing. According to a recent report [1], it is estimated that 20% of the world's data has been collected in past couple of years. Facebook, the largest online social network, collected 300 petabytes of personal data since its inception [2]. MIT Media Lab provided a mechanism called "Decentralizing Privacy" which could protect personal data [3]. In this paper, we employ a better encryption algorithm to enforce the "Decentralizing Privacy". Instead of using Proof-of-Work (PoW) for protection, we employ Proof-of-Credibility Score [4] to enforce the pervious system. The Bitcoin [5], 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 [6]. 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. Blockchain is an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, and has recently attracted intensive attention from governments, financial institutions, hightech enterprises, and the capital markets. Blockchain0s key advantages include decentralization, time-series data, collective maintenance, programmability and security, and thus is particularly suitable for constructing a programmable monetary system, financial system, and even the macroscopic societal system.

Today, data is a valuable asset in our economy [7]. Facebook, the largest online social-network, collected 300 petabytes of personal data since its inception – a hundred times the amount the Library of Congress has collected in over 200 years [8].

In recent years, a new class of accountable systems emerged. The first such system was Bitcoin, which allows users to transfer currency (bitcoins) securely without a centralized regulator, using a publicly verifiable open ledger (or blockchain). Since then, other projects (collectively referred to as Bitcoin 2.0 [8]) demonstrated how these blockchains can serve other functions requiring trusted computing and auditability.

For Bitcoin 2.0, MIT Media Lab designed a data management platform focused on privacy — "Decentralizing Privacy" [3]. They illustrated how blockchains could become a vital resource in trusted-computing. Their model stressed issues like data ownership, data transparency, data auditability and fine-grained access control. In their future extension part, they introduced the hypothesis that the alternative method instead of Proof-of-work mechanism. In this paper, we employ credibility score to enhance their hypothesis.

In the rest of the paper. Section two introduces the basic knowledge and theories of the blockchain. Section three introduce how we enhance their model [3]. Section four analyzes the attack situation. Section five concludes the paper.

II. BASIS OF BLOCKCHAIN

Blockchain is an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, and has recently attracted intensive attention from governments, financial institutions, high-tech companies, and the capital markets.

A blockchain is something like a ledger in which all transactions have been recorded, and it is shared by the participants of a bitcoin network [9]. Blockchain (Fig. 1) consists of data layer, network layer, consensus layer, incentive layer, contract layer and application layer [10].

Moreover, Data layer encapsulates data blocks of lower layer and relevant asymmetric encryption and time stamp technologies. In data layer, each node can use hash function, SHA, RSA, Merkle tree data structure and so on to encapsulate the transactions and code (which is received in a certain time) into a new block with time stamp. And the new

978-1-4673-9026-2/16/$31.00 ©2016 IEEE

block will connect to the main blockchain to become a new block in the chain.

Network layer consists of distributed network mechanism, data transmission mechanism, data verification mechanism. Network layer enables each node can participate the data verification and transaction recording process. If and only if a block is verified by most of the nodes in the network, it will be proved verified.

Consensus layer mainly encapsulates consensus algorithms for all nodes. Consensus layer makes blockchain technology sensible and reliable even in an efficient distributed network. In this layer, PoW stands for Proof-of-Work, PoS stands for Proof-of-Stake, and DPoS stands for Delegated Proof-of-Stake.

Incentive layer combines economic factors into the blockchain frame including currency issue mechanism and currency distribution mechanism for encourage bitcoin miners (who generate the next block). Essentially, incentive layer addresses the problem of crowdsourcing among different distributed nodes. Therefore, there must be an efficient crowdsourcing mechanism to guarantee maximum profit of individuals, so that the security of the whole blockchain system can be realized.

Contract layer mains contains related scripts, algorithms and smart contracts originated from the code and algorithms. Contract layer is the prerequisite of flexible programming and data operation in a blockchain system.

Application layer embodies application scenarios and cases. With the supporting of time stamp-based chain structure, consensus of distributed nodes, economy-incentive based on PoW, and flexible programmable smart contract, the blockchain is technical and creative.

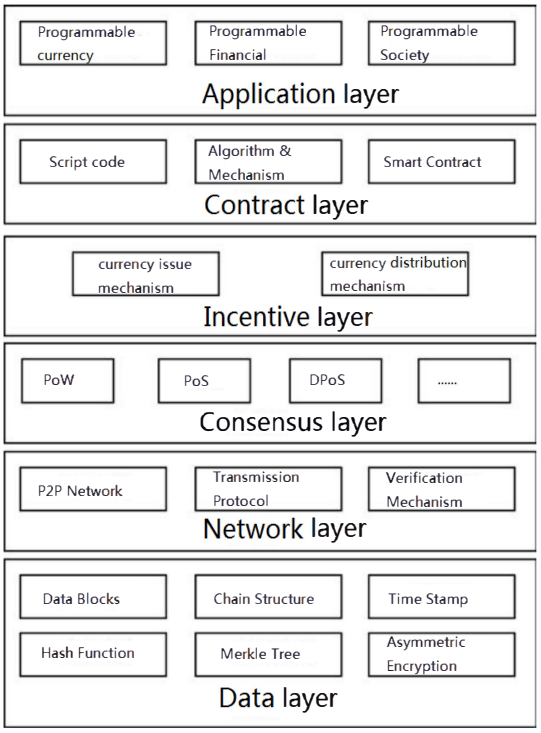

Figure 1. Basic structure of blockchain

III. PRIVACY MANAGEMENT PLATFORM

A. Overview of the Platform

As illustrated in Fig. 2, the three entities consisting the system are mobile phone users, interested in downloading and using applications; services, the providers of such applications who require processing personal data for operational and business related reasons; and nodes, entities entrusted with maintaining the blockchain and a distributed private key-value data store in return for incentives. The blockchain accepts two new types of transactions: T_{access}, used for access control management; and T_{data}, for data storage and retrieval.

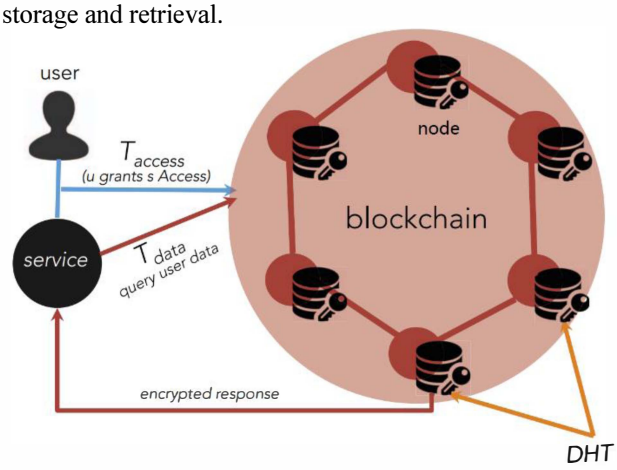

Figure 2. Structure of data privacy management platform from MIT [3].

For example, a mobile phone user installs an application that uses the platform for preserving her privacy. As the user signs up for the first time, a new shared identity (user, service) is generated and sent, along with the associated permissions, to the blockchain in a T_{access} transaction. Data collected on the phone is encrypted using a shared encryption key and sent to the blockchain in a T_{data} transaction, which subsequently routes it to an off-blockchain key-value store, while retaining only a pointer to the data on the public ledger (the pointer is the SHA-256 hash of the data).

The off-blockchain key-value store is an implementation of Kademilia [11], a distributed hash table (or DHT), with added persistence using LevelDB[2] and an interface to the blockchain. The DHT is maintained by a network of nodes (possibly disjoint from the blockchain network), who fulfill approved read/write transactions.

B. Network Protocols of the Platform

In the network protocol of the platform, the MIT Media Lab provides a completed protocol cluster which includes four relevant protocols aiming to solve the data ownership, (i.e. the data identity) , permission of operations, and access control about T_{access} and T_{data} [3]. After proposing them, MIT Media Lab carried privacy and security analysis in some user cases.

In the “Decentralized Privacy”, the blockchain protocol cluster contains four protocols.

Protocol one illustrates the implementation for a single owner (the user) and a single guest (the service). As illustrated, the identity is comprised of single signing key-pairs for the owner and guest, as well as a symmetric key used to encrypt or decrypt the data, so that the data is protected from all other participants in the system.

Protocol two verifies whether the originator has the appropriate permissions of operations.

Protocol three and Protocol four are both about access control. Protocol three is executed by nodes in the network when a T_{access} transaction is received, and similarly, Protocol four is executed for T_{data} transactions.

IV. Improvement of the Platform

In the "Decentralized Privacy", in order to give more weight to trusted nodes and compute blocks more efficiently, the MIT Media Lab conceived to define a new dynamic measure of trust which is based on node behavior (such that good actors that follow the protocol are rewarded) to replace the Proof-of-work mechanism. In this part, we employ the credibility score [4] to enhance the previous system.

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. However, solving proof-of-work puzzles wastes a significant amount of resources. 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 [12], another type of cryptocurrency. With proof-of-work, the probability of mining a block depends on the work done by the miner (who generates a block).

Especially, the resource of the proof-of-stake is the amount of coins that are held. Intuitively, nodes which pour significant resources into the system are less likely to cheat. 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.

However, there is a serious issue involved when using it in contracts management [4]. In this angle, we employ a new method (proof-of-credibility score) of securing a blockchain network.

Measuring credibility score 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 making a miner provides proof that he has a high enough credibility score. The difference between our improvement and the previous model from MIT Media Lab is that: in previous model, the trust score of the node is accumulated on how much good actions a node took; while the improvement utilizes the connection between nodes to calculate the credibility score.

There is a problem in using a credibility score instead of a stake. 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.

In order to settle the problem, a hybrid of proof-of-stake and proof-of-credibility score is utilized. The hybrid blockchain is created when the proof of stake and credibility score methods are executed alternately. As shown in Fig. 3, 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.

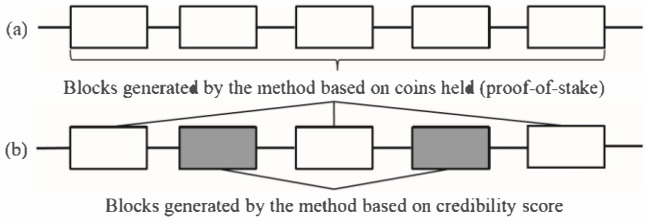

Figure 3. (a) Conventional simplex blockchain (b) Proposed hybrid blockchain

V. Attack Situation Analysis

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:

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

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

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

$$f(x) = \begin{cases} q_1/p_1\,, & if\ n = 2m-1\ \ (odd) \\ q_2/p_2\,, & if\ n = 2m\ \ \ \ \ \ \ (even) \end{cases} \qquad (3)$$

In Eq. (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. According to Hiroki [3], Table I summarizes the probabilities of completing an attack on the simplex blockchain and on the hybrid blockchain when z=6.

TABLE I. PROBABILITIES OF AN ATTACK ON EACH CHAIN [4]

Attacker's fraction q, q_1	Simplex single chain	Hybrid chain (proposed)				
		q_2= 0.1	0.2	0.3	0.4	0.5
0.1	0.00024	0.00024	0.0023	0.013	0.05	0.16
0.2	0.014	0.0032	0.014	0.046	0.12	0.29
0.3	0.13	0.021	0.057	0.13	0.27	0.48
0.4	0.50	0.090	0.18	0.31	0.50	0.73
0.5	1	0.29	0.44	0.62	0.82	1

The result confirms that it is more difficult to attack proposed hybrid chain than conventional simplex chain.

VI. CONCLUSION

This paper reviews the basic technology of blockchain, analyses the extension of the decentralized data privacy management platform from MIT Media Lab and employs the Proof-of-Credibility score from NTT Service Evolution Laboratory to replace the Proof-of-work mechanism. After the improvement, the attack situation is analyzed, the result shows that the improvement (i.e. the hybrid block chain of credibility score) is difficult to attack. All in all, this paper merely conceives new trial improvement and carries on some simple analysis, more in-depth researches and simulations focus on information propagation and blockchain fork issues should be considered for further enhancement.

REFERENCES

[1] ScienceDaily. Big data, for better or worse: 90% of world's data generated over last two years. 2013.

[2] Scaling the facebook data warehouse to 300 pb, 2014.

[3] Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", 2015 IEEE CS Security and Privacy Workshops, 2015.

[4] Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu, and Jay Kishigami, "Blockchain Contract: Securing a Blockchain Applied to Smart Contracts", 2016 IEEE International Conference on Consumer Electronics (ICCE), 2016.

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

[6] 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.

[7] K Schwab, A Marcus, JO Oyola, W Hoffman, and M Luzi. "Personal data: The emergence of a new asset class." In An Initiative of the World Economic Forum, 2011.

[8] Michael Lesk. "How much information is there in the world ?".

[9] Hiroki Watanabe, Shigeru Fujimura, Atsushi and Jay (Junichi) Kishigami, "Blockchain Contract: A Complete Consensus using Blockchain", 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), 2015.

[10] YUAN Yong and WANG Fei-Yue, Blockchain: The State of the Art and Future Trends, Acta Automatica Sinica, vol. 42, no.4, pp.481−494, April, 2016.

[11] Petar Maymounkov and David Mazieres. Kademlia: A peer-to-peer information system based on the xor metric. In Peer-to-Peer Systems,pages 53−65. Springer, 2002.

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