A Security Perspective of Blockchain Technology in the Financial Sector

Xiaonan Yuan[1*], Lin Xie[2*]

Email: ymqh7777@163.com[1] Email: lin-xie@outlook.com[2]

University of Tasmania, Hobart, Australia[1]
University of Melbourne, Melbourne, Australia[2]

ABSTRACT-The paper provides a snapshot of blockchain security technology by examining its data structure, achieving basic security requirements and some primary challenges. Blockchain qualifies as a disruptive technology. Although it started in 2008, it is now one of the popular technologies, which continues to transverse different industries. The peer-to-peer approach to sharing information, sophisticated data structure and features such as immutability, can offer solutions to identity theft, among other online-based frauds in the financial sector. Although it is a promising model, issues such as privacy concerns, regulatory uncertainty, slow adoption and lack of trust among stakeholders, will likely slow down its adoption in the financial sector.

Keywords-Blockchain, Peer-to-Peer, Identity Theft, Immutability

1. INTRODUCTION

Blockchain is an emerging technology associated with Bitcoin. This technology has elicited significant attention, mainly because of its peer-to-peer model, with many industries exploring its applicability [1]. Experts in the technology sector strongly believe that blockchain technology can transform any industry by making processes more democratic, secure, transparent and enhanced efficiency. The financial industry is a step ahead of others in the experimentation of blockchain technology. By 2017, over 90 central banks across the world indulged in blockchain technology by engaging in discussions, over 2500 patents were filled the same year, and 80% of the banks initiating Blockchain and distributed ledger technology [1].

Compared to traditional security models, the blockchain security uses cryptographic algorithms and distributed computing [2]. While there is a positive adoption rate of this model, it is slow, something attributed to potential privacy issues. Some of the concerns are legitimate, but most of them remain unproven. What is proven is blockchain's efficiency in data storage,

ICEMME 2022, November 18-20, Nanjing, People's Republic of China

DOI 10.4108/eai.18-11-2022.2327110

execution of transactions and the creation or facilitation of a trustworthy financial environment [4]. Blockchain is definitely a breakthrough, and if adopted largely in the financial sector, it will transform the industry, profoundly. Combined with artificial intelligence, and big data, blockchain technology is the cornerstone for financial services in the future (figure 1).

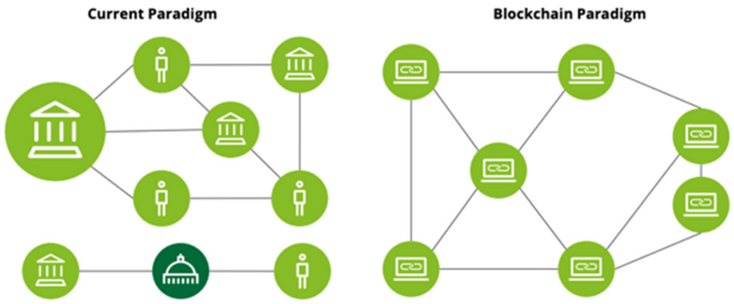

Figure 1 The traditional (current paradigm) vs. Blockchain base distributed ledger

2. BLOCKCHAIN SECURITY MODEL

Under the current paradigm, financial service providers rely on central authorities, which serve to transfer money between parties. The blockchain paradigm works differently, whereby, it has distributed nodes that facilitate sharing of information. While the current paradigm relies on multiple intermediaries to create trust, the blockchain technology uses the cryptographic algorithm, which enables trust [1]. Banks invest significantly in securing their networks to avoid instances of fraud, especially, online-based fraud. Even so, cases of fraud continue to plummet. In 2020 alone, over 40% of Americans experienced a case of identity theft [3]. In the previous year, 2019, identity theft cases in America cost $500 billion, only to increase by over 40% in 2020 to over $700 billion in costs [3].

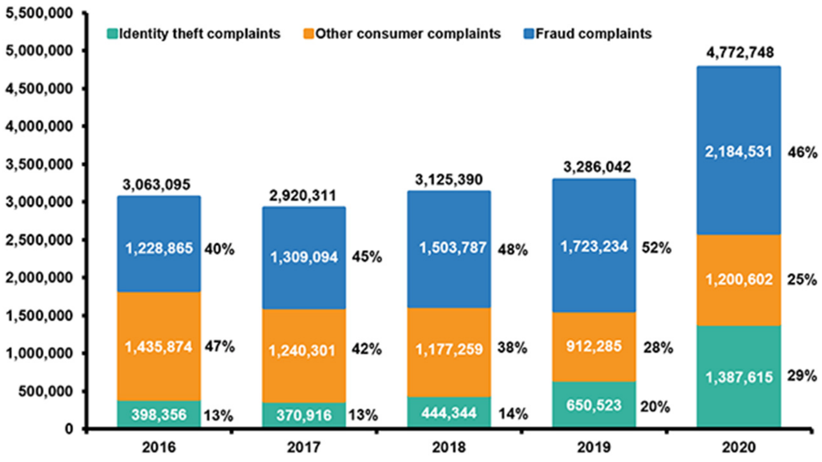

Figure 2 Identity Theft Complaints 2016-2020

Figure 2 paints a gruesome picture of identity theft cases, which are just an example of cybercrime in the financial sectors. Blockchain technology offers a viable solution. The immutability of blockchain makes it difficult for online fraud to happen. It is almost impossible for intruders to make changes to the system or model once it is established, something that increases the integrity of data, and reduces the likelihood for fraud [2]. Immutability and irreversibility in the blockchain technology is derived from its data structure.

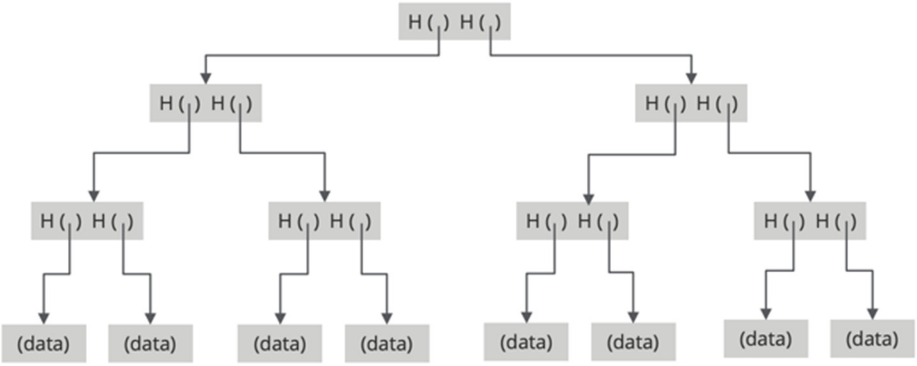

Figure 3 Blockchain Data Structure

The cryptographic security in the Blockchain model comprises a binary structure that features hash pointers. The resulting structure is known as a Merkle tree, or the distributed data structure. The blocks of data are grouped as pairs, and resulting hashs of the blocks stored in a parent node [1]. The grouping approach goes on to the root node, and this is what brings about the immutability feature. If there is interference, intrusion or tampering of the data blocks, the intruder has to tamper or alter all the hashes to the root node, which apparently is immune to tampering. Something else about this data structure is on the membership or ownership. Unlike the traditional paradigm, in blockchain, knowing the root member provides access to all members on the tree. This means that the processing of data is faster and more efficient than the traditional binary tree.

3. BASIC SECURITY REQUIREMENTS

Before banks can implement Blockchain security model, they need to evaluate the security requirements, and understand the different blockchain types. Table 1 presents the basic requirements, which are Confidentiality, Integrity and Availability [4], and Table 2 presents the blockchain types. Confidentiality is core to authorization, integrity is all about ensuring data reaches the authorized user without being changed, and availability refers to availability when needed. Any system that falls short of these security requirements does not qualify for implementation, especially in the financial services. The current paradigm does meet the security requirements, but there are a lot of loopholes that Blockchain technology can fill.

Table 1 Basic security requirements

Requirement	Safeguard
Confidentiality	Blockchain symmetric encryption
Integrity	Hashing ensures integrity
Availability	Blockchain applies limits to the acceptable transactions by devices and the miners
User control	Logging the transactions in the local Blockchain technology
Authorization	Blockchain uses policy header and shared keys

A bank that requires to follow the basics of Blockchain technology to ensure the model works. For example, for users to achieve control over their transactions, the bank will need to allocate a shared key [4]. The shared key facilitates communication between the different users. Probably, an area that might be problematic is on policy header or who gives permission for keys to be distributed. Apparently, in a normal blockchain model, a miner consults with the owner to distribute the keys. Here, probably, banks might need to come together to know who will be the custodian of the shared keys, among other things. However, it is likely that for a bank, the adopted model will not be similar as that of mining cryptocurrency.

Table 2 Comparing different blockchain types

Feature	Public Blockchain	Consortium Blockchain	Private Blockchain
Determination of consensus	All the miners	A set of nodes	One party
Read permission	Public	Public or limited	Public or limited
Immutability	Almost impossible to tamper	Possible to tamper	Possible to tamper
Centralization	No	Partially	Yes
Process of consensus	Permissionless	Permissioned	Permissioned
Efficiency	Low	High	High

In Table 2, three blockchain types are compared. Banks are free to select the type of blockchain they need, but it should be one that suits their security needs. Most banks should consider either a private or public blockchain. A private blockchain is centralized; thus, the banck can control. The problem with the private blockchain is that this type can be tampered with. Even so, it gives the bank control, which will alleviate instances of consensus hijack. On the other hand, a public blockchain is difficult to tamper with; thus, the bank is assured of security. Now, the issue lies with the process of consensus, which can expose the bank to consensus hijack.

4. PRIMARY CHALLENGES

The open ledger system in blockchain technology exposes it to privacy issues. Since it is open, customer data risks being public, or easily accessed [5]. While there is a solution to this, through probably private or permissioned blockchains coupled with encryption, the public will portray some reluctance entrusting their personal information. Also, blockchain technology is sophisticated. Questions arise on how the existing technologies in banks can integrate, including payment systems. Different stakeholders have to come together to actualize the integration, but as things stand, bringing the stakeholders together to reach such a consensus will take time. Governments across the world perceive the cryptocurrency as a disruption to the normal way of doing things, adopting blockchain security model will face regulatory uncertainty [5]. The primary challenges the security model faces are central to key management, cryptography and consensus hijack.

4.1 Key Management

The use of private keys does not alleviate, entirely, potential for intrusion. If an adversary accesses the keys, they can compromise wallets, or assets associated with the keys. This is the same risk posed in traditional systems, for example, planting malware, social engineering, among others. When an attacker accesses the encryption keys, they can read the data. This is why it is important to secure the signing key. The problem with the blockchain technology is that, while it is possible for a server administrator to identify or track hacking attempts, in blockchain, this is impossible, until the hacker is successful.

4.2 Cryptography

Blockchain relies on cryptographically generated keys. With cryptography, there is a need for strict policies, and procedures, which in turn, those mandated, must adhere to them, strictly. Key generation is done through software, for example, the Blockchain client software. The issue is that some software generates weak keys; thus, risk of brute force. In addition, quantum computing undermines asymmetric cryptography. While it is not an immediate threat, there is a need for considering a future-proof solution.

4.3 Consensus Hijack

Blockchain technology uses decentralized networks. In such networks, which are permissionless, there is a risk of consensus hijack. This happens when majority of users or clients agree to allow an attacker to interfere with the validation process. In Bitcoin, this is known as "51% attack," which is a serious security concern. Perhaps a way of centralizing networks, or penalizing users might mitigate such a risk.

4.4 Recommendations

Table 3 Challenges and recommendations

Challenges	Recommended Practices
Key - Storage - Loss	- Good key storage practices - Implement rules requiring multiple signatures for authorizing transactions

- Theft	- Encourage recovery agents, for example, third party - Create different keys for singing and encryption purposes - Create individual keys for staff
Cryptography - Key generation	- Creation of keys should follow secure and valid approaches - Ensure appropriate key length - Using different keys for signing and encryption purposes
Consensus Hijack - Fraudulent activities	- Monitor the nodes to assess the processing power and number of transactions - Increase fees for new transactions to limit transactions by a single node

5. CONCLUSION

Blockchain technology offers the financial industry a solution to the massive cases of online-related fraud. It is upon the stakeholders to come together and actualize its implementation. Attributed to efficient data storage, faster processing of transactions, and facilitation of trust in transactions, some players in the financial sector are already considering blockchain technology. While the model is not immune to weaknesses, the strengths outweigh them. The blockchain model is disruptive. Considering the benefits, it offers the financial sector; one would only recommend its faster adoption and implementation.

REFERENCES

[1]Deloitte. (2017). “Blockchain technology in India: Opportunities and challenges.” [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-technology-india-opportunities-challenges-noexp.pdf [Accessed: 07-Oct-2021].

[2]K. Zīle and R. Strazdiņa, “Blockchain Use Cases and Their Feasibility,” Applied Computer Systems, vol. 23, no. 1, pp. 12–20, 2018.

[3]“Facts Statistics: Identity theft and cybercrime,” III. [Online]. Available: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime. [Accessed: 07-Oct-2021].

[4]A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017.

[5]F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” Telematics and Informatics, vol. 36, pp. 55–81, 2019.