University of Limoges

Internship Report
BLOCKCHAIN AND ATTACKS

Students: **TRAN Ngoc Nhat Huyen**
Professor: **Emmanuel CONCHON**

July 13, 2021

Contents

1 Introduction

2 Basic Concept

2.1 Blockchain

A Blockchain is a growing list of transaction records, calledblocks, that are linked usingcryptography. For the first time, in Journal of Cryptology 1991, the idea of Blockchain camewith Stuart Haber and Scott Stornetta when they published an article [HS91] about how totimestamp a digital document. It was not until 17 years later, the birth of Blockchain isrecognized in the Bitcoin paper [Nak09] of Satoshi Nakamoto in 2008.For simplicity, a Blockchain is just a database. It differs from a typical database inthe way it stores data, Blockchains store information in blocks that are then chained to-gether. Each block contains a cryptographic hash of the preceding block, and transactiondata (represented as a Merkle tree).Bockchain technology is a recent breakthrough of secure computing without centralizedauthority in an open networked system. From a data management perspective, a blockchainis a distributed database that logs an evolving list of transaction records by organizing theminto a hierarchical chain of blocks. From a security perspective, the block chain is createdand maintained using a peer to peer overlay network and secured through intelligent anddecentralized utilization of cryptography with crowd computing.

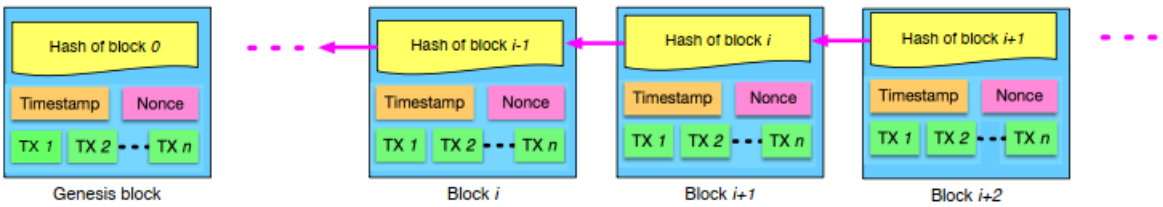

Figure 1: Blockchain which consists of a continuous sequence of blocks

2.2 Security in Blockchain

Basicly, Blockchain has some properties of security based on cryptography advances. Concretely

Consistency

The consistency of Blockchain means that all nodes have the same ledger at the same time. During the time when the distributed ledger is being updated with new data, any read/write requests will have to wait until the commitment of this update.

Tamper-Resistance

Within a Blockchain network system, the tamper-resistance model means that any transaction information stored in the blockchain cannot be tampered during and after the process of block generation. Practically, it is impossible to tamper transaction data without the network knowing about it, showing the power of storing and distributing in the Blockchain.

Resistance to DDoS Attacks

A DDoS attack refers to a "distributed" DoS attack, this occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. The serious concern in a DDoS attack is related to whether a DDoS attacker can make the blockchain unavailable by knocking out a partial or the whole network. Based on the fully decentralized construction and maintenance of the Blockchain system and the consensus protocol for new block generation and addition to the blockchain, which ensures that the processing of Blockchain transactions can continue even if several Blockchain nodes go offline.

Resistance to Double-Spending Attacks

Unlike physical cash, a digital token consists of a digital file that can be duplicated. Prevention of double-spending is usually implemented using an online central trusted third party that can verify if a token has been spent. To prove that no attempts to double-spend have occurred, the Blockchain provides a way for all nodes to be aware of every transaction.

Pseudonymity

Although users/transactions of a cryptocurrency network are not really anonymous (pseudonymous), that means users can interact with the system by using their public key hash as their pseudo-identity without revealing their real name. The pseudonymity of a system as a privacy property to protect a user's real name.

2.3 Privacy in Blockchain

2.3.1 Privacy of transaction

Blockchain offers a fully auditable and valid ledger where transactions are visible to all other users. This transaction's disclosure is necessary to reach a consensus among distributed nodes, but it goes along with serious privacy risks.
Even though blockchain address supports pseudonyms to hide the real identity, they are not totally anonymous. Concretely, it is possible to analyzing the transaction graph [2] that link all independent public key to user. From the correlation between transaction addresses, adversary can track the monetary flow, calculate approximate balance and infer the user's real identity.

2.3.2 Privacy of smart contract

Similarly, data and code are transparent to all users, which enable every miners to execute smart contract and validate transaction. However, in many scenarios of smart contract systems, the financial transaction as well as other additional data exchange need to be highly secret,(e.g: auction bids, insurance contracts, stock trading, ...)
To sum up, currently, blockchain technology

To tackle the privacy threats, there are some protection techniques, algorithms, protocols

3 Techniques

3.1 Zero knowledge proof

Zero knowledge proof, firstly introduced by Goldwasser et al. [3] in the early 1980, is one of the most important technologies to protect privacy. In a ZKP system, the prover has to convince the verifier that he knows about the secret without revealing any useful valid information beyond the validity of statement. Zero-knowledge proof is divided into 2 types: interactive and non-interactive. In the field of blockchain, the non-interactive proof is much more popular because when an user has a new transaction waiting for validation, he would not make a lot of two-way communication with every miners to prove the correctness. the non-interactive zero-knowledge proof allows prover (spender) send a single messages to verifier (miner).
Zero knowledge proof has three properties:

- **Completeness**: If the statement is true, an honest prover can convince the honest verifier of the fact.
- **Soundness**: If the statement is false, then the prover can deceive the verifier only with a negligible probability.
- **Zero knowledge**: After the proof process is completed, the verifier cannot learn anything beyond the validity of the statement.

ZKPs offer privacy to public smart contract networks in a manner that does not sacrifice the auditability that is inherent to public smart contract networks.

References

[1] N. Mladenovíc, P. Hansen. *Variable Neighborhood Search.* Computers & Operations Research 24 (11), 1097-1100, 1997.

[2] D. Ron, A. Shamir, *Quantitative analysis of the full bitcoin transaction graph*, in: International Conference on Financial Cryptography and Data Security, Springer, 2013, pp. 6-24.

[3] S. Goldwasser, S. Micali, C. Racko, The knowledge complexity of interactive proof systems, SIAM Journal on computing 18 (1) (1989) 186-208.

[4] R. Rivest, L. Adleman, M. Dertouzos, "On data banks and privacy homomorphisms," Foundations of Secure Computation, vol. 4, no. 11, pp. 169-180, Jan. 1978.

[5] B. BĂźnz, S. Agrawal, M. Zamani, D. Boneh, Zether: Towards privacy in a smart contract world., IACR Cryptology ePrint Archive 2019 (2019) 191.