The University of Sydney

School of Information Technology

INFO5993 Research Methods - Assignment II

Unforkable Blockchain Cryptocurrencies with Efficient Zero Knowledge Contingent Proof on Mobile Devices

Author:
Lin Han

Supervisor:
Dr. Vincent Gramoli

October 9, 2017


SIDERE MENS EADEM MUTATO

1 Introduction

From the time when Block 0 of the Bitcoin blockchain, the Genesis Block, is created at 18:15:05 GMT on January 3rd, 2009, the words "cryptocurrencies" and "Blockchain" become one of the most popular fields in information technology. The "decentralized" and "anonymous" nature of cryptocurrencies overcomes the weakness of traditional *trust-based* electronic payments who relies heavily on trusted third-party financial institutions. The *cryptographic proof-of-work* of bitcoin enables reliable transaction between two parties directly. Through almost 10 years development, cryptocurrencies turns out to be a large family and can be deployed onto multiple devices.

Though bitcoin give a great solution on *double spending* problem, it doesn't mean that it is secured in all aspects. One possible issue is balance attack targeting blockchain's forkable feature. Other cryptocurrencies allowing forkable chains all suffer from the very same issue. In this sense, unfokable blockchain is proven to solve this problem. On the other hand, another possible solution to secure transaction is to adopt mechanism like *zero knowledge contingent payment* which are released if and only if some knowledge is disclosed by the payee and to do this in a trustless manner where neither the payer or payee can cheat. Whilst there are several theoretical discussion and practice in a variety of contexts, this paper will concentrate on their application on cryptocurrencies blockchain, especially on mobile devices.

2 Bitcoin

2.1 Blockchain

Blockchain is the way how Bitcoin keeps its public ledger. To some extent, blockchain is simply a peer-to-peer distributed timestamp server. The ultimate goal of this design is to solve /textitdouble-spending problems and prevent modification of transaction records.

Each full node in the Bitcoin network keeps a full copy of the blockchain, in which all blocks validated by this particular is stored. When several nodes within the network independently arrive at identical blockchains, they are considered to be in *consensus*.

As its name suggests, a blockchain is a digital chain of blocks, where a

timestamp, a nonce, and a Merkle Tree is stored. The blocks are chained cryptographically using hash. In detail, each block contains the hash of its previous block ,finally leading to the Genesis Block. Any modification on blocks in the chain would violates all subsequent hashes, which is vital for consistency of the ledger. Figure 1 shows part of a blockchain.

However, computing a hash is expensive. This truth enables the adoption of *proof-of-work* in bitcoin network.

2.2 Proof of Work

2.3 Transaction

2.4 Contracts

3 Balance Attack

4 Unforkable Blockchain

4.1 Byzantine Consensus

4.2 The Red Belly Blockchain

5 Zero Knowledge Contingent Proof

5.1 Bitcoin

5.2 Zero Cash

5.3 Efficient Implementation of Zero Knowledge Proof in Cryptocurrencies

6 Conclusion

References

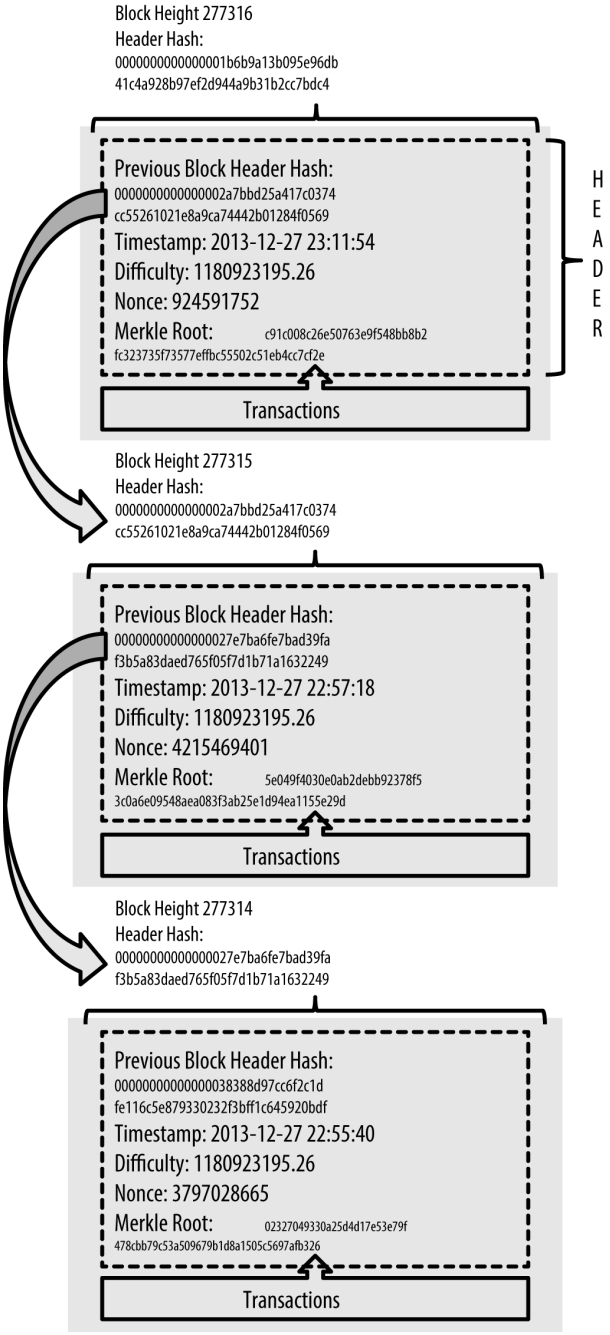

Figure 1: Blockchain