University POLITEHNICA of Bucharest

Faculty of Automatic Control and Computers,
Engineering and Management of Business Systems

RESEARCH REPORT

Blockchain for Business

Scientific Adviser:
Prof. Gabriel Neagu

Author:
Adriana Dincă

Bucharest, 2018

Contents

List of Figures

Chapter 1

Introduction

1.1 Project Description

1.1.1 Project Scope

1.1.2 Project Objectives

1.1.3 Related Work

Chapter 2

State of the Art

2.1 Blockchain technical details

The blockchain is a public ledger of all transaction sent through the network that is known by every one that holds a blockchain node. More precisely, each node has a copy of the blockchain in order to validate or invalidate a transaction. The majority of nodes decide if a transaction is valid and if so that transaction is added in the latest created block by one of the miners. The choice of using blockchain for data storing is related with the fact that the blockchain's deep history is immutable so it ensures the protocol security.

The blockchain has no central authority for managing assets flow along the network. This technology is recognized as the "fifth evolution" of computing, the missing trust interface of the Internet as stated by Laurence [2].

The blockchain structure has the following components as described in Figure 2.1:

• **The block** is an array of transactions recorded into a ledger. Depending on the blockchain the transaction has assigned a different type of value. Each block has its own hash and a merkle tree with hashed transactions. Storing transactions in a merkle tree is a design decision that saves disk space. Nakamoto [3] explains the reason why using a merkle tree makes disk space recover possible. The explanation for this is that "once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored" according to Satoshi [3].

• **The chain** is simply a hash that connects two blocks in chronological order. The hash for a new block is generated based on the data that was in the previous block. The hash algorithm used by Bitcoin is Secure Hash Algorithm 256 [1] that creates an unique (collision probability is negligible), fixed-size (256 bits) hash.

• **The network** is represented by full nodes. We can think of it as a computer that runs an algorithm for securing the network. Mining is expensive and it requires a lot of computer power so the blockchain algorithm rewards miners for their service. The payment is usually a currency or a token.

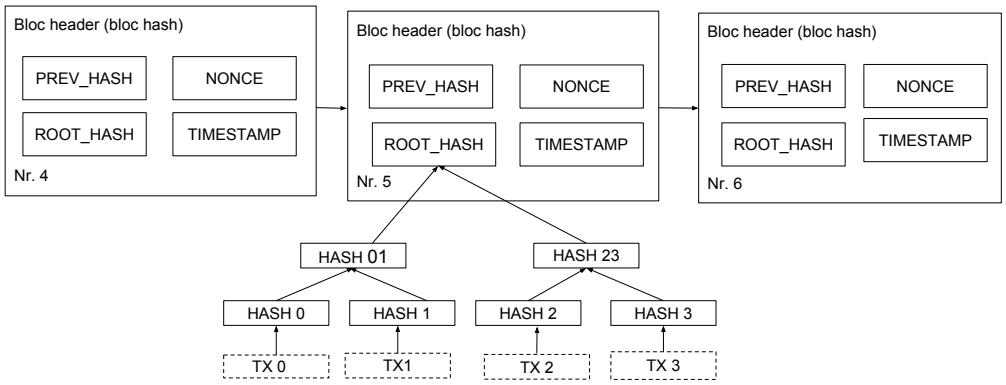

Figure 2.1: Blockchain Structure using Merkle Tree

2.2 Blockchain properties

2.3 Blockchain based projects

2.3.1 Financial

Blockchain and the financial world involve trading, money transfer and mort- gages. Right now the economic world releases on banks, governments and other financial institutions to transfer money from an account to another. Financial information transfer is monitored by governmental institutions and this type of information can be used to banks advantages in trading operations.

2.3.2 Public sector

The public sector activities can benefit from blockchain technology by chang- ing the asset registration, citizen identification process, medical records and medicine supply chain. The real power of blockchain consists of creating new solutions of performing old processes that are inefficient in the modern world. Checking paper records for validating the ownership of an asset had become very difficult and time consuming activity. The number of population is increasing at a high rate and public sector employees are forced to perform lucrative and repetitive tasks. Having all properties stored in a blockchain repository elim- inates the problems mention above and offers the guarantee of security and privacy.

2.3.3 Retail

In the retail field blockchain can change the way the supply process, fidelity programs are implemented or the information sharing process is done (from supplier to retailer and the other way around).

2.3.4 Insurance

There are many activities in the insurance industry than can be innovated such as risk provenance, claims processing, asset usage history or claims files.

2.3.5 Manufacturing

Another industry that can benefit from blockchain technology is the manufac- turing starting with the supply chain, product parts or maintenance tracking.

2.4 Bitcoin project

The Bitcoin is the first cryptocurrency developed using blockchain technol- ogy. The unique attributes of the blockchain and the cryptographic principles brought Bitcoin a huge popularity. Satoshi Nakamoto is the pseudonim of the Bitcoin inventor. The real identity of Satoshi was never revealed. There are many suppositions but not of them was confirmed. He claimed to be a Japanese male around forty years old.

Chapter 3

Conclusion

Bibliography

[1] Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva. Bicliques for preimages: Attacks on skein-512 and the sha-2 family. http://eprint.iacr.org/2011/286.pdf, Originally published in 2011. Accessed: 2017-06-28.

[2] Tiana Laurence. *Blockchain For Dummies*. 2017.

[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *The Cryptography Mailing list at metzdowd.com*, 2008.