ISSN 1512-1232

A BLOCKCHAIN-BASED TRUST MODEL FOR BITCOIN CRYPTOCURRENCY AND ITS POPULARITY IN GEORGIA

Lela Mirtskhulava
Iv. Javakhishvili Tbilisi State University, 3 University Str. Tbilisi, Georgia

Elene Esiava
Sokhumi State University, 9 Jiqia Str. Tbilisi, Georgia

Nana Gulua
Sokhumi State University, 9 Jiqia Str. Tbilisi, Georgia

Abstract
Bitcoin is a digital currency based on a decentralised system of trust dealing with Cryptography. Every time when you need to authorize a payment, you're asked for verification. An idea of the verification is that once you're authorized under your name, it is irreversible. The identification process through someone's signature is not limited to payments. This is an age-old problem. There are a number of trust models applied by various cryptographic schemes, respectively. This paper explores three of them: a) Pretty Good Privacy (PGP) allowing to use a set of the public keys, b) Kerberos permitting to use the trusted third parties, c) certificates for authentication of each other in trusted third parties. Each of the models can differ in scope, scalability complexity and applicability. In the given paper, we analyse security issues of trust models through monitoring the behavior of the blockchain transactions.

Keywords: *The Bitcoin Cryptocurrency, Blockchain, encryption, trust model, Hashing Cryptograph.*

1. Introduction

Under cryptocurrency (or "crypto") we understand a digital currency allowing us to buy some goods or services. In other words, this is an online ledger based on a system of trust protected with cryptography to secure online financial transactions [1]. Bitcoin is the most popular cryptocurrency currently having a price about $34,849.50 and 110,124.42 GEL (Georgian Lari).

Bitcoin gained its popularity in our country Georgia due to a new, revolutionary model of financial transactions completely changing the classical monetary system [2]. By Wikipedia: "A monetary system is a system by which a government provides money in a country's economy. Modern monetary systems usually consist of the national treasury, the mint, the central banks and commercial banks." But by Bitcoin.org: "Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system" [3].

The market research website (CoinMarketCap.com) announced that there are a various number of cryptocurrencies trading publicly where "the total value of all cryptocurrencies on May 27, 2021, was more than $1.7 trillion — down from April high of $2.2 trillion, according to CoinMarketCap. The total value of all bitcoins, the most popular digital currency, was pegged at about $735 billion — down from April high of $1.2 trillion."

ISSN 1512-1232

Table 1. 10 Best cryptocurrencies tracked by CoinMarketCap

Cryptocurrency	Market Capitalization
Bitcoin	$735.3 billion
Ethereum	$324.2 billion
Tether	$61 billion
Binance Coin	$57.5 billion
Cardano	$54.6 billion
XRP	$46.5 billion
Dogecoin	$44 billion
Polkadot	$22.1 billion
USD Coin	$21.9 billion
Internet Computer	$16.7 billion

Data current as of May 27, 2021.

Cryptocurrencies are popular among their supporters for a variety of reasons: [2]

1. They see cryptocurrencies especially Bitcoin as the crypto of the future
2. Cryptocurrency doesn't need to be managed by central banks avoiding the monetary inflation in this way
3. They like the blockchain technology providing a decentralized recording and processing system of financial transactions the payment system more secure.
4. Cryptocurrencies are going up in value

2. Analysis of Trust Models in Bitcoin

"Bitcoin is a form of decentralized digital currency based on a system of trust underpinned by cryptographic puzzles such as various properties of Elliptic curves" [4]. There are a number of trust models applied by various cryptographic schemes, respectively. They are:

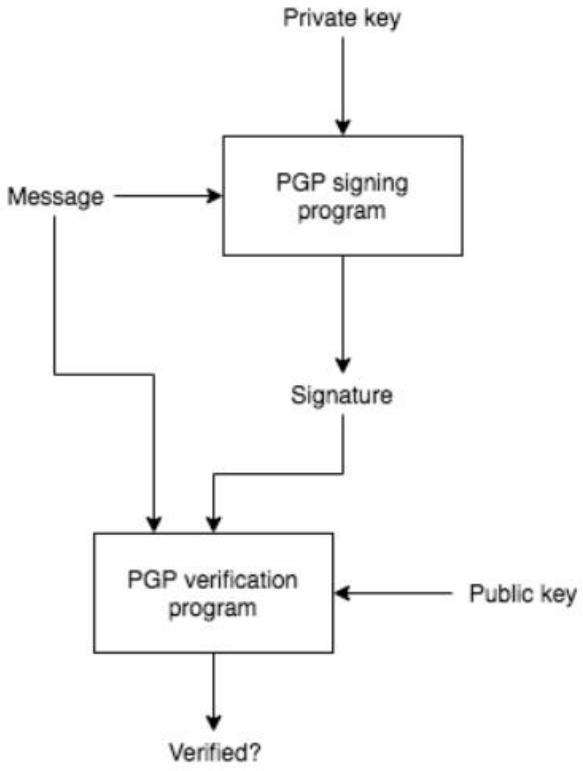
a) The web of trust employed by Pretty Good Privacy (PGP) users using their own set of trusted public keys
b) Kerberos, a secret key distribution scheme using a trusted third party
c) Certificates, which allow a set of trusted third parties to authenticate each other and, by implication, each other's users.

ISSN 1512-1232

Each of the above mentioned trust models differs in complexity, scope, scalability and general applicability. Which model of trust to apply in certain circumstances and types of wireless networks are discussed in the given paper. PGP keys replaced sealing letters. PGP keys are to Bitcoin keys.

There are two options in using a PGP key:

1. Emails encryption and decryption. In this case, the intruder can't decipher the message even if the message has been intercepted.
2. Signing messaging. According to the given method they can verify the authenticity of the message if the message has been intercepted in this case as well.



Pic. 1. PGP signing flow diagram

3. A new level of Trust based on Blockchain

Blockchain is a shared and immutable ledger processing the recording transactions. The blockchain can keep a log of financial transactions in chronological order including timestamps in every single block. Blockchain stores the data of transactions in blocks linked together and forming a chain [5-8].

Key Terms in Blockchain:

Block: A block is an individual transaction or piece of data that is being stored within the blockchain.

Blockchain: A blockchain is a "chain" (list) of "blocks" (records) growing continuously, which are linked chronologically and secured using cryptography.

Transactions: A value that are exchanged among participants accessing the blockchain network.

Participants: Individuals joining the blockchain network using computers to exchange value.

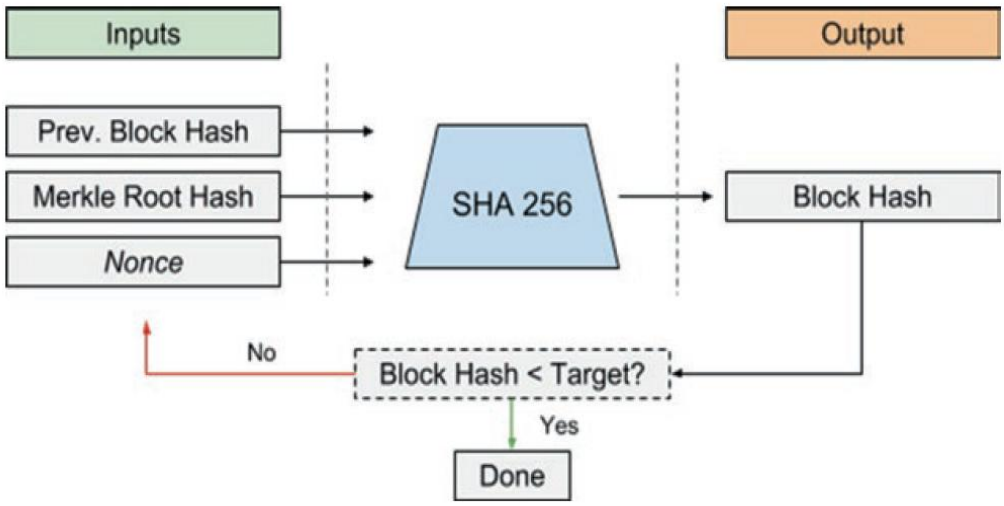
Unconfirmed: transactions and blocks which are not yet verified.

ISSN 1512-1232

The **mempool** is the network area for confirmed transactions but not yet placed into a block. Every node of Bitcoin holds unconfirmed transactions in RAM over the network and removes them once they are confirmed.

Mempool - Typically associated with the cryptocurrency Bitcoin, when a transaction has been conducted over a network, it is transmitted and held in what is known as the Mempool (Memory pool) until a cryptocurrency miner picks it up and includes it in the next block [9-11].

Main aspect of blockchain's security is represented by cryptographic hash functions for preventing the attacks. The hash value is calculated using three input parameters: the hash of the previous block, the Merkle root hash and last one is the nonce and processed using the SHA-256 cryptographic hashing algorithms. Output block hash with a fixed size represents the contents of all the blocks. Hashing in Bitcoin is calculated by miners where the hash obtained should be lower than the hash calculated by the network. To satisfy this criteria, miners need to try various nonce values and then compare the output hash with the target one. The hash values of the previous block and Merkle root hash are not changed. This is an iterative process and it runs until miners get a valid function consuming a lot of power and computing resources (Pic.2). This procedure is called proof-of-work.

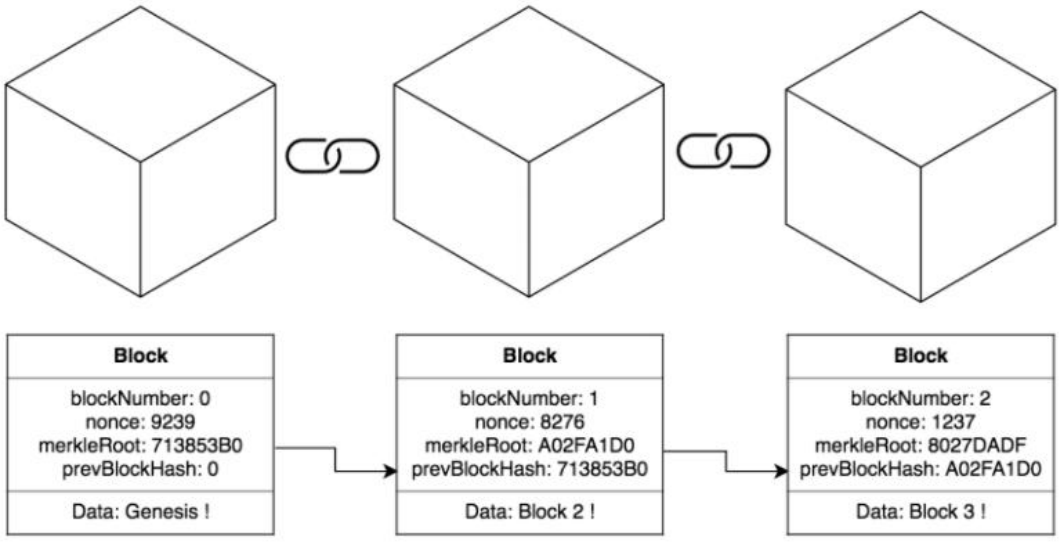


Pic. 2. Block SHA-256 calculation [10].

3.1. How does it work

Let's consider the following scenario where an attacker tries to pay some Bitcoins themselves to modify one of the blocks in the blockchain. If an attacker made changes in the transaction list he must update the Merkle root hash. Each block hash depends on the Merkle root hash and if it is altered, then the block's hash must be recalculated. But it takes too much compute power for mining one block and the attacker will spend much power and time to recalculate the altered block. Next step is to legitimate the block with a recalculated a new hash. So hash pointers play a crucial role in Bitcoin's Blockchain because if the attacker alters any block in the blockchain, every next block must be changed where all subsequent blocks point to the previous block. This attack is time consuming and pointless because the attacker is capable of using less than 51percent of the compute power of the network. These two aspects: hash pointers and proof-of-work are considered as the fundamental feature of Bitcoin's blockchain security.

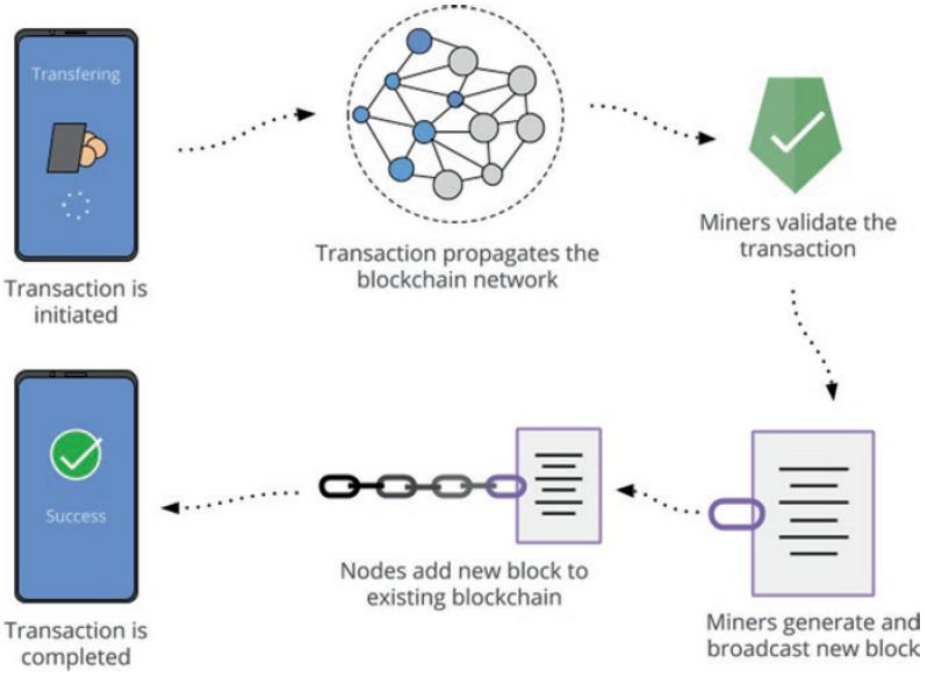
ISSN 1512-1232



Pic. 3. Bitcoin transaction execution

4. Building Mini-Blockchain!

We built a small blockchain of our own in Python! The blockchain is a secure way allowing to store and move data between chained blocks. The data consists of transactions that include the messages exchanged between two parties. In our case study, Alice is trying to transfer 30 units of some currency to Bob. These transactions are all stored inside the mempool, a pool of transactions that miners reference when selecting the set of transactions they want to verify. In reality, no coin is actually transferred but only records of executed transactions are stored in the blockchain's ledger. To broadcast the transaction securely, Alice will sign to prove that the transaction is legitimate. So this is a way to verify that nobody is capable of withdrawing coins out of Alice's electronic wallet without her permission happened using Alice's private key to Bob's public key and then only Bob is allowed to spend the coins.



Pic. 4. Bitcoin's Transactions Execution [10]

ISSN 1512-1232

5. Conclusion

A blockchain provides new benefits through the combination of novel and existing technologies allowing to build innovative blockchain-based trust solutions. A blockchain is a group of blocks chained between each other cryptographically. It keeps the record of all executed transactions on the network. We provided an analysis of how blockchains work in the case of Bitcoin. We examined how transactions can be created and broadcasted. We analysed a trust model for the Bitcoin Cryptocurrency based on Blockchain technology that showed us that the transactions are a key component in Bitcoin's decentralized electronic cash system. Cryptography provides secure transactions making it impossible to read them by third parties and change it. Double hashing makes the Bitcoin cryptocurrency more secure.

References

[1] https://www.nerdwallet.com/article/investing/cryptocurrency-7-things-to-know.
[2] http://geoeconomics.ge/?p=13291
[3] https://bitcoin.org/en.
[4] https://medium.com/coinmonks/trust-model-of-bitcoin-part-i-34aacf47d444
[5] Mirtskhulava L., Globa L., Gulua N., Meshveliani N. (2021) Complex Approach in Cham. Cryptanalysis of Internet of Things (IoT) Using Blockchain Technology and Lattice-Based Cryptosystem. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, https://doi.org/10.1007/978-3-030-58359-0_4
[6] Deploying Enterprise: BlockchainsRam Jagadeesan CTO Blockchain. Cisco, 2019
[7] https://www.uk.sogeti.com/content-hub/blog/iot-security-using-blockchain/
[8] https://www.forbes.com/sites/kateoflahertyuk/2019/04/11/flaws-in-wpa3-wi-fi-standard-allow-attackers-to-crack-passwords-and-view-traffic/#6df21b617050
[9] https://www.uk.sogeti.com/content-hub/blog/iot-security-using-blockchain/
[10] Ammar Rayes, Samer Salam. Internet of Things from Hype to Reality: The Road to Digitization. Second Edition. Springer Nature Switzerland AG 2017, 2019.
[11] Nigel P. Smart. Cryptography Made Simple. Springer International Publishing Switzerland 2016.

Article received: 2021-06-13