Comparative study of selected cryptocurrency

O Nakov, D Gotseva and Y Tomov

Department of Computer Systems, Faculty of Computer Systems and Technologies
Technical University of Sofia, 8 Kliment Ohridski blvd., 1000 Sofia, Bulgaria

E-mail: yavor_tomov@tu-sofia.bg

Abstract. In the last few years, blockchain technologies have gained immense popularity both among researchers and in socio-economic life. Companies from various fields of industry implement projects based on blockchain technology. Pandemics like Covid-19 put almost all industries to the test. The work of the transport industry during the crisis is directly related to the work of the financial and banking sector. The problems that transport companies would experience from blocking the banking system during a subsequent pandemic would be solved in an innovative way using different cryptocurrencies. This article aims to make a comparative analysis of some cryptocurrencies, as well as to comment on the problems associated with them. The analysis can be used to develop blockchain-based applications in the transport industry.

1. Introduction

In 2009, S. Nakamoto [1] published an article that aroused great interest from the scientific community. A year later, the author and a group of other researchers implemented the Bitcoin project (the first cryptocurrency). Nakamoto laid down the main features that each cryptocurrency must meet: a decentralized currency independent of a third party – a bank or financial institution, anonymity or pseudo-anonymity of participants and security of transactions. Unlike traditional currencies, where a third party (bank or financial institution) is required to enable a transaction to take place between two participants, cryptocurrencies use consensus models to validate transactions. The security of the system and the anonymity of the participants are realized through cryptographic methods.

To date, there are more than 3,000 cryptocurrencies with Market Cap about $ 270 billion (figure 1). This fact speaks of a new digital economy that is evolving every day. The development of the cryptocurrency market has led to the creation of other accompanying tools from the digital industry. There is a new way for companies to raise funds for their business through Initial Coin Offering (ICO) (figure 2), digital exchanges for cryptocurrency trading, huge projects based on blockchain technologies and smart contracts.

Bitcoin aims to perform two main tasks: making transactions and storing value. Over the next few years, currencies appeared (litecoin 2011 [2], ripple 2012 [3], monero 2014 [4], dash2014 [5]) and many others that differed in certain features from Bitcoin, but they basically had the same two functionalities – performing transactions and storing value. In 2015, Ethereum (ETH) was created [6]. This new currency added new properties to those held by previous currencies. ETH is a second-generation currency based on the idea of smart contracts first proposed by N. Scebo [7].
Smart contracts provide an opportunity to create different applications in different industries through the use of cryptocurrencies. Cryptocurrencies and smart contracts have the ability to tweak modern relationships through a new approach to digitization.

**Figure 1.** Cryptocurrencies Market Cap (tradingview.com).

**Figure 2.** ICOs Market Cap (invara.com).

In this article, we, like other authors [8], will offer features for evaluating several cryptocurrencies and related technologies, so that these features help developers in the transportation industry to
develop their applications. The cryptocurrencies that are being explored as part of this article fall into two main groups. The first one consisting of cryptocurrencies that are the most popular and well-known, while the second one involves cryptocurrencies that have huge development potential determined by the development team and applied new technology in an industry of global importance. There are different types of research that successfully integrate blockchain technology and cryptocurrencies in transport [9].

2. Background
In his article Nakamoto, describes three main technologies for the implementation of Bitcoin: blockchain, public ledger, consensus model (proof of work). These technologies are the basis of most cryptocurrencies. Blockchain technology is a data structure consisting of individual blocks (figure 3).

All blocks are connected to each other like a linked list. The transactions in each block are hashed and stored in a data structure called a merkle tree. The header of each block contains the previous block’s hash. Using this technology, the author ensures that the information cannot be replaced. Changing a single character will generate a different hash.

Unlike fiat currencies, which use a centralized system, cryptocurrencies use decentralized, where each participant in this system has its own copy of the blockchain. This technology is known as public ledger. In centralized systems, a single participant decides on each transaction if this transaction is valid. In decentralized decision-making, all participants participate. The question arises, can't such systems be manipulated by malicious participants? Nakamoto uses asymmetric encryption techniques to solve the problem of man-in-the-middle attack (MITM) attacks. Another major contribution to security is that the participants in the system participate in proportion to their computing power, and not as the number of accounts, this protects the system from Sybil attack. The main security issue that all cryptocurrencies using the blockchain need to address is related to the problem known as double spending. Numerous algorithms have been proposed, the most popular being proof of work (PoW) [10], proof of stake (PoS) [11].

Smart contracts are computer programs uploaded to the Ethereum network and executed by the Ethereum virtual machine. These contracts, once published, cannot be changed. Ethereum provides Solidity which is a “turing complete” programming language. This means that any logic can be implemented in the Ethereum network.

3. Comparative study of selected cryptocurrencies
As mentioned above, the choice of cryptocurrencies is made on the basis of well-known currencies such as Bitcoin (Btc), Ethereum (Eth), and Ripple (Xrp) while the choice of the latter ones is based on their innovative nature and the important problems they solve – Basic Attention Token (Bat) [12], Theta (Theta) [13], and Chainlink (link) [14]. The selected evaluation criteria is shown in table 1.
Table 1. Comparative evaluation of the selected cryptocurrencies.

|       | Btc  | Eth  | Xrp  | Bat  | Theta | Link  |
|-------|------|------|------|------|-------|-------|
| intended | 2009 | 2015 | 2012 | 2018 | 2018  | 2017  |
| Market cap | $166.9 Billion | $25.3 Billion | $7.8 Billion | $0.36 Billion | $0.18 Billion | $1.6 Billion |
| Blockchain | yes | yes | no   | yes  | yes   | yes   |
| Algorithm | PoW | PoW | Ripple CA | Zero Knowledge proof | Multi-Level BFT | ChainLink algorithm |
| Time confirmation | 60 min | 6 min | Such as 6 min | seconds | 6 min |
| Turing complete | no | yes | no   | yes  | yes   | yes   |
| ledger | blockchain | blockchain | Last Closed Ledger | blockchain, Brave Micropayments Ledger | blockchain | blockchain |
| Coin/Token | coin | coin | coin | token | token | token |
| Innovation | The first crypto project | Smart contracts | Ripple algorithm | Secure Brave browser, using blockchain | Video streaming using blockchain | Blockchain connection with external systems |

The first two criteria measure the capitalization of the given cryptocurrencies since their creation. They serve as proof of their viability. Bitcoin, being the first cryptocurrency in the world, has become the main currency for storing value (digital gold), which is evident from its capitalization. Ripple's capitalization currently puts it in third place. The main factors are the speed of confirmation of transactions, the low value of transactions, and security. Unlike Bitcoin, where the speed of transactions is very slow, Ripple was created to replace the banking system. Ethereum, with its smart contract-based functionality, has become an infrastructure for a vast number of projects and other cryptocurrencies based on the Ethereum network. An example of such cryptocurrency is Bat. Unlike currencies (coins) which have their own infrastructure, tokens work on a foreign blockchain network. This explains the influence of some currencies over others. An increase in the price of Bat would have a positive effect on Ethereum. Historically, the price of Btc affects the state of all other cryptocurrencies, just as the price of gold affects fiat currencies. Because cryptocurrencies are based on decentralized systems, they use different consensus algorithms. Bitcoin and Ethereum use the PoW algorithm, while Xrp uses the Ripple consensus algorithm. The main disadvantages of PoW are the huge amount of electricity consumed and the slow confirmation of transactions. As a matter of fact, the Btc network consumes as much energy per hour as a country like Austria. On the other hand, this algorithm is well scalable and solves the problem of double spending. Ripple is not based on blockchain technology. This cryptocurrency uses a public ledger in which the user's amount of each account is stored. Every few seconds a new ledger is created with new transactions. Last-Closed Ledger is the valid one, in which each transaction must have more than 80% of the validator servers confirming it.

Brave browser is the first browser based on blockchain. Bat is a token for the decentralized ad exchange. BAT connects advertisers, publishers, and users, creating a new, efficient marketplace. The token is based on Ethereum technology, an open source, blockchain-based distributed computing platform with smart contracts. These cryptographically secure smart contracts are stateful applications.
stored on the Ethereum blockchain, fully capable of enforcing performance. The token is derived from – or denominated by – user attention [12].

Unlike other browsers, where personal information is stored on servers, here the information is stored locally. This gives users much more privacy. This is realized by using the Zero Knowledge proof algorithm. The mission of Theta is to leverage blockchain technology to create the first decentralized video streaming and delivery network whereby video viewers are incentivized to share redundant computing and bandwidth resources to address today’s video streaming challenges. Using the Ethereum EVM “World Compute” metaphor, the Theta Network can be viewed as the “World Cache” formed by the memory and bandwidth resources contributed by viewers [13].

One of the main problems with smart contracts is that they are only able to validate information that can be verified by the blockchain. The connection with information from the outside world can be easily manipulated. One way is for an application to make a connection between the outside world and a smart contract. However, this would lead to a breach of decentralization, which is a key feature of all blockchain technologies. The solution to this problem is the idea of oracles offered by ChainLink.

This solution will enable the creation of multiple applications based on smart contracts.

4. Conclusion
In this paper, an analysis of six cryptocurrencies was done. The choice of these currencies shows the main trends in the development of cryptocurrencies from 2009 (Bitcoin) to now. Ripple builds on top of Bitcoin by implementing an algorithm that is not based on blockchain. The main advantage is the high speed of the transactions. Until the creation of Ethereum, blockchain technologies were seen primarily as technologies capable of decentralizing the financial world. Smart contracts enable all industries to create decentralized applications for their specific needs. Proof of this are the Bat and Theta currencies, which are based on Ethereum, but solve the problems of the advertising business and video distribution. ChainLink, on the other hand, adds the ability to create smart contracts that work with data outside of the blockchain.

The analysis performed in this article can be used to develop blockchain-based applications in the transport industry. Such applications could be related to logistics problems, electronic payments and smart contracts between customers and transport companies.

References
[1] Nakamoto S 2008 Bitcoin: A Peer-to-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf
[2] https://litecoin.org/
[3] Schwartz D, Youngs N, Britto A The Ripple Protocol Consensus Algorithm
https://ripple.com/files/ripple_consensus_whitepaper.pdf
[4] Saberhagen N 2013 CryptoNote v 2.0
https://www.allcryptowhitepapers.com/wp-content/uploads/2018/05/monero-whitepaper.pdf
[5] Duffield E, Diaz D 2018 Dash: A Payments-Focused Cryptocurrency
https://github.com/dashpay/dash/wiki/Whitepaper
[6] Buterin V A Next-Generation Smart Contract and Decentralized Application Platform
https://ethereum.org/en/whitepaper/
[7] Szabo N 1994 Smart contracts
http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinter school2006/szabo.best.vwh.net/smart.contracts.html
[8] Mauri L, Cimato S and Damiani E 2018 A comparative analysis of current cryptocurrencies
Proc. of the 4th Int. Conf. on Information Systems Security and Privacy ICISSSP (Funchal, Madeira – Portugal) pp 127–38
[9] Namiot D, Pokusaev O, Kupriyanovsky V and Akimov A 2017 Blockchain applications for transport industry Int. J. of Open Information Technologies 5(12) (In Russian) pp 130-4
[10] Back A 2002 Hashcash – a denial of service counter-measure
http://www.hashcash.org/papers/hashcash.pdf

[11] King S, Nadal S 2012 **PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake**
https://www.chainwhy.com/upload/default/20180619/126a057fe672c286accb372da46955.pdf

[12] https://basicattentiontoken.org/BasicAttentionTokenWhitePaper-4.pdf

[13] https://www.thetatoken.org/

[14] Ellis S, Juels A, Nazarov S 2017 **ChainLink A Decentralized Oracle Network**
https://link.smartcontract.com/whitepaper