Analysis of Blockchain Based Prototype for Electronic Payments

Ion-Costel-Marius Bălțoi
Doctoral School of Economic Informatics
Academy of Economic Studies
Bucharest, Romania

Abstract:- Technological development offers more and more opportunities for people to make electronic payments. From payments via credit / debit cards, then payments via mobile or IoT devices to payments via blockchain technology, they are constantly evolving and becoming simpler, faster, more convenient and more secure. This paper aims to address a number of issues such as the benefits and challenges of payments through blockchain technology. Also, based on the analysis of a developed prototype, the paper will present the sequence of blockchain money transfer operations, the possible states of a transaction, as well as the information that will be processed and stored so that the transfer is successfully completed. The research methodology is qualitative; In this sense, we conducted a research of the resources available at this time and addressing the subject of electronic payments based on blockchain technology and, in parallel, the paper will follow the analysis of the prototype developed so that the results are as objective and consistent with practical use.

Keywords:- *Blockchain, Electronic Payments, Smart Wallet.*

I. INTRODUCTION

With regard to electronic payments, a rapid increase in technology adoption and the transition to a banknote-free economy can be seen worldwide. Thus, Figure 1 shows the rapid growth rate of payments through mobile devices and electronic wallets, at a rate similar to the decrease in the utilization rate of physical money. In the context of the COVID-19 pandemic, the growth rate of the adoption of electronic payments may be accentuated due to the advantages it offers over physical money: ease of use, lack of physical contact with banknotes, shorter payment time, etc.

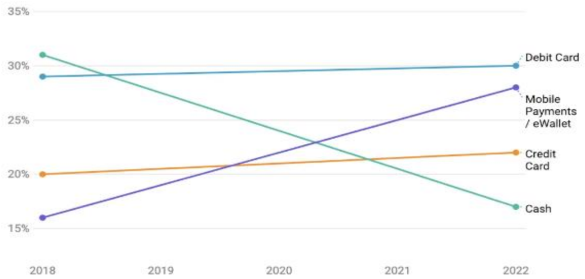

Fig 1:- The evolution of payment types [1]

The purpose of this article is to study electronic payments at the level of a prototype developed in the JAVA language and which aims to simulate money transfer between users. Within the paper, the stages of processing a transaction, the particular structure of a block within the blockchain network, as well as the states of a transaction within the money transfer processing will be analyzed.

According to statistics, electronic payments have had one of the fastest growth in terms of adoption by users. Thus, statistica.com estimates an annual increase of 12.8% between 2017 and 2023 of the total value of digital payment transactions [2].According to Worldpay, the overall utilization rate of mobile payments on POS devices is expected to reach 28% in 2022 [3]. In addition, we can notice the growth rate of electronic payments in China [4]; they had a growth level from 4% in 2012 to 34% in 2018, this evolution being supported by the emergence of digital wallets or payments based on QR code through Alipay or WeChat.

In the financial field, we can identify a series of sectors that can benefit from the advantages offered by blockchain technology:

- Digital payments between state institutions or between individual consumers
- Simplification of capital market operations; for example, real-time trading of financial instruments (shares, bonds, etc.)
- Simplify digital document signing and authentication using smart contracts
- Simplification of asset tracking (financial, real estate, etc.)
- Simplifying market trading by eliminating intermediaries
- Automation of time-consuming and costly processes from a financial or temporal point of view (for example, the purchase of a car or a home
- Fraud investigation and risk data analysis

In blockchain-based payment systems, payment processing would not be possible without the existence of a consensus protocol. This is a set of rules and arrangements that ensure that operations are performed within the blockchain.

The blockchain is a decentralized distributed network that offers immutability, confidentiality, security and transparency. Within this network, there is no central authority present for the validation and verification of transactions, but each transaction in the blockchain is considered fully secured and verified. This is due to the consensus protocol, which is the central part of any blockchain network.

A consensus algorithm is a procedure by which all nodes of the blockchain network reach a common agreement on the status of a distributed record. In this sense, consensus algorithms gain reliability in the blockchain network and establish reliable relationships with other unknown nodes in a distributed computing environment. In short, the consensus protocol provides the assurance that each new block added to the blockchain is the only version agreed between all network nodes.

The consensus protocol in a blockchain network provides security to achieve specific objectives, such as reaching an agreement, collaboration, cooperation, equal rights for each node and the mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims to find a common agreement that is a win-win for the entire network [5].

II. LITERATURE REVIEW

Emerging technologies can be defined as technologies whose development or practical applications are still undiscovered; they are characterized by the high degree of novelty it proposes, the rapid increase of the utilization rate, coherence and obvious impact on society. In the paper [6], emerging technologies are defined as “a radically new and relatively rapidly developing technology, characterized by a degree of coherence that persists over time and with the potential to have a considerable impact on the socio-economic fields that is observed in terms of the composition of actors, institutions and patterns of interactions between them, together with the processes of associated knowledge production. However, its most prominent impact is in the future, so in the emergency phase it is still somewhat uncertain and ambiguous».

The paper [7] performs a series of analyzes on blockchain technology, focusing on the limitations of this technology, differences from current technologies and how the technology will evolve in the future. The paper also analyzes issues that currently represent challenges for the blockchain, such as security, scalability, market regulation or confidentiality of processed data.

The paper [8] presents from a technical point of view a series of particularities regarding the processing of payments through the blockchain network; the analysis is performed based on an electronic wallet application and simulates the management of personal funds. Thus, a series of aspects related to network security, the protocols used, security procedures specific to the electronic wallet, as well as multi-signed transactions are analyzed.

The paper [9] presents the impact that blockchain technology has on the electronic payments industry. The authors present the current context in the payments industry and how the blockchain is innovating in this field. The conclusions of the paper present how the new payment services based on blockchain technology impact cross-border payments and between various currencies, how transactions change the financial structure of companies, the impact and potential of fintech companies on the electronic payments market.

The report [10] made by Fintech Network presents 4 scenarios for the use of blockchain technology by financial institutions; these include fraud reduction (blockchain information is verified at every step of the transaction by independent actors; there is also a real-time verification of every bit of data and all information in a transaction), KYC - Know Your Customer (customer documents can be stored in a blockchain - so, for each new customer, his documents are requested only once, and then stored securely, the risk of them being modified unauthorized is minimal; for institutions that use these documents, there is certainty that these documents have already been independently verified and no further verifications are required), trading platforms (blockchain ensures traceability and history of price developments, providing backup for each item and provides assurance that each element is authentic within a chain, and a toke is generated for each transaction n digital that functions as a virtual certificate and provides the security of the new owner who can check the history of the product in time until its creation); respectively electronic payments (the blockchain can be used for real-time, global and low-cost electronic payments; in the case of electronic payments, there is the problem of interconnection with other existing systems).

III. METHODOLOGY

The present research is based on a qualitative research, following in parallel the study of some existing resources at the moment, as well as the analysis of electronic payments based on technology within a developed prototype.

Regarding the existing resources, a series of diverse scientific resources were analyzed, such as articles published in various journals or presented at conferences or electronic resources published on various networks such as ResearchGate.net and which address the proposed topic for research. The practical part of the paper focuses on the development of a prototype to simulate the money transfer between 2 actors through the blockchain, each actor having available an electronic wallet that offers the possibility of user interface.

IV. THE ADVANTAGES AND CHALLENGES OF BLOCKCHAIN TECHNOLOGY

Blockchain technology has multiple advantages in terms of its use in the financial environment; these include data security (data stored in the blockchain are comprehensive and accurate, can be viewed at any time, are available to authorized users; in case of unauthorized attempts to alter data in a block, the attacker must modify the data on all computers which stores information, simultaneously), the lack of intermediaries in transactions (through blockchain it is possible to communicate directly between the parties involved, without the need for an intermediary - the risk of errors or data alteration is reduced), transparency and immutability (with each change of data stored in the blockchain, all changes are visible to all parties involved, also all transactions are absolute - they cannot be modified or deleted), the speed of transactions (through blockchain, the execution time of transactions has been greatly reduced, transactions can be performed at any time) and low trading costs (lack of intermediaries and associated costs).

Advantages	Challenges
Data security	High energy consumption
Lack of intermediaries in transactions	Lack of regulations on the market
Transparency and immutability	Integration and scalability issues
Fast transactions	Cultural differences
Low trading costs	Lack of technology maturity
	Limited volume and dimensions

Table 1:- Advantages and challenges of blockchain

In practice, blockchain technology faces many challenges in implementing quality solutions that meet the criteria of a reliable application that works smoothly. Thus, its challenges include high energy consumption (real-time record keeping is one of the reasons for high consumption; each creation of a node requires communication with all other nodes), lack of market regulations (no rules available and to be complied with in blockchain-based electronic payment systems; by comparison, traditional electronic payment systems must comply with the rules of central regulators in each country), integration and scalability issues (integration of blockchain technology with current systems requires investment substantial changes in the way data is stored and transferred to new systems, as well as a large number of users, there may be a problem with the high time required to process transactions), cultural differences between people (according to statistics, Asian peoples accept technological innovations much more easily compared to Europeans or Americans), the lack of maturity of the technology (being a new technology, most electronic payment users do not know in detail its capabilities and features) or limited volume and processing size (each block of the blockchain can contain only 1 Mb of data; the blockchain is restricted to processing 7 transactions per second; in comparison, VISA can process up to 56,000 transactions per second [11]).

V. TRANSACTION PROCESSING WITHIN THE PROTOTYPE

A. The stages of the blockchain transaction

Similar to traditional electronic payment systems, transactions in electronic systems based on blockchain technology involve a number of standard steps. Thus, any new transaction, initiated within blockchain-based payment systems, includes the production of another block, each record will be demonstrated and carefully marked to guarantee its legitimacy. Before adding the block to a blockchain, it must be checked by most nodes in the system. The following chart summarizes the steps taken by a transaction in blockchain-based payment systems until the new balances available in the digital wallets involved are completed and updated.

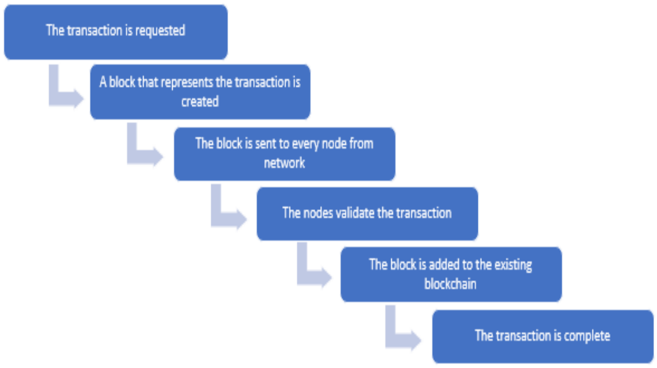
The transaction is requested
A block that represents the transaction is created
The block is sent to every node from network
The nodes validate the transaction
The block is added to the existing blockchain
The transaction is complete

Fig 2:- Stages of blockchain transaction processing

In blockchain-based payment systems, the trigger for a transaction is to send the amount of money to another person, or as payment for a purchased good or service. The next step is to verify the transaction; Depending on the network, the transaction is instantly verified or sent in a queue to verify transactions. In this case, the network nodes (computers or servers) determine whether the transaction is valid based on a set of rules agreed in the network. Each block is uniquely identified by a hash, a 256-bit number, created using a network-supported algorithm, and contains a header, a reference to the past block hash, and a gathering of changes. Inside the blockchain, associating each block to the hash of the past block gives security and chain coherence.

In the third stage, the block is validated to be added to the blockchain. The most common forms of validation for blockchain are based on the concept of "proof of work". Proof of work is one of the consensus mechanisms for a blockchain agreement to confirm transactions and add new blocks to the blockchain [12]. Based on this concept, miners compete with each other to validate transactions, and based on them they will be rewarded. The probability of being selected to build the next block is related to the computing power.

Blockchain mining involves adding transactions to the existing blockchain registry of transactions distributed among all users on the network. This process involves creating a hash of a block of transactions that cannot be easily falsified and that will protect the integrity of the entire blockchain, without the need for a central system.

The mining process takes place on a dedicated computer, requiring a fast processor, but also a high power consumption and more heat is generated than in regular computer use. The main incentive for users participating in the mining process is related to the reward offered; thus, in the case of bitcoin, this is 25 bitcoins for each hash [13].

After each node in the network adds the new node to the blockchain, it will still have immutability properties and can be checked for security. If an attack is detected by a miner trying to send an altered block to the blockchain, the hash function of that block and all subsequent ones would be changed. The other nodes can detect these changes and remove that block from the chain, preventing blockchain corruption.

B. The structure of the blocks within the prototype

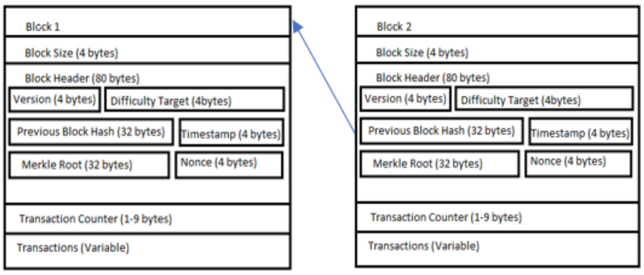

Fig 3:- The structure of the blocks

Blockchain structures comprise a series of chained blocks, each block storing the hash corresponding to the previous block. Each block comprises a series of distinct elements that can be categorized into 2 parts: block header and the body of the block (records of existing transactions in the block).

The block header contains a fixed reserved space of 80 bytes in memory and includes information such as block version, difficulty, previous block hash value, time stamp, Merkle Root and nonce, each of these elements having a specific role in the proper functioning and interconnection of blocks :

- The block version is stored on 4 bytes and stores the version number of the blockchain system;
- The difficulty represents an integer stored on 4 bytes and represents the value of the targeted difficulty within the solution of the proof of work algorithm;
- The hash of the previous block represents a value stored on 32 bytes and records the hash value of the block from which the current block is chained. As I mentioned earlier, a blockchain is a sequence of blocks. According to the principle of operation, the new blocks are added to the continuation of the old blocks, and the higher the chaining of the blocks, the more difficult it will be to change the hash value of the blocks generated earlier;
- Timestamp saves the time at which the block was generated (year, month, day, hour, seconds);
- Merkle Root is the hash of all hashes of transactions that are part of a blockchain network; it plays a role in coding data in the blockchain in an efficient way and allows the rapid verification of data, as well as the manipulation of large amounts of data from one node to another node in the network.
- Nonce the solution of the proof of work algorithm for the current block.

In particular, in the case of blockchain-based payment systems, the blockchain may retain information on transactions processed at a given time. Thus, information of the senders or recipients of transactions (name, surname, balance, currency, etc.) as well as information related to payment (amount, currency, date of processing, etc.) may be retained.

C. Possible transaction states

During the processing within the system, the transaction can have different states, these being highlighted in Figure 4:

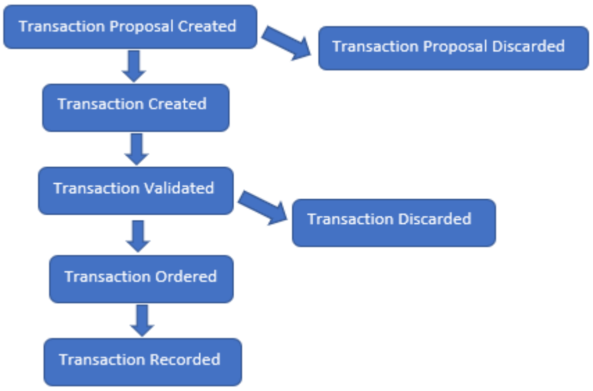

Fig 4:- Possible transaction states

In the first stage, the transaction will be created by the client application, and will be sent for processing if the verifications are successfully completed; otherwise, the transaction will be abandoned. After verifying the signature of the initiator, the transaction is proposed for validation, its inclusion in a block and transmission for processing. In case of a transaction validation error, it will be deleted. Upon receipt of the transaction, the nodes verify the integrity of the data and ensure its inclusion in a new block sent for processing; if the data has been changed, the transaction will be marked as Invalid. After registering the block in the blockchain, the transaction will be completed successfully.

Figure 5 shows the flow that is traversed in the case of a transaction from a user A to a user B. To perform the transaction, the information about the public key (address) of the sender, the public key of the recipient, the value and currency of the transaction are required. , as well as a cryptographic signature (this has the role of verifying the owner of the transaction and that the data has not been changed). In the above case, the transaction will be signed by sender A with the private key and no user on the network will be able to send money on behalf of user A without knowing the private key; therefore, the private key must be secret. The public key will also be sent to you during the transaction and can be used to verify the signature and not alter the data.

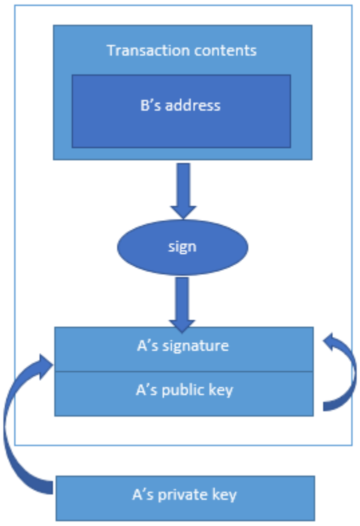

Fig 5:- Performing the transaction

VI. CONCLUSIONS

At the moment, we notice that blockchain technology offers us a lot of opportunities in diversified fields. Particularly for the field of electronic payments, blockchain technology offers us support for various operations such as the transfer of monetary value. We can consider the blockchain as a technology with a great potential for future growth due to research and new technologies that help its implementation on a large scale.

Regarding the advantages of this technology, we can list the increased security, the lack of intermediaries of transactions, transparency and immutability or fast and low cost transactions. In addition to these advantages, the technology also presents a series of challenges at the moment, but with great possibilities for improvement; among these we can list the high energy consumption, the lack of regulations in the market and diversified cultural specifics in the world, problems of integration with other systems and scalability or limited volume of transactions that can be processed in a short time.

Mobile applications for processing electronic payments through blockchain follow a set of steps so that transactions are carried out in complete safety. Distinctly, in the paper we presented the flow of a payment, starting with the initialization of a payment by a user, creating the block containing the transaction data, sending it to all nodes in the network, validating the transaction and adding the block to the blockchain network.

Within each block that is sent for validation in the system, it is essential to analyze its structure so that the data is processed correctly within the prototype. Thus, the block is structured in 2 main parts, the block header (version, difficulty, hash of the previous block, nonce, Merkle Root, timestamp) and the block body (which contains the transaction records that will be processed by the application).

Therefore, the present paper analyzes the states followed by a transaction, starting from the moment of initialization (created transaction), continuing with validated or ordered transaction and until the moment of registration of the transaction. Various processing errors may occur and the transaction may be discarded.

Regarding future research, I propose to analyze the impact that blockchain-based electronic payment processing computer systems have on end users (their degree of trust, availability of use or satisfaction with these applications).

ACKNOWLEDGEMENTS

This paper was co-financed from the Human Capital Operational Program 2014-2020, project number POCU / 380/6/13/125245 no. 36482 / 23.05.2019 "Excellence in interdisciplinary PhD and post-PhD research, career alternatives through entrepreneurial initiative (EXCIA)", coordinator The Bucharest University of Economic Studies.

REFERENCES

[1]. MerchantSavy, "Global Mobile eCommerce Statistics, Trends & Forecasts," February 2020. [Online]. Available: https://www.merchantsavvy.co.uk/mobile-ecommerce-statistics/. [Accessed 20 May 2020].

[2]. Statista.com, "Digital Payments," [Online]. Available: https://www.statista.com/outlook/296/100/digital-payments/worldwide#market-revenue. [Accessed 21 May 2020].

[3]. S. Vanthomme, "12 Global Payment Statistics Impacting Small & Mid-size Businesses," 18 February 2020. [Online]. Available: https://www.ccv.eu/2020/12-global-payment-statistics-impacting-small-mid-size-businesses/. [Accessed 21 May 2020].

[4]. S. Bansal, P. Bruno, O. Denecker and M. Niederkorn, "Global payments: Expansive growth, targeted opportunities," 21 Octomber 2018. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-expansive-growth-targeted-opportunities. [Accessed 21 May 2020].

[5]. GeeksforGeeks, "Consensus Algorithms in Blockchain," GeeksforGeeks, Noida.

[6]. D. Rotolo, D. Hicks and B. Martin, "What Is an Emerging Technology?," Research Policy, p. 44, 2015.

[7]. S. Fernandez-Vazquez, R. Rosillo, D. De La Fuente and P. Priore, "Blockchain in FinTech: A Mapping Study," MDPI, Basel, 2019.

[8]. E. Gunasena, "Peer-to-peer payment system and crypto-currency using blockchain technology with a secure wallet and multi-signature transactions," 2019.

[9]. F. Holotiuk, J. Moormann and F. Pisani, "The Impact of Blockchain Technology on Business Models in the Payments Industry," in International Conference on Wirtschaftsinformatik, St. Gallen, 2017.

[10]. Fintech Network, "Four Blockchain Use Cases for Banks," Fintech Network, 2018.

[11]. Consultancy.uk, "Blockchain Technology: How it works, main advantages and challenges," Consultancy.uk, 25 May 2017. [Online]. Available: https://www.consultancy.uk/news/13484/blockchain-technology-how-it-works-main-advantages-and-challenges. [Accessed 15 May 2020].

[12]. Ledger SAS, "What is Proof-of-Work," Ledger SAS, 23 Octomber 2019. [Online]. Available: https://www.ledger.com/academy/blockchain/what-is-proof-of-work. [Accessed 15 May 2020].

[13]. Techopedia, "Mining," Techopedia, [Online]. Available: https://www.techopedia.com/definition/32530/mining-blockchain. [Accessed 15 May 2020].