International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

BLOCK-CHAIN TECHNOLOGY IN CRYPTOCURRENCY (IOT)

DONE BY:

V.BALUSAMY,R.BALAVIGNESH,M

.BHAVADHARANI,M.DHANUSRI

ABSTRACT

Blockchain technology is a decentralized and secure ledger system that has gained immense popularity in the world of cryptocurrency. It allows for transparent and tamper-proof transactions, which has led to the development of numerous cryptocurrencies such as Bitcoin, Ethereum, and others. This paper aims to provide a comprehensive overview of the concepts and applications of blockchain technology in cryptocurrency. It will cover the underlying principles of blockchain, the structure of a blockchain network, the role of mining and consensus algorithms, and the current and future trends in the world of cryptocurrency. The paper will also discuss the benefits and challenges of using blockchain technology in the financial sector, including security, scalability, and regulatory issues. The objective of this paper is to provide an in-depth understanding of blockchain technology and its role in the rapidly evolving world of cryptocurrency.Overall, blockchain technology has the potential to disrupt various industries beyond finance, such as supply chain management, voting systems, and even identity management. Its secure and transparent nature makes it an ideal solution for many applications and its adoption is rapidly growing.

Introduction

Currency transactions between persons or companies are often centralized and controlled by athird party organization. Making a digital payment or currency transfer requires a bank orcredit card provider as a middleman to complete the transaction.In addition, a transactioncauses a fee from a bank or a credit card company. The same process applies also in severalother domains, such as games, music, software etc. The transaction system is typically central_ized, and all data and information are controlled and managed by a third party organization,rather than the two principal entities involved in the transaction.Among the various possible solutions, one of the most promising are blockchain-based online social networks (BOSN), which put themselves forward associal platforms able to over-come all current issues of centralized social networks. Actually, three specific aspects, commonto most of the current BOSNs, are: a decentralization based on blockchain technologies that mitigate data privacy and censorship problems, typical of centralized platforms (a few blockchains online social networks combine blockchain decentralization and tokenization to replace sensitive and/or personal data or have introduced self custody wallets to keep data pri- vate; nevertheless, the immutability and transparency of blockchains still pose data privacy issues since transaction history of digital wallets can be completely reconstructed); a token sys- tem based on proprietary cryptocurrency used for fostering high-quality content; and a rewarding system for distributing the wealth of the platform giving data monetization back to users and encouraging good practices.

Despite having been around for a few years, we are very far from having fully understood to what extent BOSN paradigm solves the issues of traditional architectures and what are, if exist, the other problems they potentially introduce.
The true pivot of BOSN is the introduction of a cryptocurrency that shifts the paradigm ofonline social network from being purely social to economic-social: in the traditional approach,users are engaged with social interactions, while economic ones are prerogative of platform ownership; while in BOSN users are got dragged into social-economic actions. Thus, the wayto understand the BOSN in-depth passes through the investigation of the relations between the economic and social actions carried out by users and how both relate to the value of the cryptocurrency.
To shed a light on this complex network of intertwined layers, we adopt a data-driven approach, by analyzing Steemit, one of the first and most successful BOSNs. By gathering data from the underlying blockchain Steem, we have collected a large longitudinal dataset that con- tains the main social and financial activities of Steemit users spanning more than three years,along with data external to the Steemit platform: longitudinal data of STEEM value in the cryp-tocurrency market. From these data we were able to reconstruct the high-resolution evolution of the system to address the main goal of our study: the interplay

between users' social and financial activities, resulting in social and
economic networks, and the currency price; with a specific focus on the possible effects of the currency price on the network structure. Asfor this latter aspect, our analysis based on time series correlation has pointed out a possible influence of the platform cryptocurrency on the evolution of the Steemitsocial network, i.e. "follow" or link creation actions have been partly driven by the trend of the cryptocurrency. Higher prices have attracted more users and shifted the mechanisms and the strategies ruling link creation. Strategies and action allocation, especially for the most central nodes, are a further focus of ourstudy. In particular, we highlighted which actions central nodes have mainly chosen to gain the highest cumulative rewards. Here, we observe that central nodes exploit both their high rank in the voting system and the mechanism of the rewarding system to get rewards, i.e. they tend to prefer voting operations to actions for producing content (posting and commenting).

The above findings suggest that the transformation of the actual online social platforms— which in the last years have shaped and are still changing our society—into new paradigms supported by blockchain technologies ask for new perspectives for the study of their evolution. Indeed, economic and financial aspects might play a more decisive role in how people behave in these new platforms, enough to question the relational aspects, typical of the main online social networks.

Background on blockchain-based online social networks: Thecase of Steemit

Blockchain-based online social networks (BOSNs) are an emerging application of blockchain-supported technologies and present some novel and interesting characteristics which link eco- nomical aspects to online social behaviors. In this section, we introduce the architecture and the fundamental elements of BOSNs, using Steemit as a case study. We focus on Steemit as ithas been one of the first and most successful platforms in the blockchain-based online social network ecosystem; and it has introduced most of the fundamental mechanisms which charac-terize modern BOSNs. In particular, we focus on two specific aspects, common to most of the current BOSNs: a) a token system based on proprietary cryptocurrency used both for fosteringhigh-quality content and users, and supporting the validation of all social and economic actions; and b) a rewarding system for distributing the wealth of the platform.

Launched in 2016, the platform supports the creation and sharing of content, as well as a social network based on "follow" relationships. In Steemit, users create original blog posts, thatcan be shared or upvoted/downvoted by other users. Users can be *creators*—content produc ers—or *curator*s—content promoters. The promotion and evaluation of content are made through social actions, such as upvoting (e.g. Facebook's like, Twitter's heart button), down- voting (dislike), and sharing. The role of a user towards content determines how rewards are distributed. In fact, all these actions not only increase the visibility of posts but also have an economic impact. But, unlike other popular online social networks, the economic impact of these actions is explicit and measurable through the amount of gained tokens. In fact, at the end of a 7-day period, the most popular posts are awarded through cryptocurrency tokens, and both creators and curators of the most liked posts get a share of this reward. These mecha- nisms are inspired by the attention economy and token economy principles [2]. Indeed, active users have a financial incentive for their participation, asthey are rewarded for their contribu- tions to the platform. Rewards are distributed in the form of cryptocurrency, which can be traded among users and can be exchanged for traditional currencies like the US Dollars— USD. This way the economic value of posts and users is easily quantifiable and publicly avail-able. Thislast point constitutes the pivotal link between the socio-economic dynamicsinternalto the platform and the external financial ones, first of all, the trend of the cryptocurrency market.

The token system

The rewarding system, the importance—influence—of the users, and the inter/intra financial relations are mainly based on the cryptocurrency system of Steemit, which includes three dif- ferent tokens, each with a specific purpose a) STEEM (Capitalized to avoid confusion withthe Steem blockchain); b) Steem Dollar—(SBD); and c) Steem Power—SP.

A summary representation of the token system , reporting the possibleconversion methods as well.

The first token, STEEM, is the liquid cryptocurrency at the base of the token system. This token can be exchanged by users as a form of payment and it is tradable on different exchangeswith other cryptocurrencies or more traditional currencies like US dollars. These characteris-tics cause the STEEM value to fluctuate. This is a key point of this study which has precisely the purpose of investigating how such fluctuations affect the usage of social actions, and, con- sequently, the structure of the social network. Moreover, all other tokens derive their value from the STEEM price.

Tokens and conversion operations. Main currencies (rounded rectangles) in Steemit and possible conversion operations, are depicted as arrows. For each conversion or exchange operation, we report the type of the operation and temporal constraints, when available. In fact, many operations are instantaneous, while some others require more days.

Background

Blockchain, mostly known as the technology running the Bitcoin cryptocurrency, is a publicledgersystem maintaining the integrity of transaction data . Blockchain technologywas firstused when the Bitcoin cryptocurrencywas introduced. To this day, Bitcoin is still the mostcommonly used application using Blockchain technology .Bitcoin is a decentralized digitalcurrency payment system that consists of a public transaction ledger called Blockchain . Theessential feature of Bitcoin is the maintainability of the value of the currencywithout any orga_nization or governmental administration in control. The number of transfers and users in theBitcoin network is constantly increasing . In addition, the conversions with traditional cur_rencies, e.g. KRW, EUR and USD, occur constantly in currency exchange markets . Bit_coin has therefore gained the attention of various communities and is currently the mostsuccessful digital currency using Blockchain technology Bitcoin uses the public key infrastructure (PKI) mechanism . In PKI, the user has one pair of public and private keys. The public key is used in the address of the user Bitcoin wallet,and the private key is for the authentication of the user. The transaction of Bitcoin consists ofthe public key of the sender, multiple public keys of the receiver, and the value transferred. In about ten minutes, the transaction will be written in a block. This new block is then linked to a previously written block. All blocks, including information about every transaction made, arestored in the disk storage of the users, called nodes. All the nodes store information about allrecorded transactions of the Bitcoin network and check the correctness of each new transactionmade by using previous blocks. The nodes are rewarded by checking the correctness of transac_tions. This method is called mining, and it is confirmedwith Proof-of-Work, which is one of the main concepts of Blockchain technology. When all transactions are successfully confirmed,a consensus exists between all the nodes. The new blocks are linked to previous blocks and allthe blocks are aligned in one continuous chain. This chain of blocks is the public ledgertech_nique of Bitcoin, called Blockchain.Blockchain is the decentralized managing technique of Bitcoin, designed for issuing andtransferring money for the users of the Bitcoin currency. This technique can support the publicledger of all Bitcoin transactions that have ever been executed, without any control of a thirdparty organization . The advantage of Blockchain is that the public ledger cannot be modi_fied or deleted after the data has been approved by all nodes. This is
why Blockchain is well_known of its data integrity and security characteristics. Blockchain technology can also be applied to other types of uses. It can for example create an environment for digital contractsand peer-to-peer data sharing in a cloud service . The strong point of Blockchain technique,data integrity, is the reason why its use extends also to other services and applications.Blockchain technology has also some technical challenges and limitations that have beenidentified. Swan presents seven technical challenges and limitations for the adaptation of

Blockchain technology in the future:

• Throughput: The potential throughput of issues in the Bitcoin network is currently maxi_mized to 7tps (transactions per second). Other transaction processing networks are VISA(2,000tps) and Twitter (5,000tps). When the frequency of transactions in Blockchainincreases to similar levels, the throughput of the Blockchain network needs to be improved.

• Latency:To create sufficientsecurity for a Bitcoin transaction block, it takes currentlyroughly 10 minutes to complete one transaction. To achieve efficiency in security, more timehas to be spent on a block, because it has to outweigh the cost of double spending attacks.Double-spending is the result of successfulspending of money more than once . Bitcoin protects against double spending by verifying each transaction added to the block chain, to ensure that the

inputs for the transaction have not been spent previously .This makes latency a big issue in Blockchain currently. Making a block and confirming the transaction should happen in seconds, while maintaining security. To complete a transaction e.g. inVISA takes only a few seconds, which is a huge advantage compared to Blockchain.• Size and bandwidth:At the moment, the size of a Blockchain in the Bitcoin network is over50,000MB (February 2016). When the throughput increasesto the levels of VISA, Blockchaincould grow 214PB in each year. The Bitcoin community assumes that the size of one block is1MB, and a block is created every ten minutes . Therefore, there is a limitation in the num_ber of transactionsthat can be handled (on average 500 transaction in one block) . If the

Blockchain needsto control more transactions, the size and bandwidth issues have to be solved.

• Security:The current Blockchain has a possibility of a 51% attack. In a 51% attack a singleentity would have full control of the majority of the network's mining hash-rate and would be able to manipulate Blockchain. To overcome this issue, more research on security isnecessary.

• Wasted resources: Mining Bitcoin wastes huge amounts of energy ($15million/day). Thewaste in Bitcoin is caused by the Proof-of-Work effort. There are some alternatives in indus_try fields,such as proof-of-stake. With Proof-of-Work, the probability of mining a blockdepends on the work done by the miner . However, in Proof-of-Stake, the resource thatis compared is the amount of Bitcoin a miner holds . For example, someone holding 1%of the Bitcoin can mine 1% of the "Proof-of-Stake blocks" . The issue with wastedresources needsto be solved to have more efficient mining in Blockchain.

• Usability: The Bitcoin API for developing servicesis difficult to use. There is a need todevelop a more developer-friendlyAPI for Blockchain. This could resemble REST APIs.

• Versioning, hard forks, multiple chains: A small chain that consists of a small number ofnodes has a higher possibility of a 51% attack. Another issue emerges when chains are split for administrative or versioning purposes.

Overall, Blockchain as a technology has the potential to change the way how transactions are conducted in everyday life. In addition, the applications of Blockchain are not limited to cryptocurrencies,but the technology could be possibly applied in various environments where some forms of transactions are done. The research on the possibilities of Blockchain in applica_tions is certainly an interesting area for future research, but at the moment Blockchain suffers from technical limitations and challenges. Anonymity, data integrity and security attributes set a lot of interesting challenges and questions that need to be solved and assessed with high qual_ity research. Scalability is also an issue that needs to be solved for
future needs. Therefore, to identify and understand the current status of research conducted on Blockchain, it is important to gather all relevant research. It is then possible to evaluate what challenges and questions have been tackled and answered, and what are the most problematic issues in Blockchain at the moment

References

1. Guidi B. When Blockchain meets Online Social Networks. Pervasive and Mobile Computing. 2020; 62:101131. https://doi.org/10.1016/j.pmcj.2020.101131

2. Davenport TH, Beck JC. The Attention Economy. Ubiquity. 2001; 2001(May). https://doi.org/10.1145/376625.376626

3. Steemit Whitepaper;. Available from: https://steem.com/steem-whitepaper.pdf.

4. Steemit BluePaper;. Available from: https://steem.com/steem-bluepaper.pdf.

5. Maesa DDF, Marino A, Ricci L. Data-driven analysis of Bitcoin properties: exploiting the users graph. International Journal of Data Science and Analytics. 2018; 6(1):63–80. https://doi.org/10.1007/s41060-017-0074-x

6. Maesa DDF, Marino A, Ricci L. The bow tie structure of the bitcoin users graph. Applied Network Sci ence. 2019; 4(1):56.