ISSUES AND CHALLENGES IN BLOCKCHAIN TECHNOLOGY

[1]*Nefeesath Laseedha,* [2]*Befathumma,* [3]*Aysha Suha, Mustafa Basthikodi*
Dept.of CSE, Bearys institute of Technology, Mangalore, India

Abstract- **When the whitepaper Bitcoin was released by Satoshi Nakomoto in 2008 describing a "purely peer-to-peer version of electronic cash" known as Bitcoin, Blockchain technology made its public debut. Blockchain has since been considered an emerging technology for the sharing of decentralized and transactional data across a large network of untrusted participants. It allows new forms of distributed software architectures where it is possible to reach agreement on shared states without trusting a central point of integration. It allows the creation of a decentralized environment where no third party organization controls the transaction and data. Any transaction that has ever been completed will be recorded with a time stamp and other details in a public ledger in a verifiable, secure, transparent and permanent manner. For these features blockchain developed into one of today's largest groundbreaking technologies with potential to impact every industry from financial to manufacturing to educational institutions. Blockchain technology has already changed the lifestyle of people in some areas in recent years due to its great influence on many businesses or industries, and what it can do will continue to cause impact in many places. While Blockchain technology features may bring us more reliable and convenient services, the security issues and challenges behind this innovative technique are also an important topic that we need to be concerned about.**

Keywords—Proof-of-work; Bitcoin; Smart contracts.

INTRODUCTION

Blockchain as a decentralized and distributed technology can play a key role in providing such healthcare services. The Bitcoin [1], which is the first and most popular cryptocurrency, has been receiving a lot of attention and the importance of academic research on Bitcoin is continuing to grow [2]. One of its technical features is that it enables reliable transactions without a centralized management mechanism even if there are unreliable participants in the network, and this feature is obtained by the invention of blockchain technology. The structure of a blockchain is that a block that consists of multiple transactions is connected with a previous block in chain-like form. To ensure reliability, when a new block is generated and added to the previous block, a little special process of solving a computationally heavy puzzle, called a proof-of-work puzzle, is needed and this puzzle is solved competitively by the participants. (The generating of blocks is called mining and the participants are called miners.)

In a report published at the Worlds Economic Forum in September 2015, 58% of survey respondents said they expected blockchain technology to store 10% of their global gross domestic product by 2015[1]. Therefore, it is not amazing that blockchain attracts investor throngs who invest heavily in start-ups[2]. The 2015 trend has been raising to nearly half a billion dollars.

In the document Nakamoto specifically addresses the challenge of digital currency ownership and proposes the blockchain solution prior to transactions. The functional principle of blockchain can be explained using the concept of blockchain. Blockchai has been originally developed to the cryptocurrency bitcoin and was first described in Satoshi Nakamoto's whitebook in 2008.

If a Bitcoin transaction is for instance made from user A to user B, this information is simultaneously shared with all other users of the bitcoin blockchain. The information on a bitcoin transaction(for example, the transferred sum, owner, etc.) is combined in a time-stamp information block and added to the existing blockchain[4] [5].

In other words, the bitcoin proprietary solution published by Satoshi Nakamoto; othermore in consolidating all the information necessary in a single database which was then distributed to the general public. A database which does no claim ownership of the data and which all owns at the same time [4] [5].

Ethereum is a project which attempts to build the generalised technology; technology on which all transaction-based state machine concepts may be built. Moreover it aims to provide to the end-developer a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream: a trustful object messaging compute framework.

Ethereum is based on the concept of so called smart contracts. A contract is usually a piece of code that is stored on the blockchain. It is executed by a users via sending a transaction to the contract, the code is controlling. The terminology contract suggests that an Ethereum contract is the same as a legal contract which is clearly not the case. Contracts in Ethereum are not limited to financial workflows and are much more generic. Because of that contracts are also often refered as agents or objects: Externally owned account and contract accounts. A externally owned account is controlled by a private key and owned by a real human being. This is the equivalent to a Bitcoin account. Contract accounts however are controlled entirely by code. Accounts consist of four main fields: Nonce, Ether balance, Contract code and Account storage.

As in Bitcoin every transaction: has a recipient, has to be signed by the sender and contains a field where the user can specify the amount of money he wants to transfer. The fields GasLimit and GasPrice are unique to Ethereum[6]. If an externally controlled account submits a transaction with a contract account as the recipient the transaction triggers the execution of the code of the targeted contract account that which usually alters the state of the accounts.

If a transaction is sent from an externally controlled account to another externally controlled account, this transaction is no different from a transaction made in Bitcoin and is used to transfer Ether from one external account to another external account. If a contract account sends a transaction to another contract account, the contract code of the recipient is executed. Such a transaction is called a message and can be seen as a simple function call between objects[7]. The ability of contracts to send messages to other accounts not only allows the creator of a decentralized application to split up its application into multiple contracts but furthermore makes interaction between different applications possible.

Hyperledger is a multi project, open source collaborative effort created to advance cross-industry blockchain technologies. Hyperledger fabric is one of the blockchain project within hyperledger. Like other blockchain technologies it as a ledger, uses smart contract, and is a system by which participants manage their transactions. This project is one of the present uses of the research network which involves Accenture, IBM, Bloomerg and block stream.

ISSUES AND CHALLENGES

Some of the issues and challenges are:

Complexity: Blockchain technology involves an entirely new vocabulary. It has made cryptography more mainstream, but the highly specialized industry is chock-full of jargon[8].

Network size: Blockchain are not so much resistent to bad actors as they are ‘antifragile’- that is, they respond to attacks and grow stronger. This requires a large network of users, however. If a blockchain is not robust network with a widely distributed grid of nodes , it becomes more difficult to reap the full benefit.

Transaction cost, network speed: Bitcoin currently has a notable transaction costs after being touted as ‘near free’ for the first few years of its existence. As of late 2016, it can only process about seven transactions per second, and each transaction costs about $0.20 and can only store 80 bytes of data.

Human error: If a blockchain is used as a database, the information going into the database needs to be of high quality. The data stored on blockchain is not inherently trustworthy, so events need to be recorded accurately in the first place. The phrase ‘garbage in, garbage out’ holds true in a blockchain system of record, just as with a centralized database.

Unavoidable security flaw: There is one notable security flaw in Bitcoin and other blockchains: if more than half of the computers working as nodes to service the network tell a lie, the lie will become

the truth. This is called a '51% attack' and was highlighted by Satoshi Nakamoto when he launched Bitcoin. For this reason, Bitcoin mining pools are monitored closely by the community, ensuring no one unknowingly gains such network influence.

Politics: Because blockchain protocols offer an opportunity to digitize governance models, and because miners are essentially forming another type of incentives governance model, there have been ample opportunities for public disagreements between different community sectors. These disagreements are a notable feature of the blockchain industry and are expressed most clearly around the question or event of 'forking' a blockchain, a process that involves updating the blockchains users have agreed to it.

CONCLUSION

Bitcoin, Ethereum and hyperledger we discussed probably the three most prominent state of the art representers of the blockchain technology. We saw that in recent years, people started to move away from building only economic systems on top of the blockchain. In times of a quite centralized Word Wide Web (Facebook, Google, Amazon etc.) this development seems quite refreshing. If successful, decentralzied block chain applications could play a major role in the redemocratisation of the internet, by shifting the power from the big players back to the users. On the other hand this field is still pretty young, prone to problems and seemingly quite far away from being able to replace the big players. Only time will tell how this battle turns out. Compared to Bitcoin and ethereum, hyperledger is best one. Hyperledger is permissioned network thus they are secure compared to the other two. The transaction is public and confidential therefore, privacy is maintained in the transactions.

REFERENCES

[1] J.R. Douceur. "The sybil attack," International workshop on peer-topeer systems. Springer, Berlin, Heidelberg, 2002 [2] S.Nakamoto. "Bitcoin: A peer-to-peer electronic cash system," 2008

[3] A. Back. "Hashcash-a denial of service counter-measure," 2002

[4] Blockchain.com. URL: https://www.blockchain.com/ko/charts/blockssize , Accessed 2018-06-30

[5] BitInfoCharts. URL: https://bitinfocharts.com/ethereum/, Accessed 2018-06-30 [6] G.Jeff. "Block size increase to 2MB," URL: https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki, Github Repository, Accessed 2018-06-30, 2015

[7] Bitcoin Unlimited. URL: https://www.bitcoinunlimited.info/, Website, Accessed 2018-06-30

[8] L.Johnson. "Merkelized Abstract Syntax Tree," URL: https://github.com/bitcoin/bips/blob/master/bip-0114.mediawiki, Github Repository, Accessed 2018-06-30, 2016

[9] G.Becker. "Merkle signature schemes, merkle trees and their cryptanalysis," Ruhr-University Bochum, Tech. Rep, 2008

[10] T.Kuhn, and O.Thomann. "Abstract syntax tree," Eclipse Corner Articles 20, 2006

[11] L.Eric, L.Johnson, and W.Pieter. "Segregated Witness," URL: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki, Github Repository, Accessed 2018-06-30, 2015

[12] W.Pieter. "Dealing with malleability," URL: https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki, Github Repository, Accessed 2018-06-30, 2014

[13] Bitcoincore, "Segregated Witness Benefits," URL: https://bitcoincore.org/en/2016/01/26/segwit-benefits/#linear-scalingof-sighash-operations, Website, Accessed 2018-06-30. [14] C.P.Schnorr. "Efficient signature generation by smart cards," Journal of cryptology 4.3: 161-174, 1991

[15] N.Szabo. "The idea of smart contracts," Nick Szabo's Papers and Concise Tutorials 6, 1997