Framework for Using BigchainDB in Software Application

Avni Rustemi
Faculty of Electrical Engineering and Information Technology (FEIT)
Ss. Cyril and Methodius University in Skopje
Skopje, North Macedonia

Vladimir Atanasovski
Faculty of Electrical Engineering and Information Technology (FEIT)
Ss. Cyril and Methodius University in Skopje
Skopje, North Macedonia

Aleksandar Risteski
Faculty of Electrical Engineering and Information Technology (FEIT)
Ss. Cyril and Methodius University in Skopje
Skopje, North Macedonia

***Abstract*—Recently, cryptocurrencies have become very important, as people are investing a lot of money in them, and people slowly are entering in virtual world where physical money is getting lost and all trade is being done with cryptocurrencies which we neither see nor touch, respectively they don't exist in the form of money as we are accustomed to. Cryptocurrencies are numerous and their values change day by day depending on the interest of people investing in them. In this paper we will present some of the most used cryptocurrencies and their purchase, the energy that these cryptocurrencies consume during the execution of transactions, taking as an example Ethereum. It will be given our models of how the process of cryptocurrency transactions is executed, taking also as an example Ethereum network, We will talk about the future of cryptocurrencies, architecture and data security etc. Our main focus will be on BigchainDB and the possibility of implementing the same by developers, and in particular we will provide a framework on how BigchainDB can be implemented by developers, to create their own software applications and to see in the future the possibility of how the same can be implemented in practice. Our main goal through this paper is to break the taboos of databases that we are used to working with when creating software applications, and introduce as a challenge for us the use of a new database which is less used by developers, but which is more secure, ie. BigchainDB . And the framework that we will present will be as a reference point for researchers on how BigchainDB can be used in their applications.**

Keywords—ethereum network, mining, purchase, energy consumption, architecture, data security, BigchainDB, framework.

I. Introduction

Thanks to technological developments that have caused industrial revolution, on one side, people's lives are being facilitated in many areas, but on the other side, people are doing their best to invest as much as possible in the advancement of these technologies, always based on the fact that every technological change that happens is like consequence of previous changes. Blockchain technology is one of the main topics of most people today and based on the application of the same and the interest of the people in it, it is thought to be among the biggest technological revolutions after the internet, causing major changes in the global economy. Although it is a profitable technology and people are investing a lot of money in it, in many aspects still remains an unsolved mystery as to who invented and who administers such a complex system with delicate operating structure. It was very difficult to gain people's trust in this technology, as it was thought not to be a fraudulent system aimed only at collecting money from people and ultimately failing like many fraudulent systems they had faced and are facing even nowadays. What was even more interesting and more difficult to gain people's trust was the fact that people are used to do business with money, either through physical contact or through banking transactions, but in this technology, transactions are performed only through cryptocurrencies that you need to buy in advance and the same change their value depending on the investment of people in them. Blockchain technology is a decentralized technology, which if we compare it with the way it works, to have it simpler, it resembles Google Doc, where all people can access the document at the same time, but cannot copy or transfer it to others. This creates a decentralized distribution chain that gives everyone access to the document at the same time. And this is where the essence of blockchain functionality lies, where everyone can see the blocks, access them but never modify or get the same. This creates a centralized system of operation of this technology. Every time someone performs a transaction, they go online and computer algorithms determine the authenticity of the transaction. Once the transaction is verified, this new transaction is linked to the previous transaction thus forming a chain of transactions. Blockchain technology rather encourages the redistribution and decentralization of power across wide communities of peers interacting with one another. And therefore, eliminates fraudulence or any chances of corruption entertained by mediators, consequently from time to time proving itself to be a philanthropist technology [1].

II. Cryptocurrencies and Their Purchase

Bitcoin, Ethereum, Tether, BNB, and several other cryptocurrencies seem to experience a large-scale growth in price, market capitalization and widespread public acceptance. The cryptocurrencies tend to offer a lot of features and functions that are altering the way we do and implement things. Cryptocurrencies are undoubtedly extremely intervening the global economy. Even though most investments are made in relatively established cryptocurrencies, including Bitcoin (BTC) and Ethereum (ETH), there are thousands of other smaller cryptocurrencies. These currencies are prime targets for manipulation by scammers, as evidenced by the proliferation of pump and dump schemes. Pump and dump schemes are those in which a security price inflates due to deliberately deceptive activities. Those fraudulent schemes originated in the early days of the stock market and are now growing rapidly in the cryptocurrency market [2]. Market capitalization of the crypto asset is calculated by multiplying the existing reference price of the crypto asset by the current circulating supply. The price for each individual market pair is calculated by taking the unconverted price reported directly from the exchange and converting it to USD using CoinMarketCap's existing reference prices [3].

TABLE I. PURCHASE OF CRYPTOCURRENCIES

Coin	Price($)	Market cap($)	Main Markets
BTC	39,177	742 billion	Binance, Coinbase Pro, OKEx, Kraken, Huobi Global, Bitfinex
ETH	2,589	310 billion	Binance, Coinbase Pro ,OKEx ,KrakenHuobi Global
USDT	1.00	80 billion	Binance, OKEx, HitBTC, Huobi Global
BNB	378.08	62 billion	FTX
USDC	1.00	52 billion	Poloniex, Binance, OKEx and Bitfinex
XRP	0.791	37 billion	Binance, Bith umb, KuCoin, Huobi Global, Bybit, Gate.io, FTX, Bitstamp, Bitfinex, Kraken
LUNA	89.85	33 billion	Huobi, Bitfinex and Upbit
ADA	0.8	26 billion	Binance, Bittrex, eToro, and HitBTC
SOL	81.27	26 billion	Binance, FTX, Bilaxy and Huobi Global
AVAX	72.20	19.22 billion	Binance, Bitfinex, Gate.io and Kucoin

The table above is based on the ranking of the most used cryptocurrencies, but always keeping in mind that they can vary depending on the sale and purchase of cryptocurrencies, where for the top ten cryptocurrencies are ranked the details of price, market cap and the place where the same can be bought.[1] When it comes to buying and selling cryptocurrencies, respectively the realization of cryptocurrency transactions, what is most important is the trust that people have or should create towards the resources that carry out these transactions. Lankton and McKnight [4] proposed that trust in technology "reflects beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible". Decentralized blockchain systems, such as Bitcoin or Ethereum, do not rely on a trusted third party in order to validate the transactions made by users or to maintain the security of the system [5][6]. The first thing you need to do to perform cryptocurrency transactions is to define the platforms for conducting transactions. A very important feature that should be noted is that not all countries have the same platforms offered and portfolios with which transactions can be realized through these decentralized systems. The process of creating an account is similar to many systems, however it differs in the way the data is stored and secured. Some systems require more data to be more secure in the future by the user, while others have a lower level of security. Once you have an account created, then you can start performing cryptocurrency transactions. Transactions can be performed only after you have filled your account with money, which as usual is done through your credit card. In these systems trading starts with buying cryptocurrencies like Etherium, Bitcoin depending on the money you have available as each of them has its own price. The processing time of transactions depends mainly on the quantity you buy, the cryptocurrencies you buy, the platform you use to conduct trade, etc. Once you have completed some transactions, and you already own the cryptocurrencies, you can place them in the wallet or portfolio where you can more easily control any changes to your cryptocurrencies. Within a cryptocurrency, there are more assets that can be used to conduct transactions. You can even create so-called tokens, with which you can make transactions, but they should definitely be verified and secure so that you can exchange cryptocurrencies with other people.

III. ENERGY CONSUMPTION AND THE FUTURE

Costs of processing cryptocurrency transactions are currently very high and volatile. Resolving energy spending concerns without sacrificing security and decentralization is an important challenging technique and has been the focus of studies and developments for years. Why do cryptocurrencies spend so much energy? For example, Ethereum, as a blockchain, requires that transactions and blocks to have to be validated by miners. In addition, every computational step carried out requires also some extra-charges to be paid by users. This kind of fuel is called gas, which is a unit of measuring the computational work of running transactions or SCs in the Ethereum network. In particular, gas is expressed through gwei, a subunit of ether [7]. According to a recent report by Eurelectric, the union of the electricity industry, more than 1000 projects are currently using Ethereum [8]. Energy provides the grid. Ethereum transactions are validated by miners. They merge transactions into numbered blocks and add them to the Ethereum blockchain. The blocks are then transmitted to 'node operators' who verify them separately whether they are valid or not. The possibility of a mine adding new blocks only works if there is a cost associated with mining. These conditions are met by imposing proof-of-work (PoW). To be eligible to submit a block of transactions, a miner must solve a computer puzzle faster than anyone else. Solving this puzzle creates competition between mines and costs in the form of energy expenditure. Ethereum has used proof-of-work since its inception. Migration outside of proof-of-work has always been an essential goal of Ethereum. But, technically it has been challenging because the other successful alternatives all sought to compromise the core principles and decentralization of Ethereum [9].

IV. ETHEREUM BLOCKCHAIN ARCHITECTURE AND DATA SECURITY

The data is obviously stored in certain databases, be it local databases, cloud databases, etc. It is important the data not to be misused by a third party. An Ethereum network is composed of a set of nodes running an Ethereum client (Fig. 1). Each of these nodes have a copy of the blockchain, which contains a list of all operations performed on the network. This enables nodes to prevent fraudulent activities, such as counterfeiting and duplicating cryptocurrencies, as well as containing an auditable record of all transactions performed on the network. Due to the decentralized nature of the network, the Ethereum framework preserves user pseudonymity (a weaker form of anonymity), as each user's identity is given by a public key. This enables users on the platform to perform functions such as transferring money, buying and selling, and much more [10]. The generalized structure of an Ethereum network is provided in figure below.

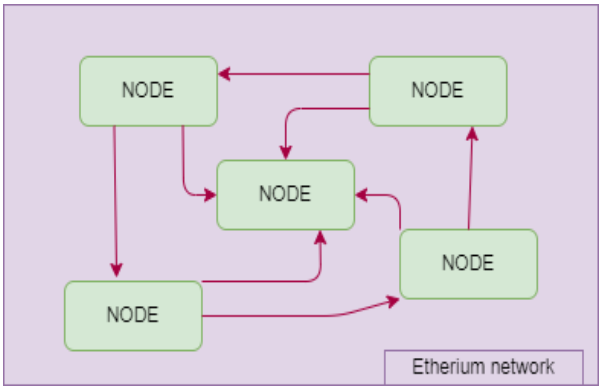

Fig. 1. Ethereum network

What exactly happens between the user and the ethereum network is shown in figure 3 to [10], where it is clearly explained that between the user and the Ethereum network we have the browser through which we access this network. It is clearly clarified that between the user and the browser there are several interfaces that serve to provide a consumer access to their Ether wallets, enabling them to use Ethereum to pay for goods online. Ethereum provides an interface with the Ethereum network for developers in the web3.js API, which is actually a collection of libraries which allow you to interact with a local or remote Ethereum node, using an HTTP or IPC connection [11]. This allows web applications to interpret events sent by the Ethereum network and submit transactions to the network. Another more elaborate version which shows the process of performing the transaction in Ethereum is shown in Figure 2. Where among other things it is clarified that the first job is for the user to create an account, and only after the account is verified you can access the execution of transactions in the Ethereum network. Access is done through certain browsers or interfaces that can be installed within them such as MetaMask or Web3.js for developers to connect with Ethereum network. Undoubtedly, in order to carry out transactions, ETH must be purchased first, where the price and the places where it can be bought are also given in Table 1. And transactions can only be done if you have enough ETH in your portfolio for the transaction you want to make. Before we continue to elaborate on whether the blockchain network can be adapted by programmers to the use of any other software application, we will first clarify some details about BigchainDB.

V. BIGCHAIN DATABASE

With the rapid development of science and technology, especially Internet technology and computing storage capacity in the last decade, data have become the most important means of production. With the rapid development of cloud computing, the database technology has become the most basic data technology facility. Especially, the Distributed Databases have been widely used to store and process large-scale data,which are applied in different scenarios than relational databases [12]. The BigchainDB is an extensible blockchain database that is the first decentralized database system to fill in the blanks of decentralized databases. It is based on a distributed database with the features of blockchain, so it has both the advantages of distributed database and blockchain. The BigchainDB is based on MongoDB. Therefore, it has these advantages: high throughput, massive data storage capabilities, NoSQL query language support, efficient query and rights management. The BigchainDB network consists of multiple nodes. Each node is a virtual concept consisting of three parts: the MongoDB database, the BigchainDB server, and the Tendermint communication node. Figure below shows the architecture.

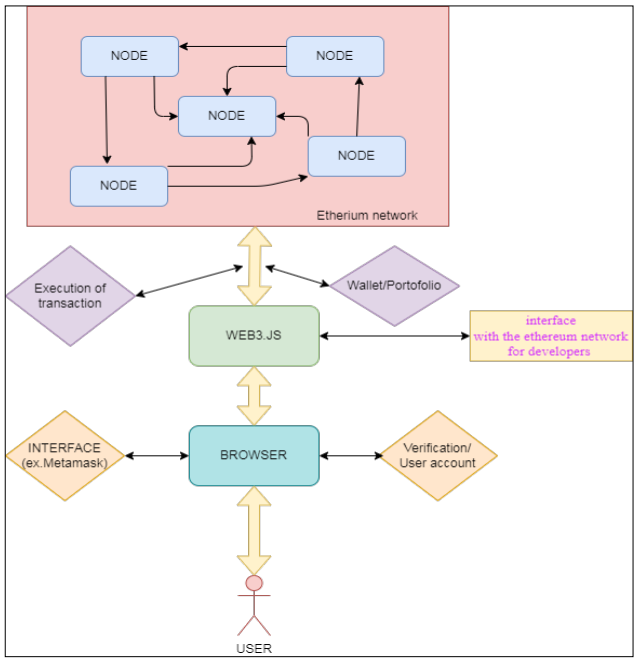

Fig. 2. Process of transaction execution in Ethereum network

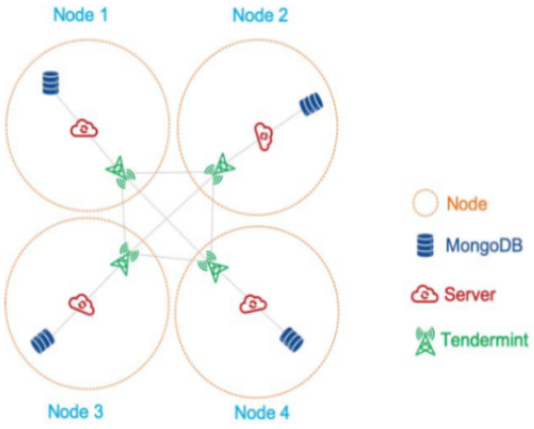

Fig. 3. A four-node BlockchainDB network
Source: http://docs.bigchaindb.com/en/latest/query.html

Rather than trying to enhance blockchain technology, BigchainDB starts with a big data distributed database and then adds blockchain characteristics - decentralized control, immutability and the transfer of digital assets. BigchainDB combines the key benefits of distributed DBs and traditional blockchains. Blockchain technology gives control back to you. On the internet, siloed, walled gardens lock up your personal data. This means it's next to impossible to port your data if you want to leave or to gain visibility into what is stored where. Blockchain technology enables sovereign personal data, a new way to manage your identity, medical records, and credentials [13]. In BigchainDB, one will store their confidential data off-chain and can also store their confidential data on-chain in an encrypted format. Through extensible

capability, the legitimately binding contracts, certificates could also be kept into the blockchain database. The authentication system permits the features starting from non-public enterprise level blockchain databases to open, government blockchain databases. If we are interested to deploy any kind of BigchainDB then we need to deploy it in the government version only. BigchainDB is taken into account in the top level distributed computing platforms like Eris/Tender mint [14], [15].

VI. Proposed Framework for Using BigchainDB in Software Application

The problem of data security and big data is more and more obvious, therefore more and more attempts are being made to create new data management opportunities and to provide more secure data transfer.. The benefits of the application of blockchain are applied in three areas namely for decentralized data storage, performing blockchain enabled data analysis and finally in maintaining blockchain enabled data security. Some of the blockchain projects for big data applications are: Story, Omnilytics, Rubix, Provenance, File Coin and Datum [16]. BigchainDB, a scalable blockchain for distributed big data was proposed by integrating the traditional blockchain with distributed databases to attain scalability through faster querying mechanisms. Blockchain network allows a user to join the chain based on the consensus. The process of communication with the set of nodes in BigchainDB are often done by employing a BigchainDB HTTP API [17] just like the BigchainDB Python Driver. There are many BigchainDB drivers provided in BigchainDB docs [18]. BigchainDB offers developers, startups and enterprises unique solutions to develop their concepts, platforms, and applications successfully. One of the main benefits of the BigchainDB is its ability to deploy a Blockchain-like decentralized system using production-ready technologies. It can be used to create new private Blockchains to take advantage of Blockchain capabilities at scale, or as a service for developers who desire the benefits of Blockchains without the stress of setting up private networks.

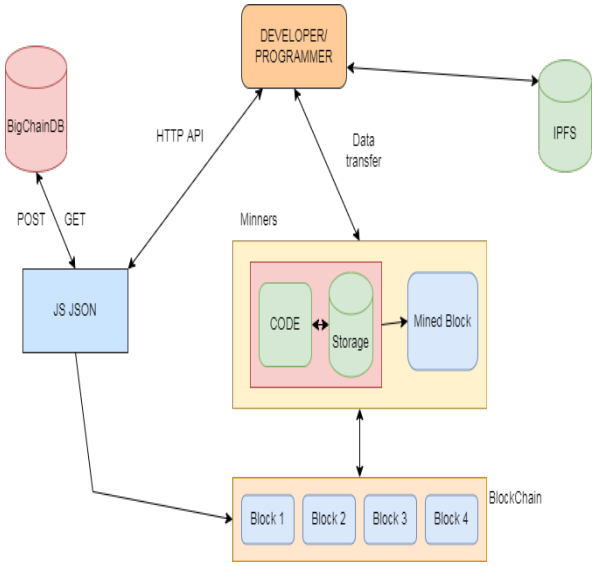

Fig. 4. Framework for using BigchainDB

Without going into the details of how BigchainDB works, we will present a framework on how it can be used the same by blockchain developers. It should be noted that it is a database with a more delicate structure, and requires good knowledge of the structure of the blockchain operation, data structures, understanding of cryptography and etc, so that it can be used rationally. Developers transfer data to the blockchain network through the mining process. Process of adding transaction records to public ledger is termed as mining where miners need to solve a mathematical problem based over cryptography hash algorithm. Each cryptocurrency has its own unique hashing algorithm. For instance, bitcoin uses the SHA-256 algorithm, Monaro uses Crypto Night, and Ethereum uses Ethash [19]. Once a miner finds the correct input, they have achieved Proof of Work (PoW). IPFS try to keep item data stored securely in a decentralized fashion. IPFS is used to help with data storage. Not all data are stored in the blockchain, but only the hash value gained while storing data in IPFS are stored into BigchainDB. Through back-end developers, the transactions are transferred to the BigchainDB, using HTML, CSS, JavaScript, and heavy use of web3js [20]. GET and POST are the two transactional methods for retrieving and validating the transactions within the BigchainDB [21]. BigchainDB transactions are within the type of JSON strings. Using BigchainDB is not at all easy. This is because you should also have knowledge of the UBUNTU (Linux) operating system, as it is the most suitable for its use. BigchainDB Server doesn't work on Windows or macOS (unless you use a VM or containers). The idea of the framework is this: developers create applications in a programming language suitable for BigchainDB, whether Java or Solidity. They build applications based on blockchain architecture and protocol. Their applications run on the blockchain too, but in advance using data selection techniques. Data transfer to the BigchainDB is done using web3.js, but always based on the way the blockchain operates. IPFS in this case it is used only as an auxiliary method for faster data processing by blockchain. Reasons why BigchainDB is being attempted to be used is the high security that blockchain technology has shown and is showing even today. Since blockchain is supposed to be extremely secure and unalterable, many individuals have dubbed this technology as "unhackable". However, recent incidents have unfortunately shown that hackers can access blockchains in certain situations. However, for now it remains one of the most secure databases of all existing databases.

VII. Conclusion

BigchainDB and distributed databases play a very important role and are seen as the future of data management, as the amount of data and their processing increases. It is very difficult to penetrate into the depths of blockchain operation because still remains a mystery, however what is possible is to use it and modify it in our applications without going into the details.. Through this paper, we tried to bring details of blockchain technology, to provide explanations for the most used cryptocurrencies and how their market values change, energy consumed by cryptocurrencies, concluding with a framework on how BigchainDB can be utilized using the network blockchain system to create our applications. We have tried to give detailed explanations regarding the process of communication between the developer and BigchainDB. Although it is still a term which is being developed, which requires greater programming skills and greater knowledge of the structure of blockchain, it remains our next challenge to get into the details of data storage and processing in the BigchainDB by describing in detail the process of searching and executing queries, as well as its connection to software

applications. And finally we will try to create our own software application using BigchainDB and describe the challenges we will face.

REFERENCES

[1] [1] Samyak Jain, Umang Rastogi, Nikita Bansal, Gagandeep Kaur, "Blockchain based Cryptocurrency for IOT", 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), 13 May 2019, Noida, India, DOI: 10.1109/SPIN.2019.8711727.

[2] [2] Mehrnoosh Mirtaheri , Sami Abu-El-Haija, Fred Morstatter, Greg Ver Steeg and Aram Galstyan, "Identifying and Analyzing Cryptocurrency Manipulations in Social Media", IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, VOL. 8, NO. 3, JUNE 2021, DOI: 10.1109/TCSS.2021.3059286.

[3] [3] CoinmarketCap, online (https://support.coinmarketcap.com/hc/en-us) Accessed: March 2022.

[4] [4] N. K. Lankton and D. H. McKnight, "Do people trust facebook as a technology or as a 'person'? Distinguishing technology trust from interpersonal trust,". Conference: Learning from the past & charting the future of the discipline. 14th Americas Conference on Information Systems, AMCIS 2008, Toronto, Ontario, Canada, August 14-17, 2008.

[5] [5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Available online (www.bitcoin.org). p. 9, 2008, Accessed: March 2022.

[6] [6] Ethereum Foundation, "Ethereum," 2022. [Online]. Available: https://Ethereum.org/. [Accessed: 30-Jan-2022].

[7] F. Buccafurri, G. Lax, L. Musarella, A. Russo, An Ethereum-based solution for energy trading in smart grids, Digital Communications and Networks (2022), doi: https://doi.org/10.1016/ j.dcan.2021.12.004.

[8] [8] Max N. Luke, Stephen J. Lee, Zdenek Pekarek, Anna Dimitrova, " Blockchain in Electricity: a Critical Review of Progress to Date", May 2018.

[9] [9]Ethereum energy consumption, available online (https://Ethereum.org/en/energy-consumption/), Accessed: Jan, 2022.

[10] [10]R. Vishnu Prasad, Ram Dantu, Aditya Paul, Paula Mears, "A Decentralized Marketplace Application on The Ethereum Blockchain", 2018 IEEE 4th International Conference on Collaboration and Internet Computing, October 2018, DOI:10.1109/CIC.2018.00023.

[11] [11] Ethereum JavaScript API, available online (https://web3js.readthedocs.io/en/v1.2.6/), Accessed: Jan, 2022.

[12] [12]Yajun Wang, Chao-Hsien Hsieh, " Research and Analysis on the Distributed Database of Blockchain and Non- Blockchain", 2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics, April 2020, DOI:10.1109/ICCCBDA49378.2020.9095589.

[13] [13] BigChainDB Features and Uses cases , available online (https://www.bigchaindb.com/features/), Accessed: February 2022.

[14] [14] Eris industries, available online (http://erisindustries.com/), Accessed: February 2022.

[15] [15] Tendermint. Available online (http://www.tendermint.com/), Accessed: February 2022.

[16] [16] Deepa N, Quoc-Viet Pham, Dinh C. Nguyen, Sweta Bhattacharya, B. Prabadevi, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Fang Fang, Pubudu N. Pathirana, " A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions", Elsevier, Volume 131, June 2022, Pages 209-226.

[17] [17] BigchainDB HTTP API. Available: (https://docs.bigchaindb.com/projects/server/en/latest/http-clientserver api.html), Accessed: February 2022.

[18] [18] BigchainDB Drivers & Tools. Available:

[19] (https://docs.bigchaindb.com/projects/server/en/latest/driversclients/index.html) , Accessed: February 2022.

[20] [19] Bhadoria, R.S., Arora, Y., Gautam, K. (2020). Blockchain Hands on for Developing Genesis Block. In: Kim, S., Deka, G. (eds) Advanced Applications of Blockchain Technology. Studies in Big Data, vol 60. Springer, Singapore. https://doi.org/10.1007/978-981-13-8775-3_13.

[21] [20] web3.js - Ethereum JavaScript API, online (https://web3js.readthedocs.io/en/v1.7.1/), Accessed: February 2022.

[22] [21] R. Vamshidhar Reddy, V. Jaya prakash Reddy, E. Madhusudhana Reddy, "Automatic Face Expressions and Gesture Detection System Using Blockchain Security", 2020 International Conference on Intelligent Engineering and Management (ICIEM), 17-19 June 2020.