International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 11 | November - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Crypto Transaction Using Blockchain

Prof. Vishal Polara[1] , Hardish Avlani[2] , Prince Sheth[3] , Smit Bhansali[4,] and Sanket Detroja[5]

[12345]Information Technology Department
Birla Vishvakarma Mahavidyalaya
Anand, Gujarat, India

Abstract. The blockchain is an element technology used, most notably, in the cryptocurrency trading. Although studies and substantiative experiments are under way for application of the technology in various financial transactions. In recent time blockchain has received extensive attentions. This chapter expounds the main concepts of blockchain technology and its cutting-edge applications. With the help of blockchain technology we can make transactions in a decentralized manner. In our project we have used Web 3.0 which is the latest internet technology that helpful in blockchain to achieve real-world human communication and for transactions we have used Solidity. First we have to connect our application to the meta-mask wallet. And then we can send Ethereum, from one account to another account using the hexadecimal address of the wallet .Here, we also have to send a message and a unique keyword for generating a GIF for the transaction. Then, this transactions can be seen at the transactions part of the page with the unique GIF, the receivers address, message, date and time etc.

Keywords: Blockchain, Meta-mask, solidity, Web 3.0,Ethereum,Decentralized.

1 Introduction

Since the modernization in Bitcoin, a digital cryptocurrency, in 2008, Blockchain technology has situated itself in the focal point of interest among a diverse range of researchers and practitioners. Blockchain is a best register that stores all transactions that have been made on the top of a peer-to-peer network in a protected, conformable and crystalline way. No doubt, there are many advantages to use blockchain like Trust, Decentralized structure, Improved security and privacy, Reduced costs, Speed, Visibility and traceability, Immutability, Tokenization, Innovation and many more.

In general, the number of electronic transactions are quickly expanding in money related educate whereas embracing rising advance (blockchain as an middle person) to decrease the chances of extortion, minimize the exchange fetched, and time -effective.

In our project, we can connect our Ethereum Wallet using meta-mask. It will allow users to send transaction through the blockchain. Each transaction paired with a GIF and it will be forever stored in blockchain.. It will send crypto across the world.

2 Literature Survey

This study aims to highlight the blockchain technology's issues which are facing the financial institutions. In this chapter, we are aiming to briefly highlight past ponders that have talked about distinctive points of view of blockchain innovation and it's importance.

The major distinction between the conventional payment show and the payment instalment through bitcoin is that there's no association of physical cash within the afterward framework. The bitcoin could be a virtual money related unit that has no physical or substantial representation.

Rosen,E.,Wengrowski,E.,Clark,G. D., & Gao,X.(2014) had done An Empirical Study of Cryptocurrency. Abdi,B.(2014) had done A case study on Cryptocurrency, Bitcoin.[3]

The applications of cryptocurrencies can run from basic to complex financial transactions. There are many applications we can use like Public.com, Ledger, Coinbase, Trust Wallet, Exodus etc.

Brain Armstrong, who is founders of Coinbase application. Coinbase supports more than 44000 digital assets. It also supports Multi-signature and two-factor authentication support. But in it's disadvantages is, Only available on mobile and tablet devices(Except for chrome extension).

Maxim Rasputin who is CEO of Trust Wallet Application. Trust Wallet supports a vast range of coins and tokens. It also earn interest on one of 12 different cryptos. And it built-in Web3.0 browser. But in it's disadvantages, Educational resource on coins and tokens are limited.

Ian Rogers who is CEO of Ledger application. Ledger application can install up to 100 apps at same time. It can buy and sell crypto directly through the Ledger Live app. It verify all transactions with 2-button presses. It can also compatible with 50 other hardware wallets. And in it's disadvantages, it is more expensive than it's original entry-level wallet.

Daniel Castagnoli who is CEO of Exodus application. Exodus Application supports over 225 crypto assets. It is compatible with Trezor One and Trezor T hardware wallets. Allows users to buy Bitcoin with Apple Pay.

And in it's disadvantages, it's transaction fees on the in-wallet crypto exchange. And Lack of native 2-factor authentication may bother to users. It is not supported in multi-signature.

Ouriel Ohayon, Who is CEO of ZenGo application. ZenGo provides keyless security system assures there is no single point of failure. We can buy crypto with credit, debit, bank transfer and Apple pay. And in it's disadvantages, it has no private key is a big source of contention for some traders. And not all feature available worldwide.

3 Methodology

3.1 Blockchain

Blockchain is a series of immutable blocks placed in chronological order of their mining. Blocks are packages of data whose value after mining can't be changed. All the blocks are chined together with help of Cryptography Hash Function.

- Immutable:- No participant can change the data once it is recorded in Blockchain.
- Distributed Ledger Technology:- Distributed ledger technology(DLT) is a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time.
- Decentralization:- Decentralization refers to the transfer of control and decision-making from a centralized entity (individual, organization, or group thereof) to a distributed group.

Inefficiencies in the present-day systems are due to one major factors – presence of too many intermediaries. Consider a Cross Border Payment System (SWIFT System) for example.

There are can be many intermediaries who eat up a share of the price we pay for products. Lets look at this in more detail.

Suppose Bob who have a bank account in Bank of America and wants to send $100 to Alice in HNBC. When Bob is transferring the amount, they will provide the SWIFT code to Bank HNBC. SWIFT will then send a secure message communication to Bank HNBC including all necessary information. When Bank HNBC receives this message payment transfer will get started. Lets see how the transfer will work. SWIFT works when banks have a direct connection to each other meaning Bank of America will have their account in HNBC and Bank HNBC will have their account in Bank of America.

- Bank of America will deduct the $100 from Bob's account.
- Bank of America will credit the $100 to their account in HNBC.
- HNBC will deduct the $100 from Bank of America account in their bank.
- HNBC will credit the $100 (excluding fee) to Alice's account in their bank.

Now, there may be case that, Bank of America may not have direct connection in HNBC. i.e., BOA may not have account in HNBC. In such case BOA will use intermediatory Banks to fulfil payment. In such case intermediatory banks will also charge their fees. According to world bank the transfer charge is **around 7%** of the Actual Money Transfer Order [1].

After seeing what is Blockchain and why we need Blockchain, let's look at the fundamentals of Blockchain. In that first is Blocks.

3.1.1 Blocks

A Blockchain is what it sounds like, it could be a chain of pieces containing a few information. The data can be anything like exchange information, code, or basic message. A Block consists of header, body, and hash of the past piece. To finalize a square a hub needs to illuminate a perplex, which is "Troublesome to unravel and simple to confirm" any hub can effortlessly verify the piece and can include the piece to the blockchain on coming to agreement.

The hash of the previous block makes sure that tempering any block will lead to recalculating the hash for all the next blocks which are difficult. Since all the blocks are distributed each peer in the network have a copy of the blockchain even though if someone solves the puzzle for all the next block it won't be possible to change the data in the blockchain because this copy can only be accepted only if 51% of the peers agree on the false blockchain.

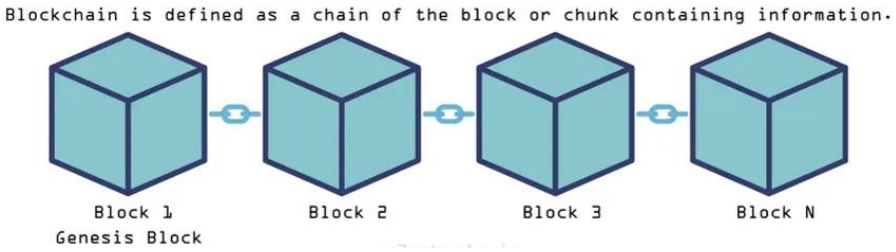

Fig 1. Understanding of Blocks

3.1.2 Nodes

A blockchain comprises of various pieces of information. These information pieces are put away on nodes, which are comparable to little servers. On a blockchain, all hubs are connected to one another and constantly trade the foremost later data on the blockchain with one another. This ensures that all hubs are up to date.

Blockchain hubs are organize partners and their gadgets that are approved to manage the dispersed record and act as communication center points for different arrange assignments. The primary work of a blockchain hub is to approve the legitimateness of each consequent batch of arrange exchanges, known as pieces.

There are two types of Nodes:-

1. Full Node: A full node is responsible to maintain all the transaction in blocks and add a valid block to the Blockchain.
2. Light Node:- A light node stores and provide data to accommodate daily activity and fast transaction.[7]

3.1.3 Consensus Algorithm

Everything in the world requires a consensus for e.g. going for a trip we might ask a group of friends to vote for a place and we decide to move to a place that has the majority. Or one might appoint a person to decide on behalf of everyone and everyone agrees on the decision made by the person appointed that's consensus in real life.

The Blockchain arrange comprises of a arrangement of hubs that frame a dispersed architecture. These hubs ought to be adjusted and run synchronously to preserve security within the network. Thus the concept of Agreement is connected to preserve concordance within the Blockchain arrange.

Proof of work (used by Bitcoin and Ethereum) and Proof of Stake (Used by Solana and Polygon, Ethereum is planning to move to proof of stack after merge.)

In Proof of work, Nodes does extensive work to mine a block. i.e., Proof of Work requires lots of electricity. In case of PoW Nodes tries to maximize its CPU Power to increase their chance of validating and subsequently earn mining rewards. This leads to pooling and increase the chances of Centralization. Bitcoin consumes 1100 MW in total, that is 9636 GWh over an entire year, or 0.829 Mtoe. [8]

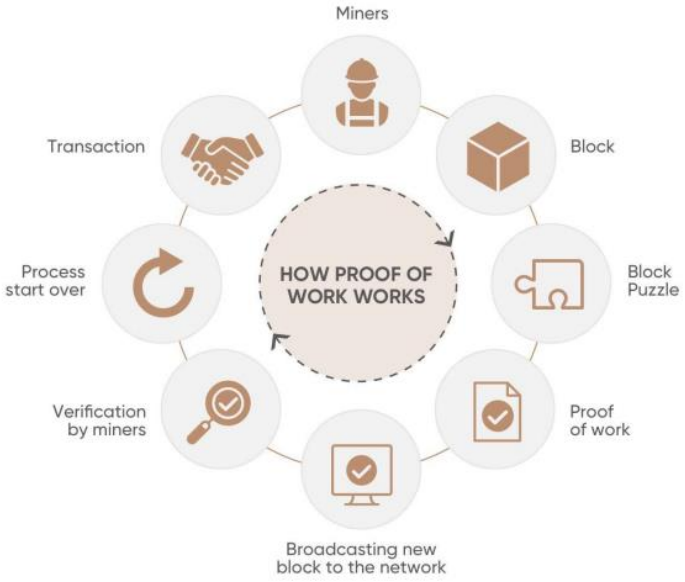

Fig 2. Proof of Work

After Proof of Work, let's see Proof-of-Stake algorithms achieve consensus by requiring users to stake a number of their tokens to have a chance of being selected to validate blocks of transactions and get rewarded for doing so. PoS shares many similarities with PoW but also differs in fundamental ways. Every validator must own a stake in the network. Staking involves depositing some tokens into the systems, locking them in what you can think of like a virtual safe, and using it as collateral to vouch for the block.

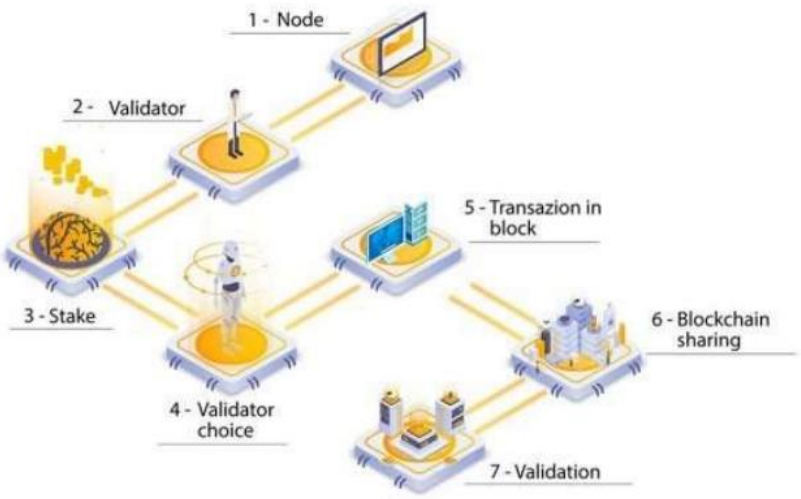

Fig 3. Proof of Stake

3.1.4 Wallets

A Cryptocurrency wallet could be a computerized holder that stores open and private keys for cryptocurrency exchanges. Since cryptocurrency may be a digital resource, it cannot be stored in a conventional wallet. A cryptocurrency wallet may be a gadget utilized to send and receive cryptocurrency. There are thousand of cryptocurrencies, and each has its unique supported wallet. No two cryptocurrency are same.

Wallet is mainly used for authentication and most Web 3.0 projects uses wallet to authorize users. Wallet will replace traditional method of remembering 100s of Id and Password. Some of famous wallets are: Meta mask, Trezor and Electrum.

3.2 Bitcoin

The Bitcoin whitepaper defines Bitcoin as a peer-to-peer electric cash system. After the crash of 2008, an anonymous person or organization named Satoshi Nakamoto proposed a whitepaper for a currency that isn't dependent or any other centralized authority. [9]

The core idea behind Bitcoin was to use digital signatures as the solution to peer-to-peer value transfer without double-spending. The issue with the financial institution as they were inheriting the weakness of the trust-based model.

3.3 Ethereum

Ethereum whitepaper was proposed by Vitalik Buterin, at the age of 19 to make Ethereum scripting language Turing complete. Vitalik believed that Bitcoin as a form of digital money is great but its scripting language is too weak. [10] Ethereum network provides a framework for creating and storing the blockchain. Each block is created and its details are stored in an encrypted ledger. These generated blocks are distributed among the nodes, providing the system with high fault tolerance. To cast a vote, a user must use Ethereum for their transactions. So Ganache is used for this. Ganache is a private Ethereum blockchain environment that allows you to emulate the Ethereum blockchain to interact with smart contracts on your private blockchain.[11]

3.3.1 Limitation of Bitcoin

- Need of Turing completeness: Bitcoin scripting bolsters a huge set of computations, but it doesn't back everything i.e., it lacks loops. Typically done to avoid infinite loops during transaction verification.

- Value Blindness:- There is no way UTXOs script to provide fine-generated control over the amount that can be withdrawn.
- Lack of state:- UTXOs can either be spent or unspent there is no opportunity for multistage contracts or scripts which keep any state beyond.
- Blockchain-Blindness:- UTXOs are blind to blockchain data such as the nonce and previous block hash. This limits several applications like gambling which requires a source of randomness from Blockchain data.

3.3.2 Ethereum Accounts

In Ethereum, the state is made up of object called accounts, with each account having 20 Bytes address and state transition being direct transfer of value and information between accounts. Fields of Ethereum Account:
• The nonce, a counter used to make sure each transaction can only be processed once • The account's current ether balance
• The account's contract code, if present
• The account's storage (empty by default)

3.4 Meta-mask

Meta-Mask may be a crypto wallet that can be utilized in a web browser and on portable gadgets to connected with the Ethereum blockchain. Meta-mask allows blockchain users to manage their wallets. Using the browser extension, users can use the wallet and perform transactions through the browser. When a transaction is performed, a meta mask pops up and asks the user to confirm the transaction. It permits you to run Ethereum Dapps(Decentralized Apps) right in your browser without running a full Ethereum node.

4 Project Description

We presently portray a normal client interaction with the proposed conspire based on our current framework usage. We make a web application. We use web 3.0 in this project. And for backend of our project, we solidity.

So basically, user have to connect meta-mask with their account. After successfully connect to the meta-mask the user have to fill the form. In that form user have to enter the address, amount, message and GIF. If the user click on send button, it will take half minute to one minute. After that user get can check their transaction. User can see their transaction details. In details user can see the date and time, address of account in which they paid the Ethereum, message, GIF etc. User can done more and more transaction with more and more security.

Below shown the flowchart diagram of our project,

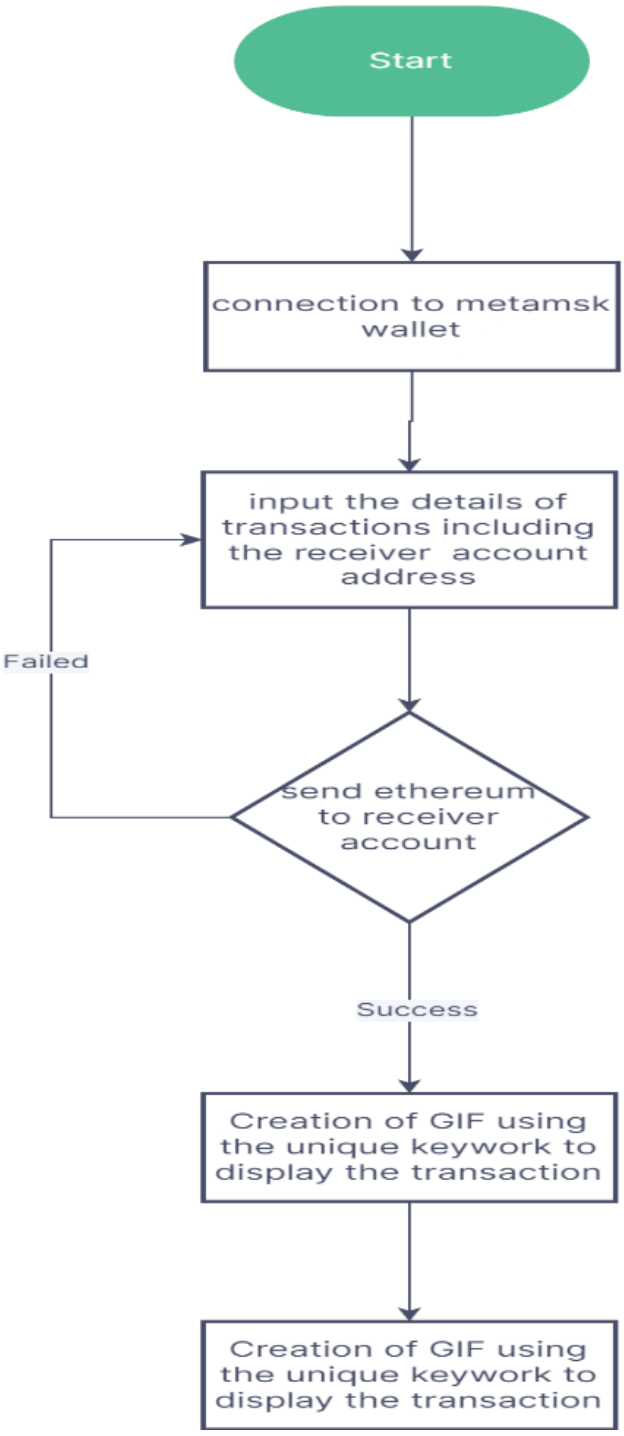

Fig 4. Flowchart Diagram

After flowchart diagram, below are screenshots of our application,

Step 1:- here we have to connect to the meta mask wallet through meta mask portal.

By connecting to the portal we can see the account details and the balance in it.

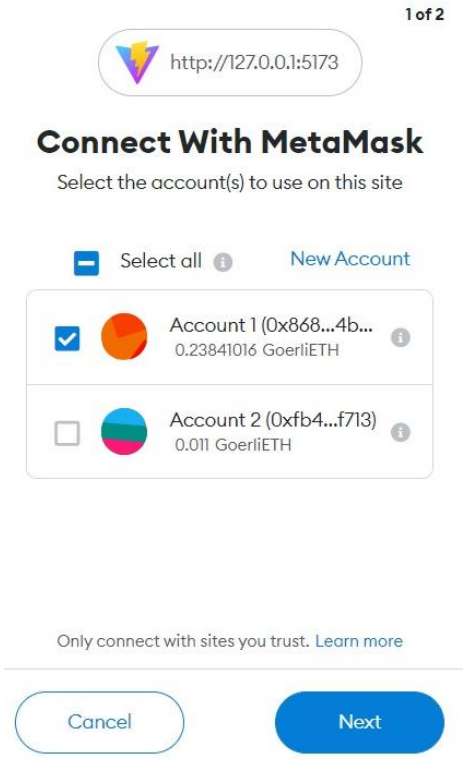

Fig 5. Connection with meta mask

Step 2:- here we have to fill up the form give with the receivers account address and the amount of Ethereum to be transferred with the unique keyword for generating the GIF.

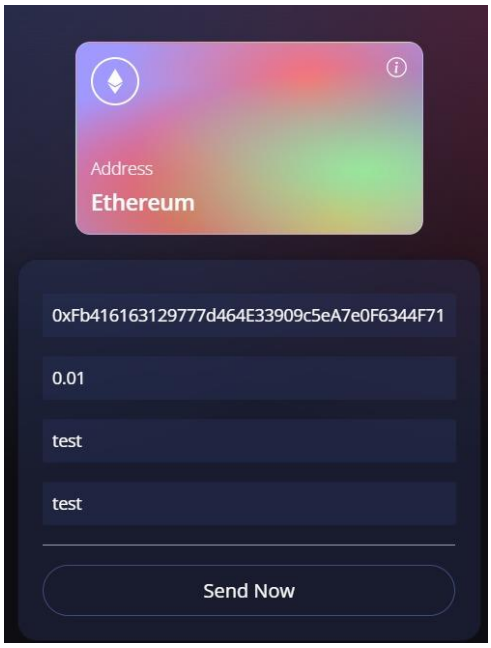

Fig 6. Step-2

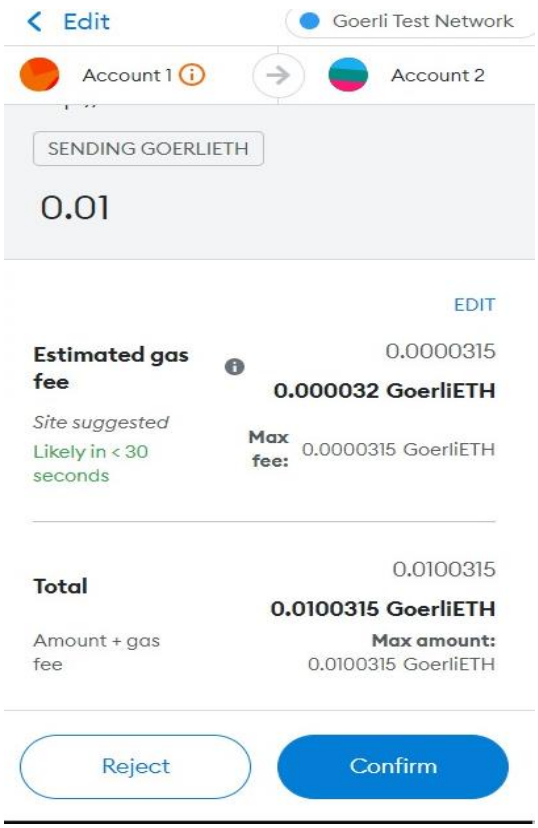

Fig 7. Conformation message

Step 3:- here after we click on the send now button we have to give confirmation for the transaction through the meta mask portal and a loader is initialized till the transcation is finished.

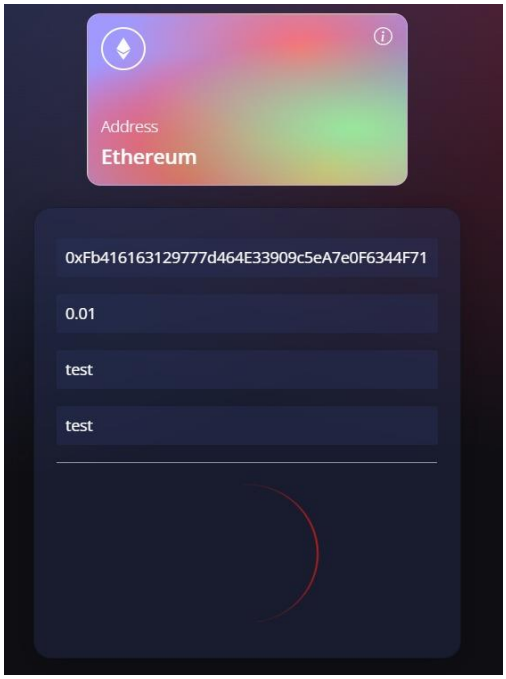

Fig 8. Loader

5 Result and Conclusion

The proposed blockchain based transaction manages the all Ethereum records. With the help of blockchain we can done transaction with more and more security. If we don't have details of account then, we can't get details back. Blockchain technology has the potential to be implemented in a far more secure and accessible transaction system. And in future we believe that blockchain based transaction system can replace any transaction system.

6 References

1. Barulli, M., Weigand, F., and Reboh, P. (2017). *Bernstein - Product Deck - Blockchain Solutions for Securing Intellectual Property Assets and Innovation Processes, 1–14.*
2. Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 10.1109/BigDataCongress.2017.85.
3. Onuklu, A. (2019), "Research on Blockchain: A Descriptive Survey of the Literature", Choi, J. and Ozkan, B. (Ed.) Disruptive Innovation in Business and Finance in the Digital World (International Finance Review, Vol. 20), Emerald Publishing Limited, pp. 131-148. DOI/10.1108/S1569-3767201
4. "8 Best Crypto Wallets of November 2022." *Money*, money.com/best-crypto-wallets. Accessed 18 Nov. 2022.https://www.techtarget.com/searchcio/feature/Top-10-benefits-of-blockchain-technology-for-business
5. Pilkington, Marc, Blockchain Technology: Principles and Applications (September 18, 2015). Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016, Available at SSRN: https://ssrn.com/abstract=2662660.
6. Blockchain Nodes: How They Work (All Types Explained) - Nodes.com, n.d.
7. L. Weese, "Bitcoin mining and energy consumption," 8 December 2017. [Online]. Available: https://blog.bitcoin.org.hk/bitcoin-mining-and-energy-consumption4526d4b56186.
8. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 06 July 2022].

9. V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.,".December,2014.[Online],.Available: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepape r_-_Buterin_2014.pdf. [Accessed 06 July 2022].

10. Catalini, C., and Gans, J. S. (2016). *Some Simple Economics of the Blockchain*. Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16. Social Science Research Network (SSRN). doi: 10.2139/ssrn.2874598

11. Pratt, M. K. (2021, June 2). *Top 10 benefits of blockchain technology for business*. SearchCIO.Retrieved November 18,2022, from https://www.techtarget.com/searchcio/feature/Top-10-benefits-of-blockchain-technology-for-business

12. "Ethereum - ETH Price, Live Chart, and News | Blockchain.com." *Ethereum - ETH Price, Live Chart and News | Blockchain.com*, www.blockchain.com/explorer/assets/[id]. Accessed 18 Nov. 2022. https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf

13. Codex (2018). *Codex Protocol - A Cryptocurrency and Decentralized Registry for Unique Assets, Starting With Art & Collectibles.*

14. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. (2017). "An overview of blockchain technology: architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)* (Honolulu, HI), 557–564. doi: 10.1109/BigDataCongress.2017.85