*International Journal of Advancement in Electronics and Computer Engineering ( IJAECE)*
*Volume 13, Issue 03, March. 2024, pp.23-28 ISSN 2278 -1412*


# Blockchain Characteristics and Smart Contract: A Review

Marc Ruben Danny[1], ,Jessica Sarah Deen[2],Juan Mark Deen[3],Amisha Michelle Danny[4]
[1]Department of BBA in Logistics, Retailing & E-Commerce
[1]INDIAN MARITIME UNIVERSITY - [IMU-K] A central university. marcruben.danny@gmail.com, Willingdon Island, Kochi-682029, Kerala, India.
[2]Department of Computer Science and Engineering
Vellore Institute of Technology, Bhopal, Madhya Pradesh 466114, . jessica.sarah2020@vitbhopal.ac.in, India
[3]Department of Computer Science and Engineering and Bioinformatics
Vellore Institute of Technology, Vellore, Tamil Nadu 632014, juanmark0521@gmail.com, India.
[4]Department of Computer Science and Engineering
Kalinga Institute of Industrial Technology, Bhubaneswar, Odisha 751024, amisha.danny@gmail.com, India

***Abstract*** *– Blockchain is making its space in almost all sorts of industries. Moreover, there will be a massive demand for industrial 4.0 growth across all over the world markets. The Blockchain as a platform, Using it, there is a possibility to replicate and distribute a digital ledger over an entire computer network. All transactions or updates on the blockchain are visible to every participant. Distributed Ledger Technology is the name of this database (DLT). Cryptographic signatures, such as hashes, are used to record transactions on the Blockchain. Because it is immutable, it offers excellent levels of data protection. If one of the blocks in the chain is changed, it's immediately evident that something has gone wrong. To hack into the system, hackers would have to modify every block in the chain across all distributed copies.In the future, a huge usage and scope of blockchain technology. Like in financial technology, new technologies make more efficient financial services. Banking, insurance, trading and investments, crowdfunding, Internet of Things, Manufacturing industry such as on-demand manufacturing, smart diagnosis and maintenance, product certifications, Record maintenance of assets and inventory, Supply Chain Management, Healthcare, Governance and Management Education and Energy Sector many more.The converter topology and energy management control schemes proposed in this thesis are expected to pave the way for novel approaches to hybridizing energy sources for EV applications.*
.
***Keywords: Blockchain characteristic, DApps, Smart contract, Ethereum, Blockchain applications.***

## I. INTRODUCTION

Initial work on the blockchain concept Haber and Stornetta are introduced in 1991[3]. A cryptographically secure document or information was a computationally procedure practically via digital time-stamping block chain. It is infeasible for a user to temper the time stamp, even with the collusion of a time-stamping service, Bayer, Haber, and Stornetta in 1992 [4]. Merkle trees were incorporated into the framework to enhance efficiency by aggregating several document assurances into a single block. Satoshi Nakamoto, the creator of bitcoin, invented it in 2008 with the blockchain as its backbone [5]. Due to the tremendous success of bitcoin in the initial years, several enhancements and alternatives were proposed by researchers and developers. Second-generation blockchain network Ethereum was proposed in 2013 by Buterin[1]. Furthermore, this introduced the concept of a smart contract. Ethereum allows a single programmable blockchain network to develop different applications instead of a separate blockchain for each type of application. Each application forms a smart contract in this blockchain network. There are many applications and potentials for blockchain technology, which is still in its infancy. For a variety of technical and non-technical concerns, an extensive range of blockchain platforms has been developed [4],[6]. The types of blockchain platforms are incredibly diverse. Since technology is developing so quickly, it is necessary to have a thorough understanding of all its characteristics. It is essential to have such a broad vision and to standardize and improve it; despite previous studies on blockchain, assessing its characteristics remains difficult due to its immaturity, rapid growth, and expansion[7].

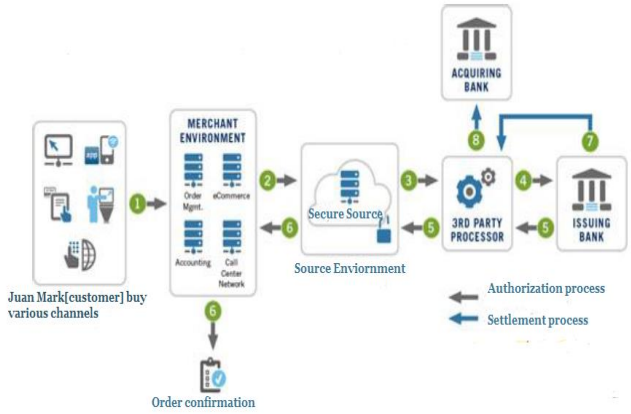



Fig.1 Shown as an example to consider the case of a typical online transaction.

Every business run based on the information and feedback analysis. Online transaction is a nowadays very demanded and necessary. Due to extensive network connectivity, many internet frauds occur, e-commerce

transactions need secure channels to receive and deliver the process in the authorized and settlement confirmation process. In order to do this, the blockchain is ideal for delivering that information because it provides immediate, shared, and utterly transparent information stored on an immutable ledger that can be accessed only by permission network members. Fig.1 shows the accurate and fast transaction system securely. A blockchain network provides a secure environment and tracks orders, payments, accounts, production, and much more. Furthermore, because members share a single view of the truth, users can see all transaction details end-to-end, giving them greater confidence and new efficiencies and opportunities. This technology needs a decentralized, trusted system of transactions and supply chain to scale up the digital economy.Various technology covers by the blockchain, however, like the advance and deepen energy-market reforms, guide the electric power residents to bring flexible energy resources into the market and conduct P2P electric power trade (PEPT) among regional residents [8]. In this work, a PEPT technique (TRTM) using blockchain and "two-round trade matching" is suggested. An initial low-computing-power consensus mechanism for Ripple consistency is given, and a P2P operation architecture built on top of the blockchain technology framework is developed. The majority of blockchain applications are created as Dapps, or decentralized apps, by utilizing smart contract functionality. Nodes, or end users, can employ smart contracts directly to conduct transactions through Ethereum clients. To implement these contracts and conduct transactions, Dapps were created with an intuitive user interface in mind. Dapp, often known as Dapp, offers a peer-to-peer transaction environment for users, apps, and systems that may not be familiar with one another. So yet, blockchain-based decentralized programs, or DApps, have not attracted widespread interest. In thestudy in article [9] authorsoffer potential solutions for the most severe adoption difficulties from a human-centered standpoint. The four key challenges highlighted for mass adoption are the incentive to change, the onboarding challenge, the usability problem, and the feature problem. The [10] authors discussed a brief, non-technical explanation of Bitcoin, a new but widely important digital cryptocurrency generated and maintained by a distributed multi-agent system. Bitcoin was the first electronic cash system to gain widespread acceptance. While Bitcoin has the potential to enable new forms of financial interaction, it has significant privacy limitations. Because the Bitcoin transaction log is entirely public, users' privacy is only protected by pseudonyms. In [11], they proposed a Zerocoin, a cryptographic extension to Bitcoin that allows for entirely anonymous currency transactions. The authors [11] suggest that the system uses standard cryptographic assumptions and does not introduce trusted parties or otherwise alter Bitcoin's security model.In order to do this, many researchers are sound studies to doing in blockchain technology in various prospective fields of world economy and development. The characteristics of blockchain mainly explore in the following area, as shown in fig.2.Blockchain technology is a peer-to-peer distributed ledger capable of storing data on a worldwide scale across thousands of collaborating servers. The technology has progressed much beyond its initial application for cryptocurrency. Because of its ability to provide security to an immutable database through decentralized networks, the technology is now used by a wide range of sectors and industries.


Fig.2 Characteristics of Blockchain

Blockchain technology is a peer-to-peer distributed ledger capable of storing data on a worldwide scale across thousands of collaborating servers. The technology has progressed much beyond its initial application for cryptocurrency. Because of its ability to provide security to an immutable database through decentralized networks, the technology is now used by a wide range of sectors and industries. Blockchain is a digital record that can be reproduced and shared throughout the whole network of communication systems. Those who are part of the blockchain network have access to all transactions or modifications on it. Disbursed Ledger Technology is the name of this database (DLT). There is an unchangeable cryptographic signature for each transaction in the Blockchain. A non-changeable ledger with great data security, hence. If one of the blocks in the chain is changed, it's obvious. Attempting to get into the system without modifying every block in the chain across all distributed versions would be difficult for hackers to do [13]. In the article [14] gave an idea for using blockchain technology in distributed manufacturing. Manufacturers can use smart contracts to automate their operations to focus on how and where data from IoT devices is stored and how entities communicate with one another remain unresolved. In this situation, the author suggested that decentralized systems have advantages over centralized approaches, particularly trust and data security.A consensus mechanism is at the core of each distributed ledger technology. An article [15] discussed a brief overview of the two most prominent consensus protocols from the blockchain universe, namely proof-of-work and proof-of-stake. They describe the fundamentals from a design perspective, highlight some crucial differences between the protocols and discuss their implications for the validity and security of the blockchain. Moreover, the focus has been based on Byzantine-Fault-Tolerance consensus, which may become a promising alternative to established consensus mechanisms in the

future.Blockchain technology can also be identified as a disruptive tool with a promise of enormous implementation potential. Nevertheless, blockchain technology should be treated only to support existing systems and models in the upcoming years. The implementation, adoption, and diffusion of blockchain technology within a global business requires capital, recourses, and reengineering to understand the global economy. Blockchain features are precious for banking, i.e., transparency, immaturity, safety, publicity, cost-saving, time-stamped, and speed. The global banking sector is currently exploring the implementation potential of blockchain technology in payments, services, and financial management. The article's [16] main aim is to clarify the implementation potential of blockchain technology, the risk related to the implementation process, challenges, and opportunities produced by blockchain for the banking sector.The Self-Sovereign Identity (SSI) model is a privacy-preserving blockchain-based on crypto-privacy technologies, which provide individuals a means to anonymize and control their data during digital transactions.The article [17] discusses the significant privacy challenges associated with this exciting and disruptive technology, along with a comprehensive review of privacy-preserving research solutions and techniques. The survey also examines privacy research proposals and solutions for permissions and private blockchains using privacy technologies. A wide range of blockchain scenarios is examined [17], including the areas of governance and eHealth, cryptocurrency, smart cities, and cooperative IT.

## II. SMART CONTRACT

Smart contracts are a robust program of the blockchain that runs when predetermined conditions are satisfied and are designed to implement blockchain technology. They are often used to automate the implementation of an agreement. Thus, it conveys results immediately to all participants without the involvement of an intermediary or loss of time, as shown in fig.3. A smart contract is a central component of the Ethereum blockchain. Nick Szabo is introduced the concept of digital currency called "Bit Gold" in 1998, defined smart contracts as computerized transaction protocols that execute the terms of a contract. Smart contracts render transactions that are traceable, transparent, and immutable [18],[19],[20]. The smart contract represents a business logic layer, where the logic is coded in a special high-level language (for example, Solidity). The year 2014 first functional implementation of Ethereum was done by Gavin Wood. He was proposing Solidity language to write smart contracts [21]. Solidity Team of Ethereum Project later developed the language. Christian Reitwiessner led the team [12]. With this evolution, "Ethereum is a global, open-source platform for decentralized applications. On Ethereum, customer can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world."

1. A smart contract is a digital agreement that executes automatically based on real world inputs in data.
2. It is a piece of code in the blockchain, identified through a unique address.
3. It includes a set of executable functions and state variables.
4. The function code gets executed when a transaction is sent to it. A transaction contains input parameters to run the code.
5. Functions in smart contracts are invoked by messages.
6. A transaction specifies these messages and input parameters for each of the messages.
7. There are multiple smart contract platforms like Ethereum, Hyperledger, Rootstock, Ripple.
8. Many of these platforms use Solidity language.

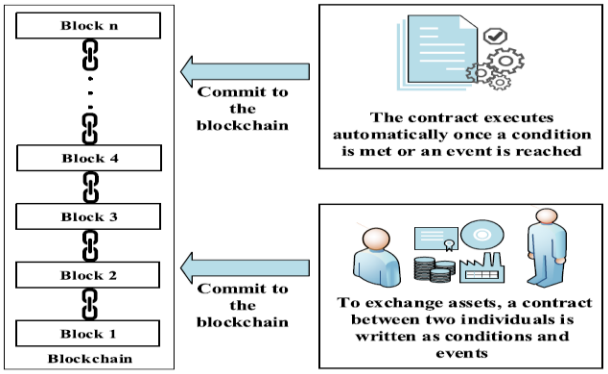



Fig.3 Smart contracts in Blockchain

## III. SMART CONTRACT ETHEREUM

Source www.ethereum.org The table. 1 shown a timeline of all the major milestones, forks, and updates to the Ethereum blockchain.

**Table.1**

| Year | Ethereum blockchain |
|---|---|
| 2013 | o Whitepaper released |
| 2014 | o Ether sale<br>o Yellowpaper released |
| 2015 | o Frontier thawing<br>o Frontier |
| 2016 | o Spurious Dragon<br>o Tangerine whistle<br>o DAO fork<br>o Homestead |
| 2017 | o Byzantium |
| 2019 | o Istanbul<br>o Constantinople |
| 2020 | o Beacon Chain genesis<br>o Staking deposit contract deployed<br>o Muir Glacier |
| 2021 | o (In Progress) Altair<br>o London<br>o Berlin |

Ethereum is a system that supports digital currency, worldwide payments, and apps. The community has created a thriving digital economy, daring new ways for creators to earn money online and much more. It is accessible to anyone, wherever in the globe.

An Example Application: Car Hiring App

**Central control network.**

-App links car drivers and riders as shown in fig.4, and all clients need is an internet connection

-Provide an optimized solution to the rider by minimizing the cost of travel time.

-Provides a mechanism to let two parties engage in trade withoutgetting to know each other.

-Trust is built through a driver's proof of identity and their reputation through ratings.

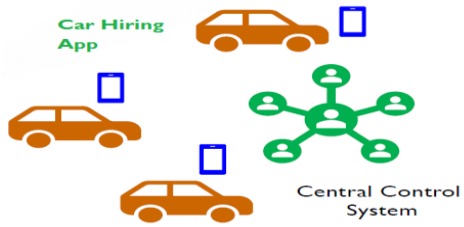



Fig .4 Central control car hiring app

**Peer to peer network**

Demand supply problem in the network of people. Think of a smart contract to decentralize the Ola or Uber app. Now, this type of network is a trustless peer-to-peer network. However, all conditions are coded and executed securely and transparently as shown in fig.5.

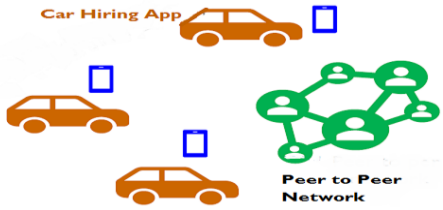



Fig.5 Peer to peer car hiring app

## IV. HYPERLEDGER FABRIC

The A global collaboration of over 80 institutional members has been formed to build a proof of concept and prototype finance systems for the real-time autonomous execution of financial transactions [22].Blockchain's private transactions require that the distribution ledger of the peer-to-peer network model maintain confidentiality. So, the business operating model is changing from time to time. When counting and analyzing blockchain platforms for business activities use cases, a smart contract who constantly evaluates the most efficient features has grown to use. Hyperledger Fabric develops open-source engine for business blockchain and technological synergies to develop revolutionary blockchain applications. Hyperledger is now one of the most preferred blockchain platforms for developing decentralized enterprise applications and business markets to suit its timing. Hyperledger Fabric is the concept of a smart contract between two parties for any transaction (information, goods, or financial), makes it easy and efficient for operational management as shown in fig.7. To keep pace with the Industrial Revolution, manufacturing companies adopt enterprise-level blockchain networks for operations and management. In order to do this, the operational efficiencies will be realized through the concepts of Smart Factories and Smart Supply Chains. Blockchain technology would play a significant role in this transformation.Blockchain characteristics are the primary role and provide a platform for various application areas for smart contractsas shown in fig.6

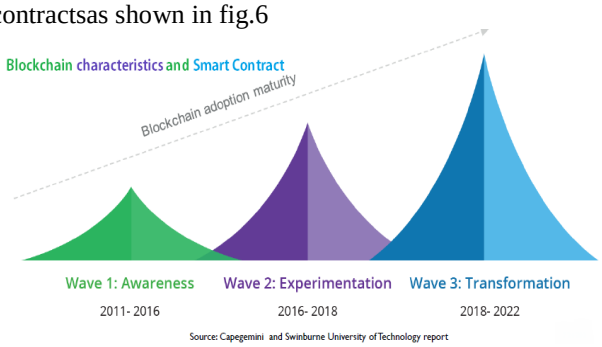



Fig.6 Blockchain characteristics

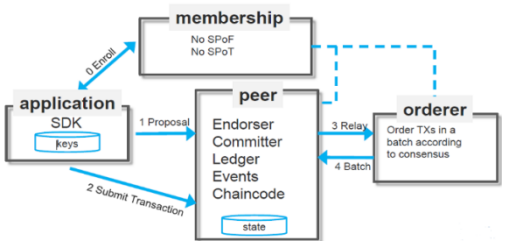



Fig.7 Hyperledger Fabric Blockchain Transaction Flow [pic source:IBM]

Blockchain Applications:The distributed ledger and smart contract are stored on all of peers of network and kept in sync. The applications of blockchain is as shown in fig.8.

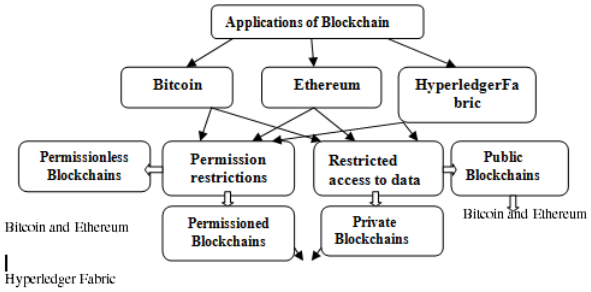


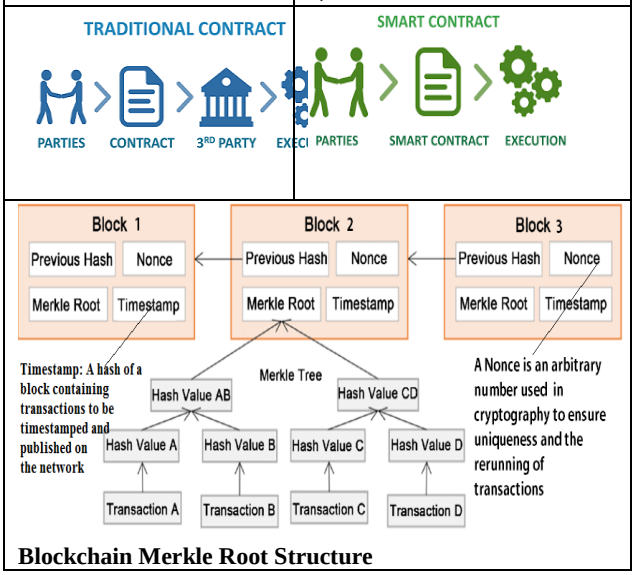

Fig.8 Blockchain Application

Most people think of bitcoin as a blockchain. But actually, bitcoin is just one of the blockchain applications. Its characteristics classify blockchain applications. Moreover, its main applications are Bitcoin, Ethereum, and Hyperledger Fabric. The basis of the creation of these applications is, in most business cases, related organizations to implement it as a consortium to

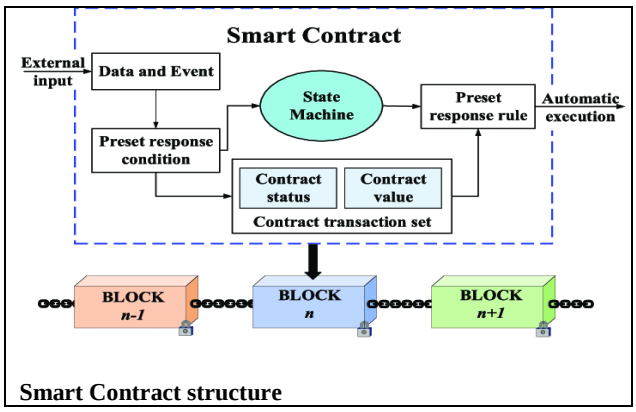
build a standard network. Moreover, this is determined by their permissions and policies agreed upon by the consortium on configuring a network infrastructure. Traditional Web applications use HTML, CSS, and JavaScript or render a webpage. This page interacts with a centralized database, where all the data is stored. In applications like Amazon, Twitter, Facebook, of Flipkart, the webpage will call an API to process and display customer data on the page. User ID and passwords are used for identification and authentication. This is a relatively low level of security since personal information is stored on the service provider's server. Were traditional Web applications use HTML, CSS, and JavaScript or render a webpage. However, Blockchain characteristics and smart contracts work on the front end of a Dapp and use the same technology to render the page. The front end contains a wallet that communicates with the blockchain. The wallet manages cryptographic keys and the blockchain address. Public key infrastructure is used for user identification and authentication. Instead of an API connecting to a database, the wallet software is used to activate smart contracts, which in their turn interact with a blockchain. Merkle Root adds each block to the network by its hash value. It also provides links to all the previous transactions done in the block. It is the hash value of the root of the Merkle tree that contains the record of all previous transactions.Table.2 shows a over view of traditional vs. block chain smart contract transaction.

**Table.2**

| Traditional websites | Web3 compatible website |
|---|---|
| **Front End → API → Database** | **Front End (including wallet) →Smart Contract →Blockchain** |




**Blockchain Merkle Root Structure**




**Smart Contract structure**

## V. CONCLUSION

Blockchain applications represent a challenge to the establishment by developing a counter-economics in industrial revolution. Their goal is money without banks, countries, and company's barriers. Cryptocurrencies intend to interact with the financial sector, decentralized applications, and various blockchain characteristics. The aim of this study discussed and formally defined the characteristics aspects of blockchain smart contract Ethereum. The users may implement a node on the Ethereum network through this protocol and join others in a decentralized, secure networking system. A smart contract can be constructed to specify and autonomously enforce interaction rules algorithmically.

## References

1.VitalikButerin, "Ethereum Whitepaper," WHITEPAPER,https://ethereum.org/en/whitepaper/ 2013

2. SA Haber, WS Stornetta Jr, "Method for secure time-stamping of digital documents." US Patent 5,136,647 1992.

3. Stuart A Haber, Wakefield S Stornetta Jr, "Method for secure time-stamping of digital documents", Publication date 995/5/30,Patent number RE34954, 1995.

4. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

5. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008, [online] Available: https://bitcoin.org/bitcoin.pdf.2008.

6. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

7. Zahra Moezkarimi, Reza Nourmohammadi, Sima Zamani, Fatemeh Abdollahei, Zahra Golmirzaei, AbuzarArabsorkhi, "An Overview on Technical

Characteristics of Blockchain Platforms", International Congress on High-Performance Computing and Big Data Analysis,pp 265-278,20 October 2019.

8. Bin Ji,LiChang,QiaDing,BinCao,LachengPang,LiyeZhu, "Design of Point-to-Point Power Mutual Transaction Between Residents Based on the Technical Characteristics of Blockchain",2020: Proceedings of 2020 International Top-Level Forum on Engineering Science and Technology Development Strategy and The 5th PURPLE MOUNTAIN FORUM (PMF2020) pp 417-432,2020.

9. Leonhard Glomann,MaximilianSchmid,NikaKitajewa,"Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective", International Conference on Applied Human Factors and Ergonomics, AHFE 2019 Advances in Artificial Intelligence, Software and Systems Engineering, pp 608-616,2019.

10. Godsiff, P.: Bitcoin: bubble or blockchain. Smart Innov. Syst. Technol. 38, 191–203,2015.

11.Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: aonymous distributed e-cash from bitcoin. In: Proceedings IEEE Symposium on Security and Privacy,2013.

12. Ethereum (2017), Solidity, https://solidity.readthedocs.io/en/develop/2017.

13 Zara Laila Abdul Hadi, Thien Wan Au,"Blockchain for the Authentication and Immutability of Academic Credentials Issued in Brunei Darussalam",International Conference on Computational Intelligence in Information System, CIIS 2021: Computational Intelligence in Information Systems pp 75-84,19 January 2021.

14. Jacob Lohmer, "Applicability of Blockchain Technology in Scheduling Resources Within Distributed Manufacturing", Logistics Management pp 89-103,2019.

15. JonaStinner, Marcel Tyrell, "The New World of Blockchain Economics: Consensus Mechanism as a Core Element," Digitalization, Digital Transformation and Sustainability in the Global Economy pp 9-19,28 July 2021.

16. Monika Kołodzie, "Development Factors of Blockchain Technology Within Banking Sector", Contemporary Trends and Challenges in Finance pp 125-138 ,12 June 2021.

17.Bernal Bernabe, J., Canovas Sanchez, J., Hernandez Ramos, J., Torres, R. and Skarmeta, A., "Privacy-preserving solutions for Blockchain: a systematic review and challenges", IEEE ACCESS, ISSN 2169-3536, 7 (1), 2019, p. 164908-164940, JRC111879, IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC https://ieeexplore.ieee.org/document /8888155 DOI 10.1109/ACCESS.2019.

18. Nick Szabo,"Formalizing and Securing Relationships on Public Networks", First Monday, Volume 2, Number 9, DOI: https://doi.org/10.5210/fm.v2i9.548, 1 September 1997 .

19. Szabo, N.(1997) The Idea of Smart Contracts. Nick Szabo's Essays, Papers, and Concise Tutorials. Available online: http://szabo.best.vwh.net/smart_contracts_idea.html, 1997.

20. N Szabo - Online at http://szabo. best. vwh. net/securetitle. html, 1998 - btc.onosendai.eu.

21. Gavin Wood,"ETHEREUM: A Secure Decentralised Generalised Transaction Ledger", Eip-150 Revision (a04ea02 - 2017-09-30),2014.

22. World Economic Forum, "The future of financial infrastructure An ambitious look at how blockchain can reshape financial services", Prepared in collaboration with Deloitte Part of the Future of Financial Services Series, August 2016,http://www3.weforum.org/docs/