JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Review of Blockchain Applications in a Variety of Fields

[1]Srinivas Vedula, [2]Mani Smaran Nair, [3]M Sumanth Sharma, [4]Amogh R Rao, [5]Varun V P

U.G. Student, Department of Computer Science and Engineering, School of Engineering
Presidency University, Bengaluru, India

Abstract: A blockchain is a distributed database of records, or public ledger, of all transactions or digital events that have been completed and shared among participants. Each transaction in the public ledger is double-checked by a majority of the system's members. Information can't be deleted once it's been entered. Every transaction ever made is recorded in the blockchain, which is certain and provable. The most well-known example of blockchain technology is Bitcoin, a decentralized peer-to-peer digital currency. Although the digital currency bitcoin is divisive, the blockchain technology that underpins it has performed well and has a wide range of uses in the financial and non-financial sectors. The basic idea is that the blockchain creates a distributed consensus system in the digital online world. By producing an irrefutable record in a public ledger, involved entities can be assured that a digital event occurred. It makes it possible to transition from a centralized to a democratic, open, and scalable digital economy. This innovative technology offers great prospects, and a revolution in this field is only getting started. This white paper introduces blockchain technology and some of its most attractive applications in the financial and non-financial sectors. Then we look at the problems and opportunities that this foundational technology, which is poised to alter our modern world, presents.

IndexTerms – Blockchain, Consensus, Immutable, Cryptographic, Cryptocurrency, Decentralization, Proof-of-work, Proof-of-stake, Smart contract.

I. INTRODUCTION

One of the biggest cybersecurity problems faced by both individual computer users and businesses is data theft, not only because it threatens an individual's privacy, but also because it undermines one of the primary purposes of cybersecurity, which is confidentiality.

Blockchain offers a fundamental shift from the traditional Internet of information and communications to the Internet of values and ensures trust-building achieved between strangers through the application of blockchain technology. This simple but revolutionary benefit is likely to spark disruptive change.

Blockchain could be viewed as a distributed digital ledger and all committed transactions are stored in a list of blocks. This chain grows if new blocks are constantly added to it. For user security and general ledger consistency, asymmetric cryptography and distributed consensus techniques were implemented. Blockchain technology generally exhibits the most important features of decentralization, persistence, anonymity, and verifiability. With these features, blockchain can significantly save costs and improve efficiency.

With the advent of contracts, blockchain technology is being applied to a wider range of business scenarios, including contract enforcement, ownership change, the Internet of things, the economy of exchange, Copyright protection, Advertising, Sharing of Data, Agriculture, and Supply Chain Management, etc. Digital Cryptocurrency is one of the prominent applications of blockchain with examples like Bitcoin and Ethereum. Blockchains can address the growing interest of customers, governments and non-governmental organizations in greater transparency of their organizations.

Blockchain is ideal for providing this information because it provides instant, shared, and completely transparent information that is stored in an immutable ledger that can only be accessed by authorized members of the network. With a blockchain network, users can track everything from orders to payments, accounts to production. And since members share a unified view of the truth, you can see all the details of a transaction consistently, giving you more confidence, as well as new efficiencies and opportunities.
Integration of previously existing tools can help increase the authenticity and security of these data. Blockchain technology guarantees the authenticity and security of the data necessary for immutable transactions.
This paper investigates applications that can combine blockchain technology and the aim is to study the feasibility of integration of blockchain technology in various fields and stages of different real-world use cases.

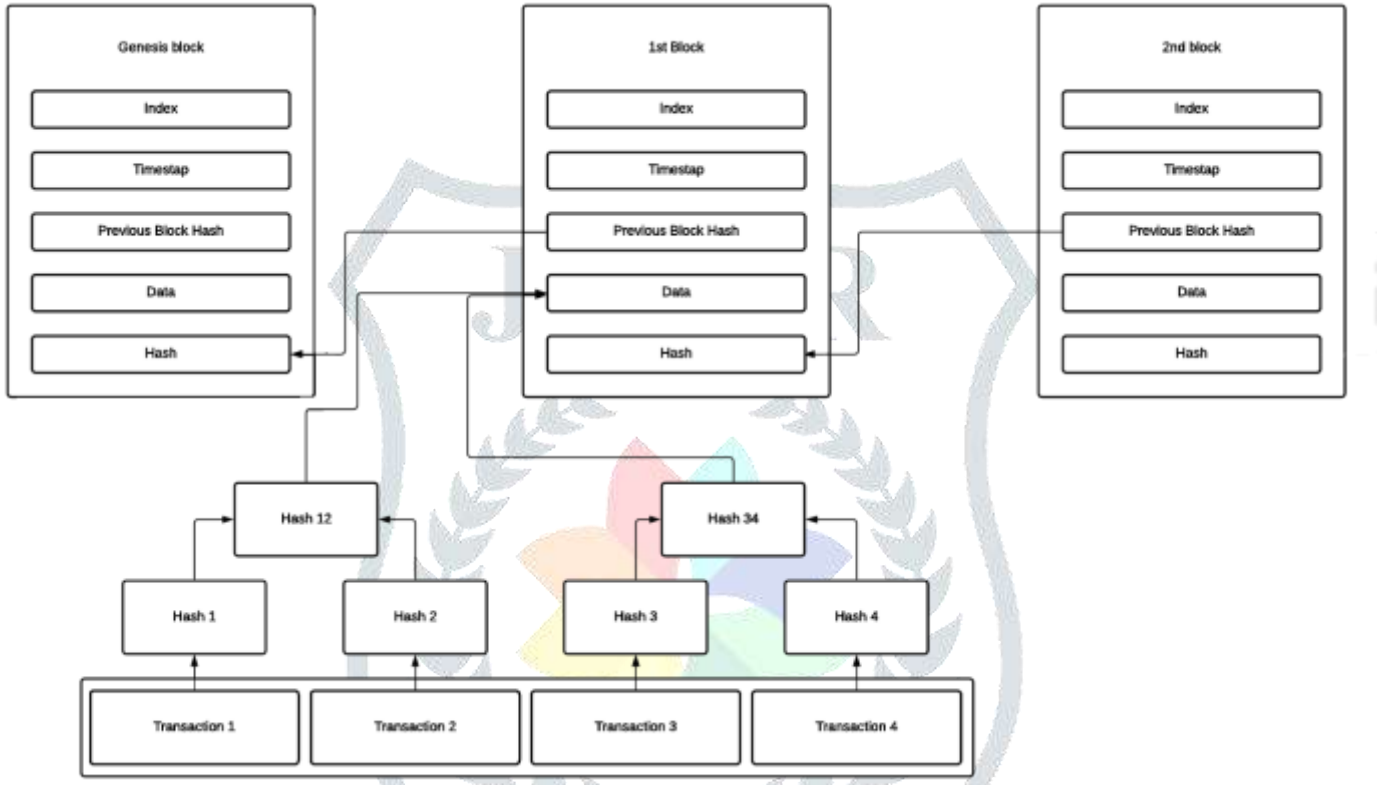
II. LITERATURE REVIEW

Blockchains are digitally distributed ledgers or databases of records, transactions, or completed events that are shared across the participating parties. Each transaction in the system is time-stamped and validated by a consensus of a majority of participants in the system. [4]

Every blockchain is made of Blocks. Each block contains a cryptographic hash function block, a timestamp, and the Merkle tree is commonly used to represent sale data. In order to get into the hash of the block, the timestamp shows that the transaction data existed when it was published.

Blockchains are normally managed by a peer-to-peer network for use as an intimately distributed expense, where nodules inclusively hew to a protocol to communicate and validate new blocks. Although blockchain records aren't inflexible as setups are possible, blockchains may be considered secure by design and illustrate a distributed computing system with high Baroque fault forbearance.

Table 2.1. Block diagram of Blockchain



Nodes - Nodes are any unit or computer that processes and verifies transactions on the blockchain network. Each node has a replicated copy of the entire blockchain database that contains all the details of a transaction. When multiple nodes have similar transaction details in their database, it is known as consensus. [31]

Blocks - Blocks are the components that group a series of transactions and distribute them to each node of a blockchain network. Each block consists of metadata and some transactions or any other data. A block is added to the blockchain when a consensus is reached. [31]

Metadata of a block may contain -

2.1. Hash of the previous block
2.2. Time of creation
2.3. Transaction, data, or smart contracts
2.4. Hash of the current block

Consensus - Consensus is the process of evaluating and verifying the authenticity of blocks before they are added to the blockchain. Consensus rules ensure that the single-node database copy in the blockchain environment is consistent with each other and is also the most up-to-date. Different types of blockchains employ different types of consensus algorithms based on their requirements. Example Bitcoin uses “Proof-of-Work”. Some other consensus algorithms are “Proof-of-Stake”, “Proof-of-Ownership” etc. [31]

III. TYPES OF BLOCKCHAINS

Public Blockchain, Private Blockchain, Hybrid Blockchain

Public blockchains - A fully decentralized blockchain with no central authority. "Proof-of-work" or "Proof-of-stake" is used to ensure record authenticity. Public blockchains are completely open to all. Users who have an Internet connection can use it to send transactions as well as become validators. [18]

Private blockchains - Permission has been granted to create a private blockchain. To control and assure record validity, a central authority serves as a trusted middleman. It is only open to those who have been invited by the network administrators. Validators and participants have restricted access. [18]

Hybrid blockchains - By merging centralized and decentralized blockchains, a hybrid blockchain provides the benefits of both. The record authenticity is controlled by a consortium of entities, which is semi-centralized. [18]

Table 3.1: Overview of common types of blockchain

Type	Public	Private	Hybrid/Consortium
Consensus/Permission	Read and Write access for anyone	Read and Write access for a single organization	Read and Write access for a group of organizations
Data storage	Record is distributed to all users of the peer-to-peer network	Records are stored by the central authority	Records are distributed throughout the consortium/ group of organizations
Advantages	Fully Decentralized Fully Immutable Transparent	Access Control Low Transaction Cost High Transaction Speed Scalable	Access Control Low Transaction Cost High Transaction Speed Scalable
Disadvantages	High Transaction Cost Low Transaction Speed Low Scalability	Partially Decentralized Partially Immutable Transparency	Partially Decentralized Partially Immutable Transparency
Use Cases	Cryptocurrencies Document Verification	Supply Chain Governmental Services	Medical Records Real Estate Records Supply Chain

Distributed ledger - The distributed ledger and its immutable transaction records are accessible to all network participants. Transactions are only recorded once with this single ledger, avoiding the twofold overhead that is typical of traditional corporate networks. [4]

Immutable records - After a transaction has been uploaded to the shared ledger, no participant can change or alter it. If a mistake is found in a transaction log, a new transaction must be added to correct the problem, and both transactions will be viewable. [4]

Smart contracts - A smart contract is a transaction log that is designed to execute, control, or document legally significant events and activities in accordance with the provisions of a contract or agreement automatically. Furthermore, they are unchangeable, ensuring that neither party may alter the agreements. [31]

IV. METHODOLOGY AND EXPERIMENTATION

4.1. Copyright protection

Copyright difficulties have accompanied the growth of the Internet on a regular basis. Copyrights have not always been respected, from peer-to-peer file-sharing programs like [23] Napster and Grokster [24] to images on the Internet. Copyrights are frequently neglected or attacked from the perspective of a file owner. As a result, unauthorized (and illegal) file-sharing and the use of copyrighted content continue to be major issues. Blockchain technology has now shed some light on the situation. Blockchain is a distributed digital ledger that is decentralized. Because a file is copied thousands of times across the network, this network is designed to update and reconfigure on a regular basis.

Given that a file may be duplicated thousands of times across the network, this network is designed to update and reconcile all copies on a regular basis to ensure that all records are accurate. The blockchain is not controlled by a single machine or entity. It's nearly impossible to alter or corrupt due to the lack of a central storage site. All changes made to the ledger, starting with the basic record, are irreversible.

As a result, anytime a copyrighted material is illegally utilized, a digital ledger including the owner's details as well as a detailed transaction history is made really public and easily provable. Take, for example, photos found on the internet. One of the most difficult aspects of copyright protection is controlling the use of photographs based on who uploads them to the internet. Platforms are cropping up to enable mechanisms for photographers to upload their photographs to a blockchain, which includes not only services of ownership authentication, but also a way to regulate unauthorized usage. [27]

Binded, for example, bills itself as "the world's first copyright platform" for blockchain, claiming that each copyright record has a "unique fingerprint (cryptographic hash)." Binded promotes copyright protection by enabling access to the circulation channel of copyright knowledge via blockchain by tracking copyright records. Photograph owners can police online sites that use them,

including media platforms like Instagram and Twitter, with a digital fingerprint at their fingers. Other blockchain-based copyright platforms, such as [28] copytrack, are also available.
However, copyright protection with blockchain has some limits. Initial authentication in uploads is one of the questions. That is, how can you prove ownership of an image when a user submits it? Other challenges, such as the difficulties in monitoring the license usage of anonymous and untraceable customers, must be addressed.

4.2. Advertising

The blockchain is a perfect fit for the digital advertising supply chain since it is a distributed, immutable, and transparent record. Advertisement fraud, inefficiency, and lack of transparency have always been major challenges that need to be addressed in digital advertising. We can dramatically enhance efficiency and transparency, decrease expenses, and prevent fraud with the use of blockchains. In 2017, advertisers spent $209 [19] billion on digital advertising worldwide.
Many firms have been actively developing blockchain-based advertising solutions in the last two years, fueled by a substantial infusion of venture funding. MetaX [20], a blockchain firm, promises to use blockchain technology to address concerns of fraud and lack of transparency in digital advertising. Some applications have been built with the intention of being tested by the general population. One of these programs is Ads.txt Plus, which is open-source software that is aimed to root out fraudulent vendors and resellers across the programmatic supply chain. Premium [21], a TEGNA branch that is a leading over-the-top (OTT) advertising platform, has teamed up with technological business.
MadHive is working on a blockchain-grounded OTT sale platform. MadHive has established MAD Network at the same time, with a far broader ambition for blockchain in OTT. Birse establishes confidence between all mates in the advertising value chain as blockchain bumps as a decentralized operation. One of the biggest MVPDs (Multichannel Video Programming Distributors) can apply blockchain technology in decoration digital channels and videotape give chains, grease marketers, inventors, and drivers to arrange, target, and report on announcement buys across digital, broadcast, and streaming.
The blockchain can improve the consumer's user experience in addition to improving quantitative measures. Marketers can now create customer profiles straight from customers, obtaining all of the information they are prepared to contribute in a single transaction, thanks to the blockchain. Without the need for intermediaries, peer-to-peer contact allows firms to communicate directly with customers and make the most of their data. Customers include those who pay with actual money or tokens in exchange for goods or services, as well as those who pay with their time and attention. All of the aforementioned factors aid in the enhancement of any company's marketing strategy. In general, it's a Turing-complete, decentralized, distributed system. The expansion of the digital advertising sector will be considerably aided by a robust blockchain network.

4.3. Society Applications

Smart contracts, the next-generation network infrastructure aimed at resolving financial issues, have the potential to upend traditional borrowing agreements. The lender in a typical lending relationship not only gives money but also accepts risks, which leads to high loan interest and the mortgage of commodities, with the value of a goods mortgage sometimes exceeding the loan amount.
Borrowers can utilize virtual assets as collateral in smart contracts to avoid discounts on physical things while simultaneously lowering lending rates. There is no need to provide the lender's credit or employment history, as well as a slew of other documentation. The property is stored on the blockchain and can be accessed by anyone.

4.4. Car/smartphone

An automobile key with an anti-theft device, for example, can only be triggered by selecting the appropriate protocol on the key. The smartphone will only work if the password is entered correctly. To safeguard ownership, they are all devoted to encryption technology. The issue with the original version of intellectual property is that the key is held in a physical container that is difficult to transfer or copy. By allowing blockchain miners to update and copy lost protocols, the blockchain ledger overcomes this problem.
Copyright difficulties have plagued music publishers throughout history, including the recording age and the digital music era. This challenge can be solved by using blockchain and smart contracts to create a traceable music copyright database. Furthermore, as consumer behavior occurs, you can transmit revenue to both the copyright owner and the musician in real-time. Music fans have the option of paying in digital currency.
In the 2016 U.S. election, both Democrats and Republicans questioned the security of the voting system. Each individual may view his vote and the whole statistical procedure thanks to blockchain and smart contracts. Furthermore, the verification of the flow of cash consumes a substantial percentage of the annual government budget, and the implementation of blockchain technology can greatly simplify the procedure. Companies, organizations, government entities, and individual people can self-manage blockchain by offering a platform. Individuals can use blockchain to ensure that their wishes are carried out.

4.5. Reputation System

A person's reputation is a significant indicator of how much the community trusts them. Such a system is useful for evaluating a person's reputation, which is based on his or her previous transactions and contacts with the community. The credit system is similar to a reputation system in that users are assigned credit scores based on their financial activity, which are then used to make decisions about other financial transactions. If the integrity of the data is compromised, the system can be tampered with. As a result, it's critical to preserve a secure record of previous transactions and accurately assess the users' reputation.

4.6. Blockchain Music

Owning products via ownership rights and benefiting from royalty distribution is a big difficulty in the music industry. Ownership rights are necessary to commercialize digital music items.
The Blockchain and smart contracts technologies can be utilized to construct a decentralized database of music rights that is complete and accurate. [30] Meanwhile, the ledger may be utilized to offer all of the labels involved with transparent information on artist royalties and real-time disbursements. Digital money can be used to make payments in accordance with contract requirements.

V. RESULTS AND DISCUSSIONS

Blockchain has the potential to transform the way companies do business and act as a catalyst for new supply chain models. Although technology has many uses, it is only just starting to develop. Therefore, there are many ways that companies can gain a competitive advantage by leveraging this technology earlier and better than the competition and by changing their market positioning.

Blockchain can increase supply chain transparency and reduce costs and risks throughout the supply chain. Additionally, companies can maintain greater control over outsourced contract manufacturing. Blockchain provides access to the same information to all participants in a supply chain, potentially minimizing communication and transmission mistakes. More time can be focused on providing goods and services rather than confirming data.
Blockchain supply chain innovations can offer the following main benefits:
Possible Benefits -

- To guarantee that company standards are met, improve material supply chain traceability.
- Reduce losses from counterfeiting/trade gray market
- Improve transparency and compliance of outsourced contract manufacturing
- Reduce paperwork and administrative costs
- Strengthen company reputation through visibility of materials used in products
- Improve credibility and public trust in shared data
- Reduce potential public relations risk of misconduct in the supply chain

Blockchain can be used in elections to increase transparency and build trust between the government and its citizens. Its characteristics such as immutability and transparency can ensure that voices are manipulated. It is also used in other records, such as the state budget and government spending, which can be stored on a blockchain to reduce corruption. Implementing the blockchain in government records can benefit both the government and citizens.

Advantages of blockchain technology in general:

- Time-saving: No verification by a central authority is required for billing, making the process faster and cheaper.
- Cost Savings - A blockchain network reduces costs in several ways. No third-party verification is required. Participants can share assets directly. The intermediaries are reduced. The overhead of the transaction is minimized because each participant has a copy of the common ledger.
- Increased security: no one can handle the data on the blockchain, as it is shared by millions of participants.

VI. CONCLUSION

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistence, anonymity, and audibility. In this paper, we present a comprehensive overview of the blockchain. We begin by providing an overview of blockchain technologies, including their architecture and fundamental properties.

REFERENCES

[1]. Michael Crosby, Nachiappan, Pradhan Pattanayak,Sanjeev Verma, Vignesh Kalyanaraman, "Blockchain Technology" (2015) https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
[2]. Morgen Peck, "Reinforcing the links of the blockchain" (2017) https://blockchain.ieee.org/images/files/pdf/ieee-future-directions-blockchain-white-paper.pdf
[3]. 2018. Proceedings of the 2018 International Conference on Blockchain Technology and Application. Association for Computing Machinery, New York, NY, USA.
[4]. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85. G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," 2015.
[5]. Tsilidou, Anna & Foroglou, Georgios. (2015). Further applications of the blockchain.
[6]. Kosba, Ahmed E., Andrew K. Miller, Elaine Shi, Zikai Wen and Charalampos Papamanthou. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts." 2016 IEEE Symposium on Security and Privacy (SP) (2016): 839-858.
[7]. Akins, Benjamin & Chapman, Jennifer & Gordon, Jason. (2015). A Whole New World: Income Tax Considerations of the Bitcoin Economy. Pittsburgh Tax Review. 12. 10.5195/taxreview.2014.32.
[8]. Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," 2015 18th International Conference on Intelligence in Next Generation Networks, 2015, pp. 184-191, doi: 10.1109/ICIN.2015.7073830.
[9]. Sharples, Mike & Domingue, John. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. 9891. 490-496. 10.1007/978-3-319-45153-4_48.
[10]. Noyes, Charles. (2016). BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning.
[11]. Eyal, Ittay & Sirer, Emin. (2013). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. 8437. 10.1007/978-3-662-45472-5_28.
[12]. Biryukov, Alex & Khovratovich, Dmitry & Pustogarov, Ivan. (2014). Deanonymisation of Clients in Bitcoin P2P Network. Proceedings of the ACM Conference on Computer and Communications Security. 10.1145/2660267.2660379.
[13]. F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, thirdquarter 2016, doi: 10.1109/COMST.2016.2535718.
[14]. "Survey on Blockchain Technologies and Related Services FY2015 Report." (2016).

[15]. Lee Kuo Chuen, David, (2015), Handbook of Digital Currency, 1 ed.,Elsevier, https://EconPapers.repec.org/RePEc:eee:monogr:9780128021170.
[16]. Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform." (2015).
[17]. Johnson, D., Menezes, A. & Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA). IJIS 1, 36–63 (2001). https://doi.org/10.1007/s102070100002
[18]. V. Buterin, "On public and private blockchains," 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
[19]. The AdChain Registry. https://adtoken.com/uploads/white-paper.pdf
[20]. Napster and grokster https://www.recode.net/2017/12/4/16733460/2017-digitalAd-spend-advertising-beat-tv.com/ethereum/wiki/wiki/Consortium-Chain-Development
[21]. Blockchain for Video Advertising: A Market Snapshot of Publisher and Buyer Use Cases https://www.iab.com/wp content/uploads/2018/02/Blockchain_for_Video_Advertising-Publisher-Buyer_Use_Cases_2018-02.pdf
[22]. King, Sunny and Scott Nadal. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake." (2012).
[23]. Blockchain in copyright 'https://us.napster.com/
[24]. Blockchain in copyright http://www.grokster.com/
[25]. J. Kwon "Tendermint: Consensus without mining 2014" https://tendermint.com/static/docs/tendermint.pdf
[26]. https://binded.com/
[27]. http://www.copytrack.com/
[28]. C. Miguel and L. Barbara, "Practical byzantine fault tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp. 173–186
[29]. Mazières, David. "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus." (2015).
[30]. A survey of Blockchain Applications in Different domain International Conference on Blockchain Technology and Applications (ICBTA) 2018, December 10–12, 2018, Xi'an, China.
[31]. BlockChain Technology Sutardja Center for Entrepreneurship & Technology Technical Report, 2015 https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf