International Conference - Innovation-2021-Innovation-2021
International Journal of Scientific Research in Computer Science, Engineering and Information Technology ISSN : 2456-3307 (www.ijsrcseit.com)
Volume 8, Issue 3, May-June-2021

A Review on Blockchain Technology and It's Applications

[1] Gajanan P. Arsalwad, [2]Dr. Sohel A. Bhura, [3]Dr. Suresh S. Asole
[1,2,3]Babasaheb Naik College of Engineering, Pusad, Maharashtra, India

ABSTRACT

In the annals of technology, blockchain is generating levels of excitement and anticipation that have never been witnessed before. It's being hailed as the next big thing in technology, one that will change the world just as much (if not more) as the wheel, the steam engine, or the Internet. According to research published by the World Economic Forum in September 2018, 60% of respondents believed that by 2030, Blockchain technology will be used to store 10% of global GDP. As a result, it's not unexpected that Blockchain is attracting a large number of investors who are pouring money into Blockchain firms. Nearly $450 million was invested in 2016, and that number is only expected to rise. However, the methods, goals, and possibilities of Blockchain are still completely unknown to the general public.

Keywords: GDP, Blockchain technology

I. INTRODUCTION

There are two primary architectural styles that may be applied to a software system: centralised and distributed [1]. In a centralised system, all of the nodes are grouped together and linked to a single hub. In contrast, distributed systems consist of a collection of interconnected nodes that are not governed by a single entity. The differences between these two layouts are seen in Fig. 1. A distributed system's advantages include enhanced computational power from pooling the resources of all linked nodes, more dependability from the lack of a single point of failure, and so on. However, a distributed system has a number of downsides, such as communication cost and security risks linked to abuse of the network by untrustworthy nodes. On the other hand, blockchain technology may be thought of as operating at the system-level implementation layer in a distributed software architecture. Blockchain is a tool that may be used to establish and preserve data integrity in decentralised systems [2]. In addition, each node in a blockchain network may be thought of as a node in a decentralised peer-to-peer system. In P2P networks, malevolent peers pose the greatest risk to data security. Because there may be unreliable or untrustworthy peers in the system, nodes attempt to gain an advantage for themselves [3]. Therefore, blockchain technology is essential to addressing these pressing issues. Nakamoto [4] created Bitcoin, the first cryptocurrency, and the blockchain technology upon which Bitcoin is based. In situations where users do not trust each other or if there are unreliable users in the network, it allows trustless and reliable transactions without the need for centralised administration. Since then, blockchain's ability to serve as a decentralised transaction log that may be used to record and confirm financial transactions and to distribute contracts has garnered considerable interest. In addition to its use in the financial industry, blockchain technology has found its way into other industries, including as healthcare, utilities, real estate, and the public sector [5]. Because the blockchain architecture created for Bitcoin may be copied and expanded upon, they are discovered to be practical. At first, blockchain's primary use was in bridging the gap between digital currencies and traditional financial institutions. Using blockchain technology, banks may conduct transactions directly amongst themselves, bypassing the need for middlemen and central agencies. Over 50% of all nodes in the network consensus are required to approve a transaction before it can be processed [6]. This ensures that no user may alter blockchain data without the consent of the network as a whole. Insight into blockchain technology and its present practical applications is the focus of this study. This study provides a comprehensive taxonomy of the many types of scholarly publications (books, articles, conference proceedings, technical reports, etc.) that may be found in the literature. Multiple papers, such as [7], [8], [9], and [10], have reviewed the research done on blockchain technology. However, a thorough consideration of the many potential uses of blockchain technology has been largely ignored in previous research.

II. Blockchain Technology

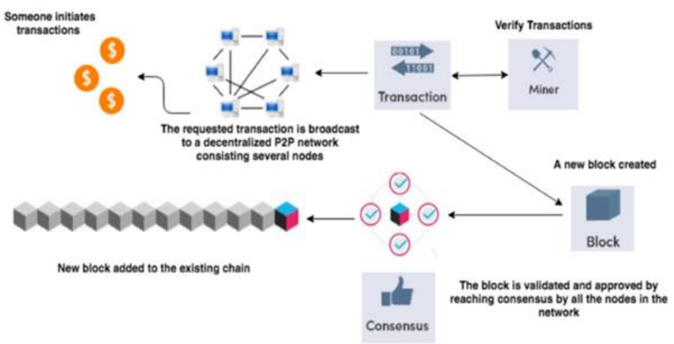

Fig 3: Blockchain Network

Block: The Blockchain is formed as a sequence of blocks, where all transaction information is stored, which can be considered as a public ledger. All blocks are inter- linked using a reference hash, which belongs to the previous block known as the parent block. The very first block in the chain is called the genesis block, which does not have any parent block. The Block Header consist of elements as follows [11]

Header Attributes	Definition
Block Version	Indicates which set of block validation rules to follow.
Previous Block Hash	A 256-bit hash value that points to the previous block.
Merkle tree root	The hash value of all the transactions in the block.
Timestamps	Current timestamp as seconds since 1970-01-01T00:00 UTC.
nBits	Current hashing target in a compact format.
Nonce	A 4-byte field, which usually starts with 0 and increases for every hash calculation.

Fig 4 : Block Header Elements

A. **Proof-of-Work (PoW):** Proof-of-Work works as mechanism of consensus, which scales over 1000 of nodes. It requires the initiator to solve a puzzle, a mathematical or cryptographic operation by brute forcing and to produce a value (also called wining value), which is less than a defined one as set forth by the network. At times, more than one node produces winning value at the same time to add block and thereafter ask for reward. This situation creates a fork and is resolved by the network by analyzing the maximum value of prove-of-work i.e. maximum work done by a node. [12]

B. **Proof-of-Stake (PoS)**: Proof-of-Stake replaces the mining mechanism of the PoWmodel which consumes power in abundance. Instead of e.g. purchasing equipment to generate wining values, PoS suggests to purchase cryptocurrency and use the same to buy chances of block creation in Blockchain. [13]

C. **Smart Contracts:** It is a chain of codes that are executed in the Blockchain environment which consist of conditions or rules for different parties to follow the terms between the nodes orusers in the network. Smart contract can be developed in the Blockchain platform using any supported programming languages. [14]

D. **Mining:** Miners use blocks of nonce values to achieve hash values in the network. Thisrequires high computation speed to achieve and obtain the reward.

E. **Decentralization:** By storing data across its network, the Blockchain eliminates the risks that come in by holding it centrally. The decentralized Blockchain may use ad-hoc message passingand distributed networking. [15]

III. Blockchain Applications

A. Internet of Things (IoT)

The Internet of Things (IoT) is a term used by the International Telecommunication Union [16] to describe a network of many Internet-connected physical things (20 billion by 2020, according to Gartner [17]). Internet-connected sensors collect data from their environments and exchange data with one another and with computer programmes. They generate a mountain of data as a byproduct of their intensive cooperation, which may then be put to good use by the dependent services that rely on it. These services are helpful, but they may also cause serious privacy concerns. This is due to the fact that people's tastes and habits may be easily gleaned from the data that is sent between their various gadgets. People's privacy is especially at risk when such sensitive data are managed by centralised companies that can make an illegitimate use of them; for example, Edward Snowden's revelations revealed that data stored by Internet and telecommunication companies have been exploited within a mass surveillance programme, namely the PRISM programme [18]. To avoid this, our study aims to promote a decentralised and private-by-design IoT, where confidentiality is built into the very architecture of the connected devices themselves. We think this is possible with the implementation of P2P networks. Particularly, the blockchain may be indispensable in developing such confidential Internet of Things. The blockchain is a distributed ledger originally used for financial transactions with the Bitcoin cryptocurrency [19]. It can't be altered and only includes genuine data; moreover, being decentralised and peer-to-peer makes it immune to censorship. Because of these factors, virtual currencies are just one of many potential uses for blockchain technology. A discreet structure. The integration of the blockchain with a P2P file sharing system may help to promote IoT. The P2P aspect of such a storage system might assure privacy, resilience, and the lack of single points of failure for sensitive data created and shared across IoT devices. In tandem with this data repository, the blockchain plays a crucial part in verifying the integrity of all transactions involving information from Internet of Things (IoT) devices. Since the blockchain records any change made to data (whether it be creation, alteration, or deletion), it may be possible to identify any data misuse. In addition, the blockchain may be programmed to adhere to a set of access controls that restrict who can make changes to its records and when. With this infrastructure in place, users won't have to give up control of the information generated by their Internet of Things (IoT) gadgets to a few large corporations; instead, data can be securely stored in various peers, with blockchain guaranteeing their authenticity and preventing unauthorised access.

B. Healthcare

Data, including health data supplied by patients, is the new gold. Medical research may benefit greatly from the massive influx of data generated by the proliferation of health applications and health wearables throughout the globe. Several uses cases exist for blockchain technology in the realm of patient-generated health data [20]. To provide just one example, healthbank, a worldwide Swiss digital health firm, approaches data transactions and the exchange of personal health data in a completely novel way. This new company provides its customers with a place to safely save and organise their medical records [21]. The user has complete control over their data. Healthbank's next step is to fully adopt and use Blockchain technology inside the core business concept [22]. Future patient-generated health data (such as heart rate, blood pressure, medications taken, sleeping patterns, eating habits, etc.) will be obtained through health applications, wearables, or doctor visits using Blockchain and safely stored in the healthbank Blockchain. People who utilise healthbanks nowadays may not only save their data there, but also make it accessible for scientific study. They are compensated monetarily for their participation in the study. Healthbank transforms into a one-of-a-kind data trading platform, opening up exciting prospects for patient-centric studies (e.g., in clinical trials for the pharmaceutical industry, in academic research projects at universities, etc.). Using Blockchain, this approach might be even more customised by allowing researchers to keep track of their own unique, patient-generated health data with a timestamp (similar to the stated Bitcoin transaction) [23]. Users of a health data bank who have made exceptional contributions to the achievement of medical research initiatives may be singled out using Blockchain and paid more handsomely than usual. With the rise of digitization, new digital business models, and digital health initiatives, Healthbank has become a symbol of end user / patient empowerment in healthcare. Patient and consumer autonomy in healthcare will get a further boost from blockchain technology.

C. Intelligent Transportation Systems

Recent years have seen tremendous academic efforts and industry growth in intelligent transportation systems(ITS)[24], influencing every aspect of our lives with smarter transport facilities and vehicles, as well as safer and more convenient transport services. This is due to the rapid development of modern sensing, communicating, analysing, and computing techniques and devices. But today's ITSs have shown a high-degree of social complexity rather than the expected intelligence, thanks to the growing uncertainty, diversity, and complexity of behaviour, mechanisms, and strategies in this ecosystem, which has resulted in the perpetuation or even worsening of many long-standing problems. The growing centralization of ITSs is a major reason for concern because of the security threats it poses. Most of the data, analyses, and decisions that make up ITSs are processed by centralised authorities or cloud-based platforms, which can be thought of as their "Achilles' heel" because they are vulnerable to being temporarily unavailable due to malicious attacks, performance limitations, or improper operations, thanks to the rapid development of technologies like the Internet of Things (IoT) and cloud computing. The second problem is that there isn't enough trust between different ITS organisations. As a consequence, ITSs have hierarchical structures, diverse procedures, and greater social complexity since money and assets cannot "flow" easily and directly from one entity to another without trusted middlemen. In the real world, ITS professionals often work to create both novel physical infrastructure (like roads) and intelligent technological tools (e.g, cameras, self-driving cars). The emphasis of ITS literature[27] has shifted from transportation management and surveillance to vehicle and vision-related subjects in recent years, mirroring this trend in reality. In the grand scheme of things, these demand-driven solutions will unquestionably play a vital part in increasing ITSs' "intelligence," but they are still far from adequate to cope with such basic challenges as security, trust, and the resulting societal complexity. We believe that without solid foundations of safety and trust, the newly emergent high-level intelligence is likely to be shaky and false. Therefore, from a research standpoint, in order to aid the ITS ecosystem in maintaining its overall stability, profitability, and efficacy, there is a crucial need to develop a secured, trusted, and decentralised architecture so as to realise the smooth, intermediatory-free flow of data, money, and assets among ITS entities, and thus constructing a more robust ITS ecosystem by making more efficient use of the supply-existing side's legacy infrastructure and resources. However, there is a severe lack of academic publications exploring this topic.

D. Financial Blockchains

A centralised system is one in which only one copy of the ledger exists. To clear over the central bank's accounts, for instance, many commercial banks must presently travel to their central banks. Central banks can handle them quickly and simply, so they are efficient and easy to control. However, this rigidity leads to islands of liquidity and collateral that cannot be moved around or traded with one another. Therefore, economies, banks, or firms with global operations are susceptible to shocks because a lack of liquidity in one location may cause a chain reaction elsewhere. Due to the sensitive nature of SIPS, the central banking system has to be completely trustworthy and dependable. The current CSD (Central Securities Depository) is an example of a centralised system that provides real-time settlement and efficient operations [25]. Because of the necessity to execute consensus procedures and store data numerous times, the cost of communicating, computing, and storing when many copies of a ledger are created is high. Due to the high volume of financial transactions, these processes come at a high cost. And because many of these protocols need sequential execution, even greater processing power and/or data transfer capacity will not improve their efficiency. Having numerous copies, however, improves the system's security and dependability. Byzantine protocols, for instance, often allow for the failure of a third of nodes in a BC before the system fails [26]. If you know the chance of a node failing and the total number of nodes in the BC, you may estimate how long it will take for the BC to fail. On the horizontal axis is the total number of nodes, and on the vertical axis is the amount of years it takes for more than one-third of those nodes to fail.

E. Digital Currency

It's been a problem that this keeps happening. To minimise the potential for payment systemic risk and guarantee the highest standards of operation, central banks focus on a number of different factors [27]. European Banking Association (EBA) has claimed that a distributed ledger may or may not result in a digital currency, but it may instead include digital references to assets like readily accessible cash liquidity, equities, and bonds. Distributed ledgers allow settlement to take place in these scenarios via the use of a consensus-based reallocation of the balance. Thus, issuance of digital money is feasible, and settlement may take place with other digital assets like tokens representing fiat cash, anything of value like airline miles, or community tokens for charitable donations. If a BC has these resources, it can settle not just digital currency transactions, but also those involving foreign exchange, remittances, real-time payments, documentary commerce, and asset servicing [28].

F. Secure Communication

One potential negative of blockchain solutions is that the content of all transaction records is visible to every node in the network. This may discourage some consumers from switching to a blockchain-based solution from an existing one. Confidentiality is compromised far more so than in traditional systems, and especially in centralised ones, where all requests for database material are sent to the database administrators. Public blockchains, which employ a public ledger, are accessible to everyone with Internet connection, unlike centralised or distributed databases, which may better protect user privacy by restricting access based on a predetermined set of criteria. Nonetheless, there are ideas to overcome this issue, such as using a combination of blockchain addresses and zero-knowledge proofs to provide privacy [29]. These other solutions inevitably come with their own set of problems, such as making blockchain more difficult to use or less scalable. When it comes to computing speed, centralised systems and older systems are undoubtedly better. Keep in mind that all blockchain transactions are completed in a decentralised, peer-to-peer manner, with records secured by public-key encryption. The computational burden of this operation is eliminated when stored in a centralised database. Furthermore, the blockchain's mining process and the miners' consensus mechanism are not present in legacy systems. These processes, which take minutes to complete on average owing to ledger size and network latency, are essential to the blockchain's functioning. In [30], the authors argue that it is a semantic error to describe blockchain as just a shared database, and that it is better understood as a technology that makes possible a new class of shared databases. Is there anything that blockchain (as a distributed database) can do that other (distributed) databases can't? A database is a collection of data that has been arranged in accordance with a set of rules and standards pertaining to the way in which the data must be stored, in particular with regard to consistency. A transaction is a set of instructions that modifies data in accordance with defined parameters and policies. If the conditions are not met, the transaction is denied. However, the trust issue that arises when numerous nodes do not trust each other is not addressed by such database management rules. Companies in the same competitive market, for instance, may be hesitant to trust one another while using a distributed data ledger. Strong consistency policy can control any writing conflicts caused by P2P replication or multi-master replication [31], but this comes at the cost of delay. By maintaining strong consistent duplication and switching solely to the unique master copy, with backup copies under eventual consistency, a high availability distributed database can stay up to date with little impact on server latency. However, the fact that there is only a single master copy is itself the limiting factor. Blockchain technology, on the other hand, allows for greater availability since numerous copies are saved on separate entities, but consistency is relegated to a lower priority until it is given by consensus.

G. Business and Industry

The introduction of IoT has provided various benefits, including the delivery of a link between inanimate items and people. For this reason, the authors in [32] suggest an e-business architecture tailored specifically to the Internet of Things. For this reason, we will use the concept of a distributed autonomous corporation (DAC) to provide transaction services without the need for intermediaries. Bitcoin and IoTcoin are used as the currency and exchange certificate, respectively, and constitute the backbone of the proposed system, which is based on a transaction mode in which peer to peer transaction is completed autonomously. In proposing a system to track agri-food products using RFID and blockchain technologies, the authors [35] factor in the significance of food safety and quality. Assuring the veracity of information that is distributed and published is a primary motivation for using blockchain technology. In addition, the concept of "smart manufacturing" in the age of Industry 4.0 is addressed at length in [36] [34]. The 4.0 industrial revolution is characterised by the widespread availability of goods and services through digital networking technologies such as blockchain. Industry 4.0 aims to realise the conditions of decentralisation and self-regulation in supply chain management. So-called fog computing or edge computing is a recent expansion of cloud computing that has piqued the interest of writers interested in creating a decentralised, Bitcoin-based payment system [35]. Fog computing is a massive, pervasive, and distributed network that can handle any kind of computer activity. The suggested method is set up to better the conventional e-cash system, which requires a trusted authority, i.e. bank, to produce payment tokens. By using Bitcoin-based payments, fog users (outsourcers) may send money to fog nodes (workers) without going through any kind of middleman. The authors of the paper claim that, whether the outsourcers are evil or not, their suggested method would guarantee payment for all completed jobs done by honest employees.

H. e-voting

Meeting basic human needs with the aid of technology is now normal. Most people nowadays don't trust their leaders, which makes elections crucial in contemporary democracies [36]. The rising use of technology has introduced new problems to the process of democracy. Votes cast in an election may profoundly affect the direction of a country or a company. As a representational democracy, the primary function of elections is to direct the will of the people. After a catastrophe, if a voter's preferred ballot option is still on the ballot, the committee will offer a vote for the choice of botanical sound votes produced by voting in the choice of letter sound, and the voter should then fold the ballot and place it in the ballot box. In most elections, tallying the votes may take anywhere from three to seven business days [37] depending on how quickly the news travels up the chain of command. Whether or not a certain vote is included in the overall tally. Data manipulation, security, and transparency issues are the most common problems during elections. The collecting procedure and its complexities have grown in importance with the advent of new technologies [38]. The safety of an electronic voting system is always a primary issue. No electronic voting system should be vulnerable to hacking and should be able to keep voter information confidential. The usage of blockchain technology is one approach that may be used to alleviate voting-related concerns. In order to secure Bitcoin transactions, blockchain technology has been used in database systems [39]. Blockchain is a distributed, immutable, and transparent ledger that can't lie [40]. consists of a series of interconnected and sequential building components. Since each subsequent block relies on the preceding one's hash, tampering with the data would require altering a large number of blocks, making the task prohibitively complex [41]. Many people now have access to the database since it was made available to the public. In the event of cheating, the databases of the cheating users and the non-cheating users will be distinct. If this is the case, the information stored previously about the user is invalid. Mining is essential to the Bitcoin network. A mechanism is developed in this study that guarantees the significance of every node that joins the blockchain by instituting a system of "turn rules" for each participant. This study focuses on how electronic voting results are recorded after the election has already taken place. Information generated by each node and disseminated according to the blockchain's permission mechanism.

IV. Conclusion

The most recent and cutting-edge research articles that have anything to do with blockchain technology have been analysed and dissected at this meeting. Following the complete selection of a number of articles from the internet database, these papers were then categorised according to a number of distinct fields. This article provides an insight of the current research around blockchain technology and its applications in the real world.

The blockchain technology offers a multitude of benefits, some of the most notable of which are its speed, resilience, and openness. It is necessary for there to be consensus among all of the network's members in order for the transaction to be added to the blockchain. However, blockchain is not a panacea that can solve all difficulties, and a number of concerns have been raised about it. These concerns include the use of blockchain technology to facilitate financial transactions for illegal operations, legal ramifications, and other economic dangers. If it is used well, blockchain has the potential to become one of the most exciting technologies of the future.

V. REFERENCES

[1]. A. Monrat et al, "Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities".

[2]. 2. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016 Up 30 Percent From 2015

[3]. NSA Prism program taps in to user data of Apple Google and others

[4]. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009,

[5]. Zyskind, O. Nathan and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", IEEE Symposium on Security and Privacy Workshops, pp. 180-184, 2015.

[6]. M. Swan, Blockchain: Blueprint for a new economy. O'Reilly Media, Inc., 2015. [7] G. Prisco (2016, April), The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab.

[7]. G. Irving, H. John (2016, May), How blockchain-timestamped protocols could improve the trustworthiness of medical science.

[8]. O. Williams-Grut (2016, March), Estonia is using the technology behind bitcoin to secure 1 million health records.

[9]. P. B. Nichol (2016, March), Blockchain applications for healthcare.

[10]. L. Li, X. Li, C. Cheng, C. Chen, G. Ke, D. D. Zeng, and W. T. Scherer, Research collaboration and ITS topic evolution: 10 Years at T-ITS, IEEE Transactions on Intelligent Transportation Systems, 11(2010) 517-523

[11]. M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc., 2015. [9] A. M. Antonopoulos, Mastering Bitcoin, O'Reilly Media, Inc, 2014.

[12]. Y. Yuan, F.-Y. Wang. Blockchain: the state of the art and future trends. Acta Automatica Sinica, 42(4)(2016) 481-494

[13]. Q.-J. Kong, L.-F. Li, B. Yan, S. Lin, F.-H. Zhu, G. Xiong, Developing parallel control and management for urban traffic systems, IEEE Intelligent Systems, 28 (2013) 66-69.

[14]. F.-Y. Wang, Parallel system methods for management and control of complex systems, Control and Decision, 19(5) (2004) 485-489

[15]. F.-Y. Wang, R. Dai, S. Zhang, G. Chen, S. Tang, D. Yang, X. Yang, and P. Li, A complex system approach for studying sustainable and integrated development of metropolitan transportation, logistics and ecosystems, Complex Systems and Complexity Science, 1(2)(2004) 60-69

[16]. F.-Y. Wang, Computational theory and methods for complex systems, China Basic Science, 6(41)(2004) 3-10

[17]. E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 459– 474.

[18]. I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous distributed e-cash from bitcoin,” in 2013 IEEE Symposium on Security and Privacy, May 2013, pp. 397–411.

[19]. T. Cui, “Ldap directory template model on multi-master replication,” in 2010 IEEE Asia-Pacific Services Computing Conference, Dec 2010, pp. 479–484.

[20]. S. Shah, Q. Kanchwala, and H. Mi, “Block Chain Voting System,” 2016.

[21]. Christian, “Desain Dan Implementasi Visual Cryptography Pada Sistem E-Voting Untuk Meningkatkan Anonymity,” Institut Teknologi Bandung, 2017.

[22]. C. Dougherty, “[Vote Chain : Secure Democratic Voting],” 2016.

[23]. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.

[24]. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” 2015 IEEE 4th Glob. Conf. Consum. Electron. GCCE 2015, pp. 577–578, 2016.

[25]. A. Back, G. Maxwell, M. Corallo, M. Friedenbach, and L. Dashjr. Enabling blockchain innovations with pegged sidechains. 2014.

[26]. R. G. Brown. The “Unbundling of trust”: How to identify good cryptocurrency opportunities?, 2014. [6] V. Buterin. On public and private blockchains, 2015/08.

[27]. C. Decker and R. Wattenhofer. Information propagation in the Bitcoin network. In P2P, Trento, Italy, 2013. [8] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse. Bitcoin-NG: A scalable blockchain protocol. In USENIX NSDI, Santa Clara, CA, 2016.

[28]. I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. In FC, Christ Church, Barbados, 2014. [10] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun. On the security and performance of proof of work blockchains. In ACM CCS 2016), Vienna, Austria, 2016.

[29]. I. Gorton, J. Klein, and A. Nurgaliev. Architecture knowledge for evaluating scalable databases. In WICSA, Montréal, Canada, 2015.

[30]. T. D. Joseph Poon. The Bitcoin lightning network: Scalable off-chain instant payments. 2016.

[31]. Y. Lewenberg, Y. Sompolinsky, and A. Zohar. Inclusive block chain protocols. In FC, San Juan, Puerto Rico, 2015.

[32]. N. R. Mehta, N. Medvidovic, and S. Phadke. Towards a taxonomy of software connectors. In ICSE, 2000.

[33]. A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz. Permacoin: Repurposing Bitcoin work for data preservation. In IEEE S&P, San Jose, CA, 2014.

[34]. S. Nakamoto. Bitcoin: A Peer-to-Peer electronic cash system, 2008.

[35]. C. Natoli and V. Gramoli. The blockchain anomaly. In NCA’16. IEEE, Oct 2016.

[36]. S. Omohundro. Cryptocurrencies, smart contracts, and artificial intelligence. AI Matters, 1(2):19–21, Dec. 2014.

[37]. Y. Sompolinsky and A. Zohar. Accelerating Bitcoin’s transaction processing - fast money grows on trees, not chains. Cryptology ePrint Archive, Report 2013/881, 2013.

[38]. M. Swan. Blockchain: Blueprint for a New Economy. O’Reilly, US, 2015.

[39]. T. Swanson. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. 2015.

[40]. F. Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3):464, 2016.

[41]. L. Valenta and B. Rowan. Blindcoin: Blinded, accountable mixes for Bitcoin. In FC, San Juan, Puerto Rico, 2015.

[42]. M. Vukolić. The quest for scalable blockchain Fabric: Proof-of-Work vs. BFT replication. In iNetSec, Zurich, Switzerland, 2015.

[43]. I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling. Untrusted business process monitoring and execution using blockchain. In BPM, Rio de Janeiro, Brazil, Sept. 2016