The All-Pervasiveness of the Blockchain Technology

•NAYANA N M. (P.G Research Scholars)
School of Social Sciences, CMR University, Bangalore.
• Prof.V.Lavanya(M.sc,M.Phil.), Assistant Professor, CMR University, Bangalore.

Abstract

Conceptually, the blockchain is a distributed database containing records of transactions that are shared among participating members. Each transaction is confirmed by the consensus of a majority of the members, making fraudulent transactions unable to pass collective confirmation. Once a record is created and accepted by the blockchain, it can never be altered or disappear.

Nowadays the blockchain technology is considered as the most significant invention after the Internet. If the latter connects people to realize on-line business processes, the former could solve the trust problem by peer-to-peer networking and public-key cryptography. The purpose of this paper is to consider distinct use cases at the all-pervasive impact of blockchain technology and look at this as an inalienable part of our daily life.

Keywords: blockchain, bitcoin, digital currency, digital economy, digital society, smart city, smart contract, digital identity, double-spending attack, 51% attack, Sybil attack

1 Introduction

There are three generations of technology platforms: the first platform being mainframes, the second Internet, personal computers, and local area networks, the third platform delivers computing anywhere, immediately, and allows organizations to deploy and consume computing resources in shared communities. The blockchain technology is based on the capability of the third platform [28].

The concept of universal digital currency without a centralized intermediary (like a bank or government) has existed for the past more than 30 years. At the time of Digicash develop- ment, a lot was said about the growth of decentralized applications that could lead to major global changes by solving problems of mass surveillance, on-line participation and democratic governance [7].

The first successful cryptocurrency Bitcoin [18] was based on the blockchain technology. And since then it is known that the blockchain is a public ledger (a distributed database) for all transactions and it resolves the double-spend problem by combining peer-to-peer technology with public-key cryptography. Literally, a blockchain is a chain of blocks of information that
registers Bitcoin transactions. The algorithms and the computational infrastructure of creating, inserting, and using the blocks are considered as the blockchain technology [31].

The key leading feature of the blockchain technology is ability to track transactions within decentralized, public databases and thereby excluding counterfeiting and fraud [15].

The essence of blockchain lies in its ability to support trustworthy transactions via networked computation in place of human monitor and control [31]. We can think of it as an ”operating system for interactions” [20]. The distributed consensus and anonymity are two important characteristics of blockchain technology [8]. A number of large industrial players, such as IBM, Microsoft, Intel, and NEC, are currently investing in exploiting the blockchain in order to enrich their portfolio of products [11].

Additionally, blockchain technology actively configures our understanding of social reality. They do so by enforcing the chronological temporal dimension in the organization of characters and events. This renders social relations increasingly rigid, at the cost of a loss of dynamism and consequently of a sense of freedom and responsibility [21].

But there are at least three key challenges to the blockchain technology that are perva- sive across applications and have not yet been solved cleanly: data privacy, scalability, and interoperability [28].

2 Development and All-Pervasiveness

Nowadays we can identify the following three phases or generations of the blockchain develop- ment: Blockchain 1.0 as digital currency, Blockchain 2.0 as digital economy, and Blockchain 3.0 as digital society [5, 26, 31].

2.1 Blockchain 1.0 – Digital Currency

Blockchain 1.0 is the first generation of blockchain technology applications. It refers to the underlying technology platform (i.e. mining, hashing, and the public ledger), the overlying protocol (i.e. transaction enabling software), and the digital currency (i.e. bitcoin or other digital tokens/coins) which represent a store of value as well as provide value to the protocol itself [5]. Bitcoin is a rare case where practice seems to be ahead of theory [19]. The main advantages of Bitcoin are:

- Bitcoin offers the possibility of largely reduced transaction fees for on-line purchases.
- Bitcoin provides greater anonymity than credit cards. Accounts are pseudonymous and the protocol is designed to encourage the use of new account numbers for each transac- tion [17].
- The decentralized design of Bitcoin and other digital currencies protects against inflation. Traditional currencies rely on a central bank to regulate the money supply, introducing new money into circulation as needed. Bitcoin, in contrast, uses cryptography to guaran- tee a relatively fixed money supply, which is allowed to grow at regular intervals [17].

2.2 Blockchain 2.0 – Digital Economy

Although the concept of the digital economy was proposed more than 20 years ago in [27], only today it received an appropriate technology platform. Blockchain 2.0 refers to the wide range of economic and financial applications that exist beyond simple payments, transfers,
and transactions. Such applications include traditional banking instruments such as loans and mortgages, complex financial market instruments such as stocks, bonds, futures, derivatives, as well as legal instruments such as titles, contracts, and other assets and property that can be monetized [5]. The payment clearing system and bank credit information systems can be the appropriate scenarios of blockchain application [10].

One key emerging use case of blockchain technology involves smart contracts. Smart contracts are basically computer programs that can automatically execute the terms of a con- tract. When a pre-configured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can automatically make payments as per the contract in a transparent manner [8]. In 2015 Visa and DocuSign demonstrated smart contracts for leasing cars without the need to fill in forms [22].

The most well-known platform that runs smart contracts is Ethereum. However there are some security problems [3] in which an adversary can manipulate smart contract execution to gain profit. Developers writing contracts for the existing Ethereum system can use a symbolic execution tool called Oyente to find potential security bugs [16].

2.3 Blockchain 3.0 – Digital Society

Blockchain 3.0 refers to a vast array of applications that do not involve money, currency, com- merce, financial markets, or other economic activity. Such applications include art, health, science, identity, governance, education, public goods, and various aspects of culture and com- munication [5].

The most promising application of the blockchain technology is smart cities, which involve horizontally cumulative elements such as smart governance, smart mobility, smart living, the smart use of natural resources, smart citizens, and smart economy [25].

Internet of Things (IoT) becomes a new platform for e-business. However, old business models

could hardly fit for e-business on the IoT. It is possible to implement the transaction of smart property and paid data on the IoT with the help of P2P trade based on the blockchain technology and smart contract [30, 1].

It is possible to successfully employ blockchain technology to facilitate machine-to- machine (M2M) interactions and establish a M2M electricity market in the context of the chemical industry via the IoT, where electricity producers and electricity consumers trade with each other over a blockchain [24].

Leveraging blockchain technology, the concept of decentralization might be applied to large scale data management in an electronic medical records (EMR) system, providing au- ditability, interoperability and accessibility via a comprehensive log [2].

Digital identity enabled by the blockchain technology has the potential to change lives. With the benefit of digital identity, many of the world's two billion unbanked individuals could store their identities on a blockchain, permit banks to fulfill regulatory requirements such as Know Your Customer, and gain access to bank accounts, loans, and other financial services previously inaccessible to them [28].

In the cyberworld, people often make transactions with others that they have not met with. Reputation systems have been widely used in cyberspace as an effective way to allow people to evaluate the trustworthiness of a potential seller. However, current reputation systems are vulnerable to fraud rating and the detection of fraudulent raters is difficult since they can behave strategically to camouflage themselves. The blockchain technology provides new opportunities for redesigning the reputation system [6].

3 Security Issues of the Blockchain Technology

One of the most attractive features of the blockchain technology is its security mechanism based on public ledger and distributed consensus. However, this does not mean that it can resist any types of fraud and hacking.

The most important security issue of the blockchain based system is the so-called 51% attack. Bitcoin measures the level of computing activity on the network in terms of the hash rate. When more than 51% of the hash rate is controlled by a single node (one miner or pool of miners), the blockchain can be distorted maliciously.

The 51% attack also results in a fork, which is where there are two conflicting blocks vying for addition to the blockchain. Because the majority of mining power on the network would support the attackers block, it would be sent to the blockchain [4, 23].

There is a well-known security concern named double-spending attack [4, 9, 12, 13, 29]. Double-spending occurs when someone makes more than one payment using one body of funds (e.g., a quantity of bitcoins). This is possible in a peer-to-peer network because there may be propagation delays when pending payments are broadcast to the network or the network's many nodes receive unconfirmed transactions at different times. Blockchain tackles this problem by requiring miner nodes to solve a complex mathematical problem (mining) in order to verify the transaction. The complexity of the computation is adjusted so that, on average, it takes 10 min to solve a problem using the miners processing powers. Because only blocks with correct answers to the mathematical problem (the proof-of-work) can be added to the blockchain, only one among multiple payments is accepted and registered on the blockchain, making it almost impossible for parties to double-spend funds [29].

Centralized data-storage and management systems are susceptible to hacking, intrusion, and breaches, but blockchains' distributed consensus mechanism prevents hacking. Each transaction must be verified by the community of miners, leaving fraudulent transactions unable to pass collective verification and validation. Because the blockchain is constantly monitored by the entire network of nodes, each of which maintains a copy of the blockchain, malicious users have no means of inserting fraudulent blocks into the public ledger without immediately being noticed by others. Thus, it is impossible to compromise the integrity of records in the blockchain. Even if one or several of the ledgers are hacked, the large number of other network copies provide reliable backup and overwrite the hacked version [29].

The ledger is also both open to the public and provably secure, almost eliminating the potential for fraud. With a customer paying in bitcoins, a merchant has the confidence that the transaction will go through and there is no danger of chargeback fraud [14]. The same is true for the insurance marketplace [20]. Blockchain systems are very effective in preventing objective information fraud, such as loan application fraud, where fraudulent information is fact-based. Blockchain systems are effective in preventing bad mouthing and whitewashing attacks, but they are limited in detecting ballot-stuffing under Sybil attack, constant attacks and camouflage attack [6].

Although blockchains preserve anonymity and privacy, the security of assets depends on safeguarding the private key, a form of digital identity. If one's private key is acquired or stolen, no third party can recover it. Consequently, all the assets this person owns in the blockchain will vanish, and it will be nearly impossible to identify the thief. The consequences may be more devastating than identity theft in the off-line world, where third-party institutions (e.g., credit card companies) or central authorities safeguard transactions, control risks, detect suspicious activities, or help find culprits [29].

4 Conclusion

This paper summarizes the most illustrative, the most prominent and the most promising use cases of the blockchain technology including cryptocurrency, smart contracts, smart cities, elec- tronic medical records, digital identity, reputation systems, machine-to-machine communication and the Internet of Things.

Considering that there is a potential infinite number of use cases of the blockchain technol- ogy, we can conclude that it has penetrated into all spheres of our life and as a result of its impact on our life.

5 Acknowledgements

This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005).

References

[1] Jean Yves Astier, Igor Zhukov, and Oleg Murashov. Smart building management systems and internet of things. *Bezopasnost informacionih tehnologija*, 2017(3), 2017.

[2] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. MedRec: Using Blockchain for Medical Data Access and Permission Management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, Aug 2016.

[3] Anastasia Barinova and Sergey Zapechnikov. On the techniques and tools for privacy-preserving smart contracts. *Bezopasnost informacionih tehnologija*, 2017(2), 2017.

[4] Danny Bradbury. The problem with bitcoin. *Computer Fraud & Security*, 2013(11):5 – 8, 2013.

[5] Kyle Burgess and Joe Colangelo. *The Promise of Bitcoin and the Blockchain*. Consumers' Research, 2015.

[6] Yuanfeng Cai and Dan Zhu. Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, 2(1):20, 2016.

[7] David Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obso- lete. *Commun. ACM*, 28(10):1030–1044, October 1985.

[8] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. Blockchain technology: Beyond bitcoin, http://scet.berkeley.edu/wp-content/uploads/blockchainpaper.pdf, 2015.

[9] Arthur Gervais, Ghassan O. Karame, Karl Wu¨st, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 3–16, New York, NY, USA, 2016. ACM.

[10] Ye Guo and Chen Liang. Blockchain application and outlook in the banking industry. *Financial Innovation*, 2(1):24, 2016.

[11] Ghassan Karame. On the security and scalability of bitcoin's blockchain. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 1861–1862, New York, NY, USA, 2016. ACM.

[12] Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 906–917, New York, NY, USA, 2012. ACM.

[13] Ghassan O. Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, and Srdjan C˘apkun. Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Trans. Inf. Syst. Secur.*, 18(1):2:1–2:32, May 2015.

[14] Akif Khan. Bitcoin payment method or fraud prevention tool? *Computer Fraud & Security*, 2015(5):16 – 19, 2015.

[15] Vasilis Kostakis and Chris Giotitsas. The (a) political economy of bitcoin. *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, 12(2):431–440, 2014.

[16] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making Smart Contracts Smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 254–269, New York, NY, USA, 2016. ACM.

[17] Tyler Moore. The promise and perils of digital currencies. *International Journal of Critical Infrastructure Protection*, 6(34):147 – 149, 2013.

[18] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf, 2008.

[19] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[20] I. Nath. Data Exchange Platform to Fight Insurance Fraud on Blockchain. In *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, pages 821–825, Dec 2016.

[21] Wessel Reijers and Mark Coeckelbergh. The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. *Philosophy & Technology*, pages 1–28, 2016.

[22] Mike Sharples and John Domingue. *The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward*, pages 490–496. Springer International Publishing, Cham, 2016.

[23] Ning Shi. A new proof-of-work mechanism for bitcoin. *Financial Innovation*, 2(1):31, 2016.

[24] Janusz J. Sikorski, Joy Haughton, and Markus Kraft. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, 195:234 – 246, 2017.

[25] Jianjun Sun, Jiaqi Yan, and Kem Z. K. Zhang. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, 2(1):26, 2016.

[26] Melanie Swan. *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc., 2015.

[27] Don Tapscott. *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*. McGraw-Hill, 1994.

[28] Sarah Underwood. Blockchain Beyond Bitcoin. *Commun. ACM*, 59(11):15–17, October 2016.

[29] Jennifer J. Xu. Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(1):25, 2016.

[30] Yu Zhang and Jiangtao Wen. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, pages 1–12, 2016.

[31] J. Leon Zhao, Shaokun Fan, and Jiaqi Yan. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, 2(1):28, 2016.