A critical approach to technology-based risks in blockchain system

Nilufer Nilufer*, Zeynep Yeni Erol

*School of Business, Ibn Haldun University, 34494, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 12 October 19
Received in revised form 08 Nov. 19
Accepted 18 December 19

Keywords:
Blockchain Technology
Bitcoin
Trust
Security
Technology-based Risks
JEL Classification:
O33

ABSTRACT

The blockchain technology has given a new shape to the world and disrupted a wide variety of technology-based industries. The disruptive characteristics of blockchain technology have molded the way of doing things. Since the importance of blockchain technology in business and social environment is increasing day by day, this study aimed to underline risks of blockchain technology within the network. Two strategies were made to infer the technology-based risk in the blockchain ecosystem. First, the study examined to find the technology-based risk at the point where a user executes the transaction from his/her computer ‘Node’. Second, this study attempts to figure out the security concerns within the web of the blockchain. After assessment of benefits and risks of this technology, this study concluded with the findings that blockchain is very much secure and trustable system which provides peer-to-peer transactions without needing any trusted third party, besides, once the information of the transaction is recorded, the system stores multiple copies of it, so there is no chance to change or delete it from the system. In the case of negligence, there is a possibility of forgery at the node, but numerous software has been developed for protecting the computer. Approach of the study is grounded in the literature review of journal articles, reports and conference proceedings from authenticated sources via content analysis of the keywords such as blockchain, security, trust, technology-based risks. Blockchain technology is not associated with finance but it has high usage in other areas like health, education, supply chain, the music industry and many more to explore.

Introduction

Blockchain is a decentralized transaction technology originally developed for bitcoin cryptocurrency, where several blocks, carrying a cryptographic hash of the preceding block and transaction data. Each block is connected to another block using cryptography as a result it is very resistant to alter the data. It doesn't demand any mediator to look after the transaction. This database technology is used by its users that grants them a trustable platform for transacting valuable assets without requiring a centralized authority (Hawlitschek, et al. 2018; Malomo, et al. 2018). Hence, blockchain technology has the potential to substitute conventional banking practice, making the business more cost-effective and trustworthy.

Blockchain technology is also known as Distributed Ledger Technology (DLT) preserves records in the form of ledger. Copies of the ledger are all over the web and users can share information within various parties, in a more assured, systematic, clear and validated manner. Both, Private or Public networks are utilized by DLT. Here comes public network, without any stipulations on membership anyone can register it and data stored in this work can be viewed by the members in engraved form. In public networks, data transactions are confirmed by the participants powered by different protocols, lack central authority. Unlike the public network, the private network can only be followed by those who had permission. By controlled access, it generates a floor where parties can trust each other. Additional, participated parties have a varied level of authority for transaction and visualization of the database(Workie & Jain, 2017). When the participants conduct any transaction then they record the valuable data on the blockchain network in an encrypted format. The data can be accessed at any time as needed. Blockchain is such a technology that can serve as an application as well as a database(Diedrich, 2016), which gives two platforms for the audience at a time, thus makes life easier.
The blockchain constitutes a database of records that are distributed in the form of ledger. These transactions are shared between parties who are participating in the system. Participating parties in the system verify every transaction in the blockchain system with a majority consensus. It is constant that if a transaction is done in the system, the information of this transaction will be in the system forever. There is no method to erase information of transaction in the blockchain system. So, the system store a precise and verifiable record of each transaction that has done in the system even once (Harris, 2018). This helps to save the data enduringly and almost impossible to delete the data from the web. Further, it uses Public key (PK) which is used to record the user's identity, an additional layer of shield for privacy.

Blockchain emerged as an enfant terrible for the economy of the world. Any single point of the breakdown is not tolerable with the decentralized technology and it generates a higher resilient environment to run the application. The algorithms used in blockchain; cryptography algorithms provide more security to the private data. To guarantee these recordings as permanent, in chronologic order and visible to each user in the system, there are multifarious computational algorithms that are placed on the network (Berke, 2017).
These mathematical algorithms, distributed consensus algorithm and cryptography amalgamate the peer-to-peer networks and extricate the security, as well as database, synchronize issues.

Banking as an intermediary for the transaction is not the only sector that will be influenced by the blockchain technology, but it will remodel the other business sectors too. Blockchain technology which was originally developed to support bitcoin digital currency is predicted to be used in many different areas such as financial applications, supply chain management, healthcare, the recording industry, and distribution as well as sharing economy (Kogure, et al. 2017). This blockchain technology is expanding like a wave all over the industries making them more productive.

As the world technology is evolving and scientists are innovating new technologies day by day so it is very essential for the managers to follow up with the tech trends. With the discovery in technology, it is quite clear that most of the business models will be affected positively especially by decreasing the cost of transactions via disintermediation systems. It is recommended that the manager should follow up on the new technology, applications of blockchain not to encounter disruptions that are likely to face (Nowiński & Kozma, 2017). For survival in the digital world, companies need to educate the employees about the new technologies’ as a result the performance of the companies will increase gradually.

**Importance of blockchain technology in business environment**

Excluding blockchain technology, digital platforms are commonly relying on central authorities in terms of trusting. Each transaction which is done online need a third party to validate the transaction with a record such as certification authority confirming the trustworthy of the certificate or a bank confirming the transaction of the financial remittance delivered to the target safely or a social network gives the promise of not sharing personal information and shared posts to the third parties. It is threatening to be in the digital world just by trusting the central authorities to protect our digital assets and transactions which can be a target for hackers or manipulators (Harris, 2018). Traditionally, institutions including banks, notaries and lawyers were performing as a middleman to manage the records and perform the transactions, sadly, it is quite unsafe. The new technology, blockchain has given more certainty because it presents a platform which does not require any third party to authenticate the transaction. The reason why the transaction we perform is registered in many places, the transaction is supported by the consensus and then unlikely for anyone to transform it.

Blockchain technology a new framework holds a commitment for fair and transparent transactions in society. Blockchain-based technologies, novel to the societies holds lots of opportunities yet still in its infancy states risks. Many governments, service companies’ enterprises and startups in the world consider it beneficial in their domains but still very few have embraced it (Rohan, 2017). One of the reports of Harvard Business Review addresses, it would be a not good decision to apply the blockchain technology in our businesses and economies, first, we need to train how it works.

Everyone is informed, blockchain revolutionizes our economies and businesses. Blockchain offers a lot of advantages like it is not associated with any sovereign entities or banks thus less prone to corruption and users can transact the value without reliance on the traditional intermediaries. It also provides a feature of pseudonymous accounts and lower transaction fees (Lo & Wang, 2014). The technology reduces operational costs such as eliminating the cost of the intermediaries and time saving by performing the activities quickly.

![Fig.2: Importance of Blockchain; Source: Editors’ search](image)

Various countries are attempting to adopting blockchain technology to compete with the world Internationally, for example, Kazakhstan desires to pursue a digitalization program to compete for the international market by linking blockchain to the old banking system to revitalize. Blockchain technologies are all over the world almost covering all the sectors in the society plus it is very practical. So why to miss the chance to be number one the world. Blockchain in the supply chain for trade purposes overcame so many costs by making everything digital. Freight Trust, Blockchain-based shipping document application designed to eliminate the need for having a physical shipping document. For example, implanted sensors and RFID tag help to track the product making it very easy for the management to keep the records. The world demands for high speed and low cost every passing day. Blockchain can be helpful in the supply chain for reducing overhead costs and reducing corruption.
Virtual computing solves large scales problems in science, engineer, and commerce, its decentralized mechanism helps to adapt changes in the environment so easily controllable and can easily be used to manage the resources (Buyya et al. 2002). By using a decentralized mechanism each user maintains a copy of records but transactions are likely to occur only if all other users agree. They will investigate the request is from the approved person and the transaction is legitimated by this means.

By under decentralization, distributed accounting blockchain resolves problems like non-disclosure and non-sharing of information in shared express delivery, difficulty in implementing real-name authentication, leakage of user privacy and complicated payment (Ding & He, 2018). Fundamentally, it hides the details of users for security purposes.

**Characteristics of blockchain technology: Efficiency and transparency**

Within the blockchain system, anyone who engaged in the system has access to see each transaction and its value. There is an identification, a special alphanumeric address which has 30-plus-character for each person using the system as a node or user. Users may favor remaining anonymous as well as they may prefer to prove their identity. These addresses are important to make transactions (Berke, 2017). Blockchain is highly versatile uses diverse applications in various fields. One of the features is using cryptocurrencies, one of characteristic using cryptocurrency is that it provides a platform to conduct anonymous transactions. Spot exchange by 2017, 83.8465 million users, the daily volume of 10.8 million transactions occur and 832 times per second. While commodity transaction the spot exchange face risks of transaction and controllability issues consequently negative effect the healthy development of spot trading market. Thanks to blockchain technology as it takes block connecter Java Blockchain Connector (JBCC) as a link object and creates a multi-blockchain application system, as a result, high efficiency, low development cost, expeditious, reliability for spot transaction. With the help of decentralization supervision but the regulators had been improved thus healthy spot trading guaranteed (Liu & Zou, 2018). This robust technology genuinely covered all the areas of the areas from health to business to music industry making it more efficient and powerful.

The information while transporting goods have become very costly. Modern technology, blockchain can be used to construct, manage and verify this information and makes it efficient (Allen et al. 2019). Reductions in trade costs such as paperless trade using technology like blockchain have propelled modern globalization. Blockchain provides trusted and reliable information in the supply chain for trading and it benefits consumers, firms and other law institutions by decreasing the risks of faulty information (Allen, B. & Markey-Towler, 2018). For example, Samsung which is supplied to almost every part of the world, using blockchain to transport 488,000 tons of air cargo and shipping containers annually (Suominen, 2018). Trust is a pervasive concern not just with new technologies but also with established technologies as they become more complex and interdependent. As in blockchain technology trust shifts from humans and central organizations to algorithmic processes, networks of computers, and decentralized anonymous organizations that have no geographic boundaries. For sharing economies users are facilitates on the demand and there is a wide spectrum of application areas P2P matching can coordinate. However, consumers' trust is based on the provision of goods or services by a provider (Hawlitschek et al., 2016). Studies show that consumer-to-consumer(C2C) transactions depend on trust. If the reputation is good consumers are satisfied (Leonard, 2012). World of the business demands the quality of the value which you are providing and if you have created a strong reputation by providing high quality then the trust will automatically build. This is the phenomenon blockchain technology is working on.
A node can be any electronic device including a computer, phone or even a printer that has IP address and connected to the internet. The nodes are the primary source to be part of the blockchain technology.

New versions of the bitcoin have already created serious problems for the bitcoin network. The nodes and the miners of the bitcoin network had catastrophic consequences because of the uneven updating to newer versions of the software by the computers. Like in 2013 the Bitcoin experience “hard fork” as a result two separate transaction history had been developed within the network because of the use of different versions of the software. This created chaos because it created two ledgers, but Bitcoin’s core principle is that the common ledger is reliable and true (Walch, 2015). Technology-based security of the blockchain is not the same as it was a few years ago, it is constantly improving and lots of modifications had been made till today.

Importantly, security begins how the architecture of the network is build, especially when building a private blockchain. To approve the transaction blockchain achieves consensus on the basis of verified transaction which is done by communication. The communication takes place between the nodes, each node contains a copy of ledger and they inform other nodes for new information. Especially, the private blockchain controls who will be responsible to operate a node and how the nodes should be connected to each other. This provides a great security as it will not allow any unauthorized person in the system (Berke, 2017). Further the nodes with more connections will get the information faster and to be an active node it is important to have a number of connections. A node that transmits incorrect information must be identify in order to maintain the integrity of the system. Nodes which are in the central positions in private blockchain requires to have a connection with other central nodes for the security measure.

Some nodes that are not permanently active or always open to communication which may cause security concerns while building the network architecture of the system. Being offline of a node should not affect the network, the network must work properly as it is supposed to in terms of verifying new transactions and delivering the information about previous transactions. Additionally, if the nodes return, they have to be updated very quickly (Berke, 2017). The consensus mechanism is important and crucial to function the blockchain correctly. It is very necessary to make sure that everyone is using the same blockchain, among all, transactions should be checked frequently, and all nodes should be audited.

To secure the end nodes different software have been developed and have been using for security purposes. For example, LANDesk Software, a leading provider of integrated systems and security management solutions. LANDesk Security Suite enables customers to proactively manage and defend against a variety of threats including attacks from malicious code, adware, system intrusion, and spyware. JPMorgan is a platform build by Blockchain technology to use the blockchain data structure to verify and store data. A distributed computer node consensus algorithm is applied to generate and update data. Therefore, from all sides, blockchain technology is protected.

**Network Related Risks in Blockchain**

The blockchain technology maintains its integrity by not relying on a single authority. It uses public-key (asymmetric) cryptography, peer to peer networking to get the consensus to get the assurance over malicious activities (Antonopoulos, 2017). Rather than relying on the single central authority blockchain uses consensus across the nodes to approve the transaction. We are aware that blockchain holds information in the form of ledger then it is very important that stored information should be valid.

Bitcoin uses blockchain technology, a potential disrupter of financial market infrastructure but prone to technology risks and governance risk. Its software nature, decentralize structure, open-source and expertise problems undermine the technology's reliability as financial market infrastructure. Though it is resistant to attack but not invulnerable, it has a susceptibility of 51% attack, which undermines its suitability to use in financial market infrastructure (Walch, 2015). The technology is algorithmically complex but very unlikely to be attacked.

Blockchains decentralized feature is likely to result in a low susceptibility to manipulation and forgery by malicious participants. There are identical data on the interlocked web of computers so if one node is attacked the system rejects it (Kestenbaum, 2017). Valuable records such as licenses, financial accounts, medical records and votes everything can be recorded virtually by expressing them in codes. This can help to save valuable data for a long time.

Even if a hacker can penetrate one network and attempts to withdraw funds, there are multiple redundant copies of the same ledger stored around the world. If one is tampered with, the others could be used as a backup to prove what funds belong in each account. For example, to hack the network almost 50% of computers need to be hacked. The blockchain is almost unbreachable because if one node is under forgery then other nodes resistant simultaneously.

Open bazar, a Bitcoin-integrated decentralized e-commerce platform, even if a hacker successfully penetrates the database of Open Bazar, the private keys of Bitcoin wallets or credit cards won’t be released. Even if the attacker somehow gets hold of the user’s private key for a Bitcoin address, the multi-signature technology will prevent the hacker from accessing the funds and moving them elsewhere (Young, 2018). Digital signatures are the main components which use asymmetric cryptography for the integrity of the information in the blockchain.

By using the “triple-blind” mechanism a user can log in the account and access other phone services by using their credentials but the information of a user and can never be seen by a third person. This mechanism provides additional security to the network.
Blockchain’s role in cybersecurity

Cybersecurity also known as information technology or electronic information security is practice, defends computers, mobile phones, electronic system, networks and data from attacks. With the passage of the time security solutions are advancing to fight with the risks and malicious attacks compare to the traditional sources of security. Like blockchain technology, which reduces breach detection gap with the help of continuously monitoring and network traffics against cyber-attacks (Malomo et al., 2018). So, this minimizing of the breach detection gap for cyber-attacks is a big achievement of blockchain technology.

Major industries and enterprise are already considering the use of this tremendous technology which has the potential to improve the cybersecurity, because relying on the third parties that have a weak cybersecurity measures can be easily targeted by the attacks. Confidentiality, integrity, availability and resilience is provided by the blockchain, (Shaverdian, 2019), so suggesting by the experts’ large companies should implement blockchain as their cybersecurity plan, as it provides core components of cybersecurity. The cybersecurity benefits that blockchain provides with the trust component makes it unique and a solution to data breach problems, thus appealing to make it as a part of comprehensive cybersecurity plan.

As an omnipotent cybersecurity solution Blockchain serves as secure reservoir of critical data which otherwise cannot be compromised with conventional means. It creates cryptographic hash functions in blockchain which produce unique characters to critical data which can only be decoded with the original cryptographic key, that is hard to replicate. Thus, this hash functions helps to protect the data from unauthorized access (Jain, 2019). It is estimated that by the year 2023, blockchain based identity management will grow at the rate of 84.5 percent because it more effective than the existing password based and multi factor authentication securities.

Having an innovative approach for storing information, executing transactions and performing functions, people consider blockchain a breakthrough technology for cybersecurity (Zhang, Xue, & Liu, 2019). Even though a little number of blockchain platforms have achieved a set of security goals in practical world but there is increasing interest of blockchain in industries and research studies. Soon this platform will help to settle the whole security problems.

Conclusion

Blockchain, an innovative technology, helps different institution in various areas including transactions, supply chain, music recordings, pharmacy, spot exchange and many more. Its vast usage make it the pioneer of the modern technology. Blockchain is a decentralized transaction technology, democratized transactions are done by taking a consensus from all the participants.Introduced as underlying technology to enable cryptocurrency in untrusted parties blockchain technology emerged as transformative invention in technology world. Even, the blockchin technology is considered as in comparison to the World Wide Web, as the technology provides many solutions to the unending problems. By substituting the banks, the block chain technology not just make the transaction very fast but it decreases the risk of securities and it also provide the feature of making anonymous transactions. Problems related securities and how blockchain helps to reduce the security issues had been mentioned in this paper.

The blockchain is very sound, efficient and trustworthy technology. As an efficient technology it decrease the cost of trades by reducing the time of deliveries and removing the intermediaries with the help of direct transactions. It is the most trustfull as when you enter the critical data and once transaction is recorded it will be very unlike to transform the data. The technology will store multiple replicas of the identical data in the form of ledgers and every node will be having the copy of ledger. Using the private key is another layer of security for this novel technology. This omnipotent technology is very secure and risky free and it can overwhelm numerous problems of conventional regulatory mechanisms and have a higher level of cybersecurity (Pokrovskaya, Khansuvarova, & Khansuvarov, 2018). There is no room for second thoughts when you are using this fascinating technology. On the other hand, when it comes to security matters personal machines utilizing for mining can be a problem. One has to be sure that they are using the updated versions in their machines but again software such as LANDesk and many additional programs are using for security objectives. Also, confidentiality, integrity, availability and resilience are provided by the blockchain, which are the components of cybersecurity, thus it has great role for cybersecurity.

Acknowledgment

We are incredibly grateful to our supervisor and mentor, Professor Umit Hacioglu, for encouraging, directing and assisting us in doing this task. He guided us and he was always available whenever we needed the feedback.

References

