Blockchain: Opportunities, Risks, and Applications

Mann Parekh

Received September 2nd, 2022
Accepted October 15th, 2022
Electronic access November 1st, 2022

Blockchain is the underlying technology of a number of digital cryptocurrencies. It's best known for its crucial role in cryptocurrency systems, like Bitcoin, for maintaining a secure and decentralized record of transactions. There are some key differences between a regular database and a Blockchain like the way data is structured in both of them. Blockchain holds data in "blocks", which are sets of information. Each block has a limited storage capacity and when filled, they are closed and linked to the previously filled blocks, thus forming a chain of data known as Blockchain. Its decentralized and secure nature makes it special and unlocks a lot of potential. However, there are always risks and drawbacks. Some notable ones are: (1) Scalability, (2) Performance, (3) Privacy, (4) Interoperability and (5) Power consumption. Blockchain can be implemented into various industries, sectors services like finance, healthcare, security and has the potential to be employed in a lot more sectors. Some examples are data analytics, cybersecurity, and transportation. While there are some weaknesses that need to be resolved before it can be introduced at a large scale, most of them can be overcome once this technology starts drawing more attention, investment and development towards itself. Although this technology isn't perfect as it stands today, it has the potential to be an industry disruptor, permanently altering the core systems and processes used in various fields.

Introduction

What is cryptocurrency?

Put simply, cryptocurrency is a decentralized form of digital money that is based on blockchain technology and is secured by cryptography, i.e., a method that secures data from unauthorized access by using encryption techniques[1]. Users today can buy cryptocurrencies from central exchanges, brokers, and individual currency owners or sell them to them. They're generated through a process called "mining", which involves the use of high-powered computer systems to "crack the code" and receive bitcoins in return.

What are the main types of cryptocurrency?

Although there are thousands of types of cryptocurrencies available today, these are some of the most significant ones:

- Bitcoin: It is the most widely accepted form of cryptocurrency and is so popular that its name is synonymous with cryptocurrency. It is very expensive and fluctuates often, but you can purchase it in small fractions[2].
- Altcoins: These are alternative currencies to bitcoin, like Ethereum and Terra.
- Crypto-tokens: Unlike coins, tokens can't be mined or linked to blockchains.

History of Blockchain and cryptocurrency? Why and how was it introduced?

Blockchain technology was first described in 1991 by research scientists Stuart Haber and W. Scott Stornetta. The scientists wanted to introduce a digitally practical solution for timestamping digital documents that could not be backdated. This led to them developing a system using the concept of a cryptographically secured chain of blocks to store the time-stamped documents. As for cryptocurrency, the concept was first introduced back in 1998 by Wei Dai. This concept finally came into existence in 2008 when Satoshi Nakamoto, a man who still remains anonymous to this day, published a "white paper" that described and explained the foundations and working of Blockchain and Bitcoin[1]. Bitcoin is the very first cryptocurrency and runs on Blockchain. About four months after the paper was published, Nakamoto mined the very first "block" of the Bitcoin network, which was known as the Genesis block, effectively bringing the concept of Bitcoin to life[1].

What is Blockchain?

Blockchain is a distributed database or ledger that is shared among the nodes of a computer network. Blockchain, as a database, stores information electronically in a digital format. It's best known for its crucial role in cryptocurrency systems, like Bitcoin, for maintaining a secure and decentralized record of transactions[2]. There are some key differences between a regular database and a Blockchain like the way data is structured in both of them. Blockchain holds data in "blocks",

which are sets of information. Each block has a limited storage capacity and when filled, they are closed and cryptographically linked to the previously filled blocks, thus forming a chain of data known as Blockchain. All new information is added to new blocks and they're also linked to the chain once filled. A regular database, in contrast, structures data into tables.

Opportunities (Positive aspects of the current technologies)

Blockchain technology and distributed database technologies that share the same principals are the key to recent developments systems involving transactions and other synchronized records. Trading records, payments, smart contracts, etc. can be built on blockchain technology whilst also ensuring security over mishaps like double payments, false disputes, forgeries, and more. In addition to that, this technology can be used for storing legal records like birth certificates, voter IDs, etc., and for the creation of "smart properties", which make use of blockchain by turning it into a buy-and-sell mechanism for hard assets like houses, cars and diamonds[3]. Another advantage of Blockchain is its ability to be utilized as a transactional mechanism for "sharing economy" services[3].

In the beginning, Bitcoin and Blockchain's popularity was mostly limited to underground crypto-communities which comprised of both enthusiasts and long-time followers. However, only recently have the digital currencies started gaining traction and popularity beyond these communities, like banks, big-time investors, law firms, etc. with increased media coverage[3]. Even the general public has started to express interest in this technology and new opportunities have been opening up at a steady rate.

Supply chain and Logistics

In almost every industry, companies have a hard time tracking their products. Since each company keeps its own record, tracking an individual product's journey from start to end can be a challenging task. As a solution, Blockchain can provide a common universal use system that can be used to track a product's journey in detail from start to finish.

Social Media

Privacy is a huge concern in today's world, where the platforms are free to use but the user's data is the product. In order to counter this, Blockchain-based social media can be the potential solution. This mode of social media guarantees privacy and full control of the user's information by making the users the owners of their personal data. This allows them to prevent social media platforms from exploiting their information for revenue and instead allows the users to monetize their data.

Public Services

To this day, Public Service offices handle and store all their records manually, which is slow, costly and prone to errors. Hence, instead of keeping thousands of files in drawers, Blockchain offers a system for government workers to store their data digitally. Having a Single Source of Truth (SSOT) for maintaining records will make it error-free, resistant to hackers or other interferences, and save money and time.

Security

Data leaks and security breaches are increasing on a daily basis. Blockchain can significantly reduce and even potentially eliminate this by limiting access to valuable records to only a few individuals. Since this process is timestamped and unvarying, any interferences or threats to the data will immediately be visible on the chain.

Disadvantages (Negative aspects of the current technologies)

Although there are still a set of unresolved questions related to digital payments and platforms in general, from trust issues to payment ecosystems, blockchain's decentralized nature has of a lot of unaddressed questions that are common when new platforms and services are designed, introduced and eventually used.

Privacy

Though Blockchain is termed to be safe and secure and provide protection for sensitive user data with the use of generated addresses rather than personal identity, researchers have suggested that the technology might be vulnerable to processes like privacy during transactions. This is because the public key required for processing a transaction is open to the network peers[4]. The main reason behind blockchain's vulnerability to information leakage is because the details and balances of all public keys are visible to everyone in the network. Therefore, the privacy and security requirements should be defined at the initial stage of Blockchain applications.

Performance and Scalability

There is a concern regarding whether cryptocurrency and blockchain-based solutions can keep up with the increasing demand coming from different government and business-based sectors, particularly concerning the performance and

scalability. Researchers are working to resolve the scalability issues regarding the number of replicas in the entire network as well as the performance's shortcomings, like latency (required time for adding a block of transactions in the blockchain) and throughput (number of transactions per second)[5]. An increase in these replicas can deteriorate performance as the network now has to handle a greater amount of processing and message exchange. While protocols such as PoW can ensure scalability, the performance hit from low throughput and high latency still exists.

Bitcoin is a PoW-based protocol that can scale a large number of replicas. In contrast, it provides low throughput considering only 6-10 transactions per second (may be less than that depending the complexity of the network) and is capable of generating a block with an average of 10 minutes. Another drawback of this consensus procedure, is that it is CPU intensive and hence, causes high consumption of electricity.

Ethereum also uses PoW in a different manner to prevent ASIC-enhanced mining, which is a hardware similar to a central processing unit (CPU) or graphics processing unit (GPU) that helps to mine faster but is very expensive and energy consuming. However, it cannot eliminate the draw- backs of Bitcoin. There is also the risk of multiple branching in PoW protocol that can lead toward the double spending problem[6]. Therefore, clients need to wait for 60 minutes or six blocks confirmation to ensure that the transaction is finalized in the longest chain. That makes the transaction duration quite lengthy and might not be feasible for adopting it in real life applications.

Energy consumption

The proof-of-work (PoW) algorithm has enabled bitcoin to perform transactions among peers in a distrustful distributed decentralized environment. However, while doing this work, miner computers are consuming a huge amount of electrical energy[7]. To provide insights about this highly unsustainable nature of the PoW algorithm, the bitcoin energy consumption index was created. The incentive mechanism motivates people around the world to mine Bitcoin. The mining process provides a solid stream of revenue that attracts individuals to run power-hungry devices to gain a chunk of it. As a result, the total energy consumption rate of the Bitcoin network reached a new high along with the value of the cryptocurrency.

Interoperability

Even though many industries are currently interested in adopting blockchain technology, there is no standard protocol that allows them to collaborate and integrate with each other. This lack of interoperability has had an adverse effect on the growth of the blockchain industry[6]. As a result, cryptocurrency stands as the sole mode of all operations for blockchain technology. It is evident that standardization is required for the different sectors and enterprises to collaborate on developing different applications that share blockchain-based systems and integrate them with the existing systems.

Applications

Blockchain technology can be used in diverse sets of applications. It is important to understand that bitcoin is not equal to blockchain; instead, it is one of the most successful applications of blockchain technology[8]. Bitcoin is a cryptographic digital currency, which is transacted over an open, public and anonymous blockchain network. However, experts claim that, this technology can be implemented for finding solutions for different domains, such as health- care, voting, identity management, governance, supply chain, energy resources and so on.

Healthcare

In the healthcare industry, blockchain can be used to trace drugs and keep track of patients' medicinal records. Managing patient data can be a tedious and complex task, even in today's world. Because each patient their unique treatment, dosage, and physical variability, a complete database of the patient's medical history is required in order to provide a personalized treatment. The existing system of bookkeeping these medical records lacks security, easy access and interoperability. Hence, it needs a complete reform in order to make it fit for use as per today's standards. This is where blockchain steps in. Blockchain can provide a secure mode of storing medical records digitally whilst also allowing integration of medical records among healthcare facilities, which grants them access to a common database shared by various facilities.

Drug counterfeiting, on the other hand, which is a major problem in the pharmaceutical industry, can be tackled via blockchain implementation. About $10-30\%$ of the drugs sold in developing countries are counterfeit, as revealed by reports from the Health Funding Research Organization. Some of these drugs either contain the wrong ingredients or have inaccurate levels of ingredients, which are a major threat to a patient's life[9]. Drug counterfeiting is also the cause of an annual loss of 10.2 billion euros for European pharmaceutical organizations. In order to address this, Blockchain can be used as a mode of transaction as all of the transactions added to the distributed ledger are digitally timestamped and permanent, which makes them easy to trace and keep the information secure[6].

Energy Industry

The traditional method of electricity consumption does not benefit from blockchain implementation as it relies on the framework of one supplier, for all customers. The ability of household generation of electricity from sources of renewable energy like solar power opens the possibility for a new market where customers become the suppliers depending on the time and situation. Therefore, a robust platform needs to be installed in order to allow the secure transactions of energy generation and consumption. Blockchain is the perfect candidate for this platform as it provides the opportunity to operationalize machine-to-machine interaction alongside creating an "electricity marketplace" that consists of various suppliers for consumers to choose from.

However, there is another problem that needs to be addressed. The continuous payment requirements among the machines that keep track of the energy supplied or provided is a mammoth task and requires a more efficient mode of transactions. This is where "micro-payments" come into the picture. To put it simply, micro-payments are a type of transactions in which payments are carried out with minimal nominal amounts of currency, specifically for smaller valued items. This permits the machines to have direct interaction with each other as the authentication process is decentralized and automated[6].

Stock Market

It takes over 3 days to finalize and process all transactions due to the role of intermediaries, the regulatory processes and trade clearances. This lengthy process is slow and inefficient for the participants of the stock market: the regulators, traders, brokers, etc. and needs to be refined. Blockchain can address this issue by automating and decentralizing the stock exchange process[10]. Intermediaries are hence eliminating, which helps speed up the process and bring down costs. By introducing smart contracts and a secured post-trade process, Blockchain acts as a regulator for all transactions.

From a cybersecurity perspective, using Blockchain makes sensitive information more secure and immune to hackers thanks to the decentralization of the ledger information. It grants anonymity from leveraging the blockchain public/private key and protects users from identity theft[6].

Identity management

Blockchain is an excellent platform for storing and securing online identities as it can be used to platform to protect users' identity from theft and fraud. It allows users to create an encrypted identity and grants more security and control over their information without having to provide a username and password. A digital ID is generated, which can later be assigned to every online transaction, while eliminating the possibility of fraud[11].

Case Studies

I. Healthcare – Using Blockchain in Estonia's Healthcare Industry

The Approach: Since the early 2000's, Estonia had declared the Internet as a basic human right and provided nationwide access soon after[12]. This robust infrastructure played a key role in adopting Blockchain. In 2011, just 3 years after the groundwork for Blockchain was laid out, Estonia in a collaboration with Guardtime, a private data security company, developed and employed blockchain-based "Keyless Signature Infrastructure" to secure the medical records of over a million citizens digitally[13]. This infrastructure guaranteed high security and easy access and availability to authorized parties[14].

Advantages: Thanks to blockchain, the medical records were now secure and scalable. It helped increase efficiency and decrease costs of medical care through improved coordination between insurance claim and treatment provided[15]. Citizens were now able to use smart cards through which they could access over a thousand online government portals to check their health records. Now that the information was immutable and safe, hackers could not tamper with it. Additionally, a large number of records can be stored under a single secure ledger, thus eliminating the need for multiple ledgers or storage units.

Risks: While scalability on a national level didn't pose as big of a challenge, scaling it on a global level is a mammoth task. It will require a long list of protocols, along with a collaboration between governments, healthcare providers, medical professionals, insurance companies etc. in order to develop and adopt a single system available to all. This system will not only consume a lot of time and resources to develop, but its implementation will be equally difficult too. Managing and transferring existing data from the previous system to the new system is no small feat.

Furthermore, thanks to past Bitcoin breaches, Blockchain suffers from a security issue, with over 554 million records being reported lost or stolen as of June 2016[16]. Also, the more the public sector leans towards a complex IT system, the more important it will become to cooperate with third parties and shareholders.

Conclusion: As emphasized by the Estonian digital authorities, this adoption of e-services does not rely solely on technological capabilities, but also on the public's perception of the system and how much they trust it. Fortunately, the perception can only increase if there is stability and proof of work.

Ripple - Digital asset created for global payments

What is Ripple(XRP)? Ripple(XRP) is a cryptocurrency token designed to migrate transactions from central databases controlled by financial institutions to a more open infrastructure while significantly cutting costs. XRP transactions are trustless, instant, and cheap, putting them at an advantage for cross-border movements.

The Bitcoin blockchain allows anyone to contribute computing power, validate transactions, and secure its software. The XRP Ledger, on the other hand, only allows select network participants to help validate transactions and secure the network.

How does Ripple work? The mission of Ripple's blockchain infrastructure, RippleNet, is to provide banks with quick, low-cost and simple cross-border transactions. As a result, it is a viable alternative to the current international payments system used by most banks. Ripple has several benefits for those who make international transactions. It utilizes a consensus system involving several bank-owned servers to verify transactions. Validators are put in place to check the validity of the transactions by comparing them to the latest version of the XRP ledger. XRP is a cryptocurrency that runs on the XRP Ledger, a blockchain engineered by Jed McCaleb, Arthur Britto, and David Schwartz. McCaleb and Britto would go on to found Ripple and use XRP to facilitate transactions on the network.

How is Ripple Mined? While Ripple cannot be directly "mined", there are more effective alternate methods that miners often use. The most widely used one is where miners mine Bitcoin(BTC) or Ethereum(ETH) first, and then trade it for Ripple(XRP) via exchanges. Ripple is created using a crypto ledger and federated by financial institutions, similar to Bitcoin.

Advantages of Ripple: XRP transactions are relatively cheap and fast and current financial institutions already use Ripple's payment network. Additionally, it can be used as a "bridge" currency for transactions involving other cryptocurrencies.

Disadvantages of Ripple: Ripple's transaction system is comparatively less safer than other crypto transaction processing systems. Moreover, Ripple's own financial partners use RippleNet over Ripple(XRP). Finally, purchasing and trading Ripple is quite difficult in the United States.

Conclusion

In this paper, the possibilities and benefits of the blockchain along with its trade-offs are discussed through a survey. Furthermore, the transaction process, system architecture, core technology, and application areas of blockchain are also explained. Blockchain technology possesses certain characteristics and features like trustless transactions, decentralization, security, and efficiency, which are the key to industry disruption. There are still many open issues like higher performance, less power consumption in order to make it greener, and the most prominent ones being interoperability and regulation, that need to be further researched and analysed to create more workable and effective industrial applications that can fully benefit from the use of blockchain and achieve the intended goals. The goal of this survey is to provide a detailed description of blockchain's current state and take a deeper dive into its potential application areas and also to serve as a reference for future researches around this topic. Finally, it can be confidently said that while this technology isn't perfect, it comes with a long list of advantages that far outweigh the disadvantages. With more development, Blockchain can be a nearly perfect platform to base new systems and architectures on. However, as more companies and industries recognize its potential and start adopting this technology, there will be a void that can only be filled by a standard protocol in order for these companies to collaborate and integrate Blockchain to existing systems. The sooner this protocol is introduced, the sooner we will get to witness Blockchain at its full might.

Future directions/Challenges/Open questions

Blockchain has immense potential in various industries. It's gaining popularity day-by-day and this technology will lure more investors by promising huge profits. A testing phase is necessary before implementation in order to determine its performance and trade-offs. If implemented the right way, it will revolutionize industries and become the key to the digital world. Its decentralized and secure nature opens up a world of countless possibilities. One of the potential implementations could be in data analytics and management, where blockchain could be used to store data in a secured manner and ensure its authenticity. Patient health records are an example of such data that can be stored via Blockchain. Another use is "smart contracts", protocol a piece of code that is deployed in the blockchain node. Execution of a smart contract is initiated by a message embedded in the transaction.

References

1 Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, *International journal of web and grid services*, 2018, **14**, 352–375.

2 D. Yaga, P. Mell, N. Roby and K. Scarfone, *arXiv preprint arXiv:1906.11078*, 2019.

3 P. Tasca, *Trends, Opportunities, and Risks (September 7, 2015)*, 2015.

4 R. Henry, A. Herzberg and A. Kate, *IEEE Security & Privacy*, 2018, **16**, 38–45.

5 M. Vukolić, International workshop on open problems in network security, 2015, pp. 112–125.
6 Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, *International journal of web and grid services*, 2018, **14**, 352–375.
7 K. J. O'Dwyer and D. Malone, 2014.
8 M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, *Applied Innovation*, 2016, **2**, 71.
9 B. D. Glass, *Research and Reports in Tropical Medicine*, 2014, **5**, 11.
10 D. Tapscott and A. Tapscott, *MIT Sloan Management Review*, 2017, **58**, 10.
11 O. Jacobovitz, *The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva*, 2016, **1**, 9.
12 T. Economist, *How did Estonia become a leader in technology?*, http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21., accessed Jun 16, 2017.
13 N. A, *Power to the People: Blockchain Replaces Government in Europe.*, https://cointelegraph.com/news/power-to-the-people-blockchain-replaces-government\-in-europe., accessed Jun 16, 2017.
14 D. R, *Does Blockchain Have A Place In Healthcare?*, https://www.forbes.com/sites/reenitadas/2017/05/08/does-blockchain-have-a-place-in-healthcare/#44d2b3df1c31., accessed Jun 14, 2017.
15 D. M. CR, *Blockchain in Healthcare: make the Industry better.*, https://www.finextra.com/blogposting/13801/blockchain-in-healthcare-make-the-industry-better., accessed Jun 12, 2017.
16 T. Heston, *Authorea Working Paper No AUTHOREA_213011_3643634*, 2017.