Blockchain: Applications and Disadvantages

Alex Pettis, David Pugh, Rob Wheelock

Introduction

Non-Fungible Tokens (NFTs), BitCoin, USD Coin, Ethereum, Binance Coin, Tether, XRP, and similar cryptocurrencies have been increasingly taking up headlines in the media - most particularly in the tech and finance realms. The underlying architecture supporting these novel technologies is called blockchain. In this paper, we will explore the nature & history, practical & business applications, disadvantages & vulnerabilities, impacts on society & culture, and the future of blockchain technology.

Ultimately, as our world becomes more heavily integrated with technology through the internet, blockchain is poised to become a cornerstone of a new digital world - in spite of the inherent risks and vulnerabilities in using it.

The Nature of Blockchain

Blockchain technology is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. Each block in the chain is a list of ordered records. Therefore, the blockchain is a distributed database that maintains a continuously growing list of blocks. Each block contains a cryptographic hash of the previous block, a timestamp, transactional data, and is linked using cryptography. A hash is a one way encrypted number that acts as a sort of signature for a test or data file. The potentials for peer-to-peer collection of data using blockchain technology are innumerable (Hayes, 2023).

The implementation of blockchain occurs through a number of steps. It begins with a transaction, where two parties decide to exchange some asset. The transaction is then packaged within a block and inserted into the chain by sending it to a network of participating computers. Machines in the network evaluate the transaction to determine the validity of the transaction in a process known as verification. After verification, a hash is created as a unique signature for the block. Finally, in a process known as execution, the asset is transferred from the first party to the second party (Somu, S. 2022, September 3).

Blockchain History

The technology upon which blockchain functions has been decades in the making. In 1979, a PhD thesis by Ralph Merkle introduced an approach to public key distribution he called, "tree authentication". From there, this patented idea became known as a Merkle tree. The Merkle tree is a data structure used in computer science applications. With regard to Bitcoin and other cryptocurrencies, Merkle trees serve to encode blockchain data more efficiently and securely. They can also be referred to as "binary hash trees". Then, in 1982, David Chaum created a system for establishing and maintaining computer systems by mutually suspicious groups in his PhD dissertation. Additionally, he went on to develop the first form of digital cash in 1989 when he founded the DigiCash corporation. A few years later, Stuart Haber and W. Scott Stornetta published an article about digital documents being timestamped, wherein they offered a solution for users who either backdate or forward-date electronic documents. Their idea was then updated to include Merkle trees in 1992, which allowed multiple documents to be on a single block. During the mid-1990s, the rising popularity of peer-to-peer networking ushered in the possibility of a distribution system that would benefit from the computational power of a network of machines. The concept of proof-of-work, a consensus mechanism that requires a significant amount of computing effort from a network of devices, was introduced around this time too. Proof-of-work is used to verify the computations and dissuade cyberattacks.

Fast forward to 2008 when Satoshi Nakamoto, believed to be a pseudonym, published a paper that introduced the concepts of Bitcoin and blockchain. Since the infrastructure of blockchain facilitates secure, peer-to-peer transactions, the need for third parties like banks was not needed to complete transactions. Over the next few years, the idea of cyber currency spread like wildfire. By 2012, *Bitcoin Magazine* had been launched, and the craze had taken hold. Vitalik Buterin, the co-founder of *Bitcoin Magazine*, proposed a platform in which blockchain technology could be decentralized. Soon after, in 2014, the Ethereum Foundation was started, which cleared the way for blockchain technology to be used in areas other than cryptocurrencies. Today, an increasing amount of businesses are using blockchain technology in some form, other than for that of cryptocurrencies. For example, about 15% of global banks were using the technology by 2017 and within two years, Walmart began a supply chain system based on the technology (Sheldon, 2021)

Practical Applications

When it comes to blockchain most people associate it with cryptocurrency, but there is so much more than just that. Blockchain can be used to share records more securely, can help make supply chain management more efficient, and can prevent fraud and streamline accounting. If we look at blockchain at a global level by industry we can see that it is mainly used in financial services, government, and healthcare. Also, when it comes to industries of blockchain, it is used in just about any industry one can think of. Blockchain has many unique applications that one would not think of such as digital voting which makes the process fully transparent, hassle-less, and universal. The pharmaceutical industry also used blockchain. When they use blockchain they are creating an end-to-end supply chain that is transparent and tamper-proof. Each step in the supply chain, from the manufacturing of drugs to their distribution and sale, can be recorded on the blockchain, creating a permanent and immutable record of the drug's journey. This makes it easier to track the origin and authenticity of drugs, thereby preventing the distribution of counterfeit drugs ("Blockchain Technology Market Size & Share Report, 2030," n.d.).

Business Applications

By utilizing blockchain technology and cryptocurrencies, businesses can potentially solve funding related problems such as non-cash payments and accounting settlements. The automation of electronic transaction management accounting can also improve the level of control of monetary business execution, both internally and externally. Additionally, blockchain technology can provide an emerging source of venture capital crowdfunding through token sales or initial coin offerings, allowing companies to handle financial-related issues more flexibly by holding, transferring, and issuing digital currencies based on blockchain technology (Eye on Tech, 2020).

Blockchain's decentralized and secure ledger allows for digital asset management and data sharing without the need for centralized agencies. By using blockchain, businesses can store data, improve transparency and security, and prevent tampering. Additionally, blockchain can support data sharing among key parties in various industries such as the accounting profession,

which uses an accountancy blockchain to aggregate and share instances of practitioner misconduct in real time (Somu, S. 2022, September 3).

By incorporating the Internet of Things (IoT) and blockchain technologies, companies can improve the transparency and traceability of their supply chain, which can help them better monitor product quality. The use of blockchain technology in the supply chain can also help reduce the potential for fraud, counterfeiting, and other unethical practices by creating an immutable record of transactions and product movements. Overall, the combination of IoT and blockchain technologies can bring greater efficiency, transparency, and security to supply chain management (Afreen, 2023).

Businesses can use blockchain technology to create "smart contracts" which are self-executing contracts that automate the negotiation, verification, and enforcement of the terms and agreements between two or more parties. Smart contracts can be used to automate business processes and collaborations, allowing for faster and more efficient transactions without the need for manual interventions or confirmation. For example, a business could use a smart contract on a blockchain to automatically file its taxes, without the need for manual input or confirmation from a tax authority (Xu, M., Chen, X. & Kou, (2019).

Disadvantages and Vulnerabilities

One major disadvantage of blockchain is its environmental impact. The process of mining cryptocurrencies requires a significant amount of computing power, and as a result, a significant amount of energy. This energy consumption leads to the release of millions of tons of CO_2 into the atmosphere, contributing to climate change (Somu, S. 2022, September 3). On top of environmental impacts, there are also threats and risks associated with using blockchain platforms.

A blockchain consists of five layers and each has its own unique vulnerabilities: Infrastructure, Data, Network, Protocol, and Application. Infrastructure is the most basic layer described as the user and their local device - the risk is private data/information theft and often is due to user risk/error. The "Data layer risk" is vulnerable to a trojan horse virus where the actual data gets manipulated or corrupted. The "Network layer Risk" is when nodes within the chain get attacked, exploited, or manipulated through weaknesses in ITP, P2P, and ISP shortcomings.

"Protocol layer risk" is interrupting the blockchain flow through users, interfaces, transactions, and verifications. The final layer is 'Application" which is the underlying mechanisms hidden behind decentralized networks. This is the least vulnerable layer and is the code between the databases and sources (Ciattaglia,Luciano Fáwọlé, John 2023).

As an example of a particular attack, a "fifty-one percent" attack on a blockchain network is where a single entity or a group of entities control more than fifty percent of the network's computing power. In such a scenario, the attackers can potentially manipulate the blockchain by creating fraudulent transactions, double-spending coins, or even preventing transactions from being processed. There are a myriad of different paths through the five layers that attackers, hackers, thieves, and pranksters can take in order to wreak havoc on vulnerable networks and blockchain systems (Ciattaglia,Luciano Fáwọlé, John 2023).

Impact on Society and Culture

The ubiquitous nature of blockchain applications has had a significant impact on society. The technology was used during the COVID-19 pandemic in the creation of a vaccine tracking system to ensure efficient distribution and the speed and reliability of contact tracing. Vaccines are not the only assets where these digital ledgers are impactful. Blockchain technology helps track and trace the origins of food, leading to safer consumption. The removal of a third party could theoretically remove control from utility companies and allow for lower electric costs. Blockchain technology in the travel industry can provide transparency and prevent inaccurate hotel bookings. In addition to the effect that blockchain technology in these industries has on our culture, we have not been immune to the excitement and popularity of cryptocurrencies. The idea of generating something that could be turned into tangible funds is too much to resist for most. Furthermore, the US government has a hard time taxing cryptocurrencies, due to their inherent anonymity of them. It is estimated that the IRS loses approximately $50 billion annually from lost taxes on cryptocurrencies (Somu, S. 2022, September 3).

The Future of Blockchain

Authors Min Xu, Xingtong Chen & Gang Kou conducted research through the Web of Science Core Collection (WOS) and filtered results to 725 sources after running a search for "blockchain." After analyzing both qualitative and quantitative literature and data the authors suggested a large area of future research should be placed on "privacy protection and security issues." (Xu, M., Chen, X. & Kou, 2019). Cyber-attacks, data breaches, and fraudulent transactions are things to watch out for when it comes to blockchain. Since blockchain is new and untested, there is a risk associated with personal information that malicious people would gain access to it (Somu, S. 2022, September 3).

According to recent market research, the global blockchain technology market was valued at USD 10.02 billion in 2022. This market is projected to experience a remarkable compound annual growth rate (CAGR) of 87.7% between 2023 and 2030. This growth is being driven by the increasing adoption of blockchain technology across various industries, as well as its potential to improve efficiency, security, and transparency in a wide range of applications. As blockchain technology continues to mature and more use cases are discovered, it is expected to play an even larger role in shaping the future of industries such as finance, healthcare, logistics, and many more ("Blockchain Technology Market Size & Share Report, 2030," n.d.).

In the face of blockchain technology, given these risks and vulnerabilities, new business models have begun to emerge in a symbiotic relationship - "Smart Contract Auditors." These companies employ sophisticated analyzing software, experts in the field, and manual audit processes to identify, trace, and verify hash transactions for validity and honesty (Ciattaglia,Luciano Fáwọlé, John 2023). Thus far it has been reported from a single company, Solidity Finance is "Now protecting over $50 billion in on-chain value across 1500+ projects."As only one company in a sea of new businesses - given the growing market of blockchain - the Smart Contract Auditing industry is only going to expand and become even more sophisticated to keep up with trends (Solidity.finance, n.d.)

Conclusion

Blockchain's variety of applications, particularly in the world of information exchange and cryptocurrency, are well documented. The popularity of Bitcoin and its rivals such as Ethereum has given rise to a market valued at 1.69 billion USD as of 2019 (Polaris Market Research, 2019). However, there are still a lot of ethical, and legal issues to be concerned about - especially in the realm of personal privacy, cybersecurity, and theft. As cryptocurrency and blockchain are projected to grow their current markets as well as expand into new ones, "Smart Contract Auditing" would appear to be part and parcel to their successful integration into the business, finance, government, and personal business.

References

Afreen, S. (2023, February 20). Why is blockchain important and why does it matters? [2022]: Simplilearn. Simplilearn.com. Retrieved May 1, 2023, from https://www.simplilearn.com/tutorials/blockchain-tutorial/why-is-blockchain-important#:~:text=Blockchain%20helps%20in%20the%20verification,the%20origin%20of%20a%20product.

Blockchain Technology Market Size & Share Report, 2030. (n.d.). Retrieved April 22, 2023, from https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market#:~:text=The%20global%20blockchain%20technology%20market%20size%20was%20valued,rate%20%28CAGR%29%20of%2087.7%25%20from%202023%20to%202030.

Ciattaglia,Luciano Fáwọlé, John, Blockchain Security: Common Vulnerabilities and How to Protect Against Them February 10. 2023 https://hacken.io/insights/blockchain-security-vulnerabilities/#:~:text=Sybil%20Attacks,51%25%20attack%20or%20even%20DoS.

Cryptocurrency Market Share, Size, Trends, Industry Analysis Report, By Type (Bitcoin, Ethereum, Cardano, Solana, Others), By End-Use (Banks, Fintech Companies, Credit Unions, Others); By Region; Segment Forecast, 2022 - 2030 https://www.polarismarketresearch.com/industry-analysis/cryptocurrency-market

Eye on Tech. (2020, August 2). 6 steps of Blockchain Storage. YouTube. Retrieved May 1, 2023, from https://www.youtube.com/watch?v=zovwM4jeYMk

Hayes, A. (2023, April 25). Blockchain facts: What is it, how it works, and how it can be used. Investopedia. Retrieved May 1, 2023, from https://www.investopedia.com/terms/b/blockchain.asp

Sheldon, R. (2021, August 9). A timeline and history of Blockchain technology. WhatIs.com. Retrieved April 25, 2023, from https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology#:~:text=A%20blockchain%20starts%20with%20an,added%20to%20the%20chain%20sequentially.

Solidity Finance. (n.d.).

Retrieved May 1, 2023, from

https://solidity.finance/.

Somu, S. (2022, September 3). How blockchain technology will change the world. Medium.

Retrieved April 28, 2023, from

https://medium.datadriveninvestor.com/how-blockchain-technology-will-change-the-worl

d-e1d915b4394f

Terrapass. (2022, December 29). Blockchain for Social Impact: The good, bad, and in between.

Terrapass. Retrieved May 1, 2023, from

https://terrapass.com/blog/blockchain-social-impact-good-bad/

Xu, M., Chen, X., & Kou, G. (2019, July 4). A systematic review of Blockchain - Financial

Innovation. SpringerOpen. Retrieved April 24, 2023, from

https://jfin-swufe.springeropen.com/articles/10.1186/s40854-019-0147-z