External Bitcoin and Blockchain Technology Audit

Posted on July 12, 2024

Encryption

Encryption is an approach to guarantee that only people with permission can access sensitive data. Spielman (2016), claims that symmetric and asymmetric encryption is important for safeguarding virtual currency transactions. Algorithms like RSA have been crucial in the evolution of built-in cryptographic policies. Using a virtual currency that is not encrypted greatly increases the risk of fraud and other forms of financial mischief. Blockchain, a sophisticated database method that improves corporate encryption by connecting multiple digital devices, is currently being adopted by businesses worldwide. Bitcoin's use of blockchain technology makes it easier for users to do financial transactions with one another. Bitcoin enabled people to use the Internet as a payment system in 2009 (Spielman,2016). Due to the possibility of fraud, data breaches, and cybersecurity issues, the usage of virtual currency now poses a significant risk to financial institutions. The security of cryptocurrency ledgers is maintained by a trusted group of individuals, such as Bitcoin miners, who secure the network in exchange for the chance to collect a randomly distributed fee. The following is a table showing an example of record keeping system for blockchain.

Block	Previous block hash	Block Hash	Transaction	Timestamp
0	N/A	N/A	Ty1, Tx2	2023-01-01 10:00
1	04f5a1	k16def0	Tx3, Tx4	2023-01-02 11:00
2	E16def2	D16ef3	Tx5, Tx6	2023-01-03 12:00
3	91dfe5	C8a2b3	Tx7, Tx8	2023-01-04 13:00
4	8jfecf4	2f19cg9	Tx9, Tx10	2023-01-05 14:00
5	6nfecm4	n16ef3	Tx11, Tx12	2023-01-06 15:00

Table 1: record-keeping system specifically for blockchain

Using the block number, transaction, and timestamp, the aforementioned block-based tracking system would aid the organization in keeping track of items. Simply put, a block is a blockchain's encrypted data storage node (Spielman,2016). Such spots are pointed out by lengthy numbers that decrypt old and new transaction data from earlier blocks. Before new blocks are generated, the network must verify a current block's data. The hash algorithm satisfies the encryption standards necessary to shield sensitive information from hackers. Typically, the hash value of the prior block in the chain is indicated by the hashtag before it.

Blockchain technology's public ledger nature makes it ideal for easily verifying and exchanging Bitcoins. Blockchains also hold other crucial information about Bitcoin transactions, like a user's payment history. Hence, Blockchain improves the transparency and trustworthiness of Bitcoin transactions. Moreover, users can keep tabs on and limit their spending thanks to blockchain technology's real-time monitoring of transactions (Spielman,2016). As a result of Bitcoin's distributed ledger technology, users may get instant notifications from anywhere in the world, improving the speed and accuracy of transactions and keeping customers up to date. Bitcoin transactions are made more private thanks to blockchain technology. This feature improves privacy by masking the user's identity during financial dealings.

Block Chain Auditing

The auditing of blockchain can enhance the accuracy of transaction verification in real time. Bitcoin users can benefit from blockchain auditing since it examines monetary transactions and flags any issues that may arise (Liu et al.,2019). Bitcoin's user interface often produces gigabytes of data from a wide variety of sources, making analysis challenging. By facilitating the identification and localization of inconsistencies and other types of errors in financial transactions, blockchain auditing can help streamline the entire process. Each transaction is validated by the blockchain node, and the user's whole history of interactions is recorded. Improved decision-making is made possible by constantly updated user information supplied by the system, thanks to blockchain technology (Liu et al.,2019). And the auditing capabilities of the blockchain allow for automatic payment processing, which makes it easier to confirm transactions. Users can instantly transfer funds between their Bitcoin wallet and their bank account or other digital money mechanism. By allowing users to detect fraud or errors, blockchain auditing generally lessens the chance of cybersecurity concerns like breaches and hacking. The auditability of a blockchain ensures the veracity and verifiability of transactions, giving users the confidence to deal freely and without worry.

Trade-offs

One of bitcoin's key drawbacks is that it is not acknowledged as a reliable medium for handling financial transactions by the vast majority of governments throughout the world. Since Bitcoin uses blockchain technology distributed across a network, it is immune to government oversight

(Yeoh,2017). Contrarily, Bitcoin users are not safeguarded from theft. Hence this increases the risk of theft involving cash or personal or company information stored in Bitcoin, such as social security numbers, bank account details, and private emails. This Bitcoin exchange has become a dangerous minefield because of the constant complaints detailing various illicit activities, placing many transactions at risk (Yeoh,2017). Experts say Bitcoin is unsafe because criminals can use it to commit fraud and steal from users. Using Bitcoin to launder money is one activity that is strongly advised against by Bitcoin's expert community. With the rise of digital money, private keys belonging to individuals are also at risk. Also, criminals utilize Bitcoins to make fraudulent investments and buy narcotics and other contraband on the dark web. Thus, governments like the United States do not recognize Bitcoin as a legitimate medium for conducting financial transactions because of the high probability that it would be used in illegal operations.

In addition, the distributed ledger technology underlying Bitcoin ensures that transactions involving the virtual money can never be undone. With bitcoin and other virtual currencies, users can never get their money back, making it difficult to track finances. Also, Bitcoin users can remain anonymous due to the anonymizing properties of blockchain technology. Because it's hard to predict who the final users will be, this feature raises the likelihood of illegal activity. As digital currency transactions cannot be undone, it is simple for individuals to lose track of their financial dealings (Farah,2018). Another disadvantage is Bitcoin's volatility. Many people consider bitcoin a valuable collectible since its creator, Mr. Nakamoto, limited the number of Bitcoins that would ever exist to 21 million. Bitcoin has flaws that make using it for financial transactions seem hazardous, but investors keep investing money. Bitcoin is accepted as payment on e-commerce platforms like PayPal, Rakuten, and Etsy.

References

Farah, N. A. A. (2018). Blockchain technology: Classification, opportunities, and challenges. *International Research Journal of Engineering and Technology*, *5*(5), 3423-3426.

Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in auditing*, *13*(2), A19-A29.

Spielman, A. (2016). *Blockchain: digitally rebuilding the real estate industry* (Doctoral dissertation, Massachusetts Institute of Technology).

Spielman, A. (2016). *Blockchain: digitally rebuilding the real estate industry* (Doctoral dissertation, Massachusetts Institute of Technology).

Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*.