VIEW POINT

SECURITY OF BLOCKCHAIN-BASED FINANCE

Abstract

Blockchain or distributed ledger technology (DLT) has emerged as a powerful tool to transform financial transactions. With its decentralised storage, cryptographic authentication, consensus protocol, and immutability, blockchain provides a tamper-proof, single source of truth for all financial records. The smart contracts feature removes the need for intermediaries in financial transactions by automating the execution of rules. Hackers have gotten around the innate security mechanisms of blockchain. Still, attacks can be prevented by analysing the potential threat based on the use case and setting up multi-level security controls, a governance structure, and incident response systems. Different financial transactions like trade finance, regulatory compliance, or financial agreements can be made more efficient, transparent, and secure by providing shared records, an authentic audit trail, error and manipulation-free payments, and automated enforcement of regulatory compliance.

Infosys®
Navigate your next

Blockchains or distributed ledger technology (DLT) have great potential to transform the financial sector. It is one of the many disruptive technologies that will pave the way for next-generation financial services.

A blockchain is a decentralised, immutable, distributed digital ledger that records transactions or assets in a business network. It works on a peer-to-peer network. Blockchains can be permissionless – allowing anyone to participate, or permissioned – where participation is based on evaluation and through invitation. The three major components of blockchain technology are distributed ledger technology (DLT), immutable records, and smart contracts.

All the members of a blockchain have access to the ledger and its records, and as it is shared, there is no duplication of information like in usual business networks. The immutability of the records ensures that nobody can alter them once records are written onto the shared block. In case of any changes, a new block with the details must be added to the blockchain, and both are visible. The smart contract is an assortment of rules that are run when the conditions for its application are met. The blockchain peer-to-peer framework can transform business processes by eliminating the necessity for intermediate central entities or processes and creating an immutable audit trail. Lowered costs, reduced risk, much-improved settlement efficiency, and transparency for all involved are the direct benefits. For financial institutions, with many of the transactions being peer-based, this could be a game changer.

Are blockchains inherently invincible? Not really. Though the framework has risk-averse properties due to the cryptographic hash and consensus protocol, it is still vulnerable to new threats that could make its use risky for financial institutions. According to the World Economic Forum, researchers have detected around 500 cybersecurity attacks with cryptocurrencies alone, leading to a loss of 9 billion dollars. Some of the attacks that blockchains are susceptible to are:

Sybil Attack: A Sybil attack happens when hackers create multiple fake nodes on the blockchain network and communicate with the genuine nodes. Once the counterfeit nodes are high enough in number to gain control over the network, they can disrupt the network operation by refusing to transmit or receive blocks or by reversing transactions. Privacy can be violated through monitoring of data transfer.

51% Attack: When a group of miners assumes control over more than half of the blockchain's computing power, it is called a 51% attack. Here, the attackers can supersede the consensus protocol. They can reorder and disallow transactions and carry out illegal actions like double-spending.

Endpoint Vulnerability: The endpoint is the interface through which users access the blockchain. They are usually devices like a laptop or a mobile. Hackers can get to the user's key by attacking the endpoint device and using it to access all the user's data on the blockchain.

Phishing Attack: In the case of blockchain, the most prevalent scam to get a user's credentials is a phishing attack. Emails that look authentic but have fake hyperlinks are sent to users to get them to divulge details. These links lead to websites that imitate the actual one, and once the users enter their information, it is used to access their accounts.

Routing Attack: Blockchains are based on real-time, high-volume data transmission. A routing attack can delay or deny some nodes' transactions or partition the blockchain network. The attacker can intercept the data by rerouting it through a different destination. When a blockchain is partitioned into disparate parts by a routing attack, nodes within one part cannot interact with the nodes in the other section, creating parallel blockchains. This partition can cause a denial of service, revenue loss, and double-spending.

Smart Contract Attack: Smart contracts are vulnerable to being manipulated. Here's an example of such an attack – hackers capitalised on an unanticipated irregularity in a smart contract, and the Decentralised Autonomous Organisation (DAO) lost around 80 million dollars in 2016.

A holistic security approach should be taken toward the implementation of blockchain. Blockchain is innately secure, but as seen in multiple instances, cryptographic protocols and decentralisation are limited. Security controls should be chosen based on use case scenarios and organisational requirements. Conventional weak points associated with the public key and the application code, like a compromised key or vulnerable code, must be identified. Attacks specifically aimed at blockchains, such as denial of service, exploitation of smart contracts, and hacking of wallets, should also be considered. Develop the threat model and implement security controls to address the risks. Classic security practices like efficient management of keys, regular review protocols for code, encryption of data, and access control can be worked into regular schedules as the first level. Additionally, deterrents like secure management of wallets, monitoring of permissioned chains, and secure development of smart contracts applicable to blockchain risks, need to be a compulsory part of the standard operating processes. People, processes, and technology play an equal role in ensuring security. So, appropriate checks for efficient governance and a robust response protocol for incidents are vital to securing blockchains.

Blockchain is expected to revolutionise the functioning of the financial sector and have far-reaching impacts. The DLT technology will be applied differently based on the requirements of each use case. Trade finance using blockchain will have tamper-proof documents without risk of forgery, real-time and transparent transaction audit trail, and error and manipulation-free trade payments and actions using smart contracts. Regulatory compliance is another area where the immutable property of blockchains leads to enhanced integrity and security. As financial systems and instruments get more complex, ensuring transparency is increasingly expensive and risky. DLT can provide real-time shared data between regulators and regulated organisations, a platform for KYC procedures, anti-money laundering checks, and smart contracts to enforce regulatory compliance. Financial agreements consist of complicated business rules to ensure that both sides meet their obligations and, when recorded on a blockchain, cannot be modified without the consensus of all parties. Every participant has both the keys – public and private. The private key is used as a digital signature for the agreement, while the public key is used to verify authenticity without access to sensitive information. Smart contracts remove intermediaries and can automate execution, lowering the risk of fraud.

The use cases for blockchain in the financial sector are wide, varied, and pervasive. It will bring simplicity, efficiency, transparency, and security. DLT is not a cure, but it will establish new financial services infrastructure, revamp processes, and reimagine functions.

* For organizations on the digital transformation journey, agility is key in responding to a rapidly changing technology and business landscape. Now more than ever, it is crucial to deliver and exceed on organizational expectations with a robust digital mindset backed by innovation. Enabling businesses to sense, learn, respond, and evolve like a living organism, will be imperative for business excellence going forward. A comprehensive, yet modular suite of services is doing exactly that. Equipping **organizations with intuitive decision**-making automatically at scale, actionable insights based on real-time solutions, anytime/anywhere experience, and in-depth data visibility across functions leading to hyper-productivity, Live Enterprise is building connected organizations that are innovating collaboratively for the future.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next