How To Secure Blockchain Transactions

TechRounder PDF Edition

Live article: https://www.techrounder.com/finance/how-to-secure-blockchain-transactions/

By Vipin PG | Published October 13, 2022 | Updated January 4, 2026 | Format: Guide | 4 min read

Quick answer

Blockchain technologies are being deeply integrated into our lives these days. This is because they are believed to be the most effective tools for making transactions protected.

Blockchain technologies are being deeply integrated into our lives these days. This is because they are believed to be the most effective tools for making transactions protected. But is this statement true or just a popular myth? How does the system protect transactional data within corporate and governmental networks? What is cryptography? What are the common concerns of users? These are the questions we will try to answer in today’s review.

Elements that provide security

To figure out how blockchain activities function, let’s get down to the definition of the concept. According to Wikipedia, "a blockchain is a type of distributed ledger technology (DLT) that consists of a growing list of records, called blocks, that are securely linked together using cryptography."

This connection ensures the pieces of encrypted information from any block cannot be hacked because to hack one block, a hacker would need to access a linked one as well, which is impossible without being detected. This method is quite efficient, but it isn’t the only tool that makes this environment hack-proof.

As mentioned earlier, the system uses cryptography to connect blocks storing data. Cryptography and its types might differ in various networks. Nevertheless, all the most popular types of cryptography follow the same concept. According to this idea, every network user receives a private key.

This private key is a form of a personal digital signature used to authorize transactions taking place within the network. If a record is altered, the signature will become invalid, and the peer network will know immediately that something has happened. Further damage will be prevented if an early notification is provided due to this violation.

One more feature that makes it so successful is decentralization. This means that there’s no single storage where blockchains are processed. Hackers cannot access it, as blocks cannot be altered through a single computer. Any swap in blocks requires authorization from an immense computing power that will exceed 50% of the whole number of network participants. Even if the blockchain-based network is small, it’s still unclear whether one can hack it. Even if possible, the result will probably not be worth the effort and the means.

At this point, it seems that we all understand how all these features combine and what they do to make the operations within the digital networks of businesses protected. Yet, when blockchain is needed in your business, you should know how to find a solution that will meet all the requirements mentioned above. Keep in mind that not all blockchains are created equal.

Blockchains might be different

If you are looking for top-notch instruments to guarantee that transactions of your business network are protected, it's vital to be aware that blockchains might differ. Currently, businesses rely upon two major types - public and private blockchains. Some variations might combine various features of both types. In addition, these blockchains are different in terms of the available safety levels.

To cut a long story short, activities in a public blockchain are validated via computing powers connected to the publicly available internet. This network isn't prohibited and doesn't require any permission. Private blockchain reduces the number of participants permitted to access the network. Private blockchains are accessible only to particular organizations, which form a private network through cooperation.

Consortium blockchains also deserve mentioning if we discuss the differences between various solutions. This is the third type of blockchain, although it isn't as popular as the two described before. Consortium blockchains include participants that were approved by a specific authority in advance.

Thanks to this concept, the network becomes decentralized, but the power doesn't lose control over it, although this control isn't significant. As a result, consortium blockchains are quite effective in different industries. Commonly, they are used in banking and supply chain management applications.

Are there any security issues?

Even such sophisticated and well-thought-out instruments as this cannot be perfect. Although blockchain transactions are secure, there's no point in denying its weak spots. The most obvious and common issues and concerns of a blockchain are:

- Routing: When blockchain transactions are processed, data between blocks are transferred in real time. That's why there is a probability that the data might be intercepted on its way to Internet Service Providers.
- 51% attacks: As we've mentioned above, there is a risk that big amounts of computing power might attack smaller networks. Although this is very resourceful, this approach might work. Nevertheless, private blockchains can prevent such hacking attempts.
- Sybil attacks: If the system isn't resilient enough, it's possible that hackers can crash it by flooding the network with an overwhelming amount of false identities.

Conclusion

To sum it up, we would like to say that although the obvious concerns, blockchain transactions have proven to be the safest. We hope that now you can better understand how blockchain-based networks work. Use this knowledge to benefit your business and take it to a higher level!

References

1. en.wikipedia.org - wiki / Blockchain - https://en.wikipedia.org/wiki/Blockchain

2. primexbt.com - for-traders / what-is-cryptography - https://primexbt.com/for-traders/what-is-cryptography/