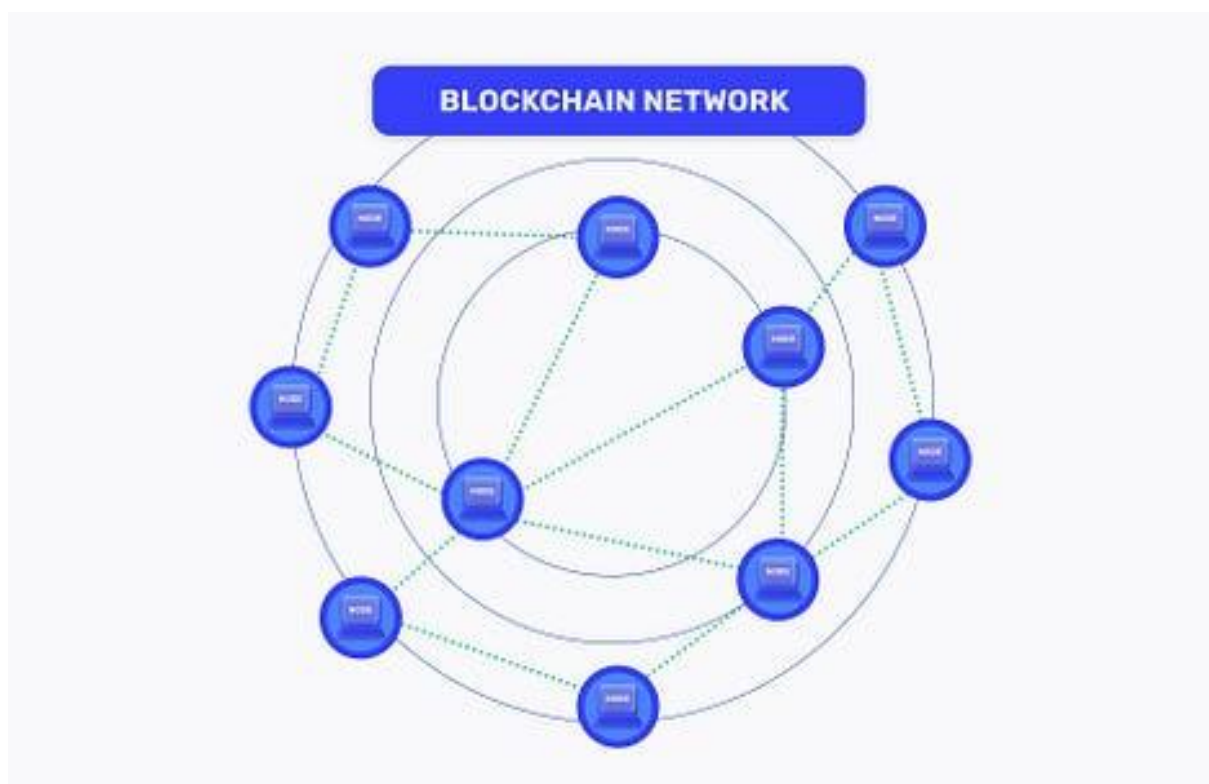# Blockchain node provider — a friend or foe?

The answer to that intriguing opening question lies in your hands, (more on that later).

First though, what comes to your mind when you hear the word **node** being used?

The term **node (or computer node)** from a blockchain context is often used to describe a **communication endpoint** that allows for the reception, creation, and transmission of digital messages. There are varying kinds of computer nodes such as **physical network nodes** and **virtual nodes.** However, in this piece, we will be focusing on virtual nodes such as the ones used in several blockchain networks today.

What are blockchain networks?

In simple words, a blockchain can be referred to as a distributed open ledger system or *distributed ledger technology* (or DLT) that contains a record of transactions (or block of transactions) taking place on the network which is virtually impossible to modify. In other words, we can refer to a blockchain as a **spreadsheet** that contains a record of

transactions that is publicly accessible for review and is not solely controlled by one entity.

The first point of contact for the average user with a blockchain network is usually through a **blockchain wallet.** By means of a blockchain wallet, a user generates a **public address** that allows them to receive value (in the form of coins and tokens) from the blockchain network. They can then transfer, and sign digital messages by means of a private key, which is a long random set of characters unique to the user.

Blockchain nodes and you

Whenever a user initiates a transaction, the details of the transaction are sent via an **RPC call (remote procedure call)** to a blockchain node, such as the amount of value to be sent, and the **recipient** of the value, which is then recorded and transmitted to the entire network by the nodes.
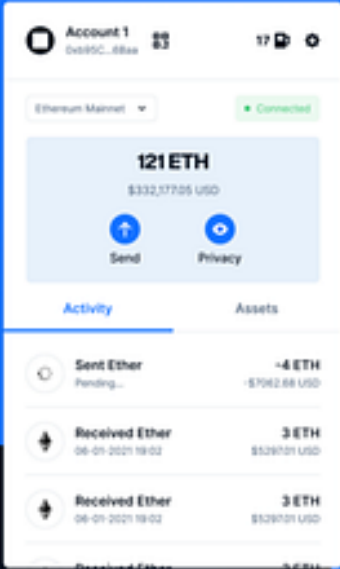
An interesting point to note though is that when the RPC call is made to the node as you initiate a transaction on the wallet, certain information about you is also sent to the node, such as your **IP address** and **other metadata.**

This seemingly non-consequential piece of information sent to the node, in reality, can leave **traces** about you, which a centralized entity or malicious actors can exploit to track you. **Did we say track you, how?** You may ask. Yes, blockchain nodes are run by *"human entities"*, often called **blockchain node providers.** These entities provide the necessary infrastructure in the form of hardware and software needed to successfully manage and run blockchain nodes. The downside to this setup is that although the original concept of blockchain is built on the primitives of decentralization, the interface (via RPC calls) with a single node provider introduces a somewhat **centralized entity** into the blockchain system that was originally intended to be completely decentralized.

Thankfully though, this often unfamiliar, yet serious downside has been addressed by an innovative solution. What solution? The solution lies in your **choice of web3 wallet** used to interact with dApps.
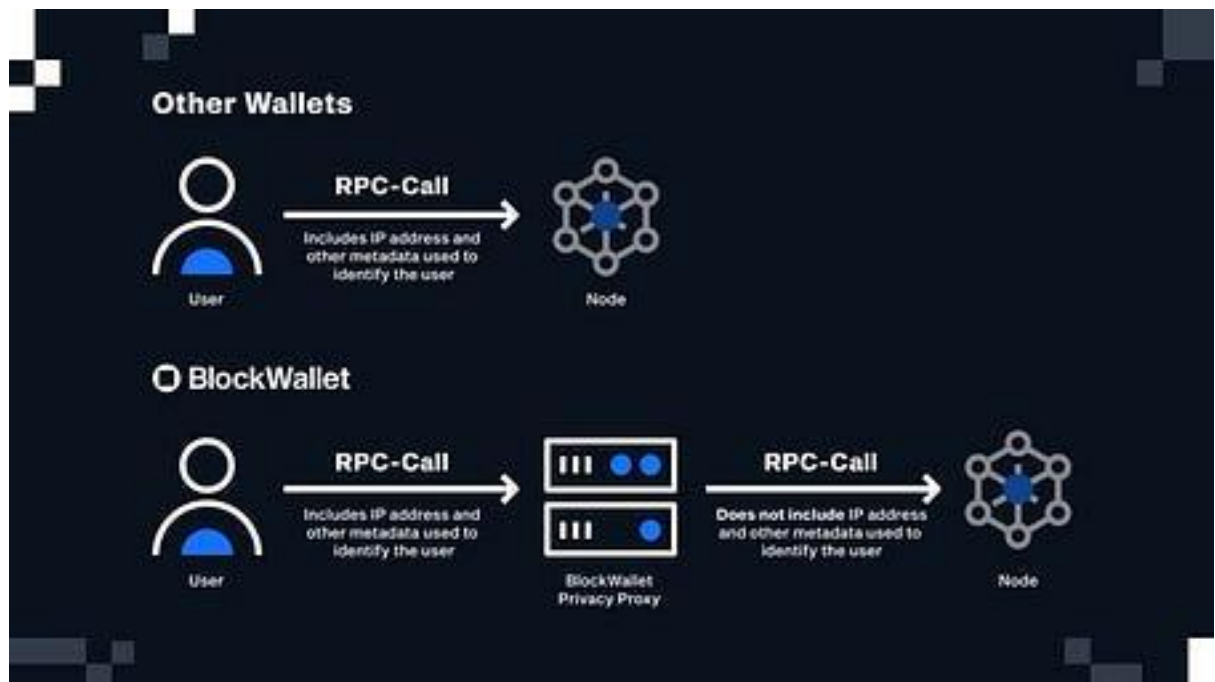

Interestingly, privacy-centric wallets like **Block Wallet** are championing efforts to protect user privacy by hiding your IP & metadata as you interact on the blockchain. This is made possible by employing the use of a privacy proxy that allows a

user to stay private as they interact with decentralized

applications on the blockchain.

But that's not all, unlike other web3 wallet providers,

BlockWallet uses 5 different node providers when

compared to other wallets that use only one. **Why is this**

important? Going back to our talk about the downsides

presented by interacting with node providers, this presents the

issue of centralization by having a single point of dependence. What do we mean?

What happens if the single node provider goes offline due to technical or legal issues?

What if malicious actors gain unauthorized control of the node provider infrastructure?

Or what if the node provider deliberately goes rogue by turning malicious?

In short, there are certain **risks of failure and privacy concerns** from using web3 wallet providers using only a single node provider. Part of the goal of this piece is to educate users about these risks, and we believe you have been well-educated.

Conclusion

Blockchain node providers play an important role (if not a very important role like *a friend*) in the functioning of blockchain networks, such as storing copies of the blockchain timely and securely, and then ensuring the stored information is shared with other connected computers on the network. However, they can easily become centralized entities (*a foe*) having access to privileged information about users who interact on the decentralized network. Thankfully, privacy-centric wallet solutions like BlockWallet give blockchain users the ability to stay private as they interact with blockchain networks. **The choice now to stay private on the blockchain lies in your hands, the users.**

The article series continues. **Front-running** remains another issue that currently affects users of decentralized finance applications. You can learn smart ways to protect yourself and others from front-running here.

Join the BlockWallet community today

Disclaimer: The information presented in this piece is merely for educational purposes only, it contains the viewpoint of the author, and does not constitute investment advice. Readers are kindly advised to do their own research on the subject and are free to disagree with the viewpoints shared by the author here. Thank you.