Team develops a bridge between different cryptocurrencies

June 26 2023

Credit: Pixabay/CC0 Public Domain

Bitcoin is probably the best-known cryptocurrency in the world today—but there are many others, each implementing and offering different technical features. For exchanging a cryptocurrency for another, so-called "bridges" are used, often provided by companies that hold large sums of different cryptocurrencies and offer to exchange them. However, this has repeatedly led to security problems and

spectacular criminal cases; cryptocurrencies worth billions of euros have been stolen in the process.

Researchers at TU Wien have now developed a novel protocol that enables the exchange of one cryptocurrency for another in an efficient and secure manner—and in a completely decentralized way, without having to use a large crypto-depot of commercial providers. "Glimpse" is the name of the new protocol, which is now expected to open up entirely new options for the crypto world. The paper presenting this new tool was accepted at the USENIX Security Symposium, which will be held in Los Angeles in August.

Simple transfers and smart contracts

With cryptocurrencies, every transaction is stored in a public ledger containing the complete history of transactions, the so-called blockchain. In blockchains there is always agreement who moved how much money to whom and on account balances. Transactions can also be more complicated than simple bank transfers.

"Cryptocurrencies offer some degree of programmability; for example, you can enter transfers into the system that only become valid when certain conditions are met," explains Giulia Scaffino, the paper's lead author.

These conditions are defined in a computer-readable contract, called "smart contract," and they are verified at a later point in time, thereby successfully completing the money transfer when the specified conditions have been fulfilled, or aborting it otherwise.

While this type of transactions are inherently possible within a specific blockchain, cross-currency transactions from one cryptocurrency to another are more complicated and are not supported by default. This is

exactly what the newly developed protocol makes possible in an efficient, decentralized and secure way. The research was conducted as part of the collaboration between TU Wien and Pantos, a decentralized multi-blockchain token system. In addition to Giulia Scaffino, Lukas Aumayr and Zeta Avarikioti were involved in the research.

Bitcoin for Ethereum

Suppose a Bitcoin owner wants to exchange Bitcoins for Ethereum. After finding an Ethereum owner willing to exchange the currency, how can this transaction be done reliably and efficiently if Bitcoin and Ethereum are technically not connected?

The basic concept is simple. First, the Ethereum owner generates a random number and gives it to the Bitcoin owner. Then, a smart contract is set up in the Ethereum blockchain that guarantees that a certain amount of Ethereum will be transferred to the Bitcoin owner—but not immediately; only after certain conditions have been met. In the Bitcoin blockchain, the Bitcoin owner has to first transfer Bitcoins to the Ethereum owner and include the random number in the transfer to avoid security attacks. Now, the Bitcoin owner can use the block of the Bitcoin blockchain including the transfer and the random number as well as an agreed-upon number of subsequent blocks to prove on the Ethereum blockchain that the Bitcoins were indeed transferred. This fulfills the smart contract conditions, and allows to finally transfer the agreed amount of Ethereum.

Efficient, compatible and expressive

"The protocol we developed had to meet several important efficiency properties," says Zeta Avarikioti. "It has to prove that the amount was actually transferred by only using a relatively small amount of data. If

large parts of a blockchain were needed for this, with hundreds of gigabytes of data, it would be completely impractical. In addition, the protocol should have the greatest possible compatibility with existing blockchains—as many cryptocurrencies as possible should be supported."

The newly developed protocol could be integrated directly into existing crypto software. Talks are underway with Bitpanda, with which the research team is cooperating closely.

"The possibilities of the new protocol go far beyond the exchange of one cryptocurrency for another," says Lukas Aumayr. "For example, we show that Glimpse can be used to express crypto-loans within smart contracts, as well as other exciting decentralized financial instruments such as asset migrations, and wrapping and unwrapping of tokens."

More information: Giulia Scaffino et al, Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi (2023)

Provided by Vienna University of Technology