Blockchains in re

Blockchains promise widescale open Internet applications that are organised decentrally. This comes at the price of slow performance for every transaction processed by the system. Cryptography researchers around Professor Sebastian Faust have achieved global awareness with their approach to facilitating real-time transactions using blockchains such as Ethereum.

By Boris Hänßler

Paying by credit card is a quick process: the money transfer is completed only a few seconds after customers place a card in a reader or enter their details online. This process enables a centrally organised company such as Visa to handle over 50,000 transactions per second at peak times. Using a cryptocurrency such as Bitcoin, where transactions are processed locally via a blockchain, a maximum of seven transactions can be processed per second – a tremendous difference that greatly hinders applicability of the technology. Even worse, it can also take several minutes to process a single transaction. These drawbacks do not only apply to Bitcoin. Even more complex applications that are processed using smart contracts over Ethereum are expensive and slow as well.

"A blockchain only becomes relevant in the event of a dispute."

Yet the blockchain is designed for just these cases. Any user can upload and distribute something via a blockchain, and anyone can become part of it. It is decentralised, neutral and effectively the perfect combination of intermediary and judge – but it is also slow. To interact with it inexpensively and in real-time – that is the vision of Sebastian Faust, Professor of Applied Cryptography, and his team. The challenge is that the increase of performance must not be at the expense of safety. The research is part of the Collaborative Research Centre CROSSING, which is supported by the German Research Foundation.

A blockchain is a chain of blocks that contains the state of the decentralised system. In case of a currency such as Bitcoin, this would be payment transactions: who is paying whom how much. Each block also contains a so-called hash of all the data in the block, a kind of fingerprint of the data. If any of the data is changed, this changes the hash value. Furthermore, each block contains a cryptographic hash of the previous block. This results in a linked chain. A new Bitcoin block is created by a network participant – known as a miner – on average every ten minutes. This block is then checked by all the other participants and accepted as a new block in the chain if all the transactions and calculations are correct. This makes the block part of the blockchain, based on which all the miners attempt to find the next block. If the block is incorrect it is ignored. A transaction in a block is only accepted if it has been published in the blockchain and ideally confirmed by several blocks, usually six. This prevents an attacker from being able to publish incorrect transactions or blocks. While this process offers strong security guarantees one of its main shortcomings is that users may have to wait up to 60 minutes for confirmation of new transactions.

Smart contracts allow particpants to carry out transactions that are significantly more complex than simple payments. These complex rules may be written in a programming language, where payments are then carried out depending on the execution of the code. „These are contracts that are processed by the blockchain," explains Sebastian Faust. „Smart means that the contracts contain logical conditions. If, for instance, someone wants to sell a file online, then the smart contract contains the condition that the money will not be paid until the correct file has been delivered." This happens automatically, which is safe for both parties. The money stays in the blockchain until the file is sent, but the seller cannot spend it elsewhere.

Another example of smart contracts are applications for communication between autonomous vehicles. Some lorries are able to drive autonomously on roads. However, they are expensive because they require a large amount of sensor technology. A semi-autonomous lorry cannot drive itself, but could be co-controlled by an autonomous one. For this to work, the driver of the semi-autonomous lorry would have to enter into a contract with the autonomous one. The driver could sleep during this time without having to take a break to specifically do so. A smart contract could do all this if there would not be the problem that the blockchain is currently too slow for speedy transactions on the road.

„Our idea is not to move everything to the blockchain," says Faust. This means that contracts are first executed directly between the involved parties and only in case of dispute the parties use the expensive blockchain mechanism." „It's a bit like being in court," says Faust. „As the processes in court are slow and costly, parties only go there if they are unable to agree between themselves." The advantage of this approach is scalability. As disputes are an exception in normal daily life, thousands of contracts could be carried out in real-time, thereby significantly reducing the load on the blockchain.

Complex computer programs may also contain fatal security problems. „Smart contracts are often implemented incorrectly, which makes it hard to guarantee that they will work correctly once integrated into a larger

Information

Department of Computer Science
Prof. Dr. Sebastian Faust
Phone: +49 (0)6151/16– 25710
Email: sebastian.faust@cs.tu-darmstadt.de
https://bit.ly/2QtCzRS

al-time

system," says Sebastian Faust. One prominent example is the case of the „The DAO" smart contract. In "The DAO" a hacker was able to use a programming error to steal cryptocurrency worth US$ 50 million. One of the main aims of the research being carried out at TU Darmstadt is to improve the efficiency of blockchain systems while at the same time offering strong security guarantees.

Developing the cryptographic protocols for these processes is a complex undertaking. The researchers need to define the protocols run by the different parties as well as the underlying smart contracts. One particular challenge is to minimize the interaction with the blockchain, while at the same time the security of the protocol has to be guaranteed. Using formal models from cryptography the researchers have confirmed the security of the protocols. The next steps are now to release the Perun system as an open source software, and integrate blockchain systems that are different from Ethereum.

The system is called Perun – after the Slavic god of thunder and lighting. And they had an impact: the results received broad attention, both from the academic security community and from companies such as Bosch and the Ethereum Foundation, whose blockchain supports smart contracts.

The author is a technology journalist.

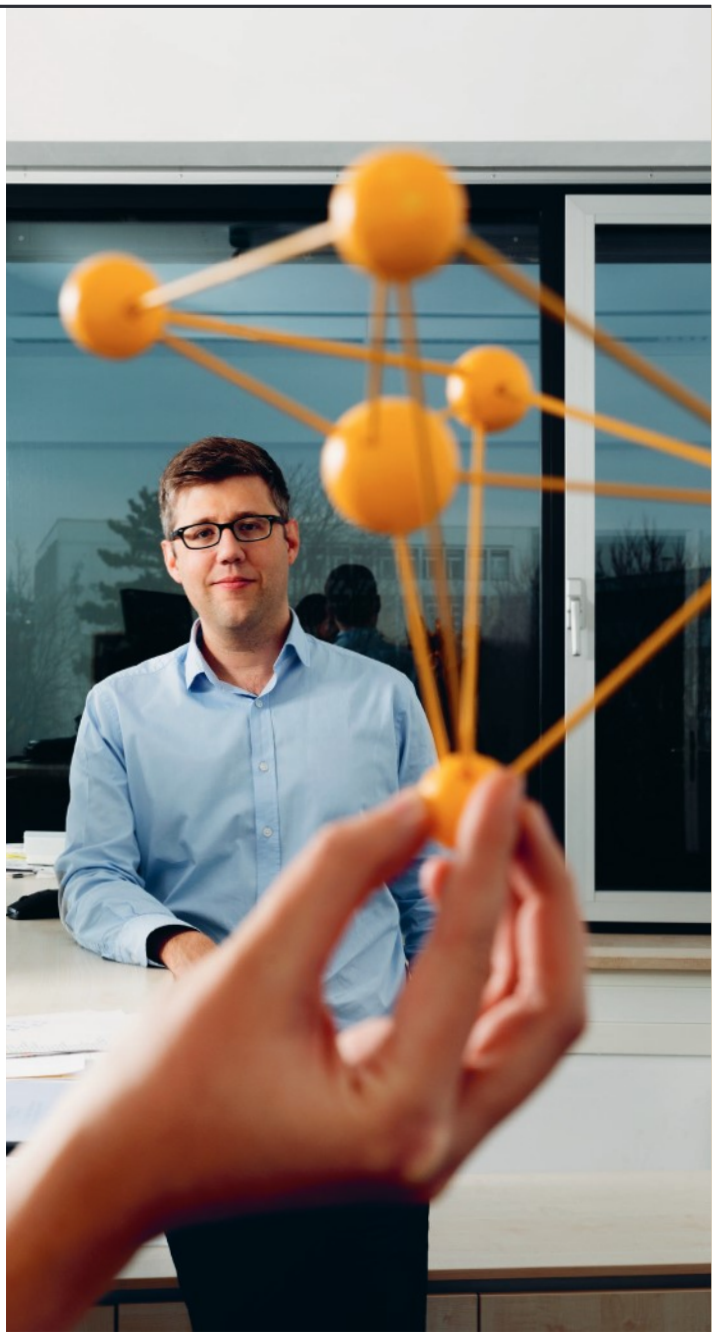

Photo: Katrin Binner

Professor Sebastian Faust, expert in cryptography processes.

Facts and figures

Since 2018, research into „Secure and Scalable Blockchain Technology (S07)" has been part of the Collaborative Research Centre 1119 of the DFG entitled project „CROSSING - Cryptography-Based Security Solutions: Enabling Trust in New and Next Generation Computing Environments". Prof. Dr. Sebastian Faust of the Department of Computer Science is responsible for the project „Secure and Scalable Blockchain Technology (S07)".

Three papers by the researchers from the group of Sebastian Faust were accepted at the leading conferences on IT Security, the IEEE S&P and ACM CCS, including:

Stefan Dziembowski, Lisa Eckey and Sebastian Faust: PERUN: Virtual Payment Hubs over Cryptocurrencies. In: 40th IEEE Symposium on Security and Privacy (S&P), 2019

Stefan Dziembowski, Sebastian Faust and Kristina Hostakova: Generalized State Channel Networks. In: 25th ACM Conference on Computer and Communications Security (CCS), 2018