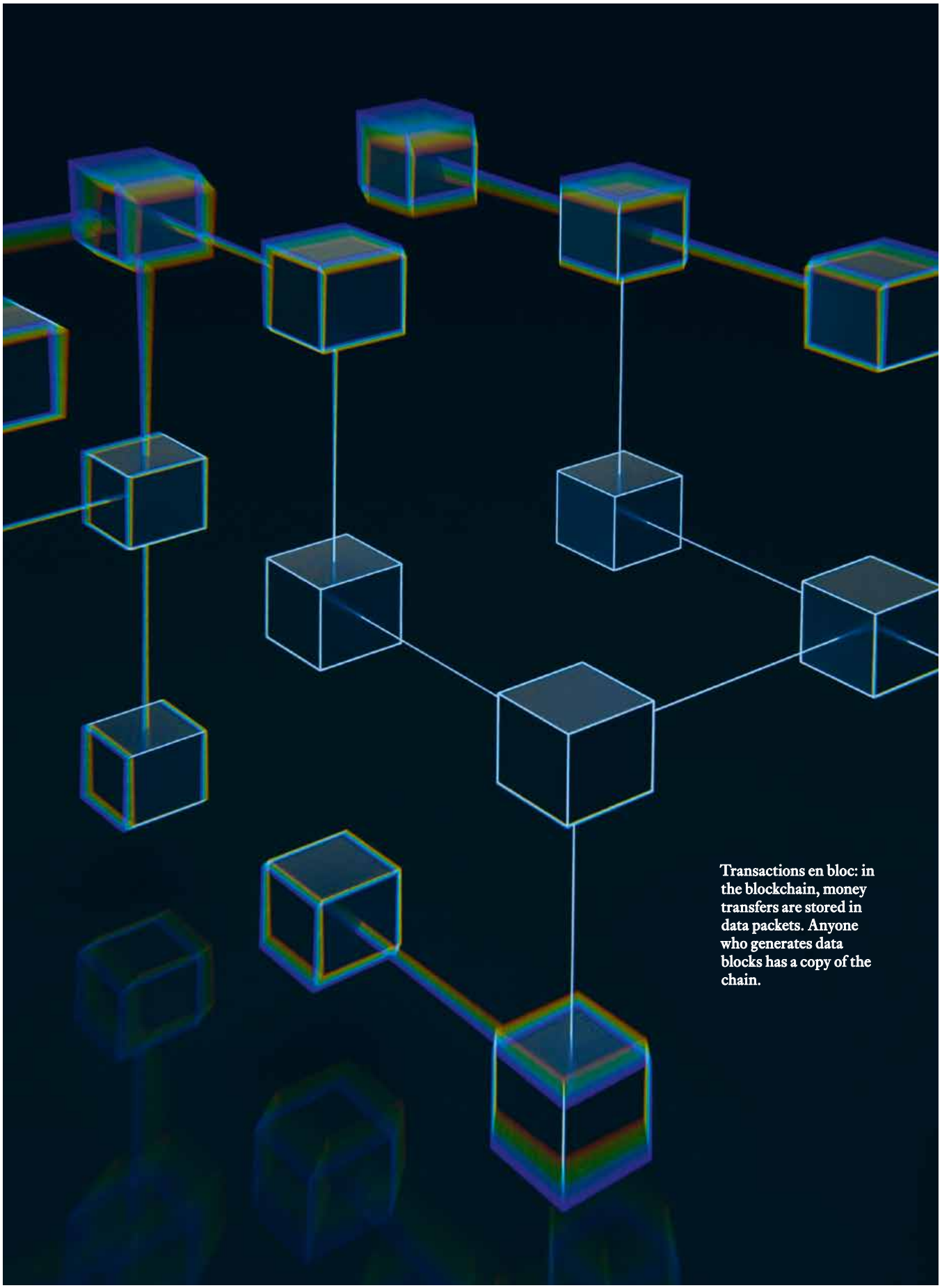


Transactions en bloc: in the blockchain, money transfers are stored in data packets. Anyone who generates data blocks has a copy of the chain.

PHOTO: UNSPLASH / SHUBHAM-DHAGE

GAPS IN THE BLOCKCHAIN

TEXT: THOMAS BRANDSTETTER

Blockchains form the backbone of cryptocurrencies such as Bitcoin, but they can also be used to process all kinds of transactions. They not only avoid the need for institutions such as banks or notaries, but they are also designed to be inherently secure against theft and fraud. However, blockchain-based applications are by no means invulnerable. Clara Schneidewind and her team at the Max Planck Institute for Security and Privacy in Bochum are identifying security vulnerabilities in applications of this kind.

It is an attempt to reorganize the world of business: blockchains take on functions normally performed by banks or notaries, such as confirming transactions and documenting digital ownership. The most prominent examples are cryptocurrencies such as Bitcoin and Ethereum. Blockchains are, in essence, a form of digital authentication – carried out not by individual institutions, but rather by a multitude of participants who neither know nor need to trust one another. This technology is based on encrypted, or at least digitally signed, data packets that are managed and monitored in a decentralized manner. Trusted central authorities are therefore no longer needed. Additionally, the blockchain aims to enhance the security of certain transactions through smart contracts.

The blockchain is in fact based on state-of-the-art cryptography. Data blocks are linked together like beads on a necklace. In addition to their content, they contain the cryptographic fingerprint of all previous blocks. Once the chain is created, it can no longer be altered. Any manipulation of a block would be immediately noticeable because the subsequent blocks would no longer match the original block. Additionally, identical copies of the blockchain are stored on multiple independent servers. When blocks store a history of money transfers, what you have is a cryptocurrency. This includes private individuals as well as institutional players, such as companies and public institutions.

So far, so secure. However, the blockchain is not the end of the story, despite being the flawless backbone of its applications. "The cryptography →

is secure, but it only ensures that no one can retroactively alter the history," says Clara Schneidewind, who heads the Heinz Nixdorf Research Group for Cryptocurrencies and Smart Contracts at the Max Planck Institute for Security and Privacy. The mechanisms for generating the chains are not nearly as secure as the result. The same applies to the interfaces with the outside world, through which Bitcoins can be exchanged for other currencies, for example. And when blocks contain not only simple transactions, but also more complex constructs, such as digital contracts, hackers repeatedly find vulnerabilities. As a result, Schneidewind and her team have set out to find solutions to the security challenges posed by blockchain applications.

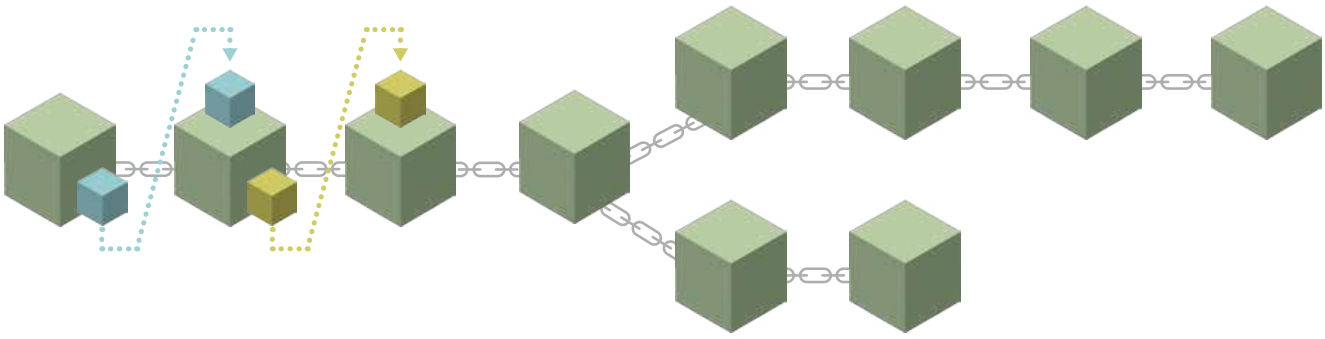
One vulnerability stems from the blockchain's most fundamental characteristic: its decentralized structure. All participants have the same information about its content because the blockchain exists as identical copies on multiple different servers, known as nodes. Participants are also equal in other respects. Unlike government-issued currencies, there is no higher authority that can make decisions or adjudicate disputes. Nevertheless, someone must document current transactions in a new block and add them to the chain to keep the blockchain running.

Computing Power Wins

"Ideally, the system should randomly select someone to generate the next block of transactions," says Schneidewind. This would ensure that the expansion proceeds fairly and that no one is censored. In practice, however, random selection is difficult because individual participants could create multiple identities to gain an advantage during selection. Interest in creating blocks is high because participants are rewarded with new cryptocurrency for doing so. Therefore, the participant who gets to create the next block must be determined by other means. For example, the proof-of-work mechanism that powers Bitcoin does not select participants at random but rather based on their available computing power.

This computing power is required for a process known as mining. The blockchain automatically generates a complex mathematical puzzle, and the first person to solve it is allowed to create the next block containing the transactions that took place during the calculation. This computational task simultaneously produces the cryptographic fingerprint of the chain to date. These calculations consume enormous amounts of energy, making any potential manipulation extremely costly. This is precisely the core of the blockchain's security. "Back then, it was a very elegant solution to Bitcoin's challenge of selecting people at random," says Schneidewind.

However, if an attacker had more computing power than all the other participants combined, they could throw the system into chaos. They could secretly build their own private chain in parallel to the public blockchain. Although this chain's content would largely match that of the public blockchain, the attacker could hide their own transactions. Meanwhile, they could continue making purchases via the original blockchain, and these



GRAPHIC: GCO

An encrypted chain: each new link in the blockchain contains a cryptographic fingerprint of the previous one, as shown by the blue and yellow blocks. Forking may occur when new data blocks are created. After a short time, however, one branch gains the upper hand and is continued exclusively.

transactions would initially be confirmed. However, due to their superior computing power, the attacker's chain would grow faster than the public one. If the decentralized versions of the blockchain stored by the various participants are not the same length and are not equally up to date, the consensus protocol stipulates that work should always continue on the longest existing chain. Therefore, as soon as the attacker publishes their version, the collective will automatically regard it as the valid chain and adopt it, even if the attacker omitted their own transactions. Their previously confirmed payments would never have occurred in the new blockchain, yet they could keep the goods purchased with them. "However, it's unclear whether there actually are actors who can concentrate enough power to carry out such an attack," says Schneidewind.

Danger in the Dark

Another way to attack blockchain networks is what is referred to as an eclipse attack. In this scenario, an attacker deliberately isolates a single participant from the rest of the network. The attacker surrounds the victim with manipulated nodes, cutting them off from the real blockchain – hence the name "eclipse." The isolated victim then only receives information controlled by the attacker, which presents a distorted view of the blockchain's state. For instance, the attacker can falsify a payment to trick the victim into delivering goods without receiving any actual compensation. "However, such attacks require enormous infrastructure and involve attacking routers or specific locations," says Schneidewind. "That makes them very complex and often simply too expensive."

However, cryptocurrencies can be more easily manipulated, at least in theory. In addition to its exorbitant energy consumption, the proof-of-work mechanism has another drawback: there can be long wait times until the current puzzle is solved and a new block is generated. Current transactions cannot be recorded immediately in the blockchain and remain in limbo for a while. "If you want to use cryptocurrencies for instant payments, you'd theoretically have to wait minutes at the till until the payment is secure," says Schneidewind. "Otherwise, there's a risk of fraud." For example, by displaying a freshly sent but still unconfirmed transaction in their wallet app, a malicious user could trick a merchant into believing that they have already paid for an item, only to use the same coin – a specific digital unit of currency that is often the subject of cryptocurrency transactions – again shortly thereafter. If the fraudster also has a good connection to a miner, they might succeed in having the second transaction recorded in the blockchain first. Thus, they would have effectively used the same coin twice. "That would render the first payment attempt invalid," says Schneidewind. "So, you can only be truly certain once the transaction is firmly recorded in the blockchain."

If payment recipients always wait for the transaction to be recorded in the blockchain before providing the goods or services, such an attack is highly unlikely to occur. This is illustrated by the history of the most prominent cryptocurrency: Bitcoin. Launched by anonymous developers, Bitcoin was the first functioning implementation of the proof-of-work mechanism. "That was over 17 years ago, and although Bitcoin is a highly lucrative target, its blockchain has never been hacked," says Nils Urbach, a professor of business informatics at Frankfurt University of Applied Sciences and a Director of the Fraunhofer Blockchain Lab.

However, the reasons for this are not only technical but also economic. Even if an actor had the computing power required to mount an attack, doing so would harm their own interests. The market value of the affected currency would likely plummet, causing the value of the bad actor's coins and mining-specific hardware to decrease as well. Rapid technological progress does not currently pose a threat to Bitcoin either. Quantum computers, for example, which are currently under development, are said to have the potential to undermine traditional cryptographic methods. "Theoretically, they could crack the signature methods used by blockchains," says Urbach. These signatures serve as proof that someone is authorized to own a specific unit of currency. If they are cracked, an attacker could spend other people's money. However, cryptocurrencies benefit from the fact that quantum computer development is progressing slowly, and in any case, alternative, quantum-secure signatures already exist.

Artificial intelligence, on the other hand, cannot compromise blockchain encryption. Still, it could be used to search through large amounts of data for vulnerabilities in the →

SUMMARY

Blockchains form the backbone of cryptocurrencies and perform the functions of institutions like banks and notaries for multiple participants. They are designed to be secure. However, security vulnerabilities can arise during their creation and in the applications running on them.

For instance, attackers with significant computing power could hijack nodes in the participant network and trick individual participants into making payments. The biggest security vulnerabilities arise from poorly programmed applications, such as smart contracts. Cybercriminals have stolen millions of US dollars through these vulnerabilities.

A team at Max Planck identifies security vulnerabilities in blockchains and develops protocols designed to secure transactions, such as those between different blockchains.

applications built on top of blockchains. Minor security flaws in cryptocurrencies have already been identified even without the use of AI. This often affects the interface between blockchain technology and the rest of the digital world, such as when traditional currencies are exchanged for Bitcoin, for example. "These are often entry points for hackers, as has already happened in the past," says Urbach.

Automated Transactions

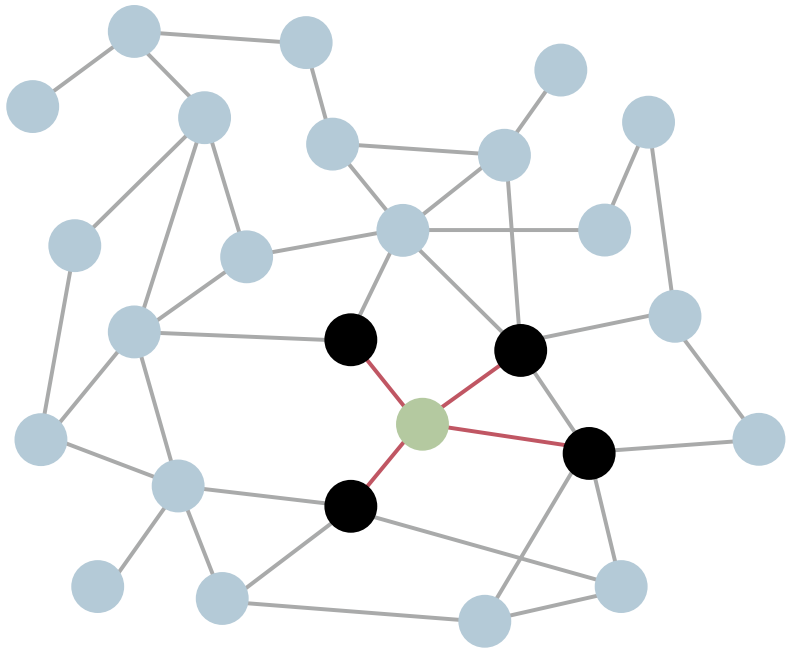
The use of blockchains is not limited to managing cryptocurrencies. Automated processes for all kinds of transactions, or smart contracts, can also be stored in their blocks. Smart contracts are nothing more than program codes on a blockchain that act as automated trustees. This means you can specify in advance what should happen to a sum of money, and the system will execute these instructions exactly. A typical example of this is crowdfunding. Multiple people transfer funds to a recipient, who can only withdraw the money once the funding goal has been reached. If the goal is not met, everyone automatically gets their money back. However, for this to work reliably, the contract's programming must be airtight. "Unfortunately, security risks arise time and again due to errors that creep into the contracts," says Urbach.

A prominent example of this is the 2016 DAO hack. The DAO, a decentralized autonomous organization based on blockchain technology, wanted to raise money through crowdfunding. However, attackers found a software bug and exploited it. The smart contract was programmed so that all parties involved could request an advance refund of their deposited funds. However, the sequence of events was incorrect. To prevent fraud, the new account balance should have been recorded first, and then the funds should have been transferred. But, due to an error in the program, the account balance was only updated afterward. This created a brief window during which the attacker could initiate another refund before the contract registered the first payout. This allowed the attacker to steal cryptocurrency worth USD 50 million by getting the money refunded multiple times in a row.

Problems with smart contracts are one of Schneidewind's primary areas of research. In a current study, she and her team at the Max Planck Institute for

PHOTO: JUDITH WALLERIUS

Searching for gaps in the chain: Clara Schneidewind investigates security vulnerabilities on the blockchain and its applications.



GRAPHIC: GCO

Compromized neighborhood: fraud on the blockchain is possible through methods such as an eclipse attack. In this scenario, cybercriminals in the participant network can hijack a participant's neighboring nodes and use a manipulated blockchain to trick the participant into believing that payments have been made.

Security and Privacy have been examining a particularly challenging case involving smart contracts designed to function across different blockchains. "It's hard enough to write the code correctly for a single blockchain," says the researcher. "But it becomes a whole lot more complicated when different cryptocurrencies are involved." In this case, two contracts – one on each blockchain – must communicate with each other. Complex cryptographic protocols are required to ensure that users can interact securely. Schneidewind's team developed BitMLx, a protocol for cross-chain communications. It can be simply illustrated by the example of exchanging different cryptocurrencies: Person A has Bitcoin, and Person B has an equivalent amount of Ethereum. They want to trade but don't trust each other. This issue can be resolved with a cryptographic secret, which is like a password that must be known to withdraw the other person's funds and prevent third parties from accessing them. Initially, only Person A knows the secret, and they are the first to deposit their money into a sort of escrow account on the blockchain. Then, Person B also deposits their funds into an escrow account. Once Person A withdraws the funds deposited by Person B, the secret automatically becomes visible to Person B, who can then withdraw the funds deposited by Person A. "We have proven that with our protocol, an honest user will never lose money when executing such a contract, no matter what other parties do," says Schneidewind.

In this way, Schneidewind and her team are gradually closing existing security vulnerabilities in smart contracts and cryptocurrencies. Nevertheless, she herself says she would not want to invest in Bitcoin or similar cryptocurrencies. As a researcher, she finds that it's more important for her to remain unbiased. After all, anyone who holds large amounts of a currency can quickly find themselves in a conflict of interest. Who would disclose a security vulnerability that could wipe out their fortune? There is another reason for her reluctance, though: "When you look at it from a research perspective and consider everything that could go wrong, it's easy to want to stay away from it." ←

GLOSSARY

BLOCKCHAIN
A decentralized database of financial and business transactions stored across all participants. Money transfers and other changes in ownership are stored in newly generated, cryptographically secured blocks.

PROOF OF WORK
A method in which participants in a blockchain network must demonstrate their computing power. In a blockchain, this involves solving a cryptographic puzzle, which simultaneously generates an encrypted fingerprint of the existing chain. The first person to solve the puzzle is allowed to create the next block and is rewarded with cryptocurrency for doing so.

SMART CONTRACT
A program that maps an automated business process, such as a change in ownership, onto the blockchain.