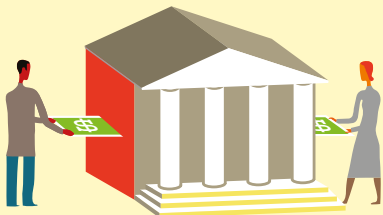


TRANSACTION TECHNOLOGY

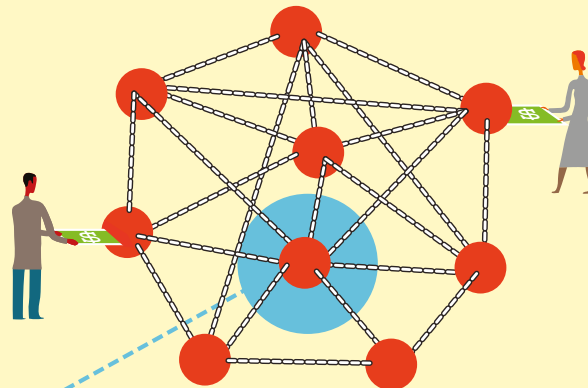


1 Most transactions rely on third parties. To transfer money, a bank processes the request, makes the payment and updates account information.

The system is centralized - everything goes through the bank - and requires high levels of trust in the institution handling the transaction

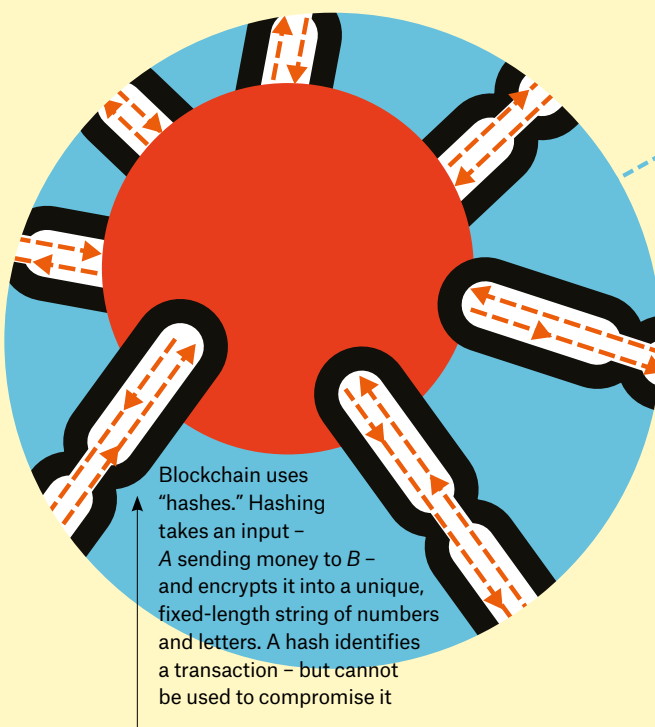
2 Transactions on a blockchain are decentralized. Each transfer is encrypted and distributed across the entire blockchain network of "nodes."

Every node has a copy of the encrypted data. However, the information cannot be deciphered, changed, hidden or deleted through any node



3 Blockchain is what its name suggests. When a transaction, or a block of data, is transmitted, it is then verified by a majority of nodes

within the network through a process called "consensus by distributed cooperation." Once verified, that block of data is added to the chain



Blockchain uses "hashes." Hashing takes an input - A sending money to B - and encrypts it into a unique, fixed-length string of numbers and letters. A hash identifies a transaction - but cannot be used to compromise it

4 Blockchain uses layers of encryption to verify and protect transactions across its huge network, making it much harder to attack than a single database. Even if one node is hacked, the blockchain

updates continually as new transactions take place. Each new block contains code from the one before, locking the transaction in time, so a hacker could not alter data without alerting the entire network



Blockchain explained

From *Vice* to the *Financial Times*, blockchain - the "distributed ledger" technology that underpins the digital currency bitcoin - is being talked about as the future of cybersecurity. One of its defining features, that it is decentralized, is what makes blockchain so safe and potentially transformational.

Used mostly for financial transactions, blockchain could be applied to any task that keeps records. Votes could be tallied or company shares stored and traded on a blockchain network. Personal identities and land titles could also be treated as blocks of data to be recorded, protected and verified.

"The notion of shared public ledgers may not sound revolutionary or sexy. Neither did double-entry book-keeping," said *The Economist* in 2015.

Blockchain's transparency is considered one of its greatest strengths - a feature not often associated with security. Take political elections, for example. With blockchain, every voter would be able to track their vote and check that it had been awarded to the correct candidate. Each vote would have to be verified by a majority of the network, greatly reducing the risk of it being excluded or counted twice. And even though the ballots cast would be visible to everyone on the network, encryption would ensure they remained anonymous.

There is, of course, no guarantee that blockchain is perfectly secure. But at a time when trust in public and private institutions is waning, blockchain challenges the idea that you need to trust those with whom you do business. Blockchain is so secure and transparent, some believe, you can simply trust the system instead.