

Cryptocurrency has gone from something you'd only hear about if you were a geek intrigued by the promise of a decentralised currency to being talked about by your grandma and her friends. Based on blockchain technology, cryptocurrencies are secured through advanced cryptographic techniques and enable secure payments via the internet for a wide range of businesses, governments and individuals. The decentralised nature of these currencies shakes the foundation of conventional monetary systems since they are trustless to banks, central governments and payment processors. As cryptocurrency rises in popularity, it's increasingly important to understand what this technology does, what tech underpins it and how its benefits add up. This article looks at how cryptocurrencies are evolving, the interplay between blockchains and cryptographic functions, and more generalised implications for decentralised digital money.

Digital or virtual currencies that use cryptographic techniques to ensure that they are not counterfeit or copied without authority are called cryptocurrencies. Cryptocurrencies are not created by central banks or any other authority, but rather on a decentralised network. The networks leverage distributed ledger-based technologies to keep a transparent and tamper-free transaction history. Examples include Bitcoin, the first decentralised cryptocurrency, launched in 2009, and Ethereum, which facilitates trading of money without needing third parties. Many other alternatives like Litecoin, Ripple (XRP) and Cardano. The specifics of validating transactions, creating new units and security of the network all vary for different cryptocurrencies, indicative of how different each digital financial ecosystem can be.

A blockchain is essentially a shared, public database that's maintained by a network of computers in which information can only be added after consensus has been reached between

participants. Rather than trusting a single central entity to maintain and update the records, blockchains keep identical copies of the records on many servers distributed across the network. A blockchain consists of a series of blocks, each including a set of verified transactions, a time stamp, a hash based on the previous block, and an extranonce or value used in cryptographic puzzle solutions; a block header keeping metadata about its verification level is also part of everything. Encrypting blocks together is done using hashes, which act as digital thumbprints. A new block carries with it the hash of the previous one, creating a connected chain that can't be tampered with. An effort to alter any record in any block would change the data's hash and alert the network that something does not add up.

Only after consensus is reached across the network that the new block is valid, are blocks added. In Proof-of-Work blockchains like Bitcoin, miners race to solve a computationally difficult puzzle and once solved, they win the right to add a block. In Proof-of-Stake cryptocurrency systems, the validators are chosen depending on the tokens they deposit. Both employ decentralised servers as opposed to a central authority to keep the blockchain from being hijacked by any one person or entity.

While blockchains, in theory, can continue to expand indefinitely when new blocks are appended to them, expanding a blockchain grows computational and performance challenges. Larger blockchains need orders of more space on all nodes in the network. As the chain grows, transaction verification takes longer and longer since nodes have more and more data to work with. Transmission between communicating parties could also be delayed if there is congestion on the network, which can cause transaction processing rates to fall. This problem is particularly prevalent in PoW systems where the computational requirement scales with the number of miners, and the difficulty of solving puzzles adjusts upward. Developers are also working on

scalability improvements so that projects can scale without compromising security or performance, and we're seeing sharding, layer two protocols and more efficient consensus mechanisms being developed to support larger blockchains.

As blockchain information is stored across a network of machines, synchronisation must be maintained using consensus rules dictating that all nodes have the same version of the ledger. In PoW-based systems, the authoritative blockchain is the longest chain, measured by the number of puzzle solutions. Under Proof-of-Stake validation, forgers as a group decide the correct ledger is penalised if they are not honest, deterring the possibility of attempting to rewrite history. These consensus mechanisms ensure that blocks are ordered properly, unwarranted reversals of transactions are prevented, and no single party is able to perform the costly rewriting of history. This decentralised consensus is one of the key reasons blockchains are thought to be reliable and secure.

Blockchain is more than just cryptocurrencies and is seen across multiple industries. In supply chain management, blockchains are used to trace the flow of goods from production to delivery, lending transparency that lowers fraud and generates consumer faith. Healthcare, for example, secure and decentralised patient records storage will help to prevent the prescription of harmful drugs and to provide better care based on accurate data. Blockchain can also be harnessed by voting systems to create secure, tamper-resistant records, which in turn support electoral integrity. Furthermore, online identity verification systems such as blockchain can also offer secure diploma and transcript credentials, while platforms like Ethereum support programmable smart contracts, which self-execute according to pre-set terms. Financial services are also leveraging blockchain technology with decentralised finance platforms, cross-border

payment solutions and tokenised assets. These use cases show how blockchain systems can change the way information is managed and verified.

Cryptocurrencies are often considered safe because they have tamper-proof records, thwart double-spending and use decentralised networks that are tough to attack. Once recorded, the data in any given block cannot be altered without changing all subsequent blocks, which require a consensus of the network majority. Double-spending is avoided by validating all transactions through consensus in the network before committed to the blockchain. The network is not relying on any single central authority, so there is no single point of failure. Such decentralisation is synonymous with trust and helps to avoid the potential for overall system fraud or manipulation. Altogether, these properties endow cryptocurrencies with resistance to counterfeiting, unwarranted reproduction, and hacking.

Solving puzzles is part of the process in the cryptocurrency system built on Proof-of-Work. In these platforms, miners take part in a system in which they compete to solve cryptographic puzzles that depend on significant amounts of computational power. The complexity of these puzzles acts as a cryptographic defence by requiring attackers to expend large amounts of computational work on adding fake blocks. The solving of puzzles also controls the amount of new blocks that are added to the blockchain, ensuring that the network is not moving too fast or too slow. Such kind of puzzles are based on cryptographic building blocks like hash functions or one-way computations that are efficient to verify but hard to invert or predict. As such, puzzle solving is now an integral part of building trust and stability in cryptocurrencies like Bitcoin.

Cryptocurrencies rely heavily on different cryptographic methodologies to provide blockchain security and integrity. Hash functions, including SHA-256, produce digital fingerprints that are used to ensure the integrity of blocks and chain them. Public-key cryptography enables signing transactions with a private key and having others verify authenticity using the corresponding public key. With the help of the digital signature, we can assure that no one has made any changes to the transaction, and this is really from a particular person. The security and efficiency of the system are increased through Merkle trees, which organise large blocks of transaction data into layers in their hash that can be better verified more quickly. These two methods combined are the cornerstone in securing blockchain and guarding against external intrusion and interference.

Here are some of the reasons why cryptocurrencies beat regular money and other electronic payment methods. Their decentralised structure eliminates the need for banks or other financial institutions to approve or facilitate transactions, potentially reducing fees and making financial services more widely available. Cross-border transactions can be completed at pace and well beyond the typical time lines of the traditional banking systems. Blockchain's cryptographic properties ensure that transactions are transparent, traceable and tampering-resistant. For people who are unbanked anywhere in the world, cryptocurrencies offer the possibility of participating in digital commerce even if you don't have a traditional financial account. Price volatility and regulatory uncertainty of cryptocurrencies are significant challenges; however, the decentralised nature, security, and global availability are some of the appealing factors to choose cryptocurrency over traditional payment modes.

Cryptocurrencies are a major technological innovation in the global Pacific arena, thus making an intersection of both computer science and the financial system. Applying blockchain

technology to this industry results in decentralised transaction verification and recording, ensuring the records are secure and transparent. Some basic cryptographic tools like hash functions, public-key cryptosystems, digital signatures and Merkle trees are the foundation of this security model. While cryptocurrencies have their benefits such as decentralisation, security and financial inclusivity, they are also met with limitations like scalability restrictions, high energy consumption, technological immaturity, regulatory uncertainty and price fluctuations. Notwithstanding these misgivings, cryptomarkets have had an impact and are changing the world economic order. Their lasting effects will depend largely on how well developers, governments, and users can manage these risks while making use of the benefits they provide.