Devorah Sachs
March 10, 2021

Blockchain Technology

CS53A Introduction to Cybersecurity Research Report

What is blockchain?

Blockchain, a type of Distributed Ledger Technology, is a collection of "blocks" of data that are linked together through encryption. This collection of records, or ledger, is stored as a distributed, decentralized database, where every node on a peer to peer network has its own constantly updated copy. A combination of Blockchain's properties make it virtually impossible to change existing data or falsify data recorded in a block, prompting some to call the technology "secure by design".

How does it work?

A unit of data, often some kind of transaction, is recorded in a timestamped block. Each block contains three principal pieces of information: the data (sometimes multiple transactions), the block's unique hash (generated by the SHA256 hashing algorithm), and the hash of the block that came before it. This is what makes the ledger a "chain" – each block is tied to the previous one because it contains the previous one's hash. Changing the record in a block results in a new hash, which is different from the previous-block-hash assigned to the next block in the chain, so any change to a block is easily detectable.

When a new block is ready to join the chain, a hash must be calculated for it that meets the set "difficulty" requirement – it must equal a number lower than the predetermined target number. The hash is calculated using the different components of the block, like timestamp and data, as well as a unique, random number called a nonce. This is what makes "mining", or adding a new block to the chain, so challenging: it takes many, many trial and error attempts and lots of computing power to find the "Golden Nonce" which, when fed to the hashing algorithm, will produce a hash number lower than the difficulty. When the proper outcome, or Proof of Work (PoW), is reached, the block can be verified and added to the chain, and the successful miner is rewarded. Blocks are verified by consensus – any change or addition must be accepted by at least 51% of the nodes on the network. If less than 51% accept it, the change is ignored. The distributed chain copies are constantly, simultaneously updated, so changes are seen right away.

Note: PoW is one well known consensus mechanism. Other consensus mechanisms are used in different blockchain situations.

Devorah Sachs
March 10, 2021

Security Advantages of Blockchain:

Blockchain's properties promise extremely tight security for the data it stores. For one thing, hashing keeps blocks of data virtually immutable, while the ledger's distributed nature makes it very hard to tamper with them. It's easy to detect when a bad actor does the work to change a block's data and recalculate its hash, because the subsequent block's 'previous-block hash' becomes a mismatch. Even if he takes the time and computing power (no mean feat) to change the hashes of all subsequent blocks, all the other nodes on the network can see and reject the change; unless he somehow gets control of more than half the network, he cannot make any meaningful changes to the information. Adding to the blocks' unchangeability is the fact that they are often digitally signed to provide nonrepudiation.

The permanence of these records provides each member of the blockchain with the ability to see and trace every transaction that's recorded. Attempts to falsify information or cheat in some way are therefore unlikely. This, along with the absence of a single central authority, promotes trust among the users (or just eliminates the need for trust – blockchain has been called a trustless system). Decentralization of information has other security benefits. Traditional databases are dangerous in that a hacker who breaks into them gains access to large amounts of sensitive information. The fragmented, distributed blocks of a blockchain only ever provide small bits of information. Additionally, blockchain systems have no single point of failure. The redundancy inherent in these distributed databases ensures that if one node, or a copy on one node is corrupted or lost, the compromised information is very easily recovered with help from the other nodes.

A note about transparency of data: anyone on a public blockchain can see any transactions, but the identifying information of the people involved is concealed by special blockchain addresses. Sensitive data can also be secured by extra encryption that makes it useless for others who are able to see it. Private or permissioned blockchains are slightly different – there, access management is overseen by an administrator.

Using Blockchain:

Blockchain was originally developed for use by Satoshi Nakamoto as the system underlying Bitcoin. The permanent, transparent, and digitally signed records of Bitcoin transactions are the basis for the cryptocurrency's value – even though the coins are digital and therefore reproducible, the blockchain ensures that no coin can be spent twice.

With the success of blockchain-based cryptocurrencies like Bitcoin, people realized that blockchain technology could be harnessed for greater security and productivity in sectors other than virtual money. Walmart (with IBM) developed a blockchain system that tracked a food's journey at every step of the supply chain, making it fast and easy to trace damaged or contaminated products to the source of the problem. Smart contracts are little programs stored on the chain that can self-execute in pre-set conditions. Musicians can use blockchain and smart contracts to monitor when their music is streamed and get automatically paid a royalty each time. In government, the possibility has been explored of using blockchain to decrease election fraud by making sure each vote is permanently, securely and transparently recorded.

Blockchain has tremendous potential in cybersecurity specifically. Governments can use blockchain to better encrypt data and to decentralize the risk of attack, as well as to be more easily able to identify and trace attacks on data that has been compromised. In the US, the Defense Advanced Research Projects Agency (the Army's technological development division) started to develop an encrypted messaging system for military personnel. Using blockchain, this system would allow them to quickly send information from/to anywhere in the world, while denying access to hackers. Other institutions like banks and healthcare companies, which store reams of sensitive client or patient data, are also beginning to capitalize on blockchain's power to store and disseminate data more securely.

The Internet of Things industry (IoT) is full of the exciting possibilities that come from "smart" internet-connected devices. However, this convenience does not come without risk. Each internet-connected device provides more vulnerabilities for hackers to exploit. For instance, attackers got to the database in a casino by hacking the smart thermometer of an aquarium in the building. Another time, cybercriminals were able to spy on people using the camera and microphone of a hacked smart baby monitor. Blockchain technology can help combat these security problems. Securely encrypted in the first place, the blocks' small bits of data can't benefit a hacker too much for too long until other nodes on the chain detect that there's been a change. When implemented correctly, blockchain technology provides a secure, transparent, permanent way to store data, promoting and protecting the confidentiality, integrity and availability of our information.

Devorah Sachs
March 10, 2021

References:

https://www.comptia.org/content/infographic/7-myths-about-blockchain-busted

https://www.comptia.org/content/research/understanding-emerging-technology-blockchain

https://www.comptia.org/content/articles/blockchain-terminology

https://www.comptia.org/blog/what-is-blockchain

https://www.comptia.org/content/research/harnessing-the-blockchain-revolution-comptia-s-practical-guide-for-the-public-sector

https://paybis.com/blog/what-is-a-blockchain-nonce/

https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/

https://theleadershipnetwork.com/article/how-walmart-used-blockchain-to-increase-supply-chain-transparency

https://builtin.com/blockchain/blockchain-cybersecurity-uses

https://builtin.com/blockchain

https://builtin.com/blockchain/blockchain-iot-examples

Savjee's Simply Explained YouTube videos on blockchain and it's uses and coding a simple blockchain cryptocurrency

Note: There were other sources that I used at the beginning of my research while trying to understand what blockchain is (it's hard to find a good in-depth understandable explanation). The sources above are the ones I used as my research was becoming successful. They are the ones where I got the majority of or all of the information here.