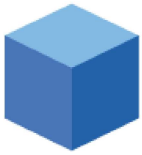

Insight & Resources

HOW DOES BLOCKCHAIN USE PUBLIC KEY CRYPTOGRAPHY?

27 JANUARY, 2018 (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/BLOCKCHAIN/HOW-DOES-BLOCKCHAIN-USE-PUBLIC-KEY-CRYPTOGRAPHY/) BY TOSHENDRA KUMAR SHARMA (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/AUTHOR/TOSHENDRA/)

Asymmetric cryptography or public cryptography is an essential component of cryptocurrencies like Bitcoin and Ethereum. These advanced cryptographic techniques ensure that the source of transactions is legitimate and that hackers can not steal a users funds. Here's an in-depth look at how blockchains accomplish this with public key cryptography:

What is Public Key Cryptography?

Public Key Cryptography is a cryptographic system that relies on a pair of keys, a private key which is kept secret and a public key which is broadcasted out to the network. This system helps ensure the authenticity and integrity of a message by relying on advanced cryptographic techniques.

Here's an example of how public key cryptography is used in practice: Let's say a user Alice wants to send a message to Bob over an unreliable channel of communication like the internet. Alice could use public key cryptography by generating a set of public and private keys. She could then post her public key to Bob. Now, whenever she wants to communicate to Bob, she can add a digital signature to her message by using her private key. This would prove that she is the creator of the message. Bob can verify the same using the message he received and Alice's public key.

Public Key Cryptography in Bitcoin

Public Key Cryptography is an essential part of Bitcoin's protocol and is used in several places to ensure the integrity of messages created in the protocol. Wallet creation and signing of transactions, which are the core components of any currency rely heavily on public key cryptography. Bitcoin's protocol uses what's called the Elliptic Curve Digital Signature Algorithm (ECDSA) to create a new set of private key and corresponding public key. The public key is then used with a hash function to create the public address that Bitcoin users use to send and receive funds. The private key is kept secret and is used to sign a digital transaction to make sure the origin of the transaction is legitimate.

Digital Signatures

Digital signatures are quite similar to actual signatures on a document. They help ensure that the author of a transaction is, in fact, the individual who holds the private key. Digital signatures are the backbone of Bitcoin and every transaction has a different digital signature that depends on the private key of the user. Also, given the message, the public key of the user and the signature, it is non-trivial to check if the signature is authentic. More formally, digital signatures depend on two functions:

Sign (Message, Private Key) -> Signature
Given the message we want to sign and a private key, this function produces a unique digital signature for the message.

Verify (Message, Public Key, Signature) -> True/False
Given the message we want to verify, the signature and the public key, this function gives a binary output depending on whether the signature is authentic

Once the transaction is signed by the owner, the transaction is sent to the memory pool where it sits to be processed by miners. The miners use the sender's public key to ensure that the digital signature is authentic so that a hacker cannot spend a user's funds without their consent. If the ownership and digital signature check out, they include the transaction in the next block, and the money is sent from one wallet to another.

Proof of Work

The other major use of cryptography in the Bitcoin protocol is in computing the proof of work function. Miners rely on computing the "SHA256 Hash Function" for a lot of inputs until they find the nonce for a given block before adding it to the blockchain. The difficulty of the mining process is changed by how many zeroes the hash must begin with to be added to the blockchain. This is a unique system as it adjusts higher or lower depending on how many people are mining at any given time. It also makes it computationally infeasible for an attack vendor to go and edit transactions that are already recorded on the blockchain.

Learn more about Blockchain with our Certified Blockchain Expert Certification (https://www.blockchain-council.org/certifications/certified-blockchain-professional-expert/?utm_source=organic&utm_medium=links&utm_campaign=bloglinks)

BLOCKCHAIN (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/CATEGORY/BLOCKCHAIN/)

BITCOIN (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN/), BITCOIN ATM (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-ATM/), BITCOIN ATM NEAR ME (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-ATM-NEAR-ME/), BITCOIN CALCULATOR (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-CALCULATOR/), BITCOIN CASH (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-CASH/), BITCOIN CASH PRICE (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-CASH-PRICE/), BITCOIN CHART (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-CHART/), BITCOIN CONVERTER (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-CONVERTER/), BITCOIN EF (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-EF/), BITCOIN EXCHANGE RATE (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-EXCHANGE-RATE/), BITCOIN GOLD (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-GOLD/), BITCOIN INVESTMENT (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-INVESTMENT/), BITCOIN MINING (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-MINING/), BITCOIN NEWS

(HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-NEWS/), BITCOIN PRICE (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-PRICE/), BITCOIN PRICE CHART (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-PRICE-CHART/), BITCOIN PRICE HISTORY (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-PRICE-HISTORY/), BITCOIN PRICE TODAY (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-PRICE-TODAY/), BITCOIN PRICE USD (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-PRICE-USD/), BITCOIN STOCK (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-STOCK/), BITCOIN STOCK PRICE (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-STOCK-PRICE/), BITCOIN TO USD (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-TO-USD/), BITCOIN USD (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-USD/), BITCOIN VALUE (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-VALUE/), BITCOIN WALLET (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-WALLET/), BITCOIN WORTH (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOIN-WORTH/), BITCOINS (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BITCOINS/), BUY BITCOIN (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/BUY-BITCOIN/), CRYPTOGRAPHY (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/CRYPTOGRAPHY/), CURENT BITCOIN VALUE (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/CURENT-BITCOIN-VALUE/), CURRENT BITCOIN PRICE (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/CURRENT-BITCOIN-PRICE/), HOW MUCH IS BITCOIN WORTH (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/HOW-MUCH-IS-BITCOIN-WORTH/), HOW TO GET BITCOINS (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/HOW-TO-GET-BITCOINS/), KEY (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/KEY/), PRIVATE KEY (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/PRIVATE-KEY/), PUBLIC KEY (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/PUBLIC-KEY/), REDDIT BITCOIN (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/REDDIT-BITCOIN/), WHAT IS BITCOIN (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/WHAT-IS-BITCOIN/), WHAT IS MONEY LAUNDERING (HTTPS://WWW.BLOCKCHAIN-COUNCIL.ORG/TAG/WHAT-IS-MONEY-LAUNDERING/)

About Us

Blockchain Council is an authoritative group of subject experts and enthusiasts who are evangelizing the Blockchain Research and Development, Use Cases and Products and Knowledge for the better world. Blockchain council creates an environment and raise awareness among businesses, enterprises, developers, and society by educating them in the Blockchain space. We are a private de-facto organization working individually and proliferating Blockchain technology globally.

Related Links

- Member Network (https://www.blockchain-council.org/member-network/)
- Certifications (https://www.blockchain-council.org/blockchain-certification/)
- Training (https://www.blockchain-council.org/online-training/)
- Careers (https://www.blockchain-council.org/careers/)
- Scholarship (https://www.blockchain-council.org/scholarship/)
- Partner With Us (https://www.blockchain-council.org/partner-with-us/)
- Advertise With Us (https://www.blockchain-council.org/advertise-with-us/)
- Affiliate Program (https://www.blockchain-council.org/affiliate-partner-program/)
- Support & FAQs (https://help.blockchain-council.org/en/)
- Terms and Conditions (https://www.blockchain-council.org/terms-and-conditions/)
- Support Policy (https://www.blockchain-council.org/support-policy/)
- Privacy Policy (https://www.blockchain-council.org/privacy-policy/)
- Refund Policy (https://www.blockchain-council.org/refund-policy/)
- Notices (https://www.blockchain-council.org/notices/)
- Jobs (https://www.blockchain-council.org/jobs/)

Address

Blockchain Council,
340 S Lemon Ave #1147
Walnut , CA 91789

Phone: +1-(323) 984-8594 (tel:+1-(323) 984-8594)

Email: hello@blockchain-council.org (mailto:hello@blockchain-council.org)

Get In Touch With Us

Blockchain Council | Blockchain-council.org (https://www.blockchain-council.org)

Get a Flat 25% Discount on Blockchain Council.

MEMBERSHIP

Instructor-Led Training (https://www.blockchain-council.org/instructor-led-training/)

Certifications (https://www.blockchain-council.org/blockchain-certification/)

Online Degree (https://www.blockchain-council.org/online-degree/)

Resources

Others

Contact Us (https://www.blockchain-council.org/contact-us/)