

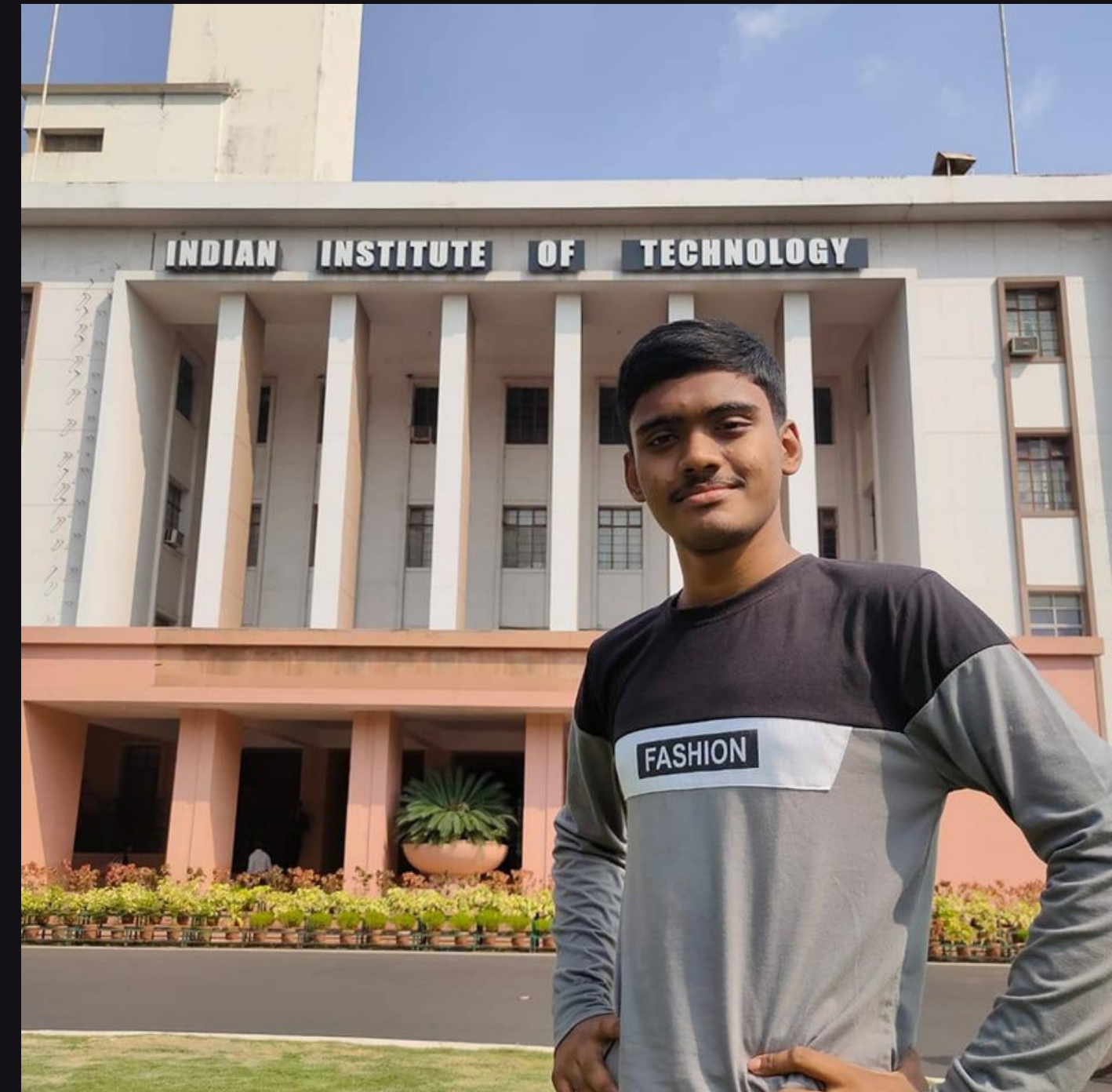


Exploring Public-Private Key Encryption and Bitcoin Wallets



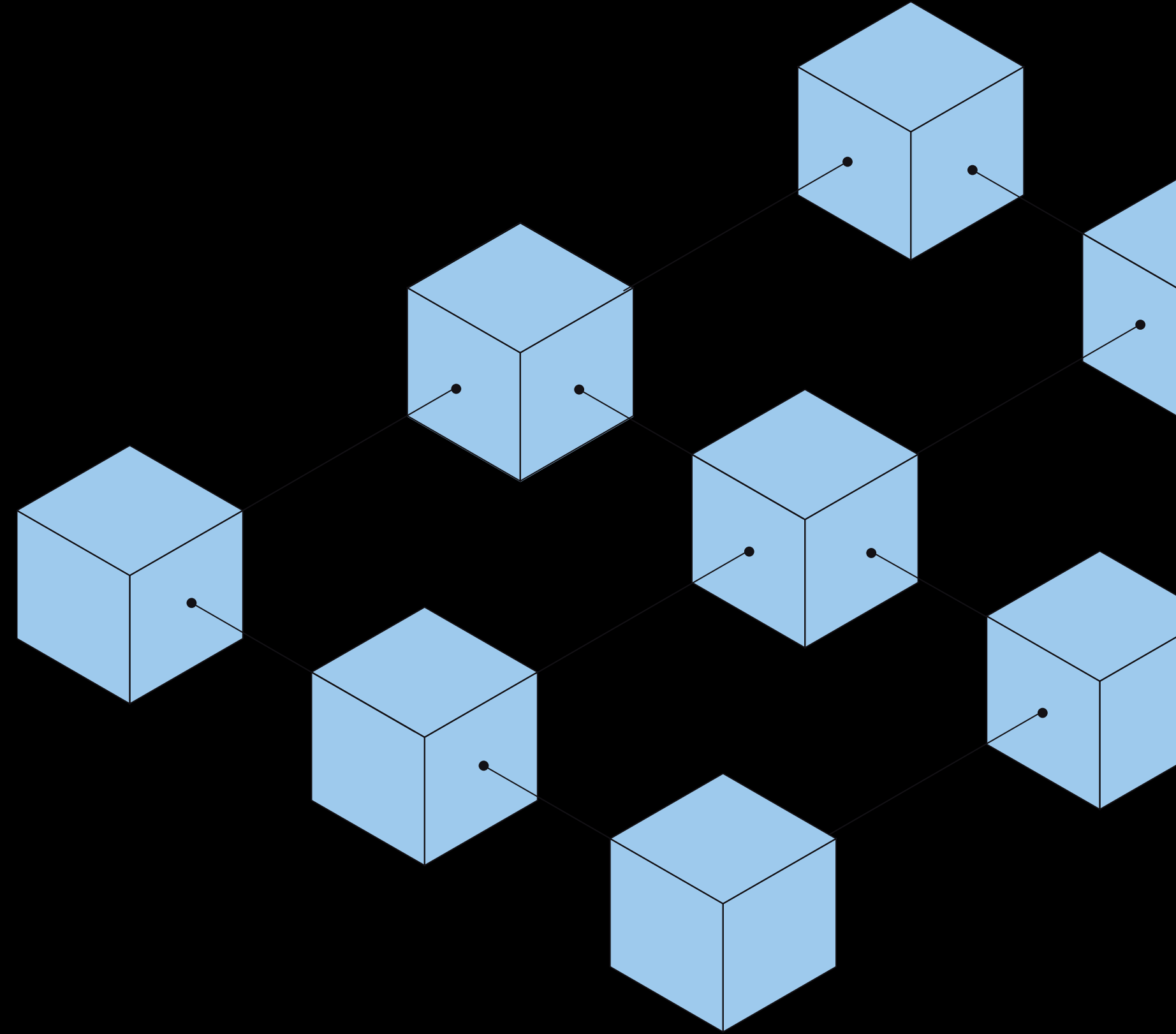
Introduction

Hello, I am Srinjoy Das, a first year undergraduate student of the department of Computer Science and Engineering, enrolled in it's dual degree course. I am boarder of Pandit Madan Mohan Malviya Hall of Residence. I am from Kolkata, West Bengal. My hobbies include learning about new technologies and playing cricket.



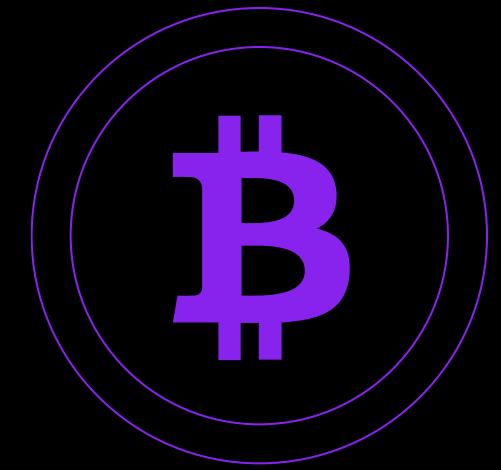
Objectives

1. Concept of public-private key encryption.
2. Explore the applications of public-private key encryption in Bitcoin wallets.
3. Discuss the advantages and challenges of public-private key encryption in Bitcoin wallets.
4. Provide practical tips and best practices for using Bitcoin wallets securely.



Cryptography

Cryptography is crucial in modern technology, providing a foundation for secure communication and data protection.



Cryptographic Keys

Symmetric key

Asymmetric key

Hashing Key



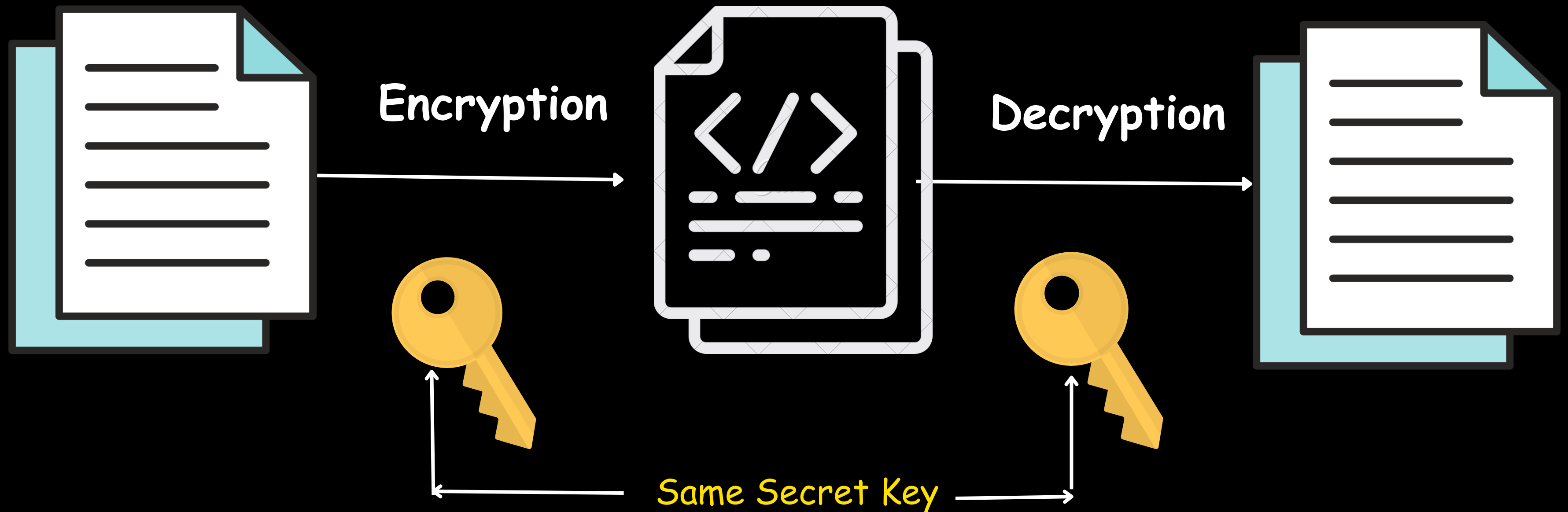
How Symmetric Key Works



Plain Text

Cipher Text

Plain Text



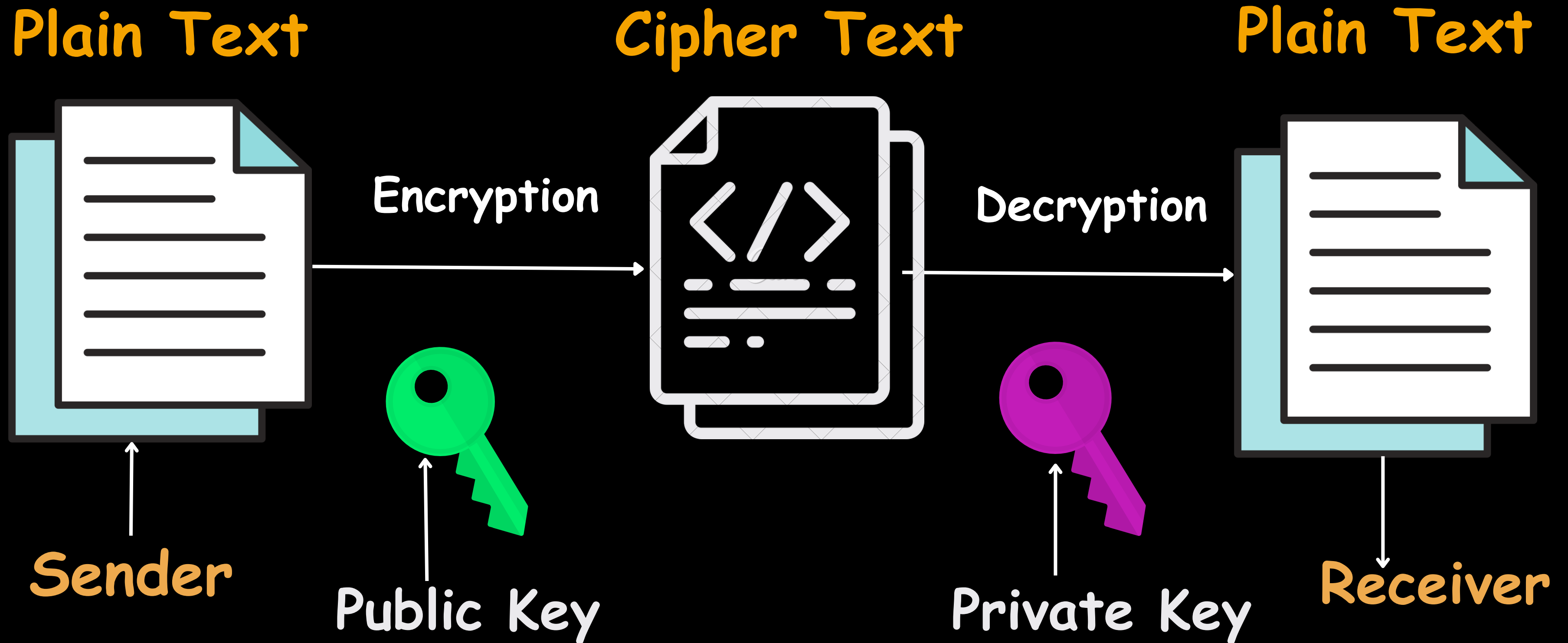
Asymmetric Keys

Asymmetric keys, also known as public-private key pairs, are used in asymmetric encryption algorithms.

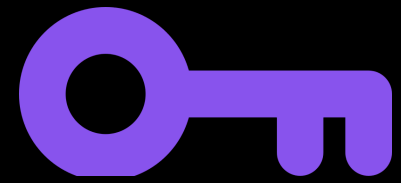
The public key is shared freely, while the private key is kept secret, allowing for secure encryption, decryption, digital signatures, and secure communication in various applications



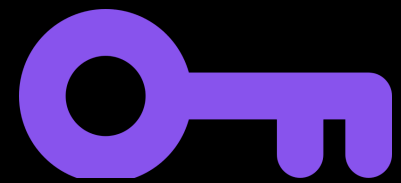
How Asymmetric Key Works



Generation of Public and Private Keys



Public and private keys are generated through cryptographic algorithms.



The RSA (Rivest-Shamir-Adleman) algorithm is commonly used for key pair generation.

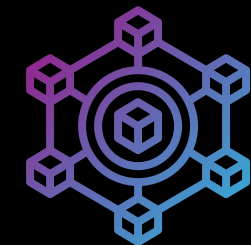
RSA Algorithm for Key Generation

- Generate two large prime numbers, p and q .
- Compute the modulus, $n = p * q$.
- Calculate Euler's totient function, $\phi(n) = (p - 1) * (q - 1)$
- Choose a public exponent, e , which is relatively prime to $\phi(n)$.
- Compute the private exponent, d , as the modular multiplicative inverse of e modulo $\phi(n)$.
- Public key: (e, n) . Private key: (d, n) .

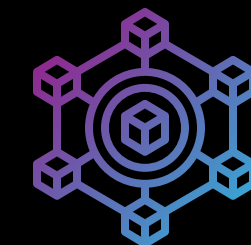
Encryption



To encrypt a message M is converted it into a numerical value ' m '.

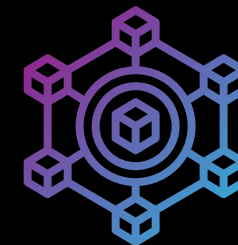


The ciphertext, c , is calculated as $c = m^e \bmod n$.

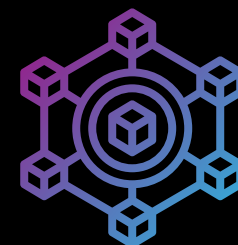


The ciphertext can be shared with the recipient

Decryption



Obtain the private key, which consists of the modulus, n , and the private exponent, d .



For decryption, the ciphertext, c , is raised to the power of d modulo n : $m = c^d \bmod n$.



The decrypted message, m , is the original plaintext.

Concept of Digital Signature

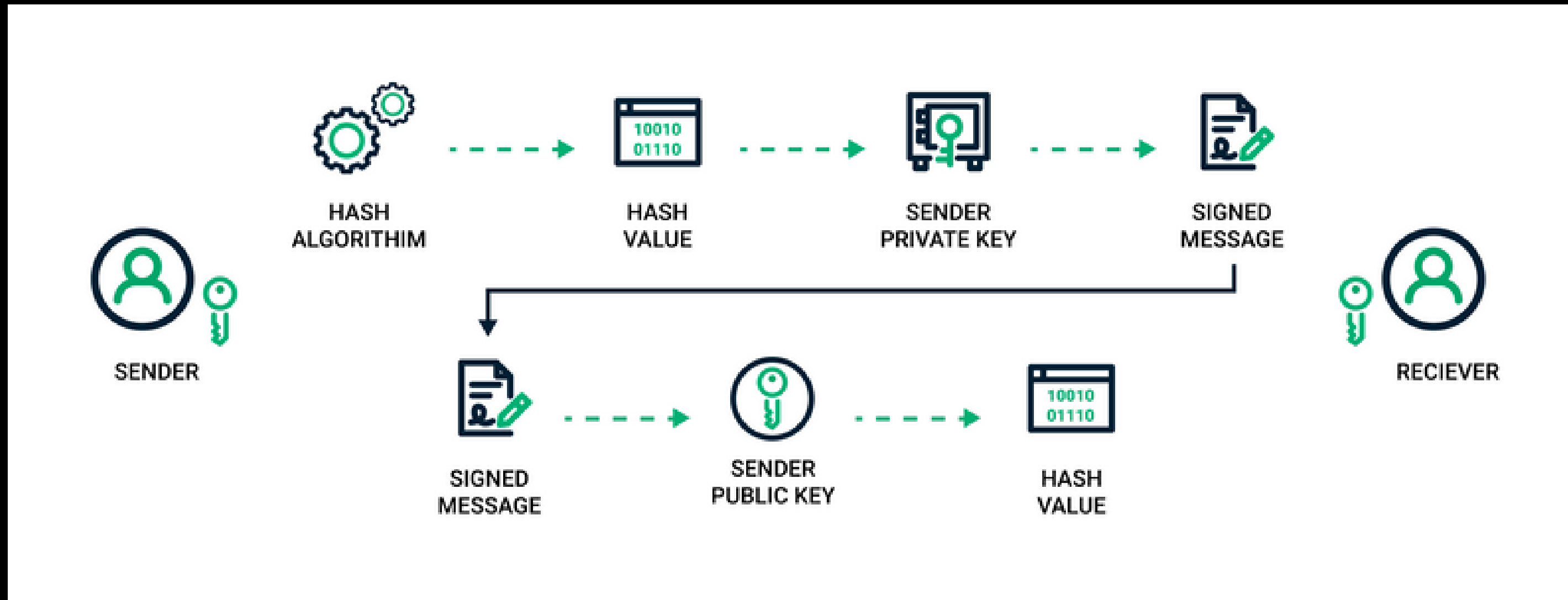


A digital signature is a cryptographic technique used to verify the authenticity and integrity of digital documents or messages.



It provides assurance that the document or message has not been tampered with during transmission or storage.

This is how Digital Signature works



Benefits of Digital Signature



Authenticity



Integrity



Non-repudiation



Securing Your Digital Assets

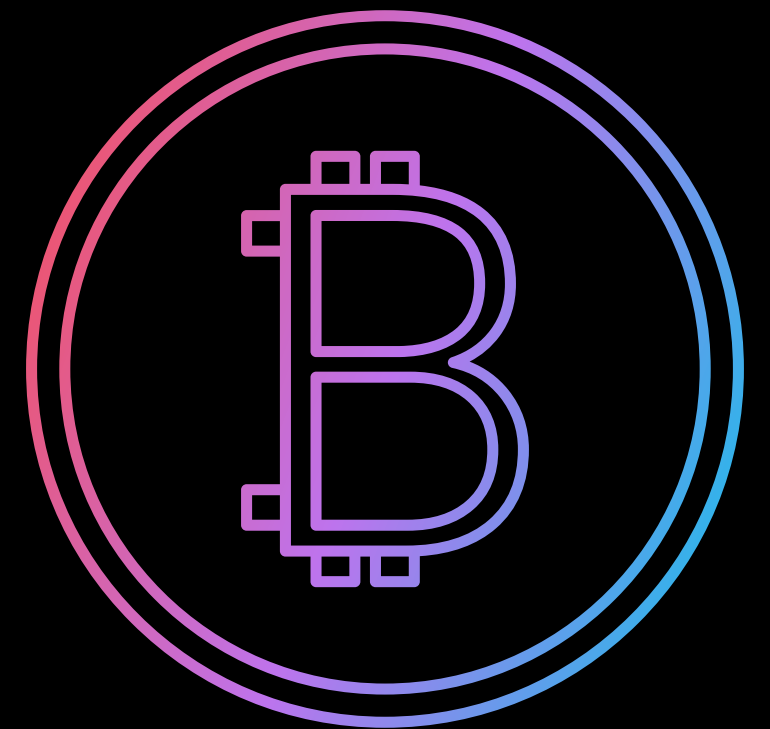
Introduction to Bitcoin



Bitcoin is a decentralized digital currency created in 2009 by an unknown person or group of people using the pseudonym Satoshi Nakamoto.



It operates on a peer-to-peer network called the blockchain, which ensures transparency, security, and immutability.



Bitcoin Wallets: Safeguarding Your Digital Assets



A Bitcoin wallet is a digital application or device that enables you to store, send, and receive bitcoins.



It stores your private keys, which are necessary to access and control your bitcoins securely.



Public-Private Key Encryption in Bitcoin Wallets

Sender's Wallet:



The sender uses their private key to digitally sign the transaction, ensuring its authenticity and integrity.

Network Validation:



The signed transaction is broadcasted to the Bitcoin network, where it is verified by network participants (nodes) through consensus algorithms.

Recipient's Wallet:

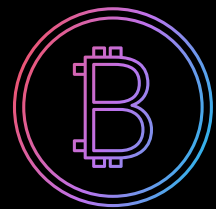


Upon confirmation, the recipient's wallet uses their private key to unlock and access the received bitcoins.

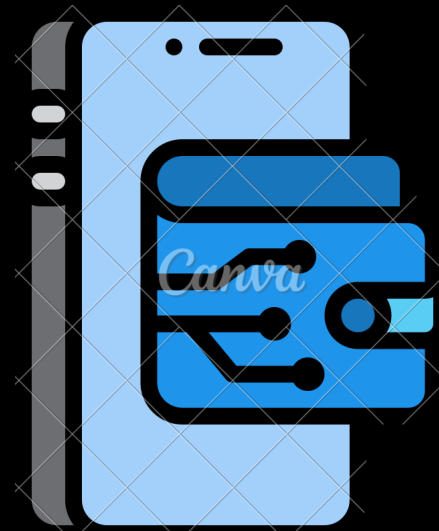


Types of Bitcoin Wallets: Hot Wallets vs. Cold Wallets

Hot Wallets



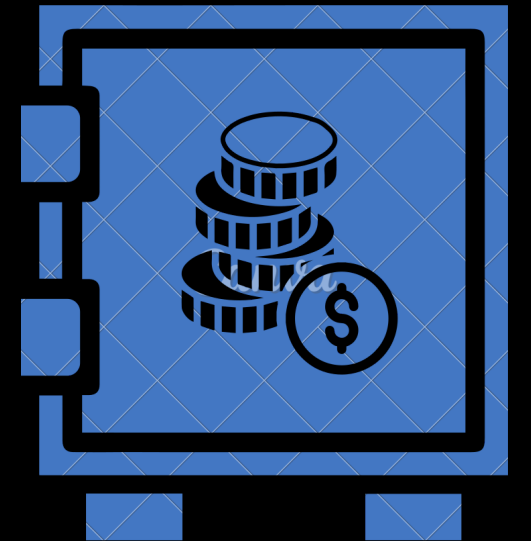
Hot wallets are Bitcoin wallets connected to the internet, allowing quick and convenient access to your funds.



Cold Wallets






Cold wallets are Bitcoin wallets kept offline, providing enhanced security by minimizing exposure to potential risks.



Hot Wallets

Advantages

-  Accessibility
-  Convenience
-  Integration



Disadvantages

-  Higher Risk and Dependency

Cold Wallets

Advantages

-  Security
-  Offline Storage
-  Long-term Storage



Disadvantages

-  Accessibility Delay and Physical Vulnerabilities

Best practices for securing Bitcoin wallets

Backing Up Private Keys

Private keys grant access to Bitcoin holdings and enable transactions.



Best Practices for backing up Private Keys



Use hardware wallets or paper wallets for offline storage.



Multi-factor authentication adds an extra layer of security to Bitcoin wallets



Create multiple copies of private keys.



Avoid relying solely on email-based authentication.



Do you have any questions?
Feel free to ask



Thank You