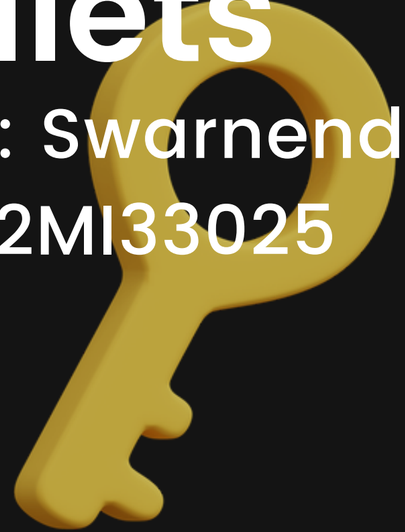
# Exploring Public-Private Key Encryption and Bitcoin Wallets

Name : Swarnendu Bhandari,
Roll : 22MI33025



# Topics

## Public-Private Key Encryption and Bitcoin Wallets

The basics of public-key cryptography and how it differs from traditional symmetric-key cryptography.

How public and private keys are generated and used to encrypt and decrypt data.

The concept of digital signatures and how they are used to verify the authenticity of data.

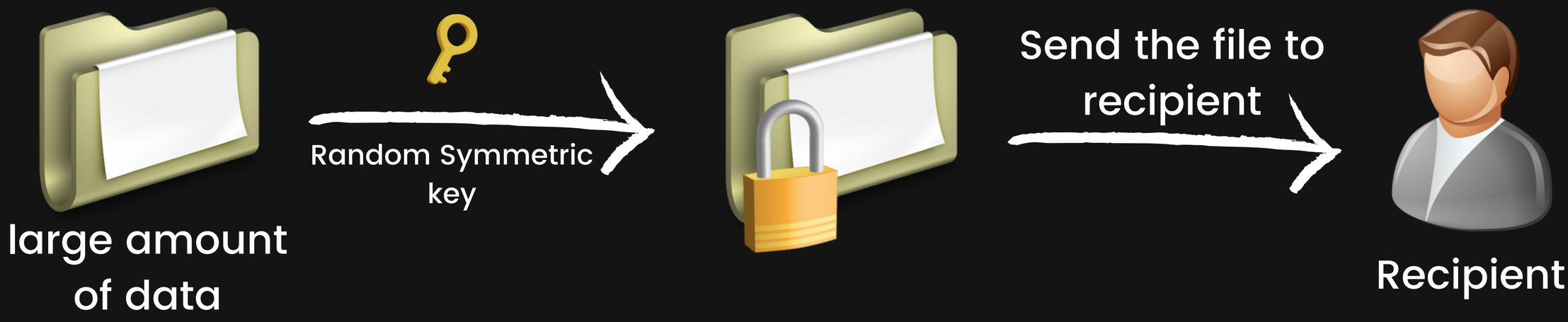
How public-private key encryption is used in Bitcoin wallets to secure and manage Bitcoin transactions.

The different types of Bitcoin wallets, including hot wallets and cold wallets, and the advantages and disadvantages of each.

Best practices for securing Bitcoin wallets, including the importance of backing up private keys and using multi-factor authentication.

# The basics of public-key cryptography and how it differs from traditional symmetric-key cryptography.

# Traditional symmetric-key Cryptography




# Public-key cryptography

User

## Private Key

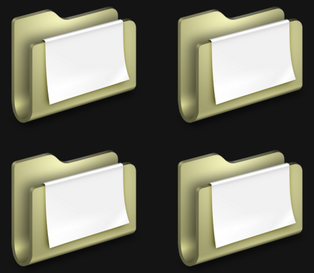
- Private
- The corresponding private key is kept secret and known only to the owner. It must be securely stored and never shared.

## Public Key

- Publically Visible
- A user generates a public key and freely distributes it to others. It is derived from the private key using specific mathematical algorithms.

# Encryption Process

large amount of data



Data is divided into fixed size of block

Random Symmetric key

Recipient's Public key

Encripted file

Send the file to recipient

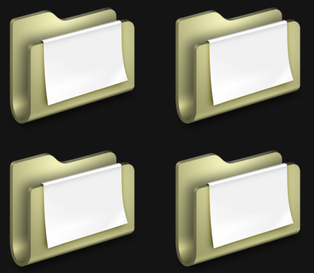
Recipient

# Deception Process

Encripted file

Recipient's
Private key

Random
Symmetric
key



Data is divided into
fixed  size of block

Combined data

# Traditional symmetric-key cryptography

- In symmetric-key cryptography, both the sender and receiver share the same secret key
- Symmetric cryptography is not scalable as it does require many keys
- Symmetric-key cryptography is generally faster and more efficient for bulk data encryption compared to public-key cryptography

# Public-key cryptography

- In public-key cryptography, the public key is freely distributed, eliminating the need for secure key exchange
- Public-key cryptography is scalable as it does not require a unique key for each pair of communicators
- Public-key cryptography is generally more efficient for small amount of data

# Process of Digital Signature

# Signature Creation

data

Standared hasing
function (Eg: SHA-256)

...q2b!21nggj98bgreno...
Hash Code

Senders private key
and cryptographic
algorithm

## Digital Signature

Publically available

# Signature Validation

data

Standared hasing
function (Eg: SHA-256)

...q2b!21nggj98bgreno...
Hash Code

(Matched)

Valid data

Digital Signature

Decrypting the
digital sign

Senders public key
and cryptographic
algorithm

...q2b!21nggj98bgreno...
Hash Code

# The Advantages of Digital Signature

# The Advantages of Digital Signature

Authentication

Non-repudiation

Integrity

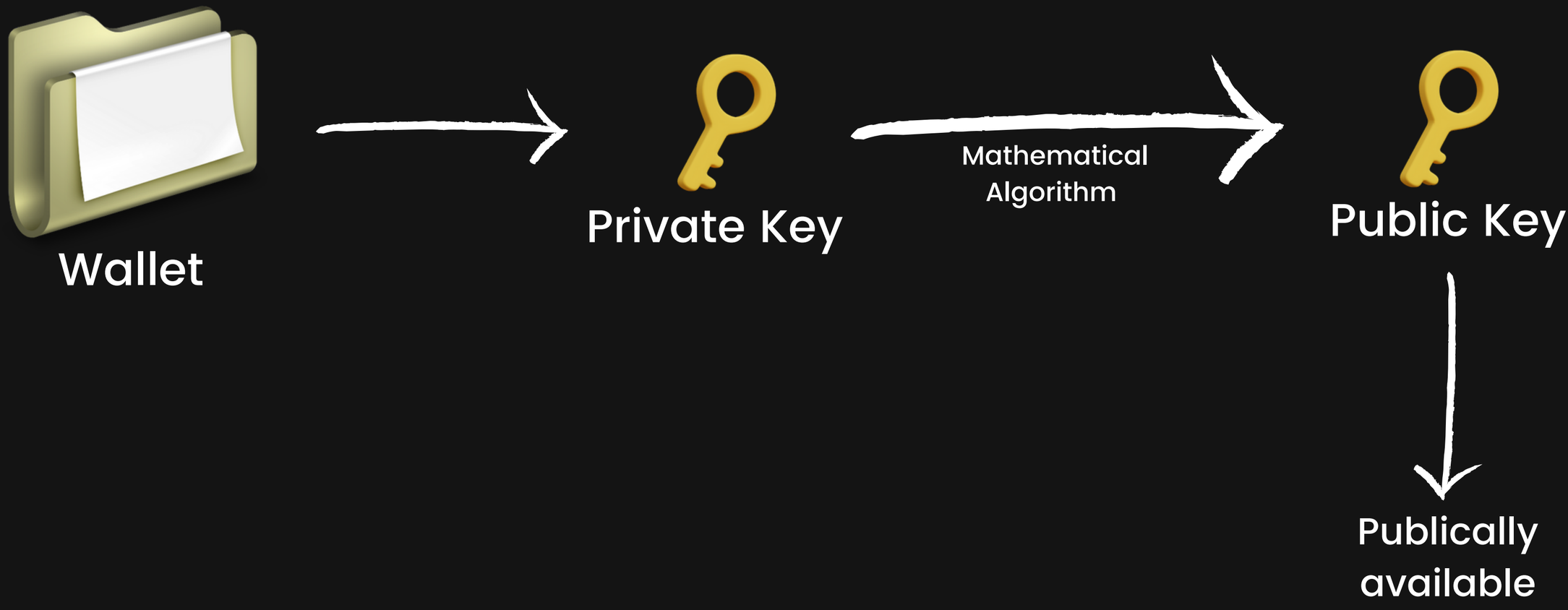
Efficiency and speed

Security

User-friendly

# Bitcoin Wallets to secure and manage Bitcoin transection

# Key Generation



# Transaction Generation and Verification

Wallet

new Transaction

Receiver's public key

Previous Transaction Output
(Proof of ownership of bitcoin)

Owner's private key

Digitally Signed Transaction

Owner's public key

Merged to Bitcoin Network

The Receiver will receive bitcoin

## Hot Wallet

- Connected with network and accessible online
- Softwere-based wallets, including mobile wallets, desktop wallets and web wallets.

## Cold Wallet

- Bitcoin wallets that are kept offline, disconnected from the internet,
- They are typically hardware based

# Hot Wallet

## Advantages

- Easy and quick access to Bitcoin.
- Easy to manage.
- Real-time balance update
- It often has user-friendly interface to manage

## Disadvantages

- They can be targeted and hacked by hackers.
- If the private key is exposed by mistake, it can cause theft.
- Some hot wallets are managed by third-party services. This means users have to trust them to handel the private key.

# Cold Wallet

## Advantages

- Higher level of security
- Protection against hacking
- Full control over the private key

## Disadvantages

- It is a normal process, so it can be less convenient for frequent transaction
- If it is lost or damaged then, and there is no backup option, it can result in parment loss.

# Best practices for securing Bitcoin wallets?

- Choose a trusted wallet software
- Enableing Multifactor authentication
- Strong and unique password
- Regularly back up the private keys in an encrypted storage
- Inpliting cold wallets
- Enable wallet encription

## Constantly keep update yourself with new technologies

# Do you have any questions?

# Thank You

Name: Swarnendu Bhandari,
Roll: 22MI33025