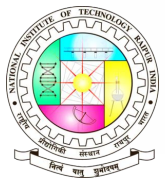
Bitcoin

Dr. Preeti Chandrakar
Assistant Professor

Department of Computer Science and Engineering
National Institute of Technology, Raipur
September 2021

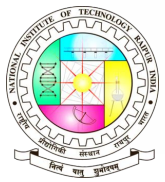
Outline

- Bitcoin
- History of bitcoin
- Blocks in bitcoin
- Use Bitcoin
  - Bitcoin wallet
  - Sending and receiving bitcoin
- Advantages and disadvantages.



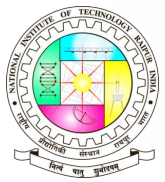
Bitcoin

- Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem
- The unit of currency , which is used to store and transmit a value over the bitcoin network is known as bitcoin.
- User can do transfer bitcoin, trading, currency exchange, money transfer, thorough bitcoin network
- Bitcoin in a sense is the perfect form of money for the internet because it is fast, secure, and borderless
- Users of bitcoin own keys that allow them to prove ownership of bitcoin in the bitcoin network
- With these keys they can sign transactions to unlock the value and spend it by transferring it to a new owner



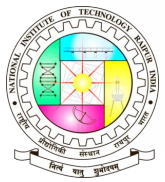
Bitcoin

- Keys are often stored in a digital wallet on each user's computer or smartphone.
- Bitcoin are created through a process called "mining,".
- Bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank and replaces the need for any central bank.
- Bitcoin is also the name of the protocol, a peer-to-peer network,
- Bitcoin consists of:
  - A decentralized peer-to-peer network (the bitcoin protocol)
  - A public transaction ledger (the blockchain)
  - A set of rules for independent transaction validation and currency issuance (consensus rules)
  - A mechanism for reaching global



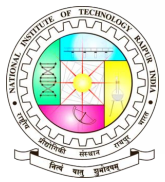
History of bitcoin

- Bitcoin was invented in 2008 with the publication of a paper titled **"Bitcoin: A Peer to-Peer Electronic Cash System,"** Written under the alias of Satoshi Nakamoto
- Nakamoto combined several prior inventions such as b-money and HashCash to create a completely decentralized electronic cash system
- That does not rely on a central authority for currency issuance or settlement and validation of transactions
- The bitcoin network started in **2009**, based on a reference implementation published by Nakamoto and since revised by many other programmers



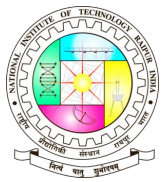
History of bitcoin

- Bitcoin’s total market value has at times exceeded $35 billion US dollars
- The largest transaction processed so far by the network was $150 million US dollars
- Satoshi Nakamoto withdrew from the public in **April 2011**
- The identity of the person or people behind bitcoin is still unknown.



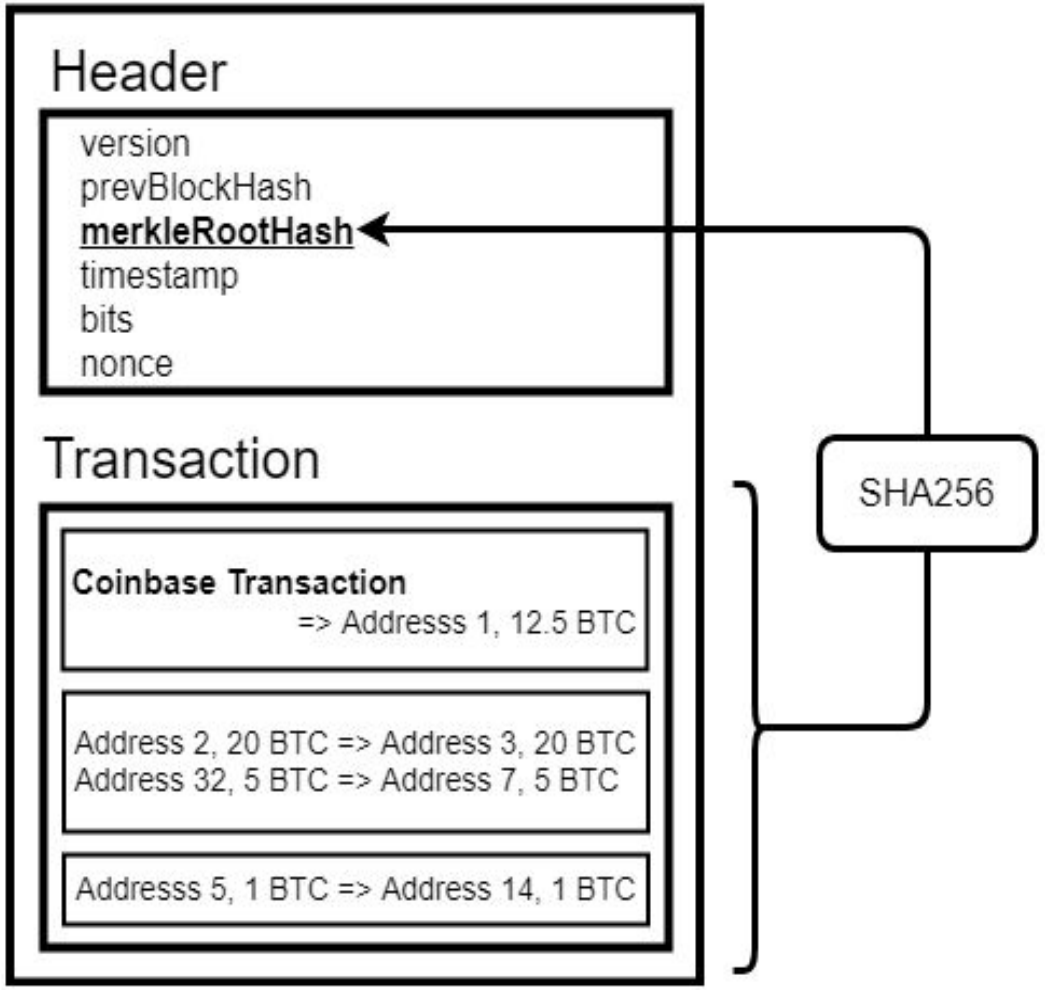
Bitcoin block

- Blocks are data structures within the blockchain database
- Where transaction data in a cryptocurrency blockchain are permanently recorded
- A block records some or all of the most recent transactions not yet validated by the network
- Once the data are validated, the block is closed
- Then, a new block is created for new transactions to be entered into and validated.
- A block is thus a permanent store of records that, once written, cannot be altered or removed.



Structure of a bitcoin block

- **Version**: The cryptocurrency version being used.
- **Previous block hash**: Contains a hash (encrypted number) of the previous block's header.
- **Hash Merkle root**: Hash of transactions in the Merkle Tree of the current block.
- **Time**: A timestamp to place the block in the blockchain.
- **Bits**: The difficulty rating of the target hash, signifying the difficulty in solving the nonce.
- **Nonce**: The encrypted number that a miner must solve to verify the block and close it.

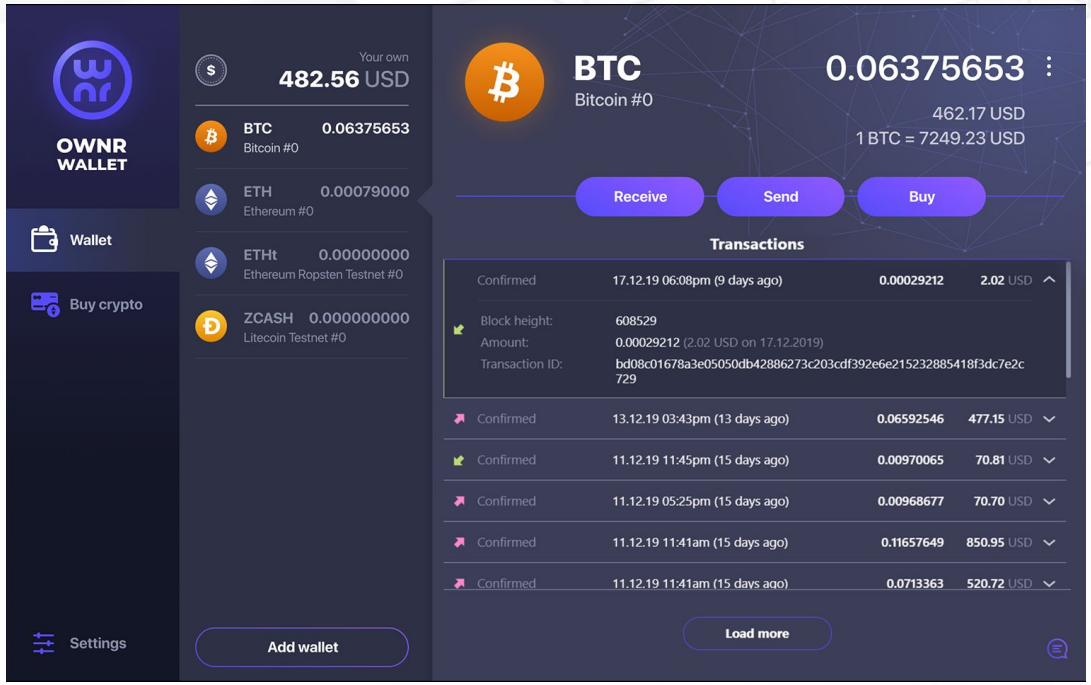


Bitcoin wallet

"A Bitcoin wallet (and any crypto wallet, for that matter) is a digital wallet storing the encryption material giving access to a Bitcoin public address and enabling transactions,"

~Alexandre Kech

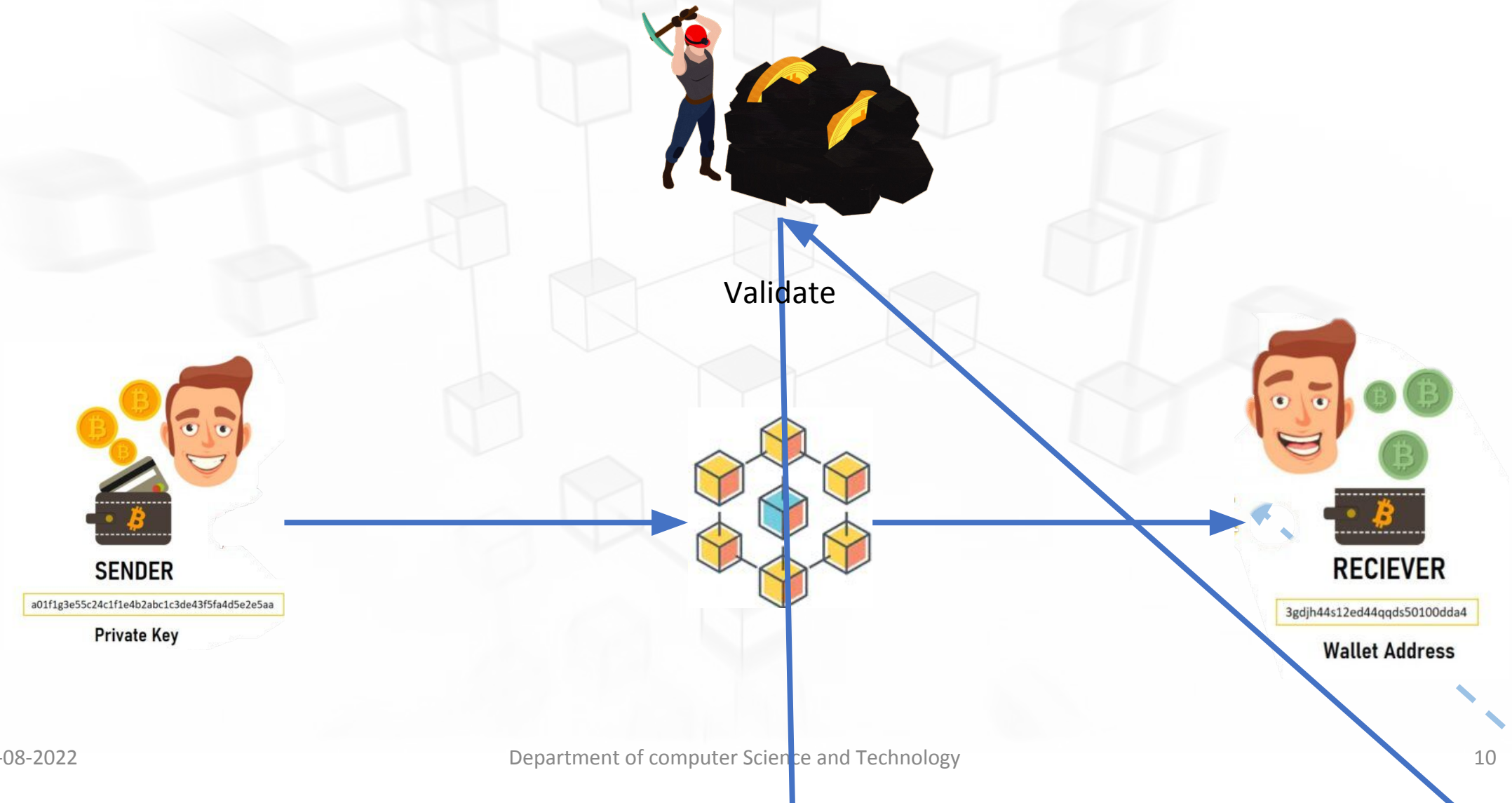
- **Example of a bitcoin wallet**



- **The Different Types of Bitcoin Wallets**
  - Mobile Wallet
  - Online or Web Wallet
  - Desktop Wallet
  - Paper Wallet
  - Hardware Wallet

Bitcoin wallet

- **Working of bitcoin wallet**

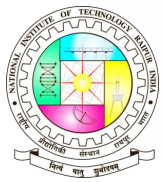


Sending and receiving bitcoin

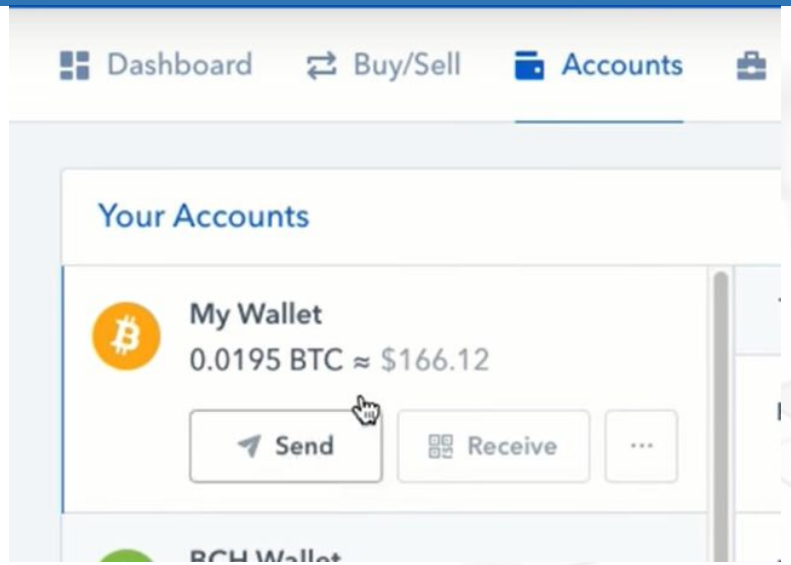
- For sending and receiving bitcoin following are required
  - Bitcoin wallet
  - Bitcoin amount to be sent + some extra bitcoin(for transaction fee)
  - Address
- **Sending bitcoin**

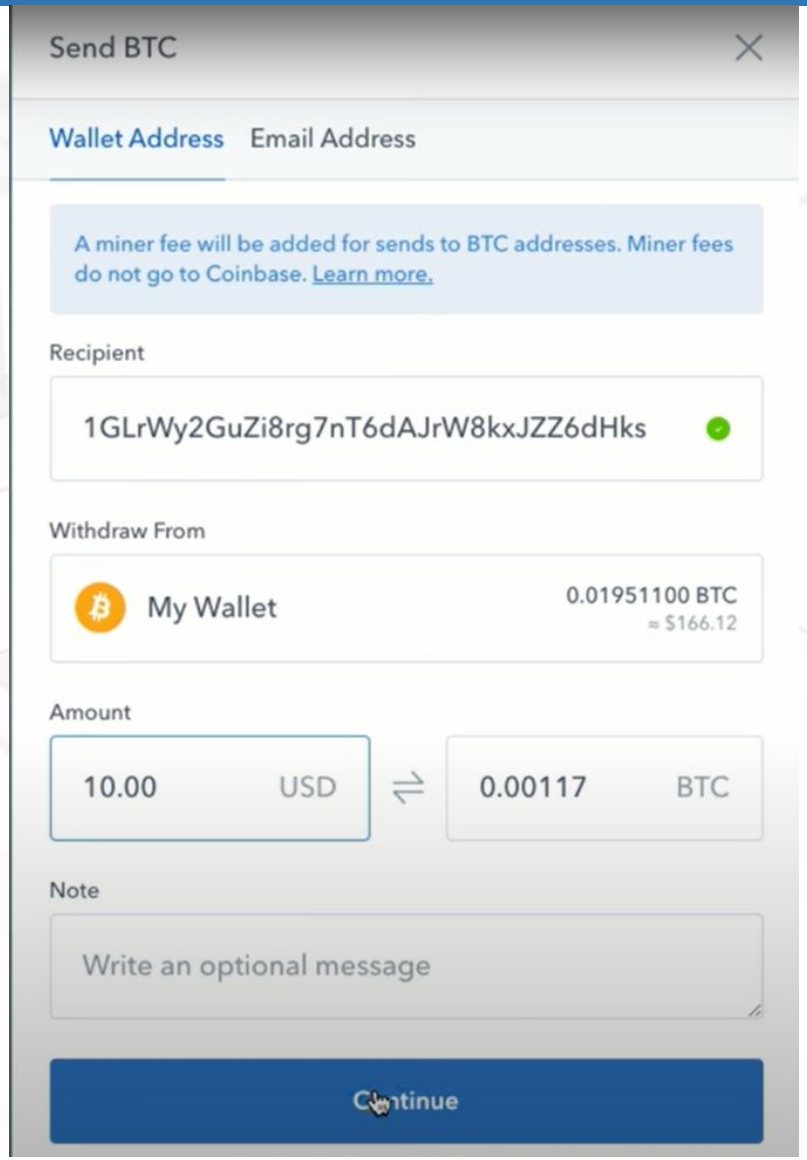
1. Open your bitcoin wallet
2. Click on send (make sure you have bitcoin)
3. Enter the recipient's address (public key of receiver)
4. Enter the amount
5. Hit the continue then confirm button
6. It takes hours to days to confirm the transaction

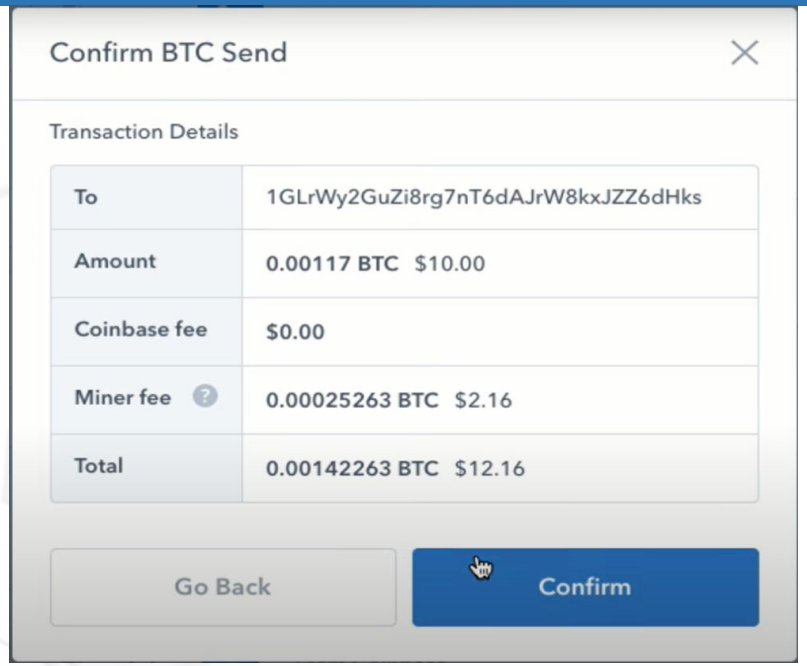
*Always ensure that when you sending bitcoin, keep some extra because the transaction fee is automatically deducted from your wallet



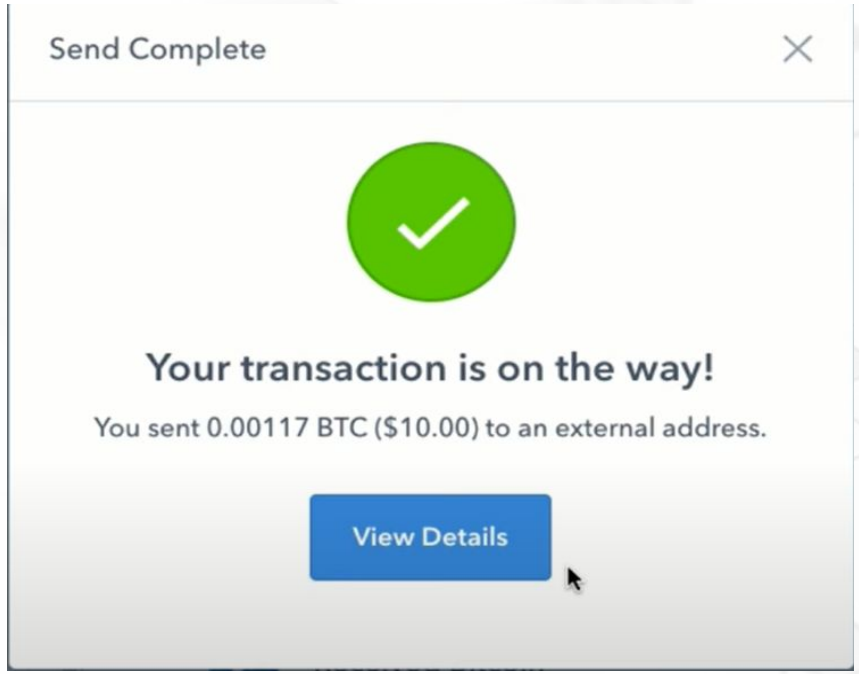
Sending and receiving bitcoin

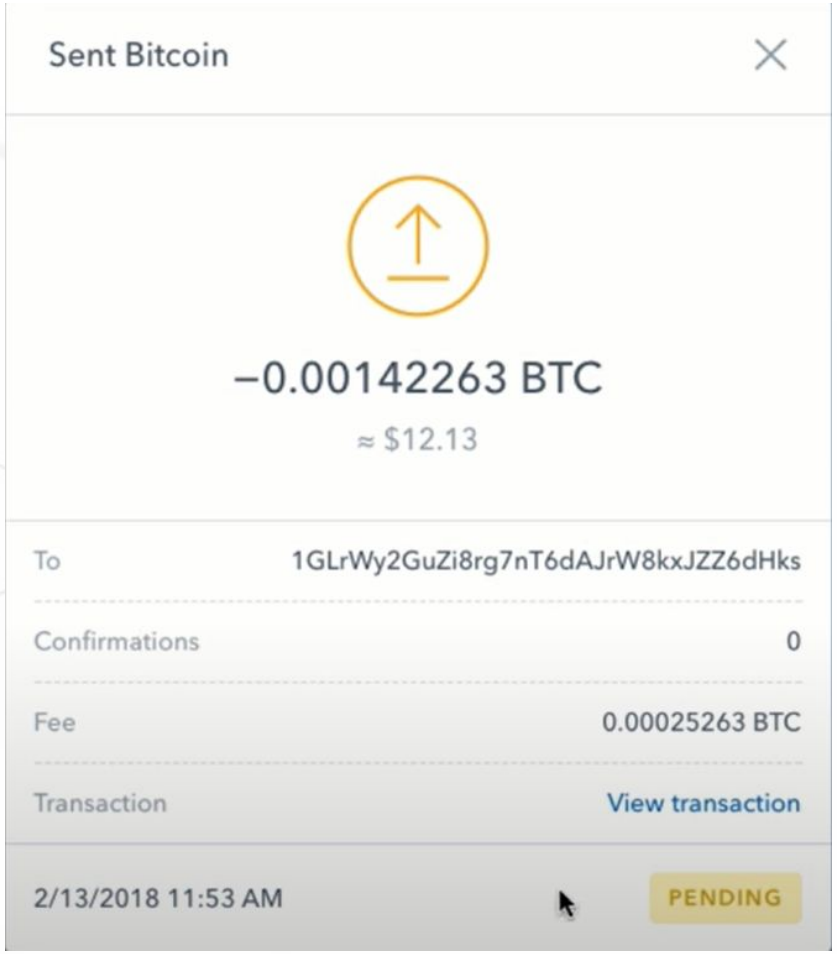






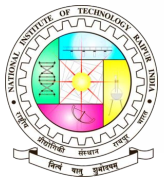
Sending and receiving bitcoin



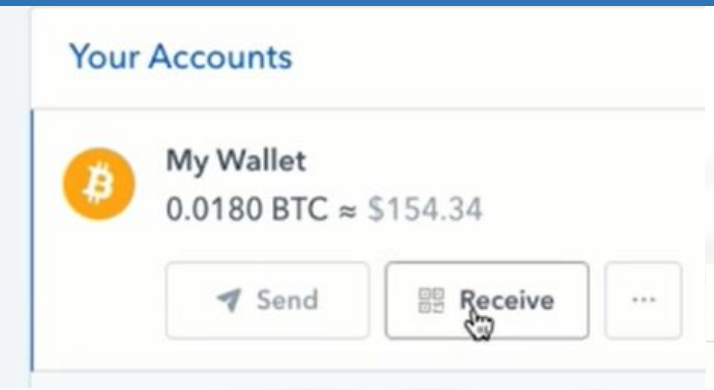


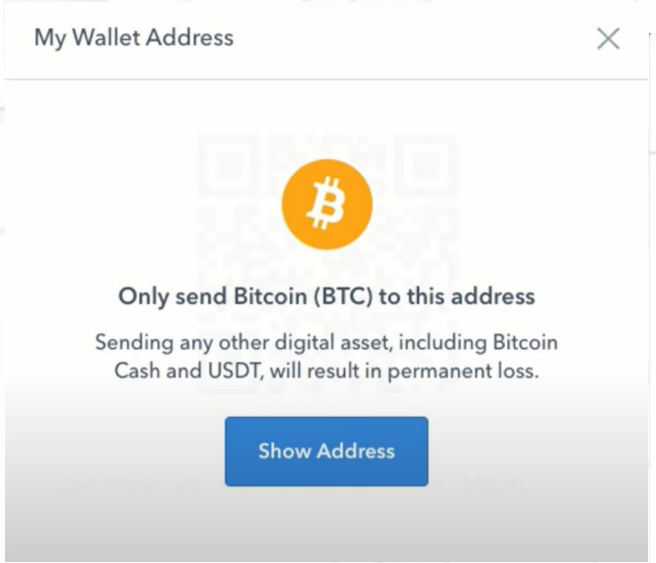
Sending and receiving bitcoin

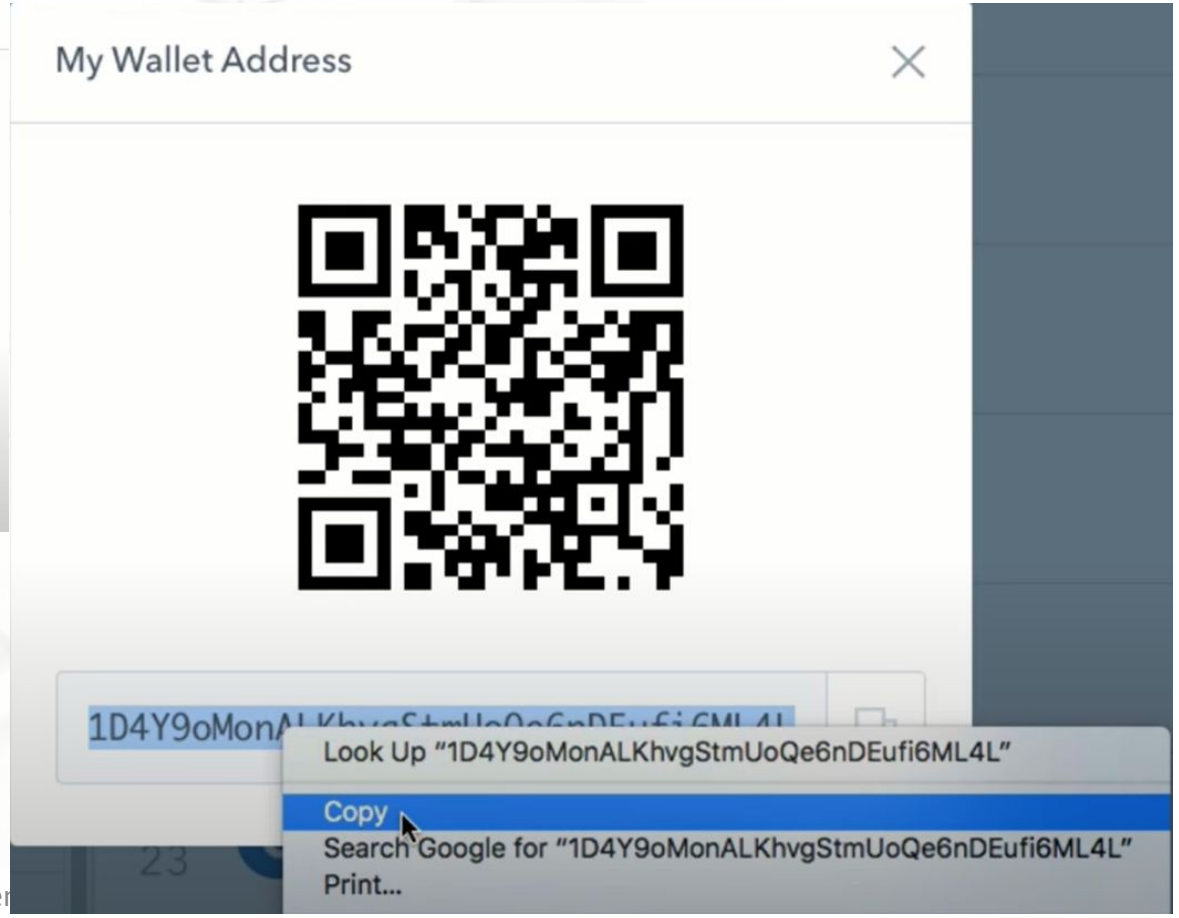
- **Receiving bitcoin**
  1. Open your bitcoin wallet
  2. Click on receive
  3. Click on show address
  4. Copy the address and share it with the sender
  5. Transaction may take hours to days to confirm



Sending and receiving bitcoin







Advantages and disadvantages

Advantages

- No restrictions on payment
- Maintain anonymity
- Complex algorithm
- Fast and secure
- No third party
- No inflation

Disadvantages

- Lack of Awareness
- Use of complex technique
- Highly volatile
- Not accepted everywhere
- Victim of Theft and Scam
- No reverse of payment and recovery
- Black market
- Scaling issues