BITCOIN

Presentation by: Michael Wang @ LUG
bitcoin (BTC) is:

- Digital currency
- Peer-to-peer
- "Anonymous", but public
- Cryptographically secured
How it works

Each user has a bitcoin wallet.
A wallet contains bitcoin addresses.
To make a payment, users reference these addresses in a transaction.
Transactions are publicly validated and stored in the **block chain**.
Cryptography ensures the integrity of the block chain (that is, the integrity of all transactions).
Cryptography background

Public-key cryptography

- Public key and private key
- To sign data: encrypt (sign) with private, decrypt (verify) with public
- Bitcoin uses ECDSA (Elliptic Curve Digital Signature Algorithm)
Hash function

- Input: data, of any length
- Output: fixed number of bytes
- Bitcoin uses SHA-256 and RIPEMD-160
Your bitcoin wallet

Contains one or more public/private key pair(s).
A bitcoin address is simply (a hash of) your public key.
Making a payment

To make a transaction, sign the transaction with a *private* key.

Others verify that the transaction is legitimate with the corresponding *public* key.
Transactions in-depth

All transactions have **inputs** and **outputs**.
Each input must reference bitcoins received (an output) in a past transaction.

Each output must be sent to an address.
What if inputs > outputs?

Split the input
Example:

Amounts of 50 BTC and 0.1 BTC have been sent to address ABCD. To send 0.5 BTC to address F000, must use 50 BTC as input.
Example:

Therefore, send:

- 0.5 BTC to address F000
- 49.5 BTC to a newly created address
After being signed with a private key, a transaction is *broadcast* to a network of nodes to be validated.
Nodes (called **miners**) verify these transactions and group them into a *block*, and each try to be the first one to add the block to the *block chain*.

The block chain is a distributed database that contains all validated transactions.
Determining consensus:

What if multiple nodes add different blocks to the block chain at separate times?
Proof-of-work

Nodes achieve consensus through proof-of-work.
To validate a block and add it to the block chain, miners must compute a specific hash.
The added block/hash is then broadcast and verified by the rest of the network.
Hash(block) = hash_func(Hash(block_prev), block, nonce)
Why is there a nonce?

Block target requirement: make blocks hard to validate, but easy to verify.
Computed hash must be below a certain target. This 256-bit target is adjusted every 2016 blocks to ensure constant difficulty.

On average, a block is validated ("mined") every 10 minutes.
This prevents tampering with previous blocks.

To replace a block with a fraudulent one, you would have to recalculate the hashes of all subsequent blocks.
Which branch from the block chain does a miner add to?
The longest, of course.
That is, the branch that took the most work to validate. This is calculated based on the block target.
A transaction is (finally) "confirmed" when:

1. It is part of the longest branch
2. There are >= 5 blocks following it
Why mine?

Verify others' transactions!

Miners get 25 BTC (currently) for each validated block

Current price per BTC: ~465 USD
Bitcoin software

Wallets store your keys/addresses

Clients help you make transactions

Exchanges allow you to buy BTC with money
Q: People who try to spend my BTC?

A: Public key cryptography. The hash of their public key (i.e., their address) would have to be same as yours. This is because transactions must reference a past output; the public key of an input is checked against the (recipient) address of an output.

(If they use your public key, they won't be able to sign it properly because they don't have your private key.)
Q: People who try to spend an output twice?

A: Proof-of-work. To do so, they would have to validate two transactions, one of them fraudulent (network nodes will realize the fraud). They would have to build the block chain faster than everyone else combined to include their block in the block chain. This is highly unlikely (but technically possible).
Q: Someone who has enough power to outpace others to build the block chain?

A: If someone did, they would only be able rollback past transactions by adding fake blocks. They would not be able to steal others' BTC without others' private keys. Proof-of-work is designed so it would be more profitable for them to mine bitcoins.

(Assuming everyone realized that one node is dominating the network and stopped building on their branch.)
Q: Someone who steals my private key?
A: It's not :(
Q: The government cracking asymmetric encryption?

A: Again, it's not :(
More resources

Bitcoin exchanges: Most popular bitcoin exchanges

Bitcoin mining: Bitcoin mining software

Bitcoin wiki: Bitcoin Wiki

Original paper: Paper

Explanation of bitcoin: How the Bitcoin protocol actually works