# Introduction to Bitcoin

# CONTENTS

What is Bitcoin

Who created it?

Who prints it?

How does Bitcoin work?

The characteristics of Bitcoin

# WHAT IS BITCOIN

Bitcoin is a form of digital currency, created and held electronically. No one controls it. Bitcoins aren't printed, like dollars or euros – they're produced by people, and increasingly businesses, running computers all around the world, using software that solves mathematical problems.

It's the first example of a growing category of money known as cryptocurrency.

# The characteristics of Bitcoin

EASY

**Person to Person**

Send bitcoin from your computer, tablet, smart phone or other device, to anyone, anywhere in the world, day or night.

SECURE

**Strong cryptography**

Bitcoin verifies transactions with the same state-of-the-art encryption used in banking, military and government applications.

OPEN

**Fully decentralized**

Bitcoin is open-source. Nobody owns it; the most popular client is maintained by a community of open-source developers .

FAIR

**Minimal Fees**

Using the Bitcoin network is free, except for a voluntary fee you can use to speed up transaction processing.

# Who created it?

A software developer called Satoshi Nakamoto proposed bitcoin, which was an electronic payment system based on mathematical proof. The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with very low transaction fees.

# Who prints it?

No one. This currency isn’t physically printed by a central bank.  Some argue central banks are unaccountable to the population  and can simply produce more money to cover the national debt, thus devaluing their currency.

Instead, bitcoin is created digitally, by a community of people anyone can join. Bitcoins are ‘mined’, using computing power in a distributed network.
This network also processes transactions made with the virtual currency, effectively making bitcoin its own payment network.

# How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

## WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

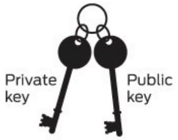
Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

Each address has its own balance of bitcoins.

## CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.



**Public Key Cryptography 101**
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

## SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

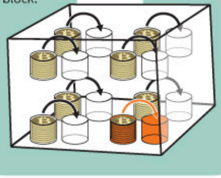
Private key
Public key

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

## VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.



Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

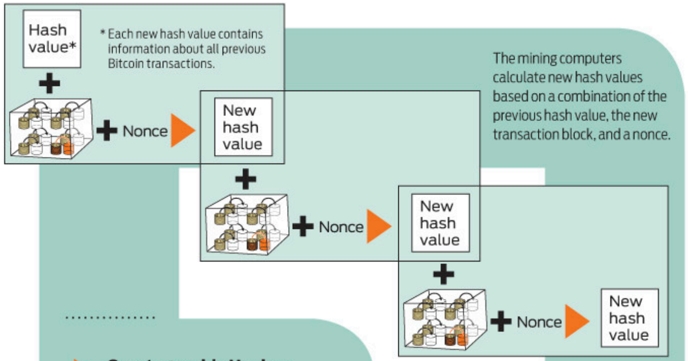
### Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

| | | |
|---|---|---|
| The root of all evil | ▶ | 6d0a 1899 086a... (56 more characters) |
| The root of all euil | ▶ | 486c 6be4 6dde... |
| The root of all veil | ▶ | b8db 7ee9 8392... |

### Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

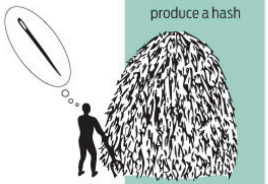


* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

| | | |
|---|---|---|
| The root of all evil ??? | ▶ | 0000 0000 0000 ... |

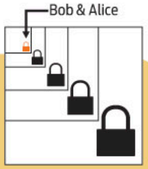
Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.



The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

## TRANSACTION VERIFIED



As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

JOSHUA J. ROMERO, BRANDON PALACIO & KARLSSONWILKER INC.

# Security in Bitcoin

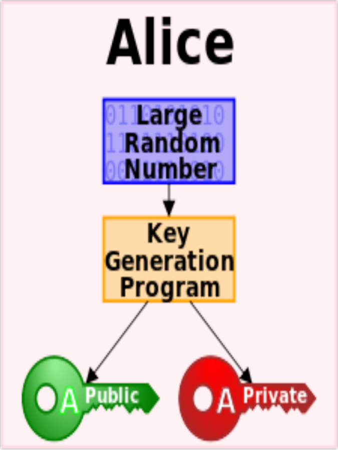
- Authentication
  - Am I paying the right person? Not some other impersonator?
- Integrity
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Are my transactions private? Anonymous?

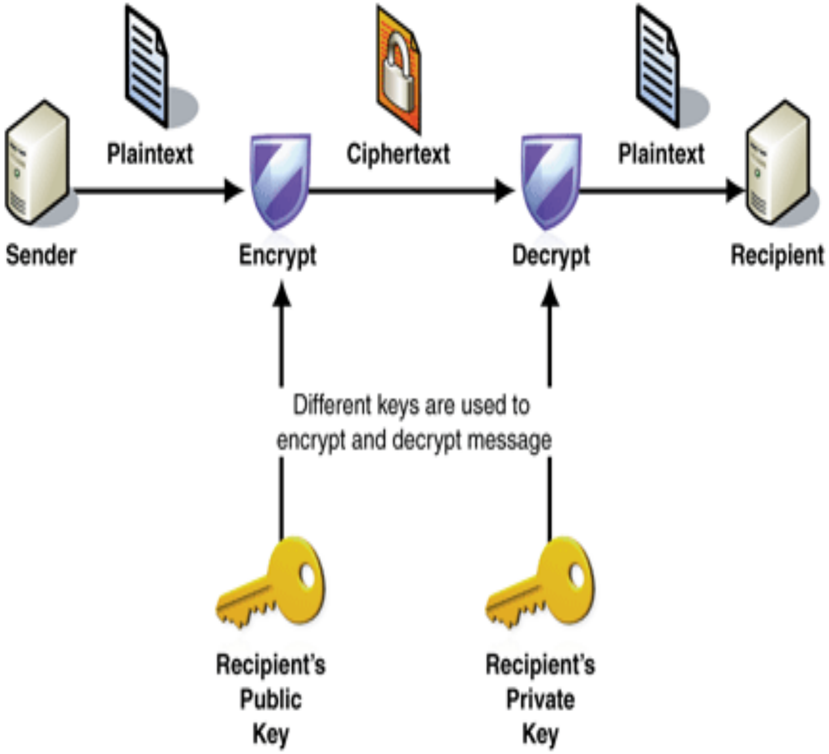
# Security in Bitcoin

- Authentication → Public Key Crypto: Digital Signatures
  - Am I paying the right person? Not some other impersonator?
- Integrity → Digital Signatures and Cryptographic Hash
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability→ Broadcast messages to the P2P network
  - Can I make a transaction anytime I want?
- Confidentiality→ Pseudonymity
  - Are my transactions private? Anonymous?

# Public Key Crypto: Encryption

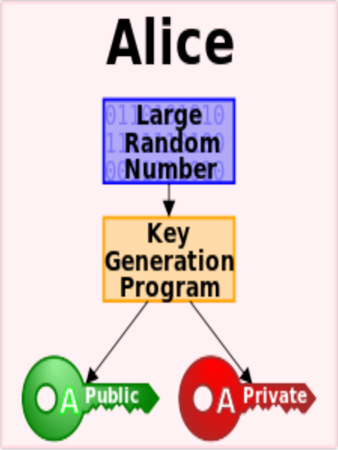
- Key pair: public key and private key

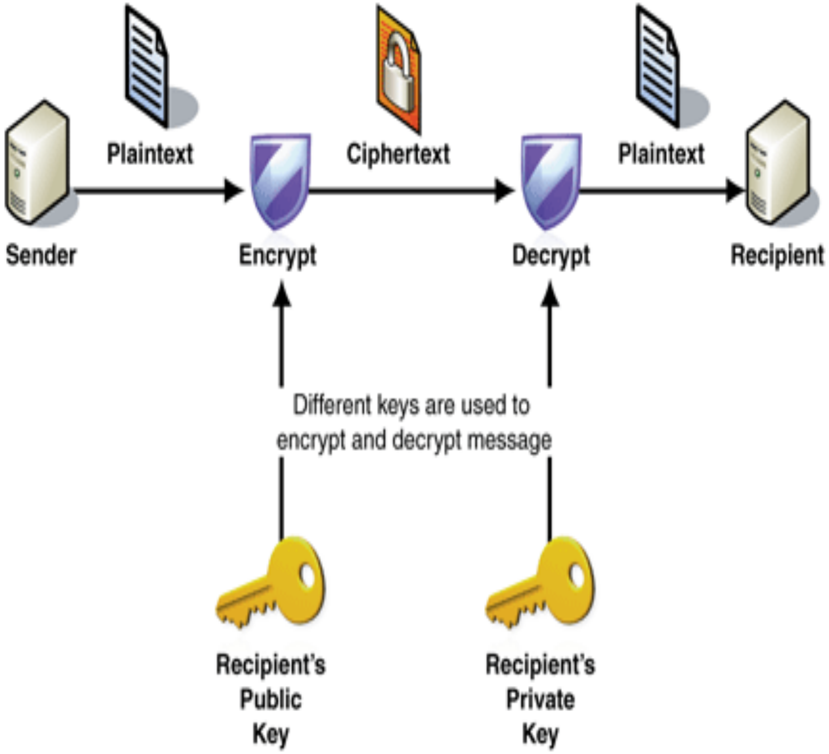




# Public Key Crypto: Encryption

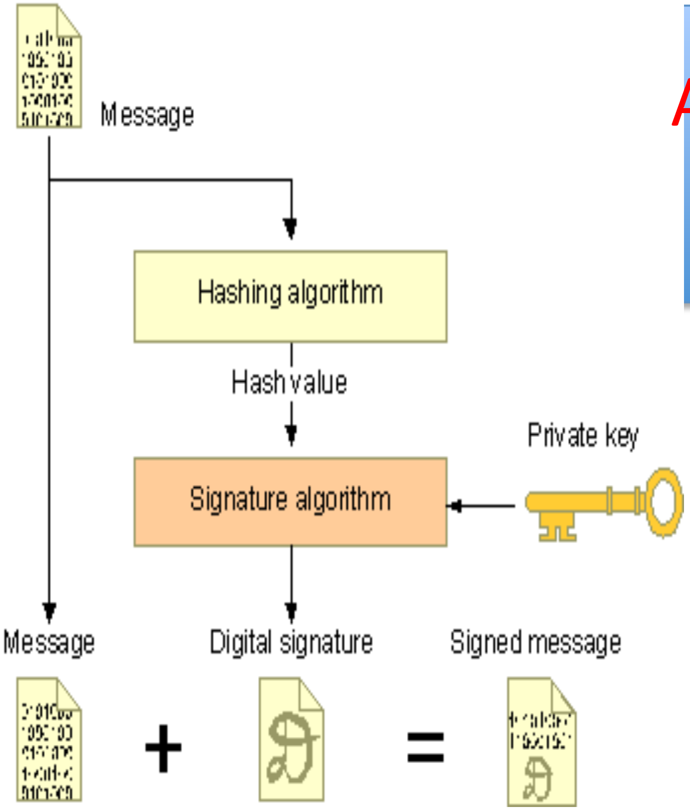
- Key pair: public key and private key





# Public Key Crypto: Digital Signature

- First, create a message digest using a cryptographic hash
- Then, encrypt the message digest with your private key

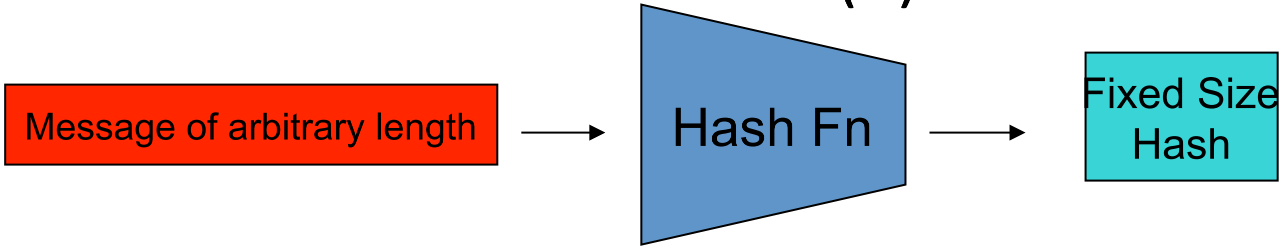


Authentication

Integrity

# Cryptographic Hash Functions

- Consistent: hash(X) always yields same result
- One-way: given Y, hard to find X s.t. hash(X) = Y
- Collision resistant: given hash(W) = Z, hard to find X such that hash(X) = Z



# Back to BitCoin

- Validation
  - Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  - How do you prevent a coin from double-spending? → Broadcast to all nodes
- Creation of a virtual coin/note
  - How is it created in the first place? → Provide incentives for miners
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins

# Preventing Double-spending

- The only way is to be aware of all transactions.
- Each node (miner) verifies that this is the first spending of the Bitcoin by the payer.
- Only when it is verified it generates the proof-of-work and attach it to the current chain.

# Bitcoin Network

- Each P2P node runs the following algorithm:
  - New transactions are broadcast to all nodes.
  - Each node (miners) collects new transactions into a block.
  - Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
  - When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
  - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

# Practical Limitation

- At least 10 mins to verify a transaction.
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction ($$$) wait longer. Because if you wait longer it becomes more secure. For large $$$, you wait for six blocks (1 hour).