

Blockchain Technology 2

Beni Iyaka H00181266

bi34@hw.ac.uk

MSc Software Engineering

2016 - 2017

Outline

- Overview
- Objectives of the internet
- Blockchain vs Internet
- Internet
- Blockchain
- Bitcoin
- Bitcoin Transaction
- Further Readings



Blockchain Technology the second coming of the Internet

Overview

- Before talking about how blockchain is competing with the internet, let's first talk about the internet.
- Internet was created in 1958 in America.
- Internet began to grow in 1970 as the knowledge of networking was growing more and more rapidly.
- Internet allows people to send and receive data wherever they are in the world if they have internet access.

Objectives of The internet

- The main purpose of the Internet is offering effective information sharing and communication globally using computers. Notably, the Internet is the biggest player in the realization of the concept of globalization today. With the Internet, the world has become a global village.
- The internet in our day is used for many different things such as:
 - Online shopping.
 - Watching videos.
 - Research.
 - Downloading or listening to music.

Blockchain Vs Internet

- With the internet technology, data is shared at the application layer and not the protocol level.
- With internet technology, many applications have become valuable by capturing data from users. Because this data is isolated, therefore valuable.
- Blockchain technology acts the opposite. The network runs on the protocol layer.
- Blockchain technology is based on shared information; which means that the shared information is not very valuable because everybody has it.

The internet

1. Application
2. Application Protocol
3. Application Low

Application

Application Protocol

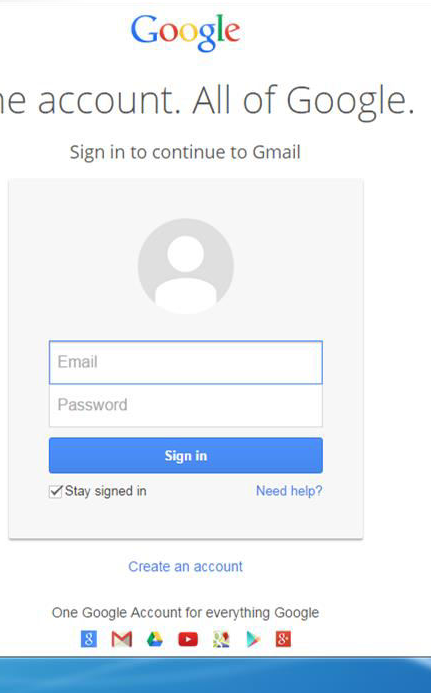
Application Low

SMTP

IMAP

POP3

TCP/IP



Application

- Gmail which stands for Google Mail, this is one of the internet application.
- Gmail was released on April first 2004.
- This is used for mailing conversation and adverts email service developed by Google.

Application

- Gmail which stands for Google Mail, this is one of the internet application.
- Gmail was released on April first 2004.
- This is used for mailing conversation and adverts email service developed by Google.



Application Protocol

- This is a mechanism that help govern communication on the internet network through various protocols.
- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is an internet protocol standards for electronic mail transmission.
- SMTP is used for sending and receiving mail.

Application Protocol

- But very limited when it comes to queuing messages at the receiving end.
- That's why SMTP uses POP3 or IMAP so as to allow the user to save the messages in the server.
- POP3 stands for Post Office Protocol 3.
- POP3 is known to be the most recent standard protocol used for receiving emails.

Application Protocol

- POP3 is a protocol used by both client and server end.
- POP3 allows the user to receive and save the email in the internet server.
- IMAP stands for Internet Message Access Protocol.
- IMAP is a standard email protocol that helps retrieve email messages on a mail server.

Application Low

- The google mail uses TCP/IP to enable better transmission of mail from the sender to the receiver.

TCP/IP

- This is a two layer program.
- The top layer is Transmission Control Protocol layer and the bottom layer is Internet Protocol.

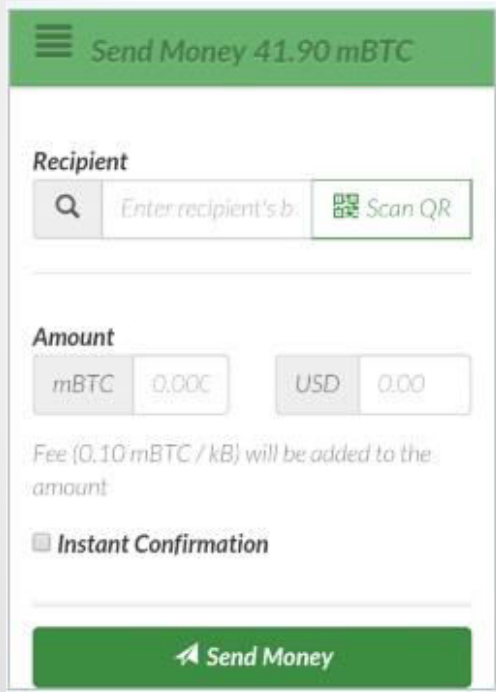
- Transmission Control Protocol helps manage the assembling of a message into small packets.
- Those packets are then transmitted over the internet and then received by a TCP layer that reassembles the packet into the original message.
- The Internet Protocol handles the address part of each packet so as to make sure that they get to the right destination.

Blockchain

Application

Application Protocol

Application Low



The screenshot shows a mobile application interface for sending Bitcoin. At the top, a green header bar contains a hamburger menu icon and the text "Send Money 41.90 mBTC". Below this, the "Recipient" section has a search icon, a text input field with the placeholder "Enter recipient's b...", and a "Scan QR" button with a QR code icon. The "Amount" section features two input fields: one for "mBTC" with the value "0.000" and another for "USD" with the value "0.00". Below these fields, a note states "Fee (0.10 mBTC / kB) will be added to the amount". There is a checkbox labeled "Instant Confirmation" which is currently unchecked. At the bottom, a large green button with a paper plane icon and the text "Send Money" is visible.

Bitcoin Protocol

Chain Block Protocol

Ethereum Protocol



Arrington, M., 2006. Gmail disaster: Reports of mass email deletions.

Overview

- Bitcoin is an innovative payment network and a new kind of money.
- Bitcoin, the online, digital currency and also the internet of money.
- Bitcoin uses peer-to-peer technology to operate with no central authority or banks

- Bitcoin is an innovative payment network and a new kind of money.
- Bitcoin, the online, digital currency
- Bitcoin uses peer-to-peer technology to operate with no central authority or banks
- Bitcoin is open-source; its design is public, nobody owns or controls

- Bitcoin is open-source; its design is public.
- Nobody owns or controls it.
- Bitcoin is the first successful implementation of a distributed crypto-currency, described in part in 1998 by Wei Dai
- In 2007, Satoshi Nakamoto began working on the Bitcoin although Craig Steven Wright claims to be the real person behind the pseudonym.

- In 2008, Nakamoto published the first design paper. And Bitcoin.org was registered.
- In 2013, the first Bitcoin ATM in the world is debuted in San Diego and california.
- Bitcoin is a peer to peer network that maintains a public decentralised ledger of digital math based assets.
- Bitcoin is an open source cryptocurrency.

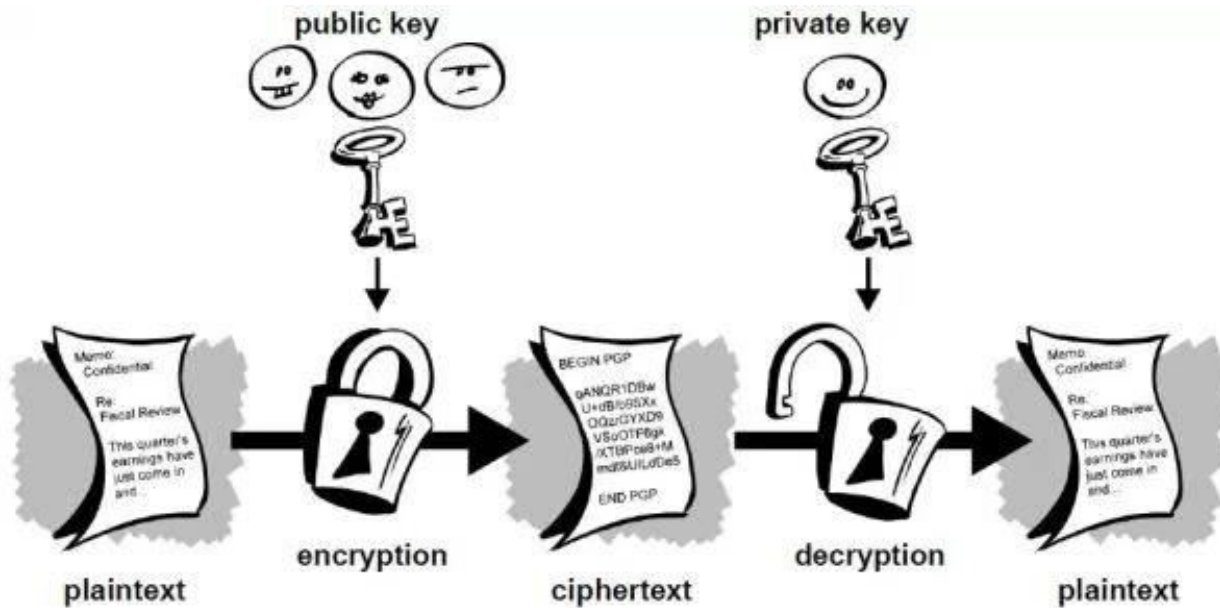
- Bitcoin can be categorised as a distributed accounting system.
- In bitcoin, the transaction is verified through the proof-of-work system of computers running a mining software

- Bitcoins can easily be sent through the internet without the need of the third party.
- The supply of bitcoins is regulated by software.
- The agreement of users of the system and cannot be manipulated by any government, bank, organization or individual.

- Bitcoin transactions are irreversible by design.
- They are fast.
- Funds received are available for spending within minutes
- Cost very little, especially compared to other payment networks

- In Bitcoin, anonymity and traceability are user defined. This means that the counterparty can be anonymous as they take steps to be even to each other.
- All the transfers in Bitcoins consist not of physically moving an object from A to B but simply by adding a new and publicly accepted transaction to the blockchain.

What Do Bitcoins look like?



Public Key

- This is also known as address. This key is known by other users. It is 34 characters long starting with 1 or 3 which represent a possible destination for payment.
- Example of a public key:
- 1FfmbHfnpaZjKFvyi1okTjJJusN455paPH



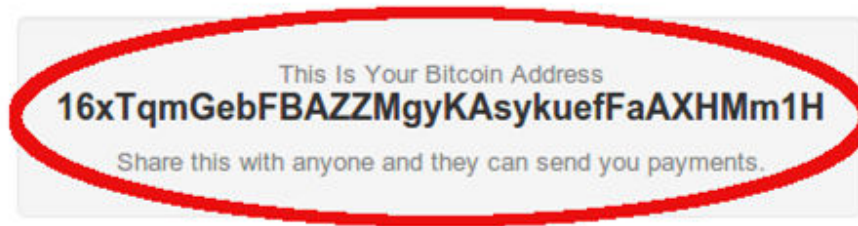
Private key

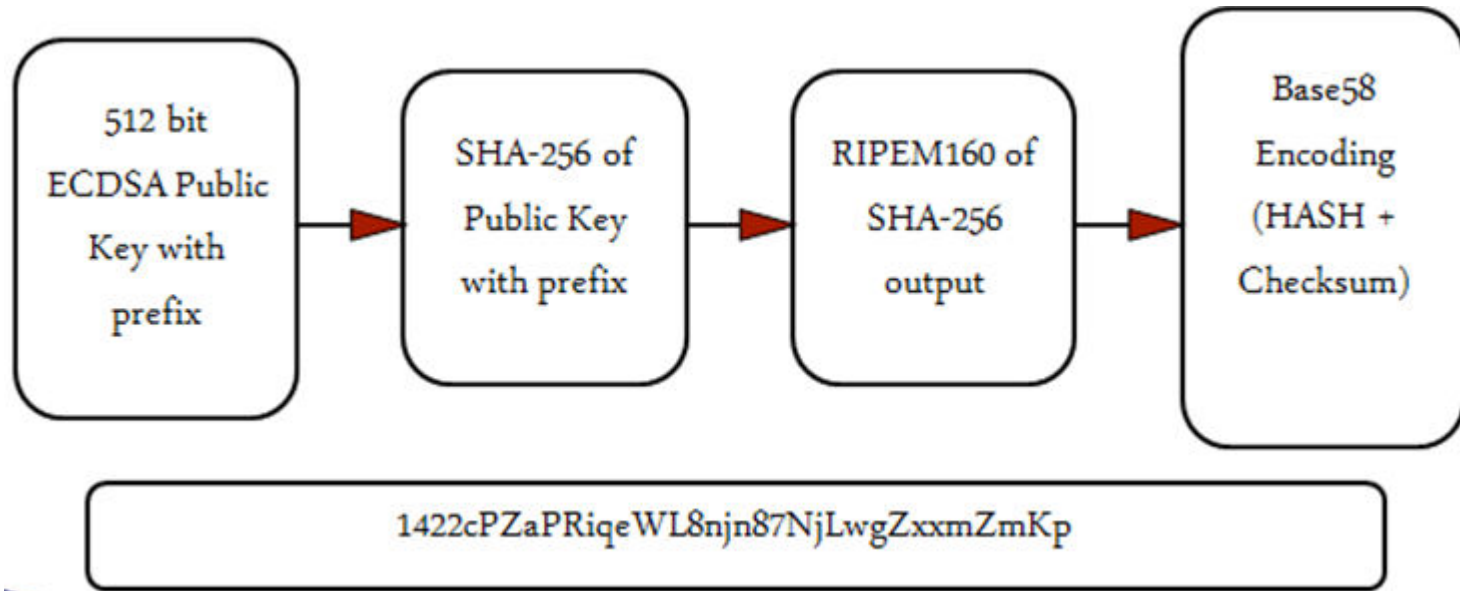
- This is only known by the owner. It is 51 characters long starting with 5. This key is required to transfer value from the address.
- Example of a private key:
- 5J4UA9wdxyicQgjAyMZUazcwwAf6Lz3afTcSXxi4fSpQmeXRQdY



Address

- A Bitcoin address is similar to a physical address or an email
- A Bitcoin Address is derived by a ECDSA (Elliptic Curve Digital Signature Algorithm) Public Key by using hash functions.





Application protocol

Bitcoin Protocol

- This is also known as Cryptographic protocol.
- This protocol handles security based functions and applies cryptographic methods to it.

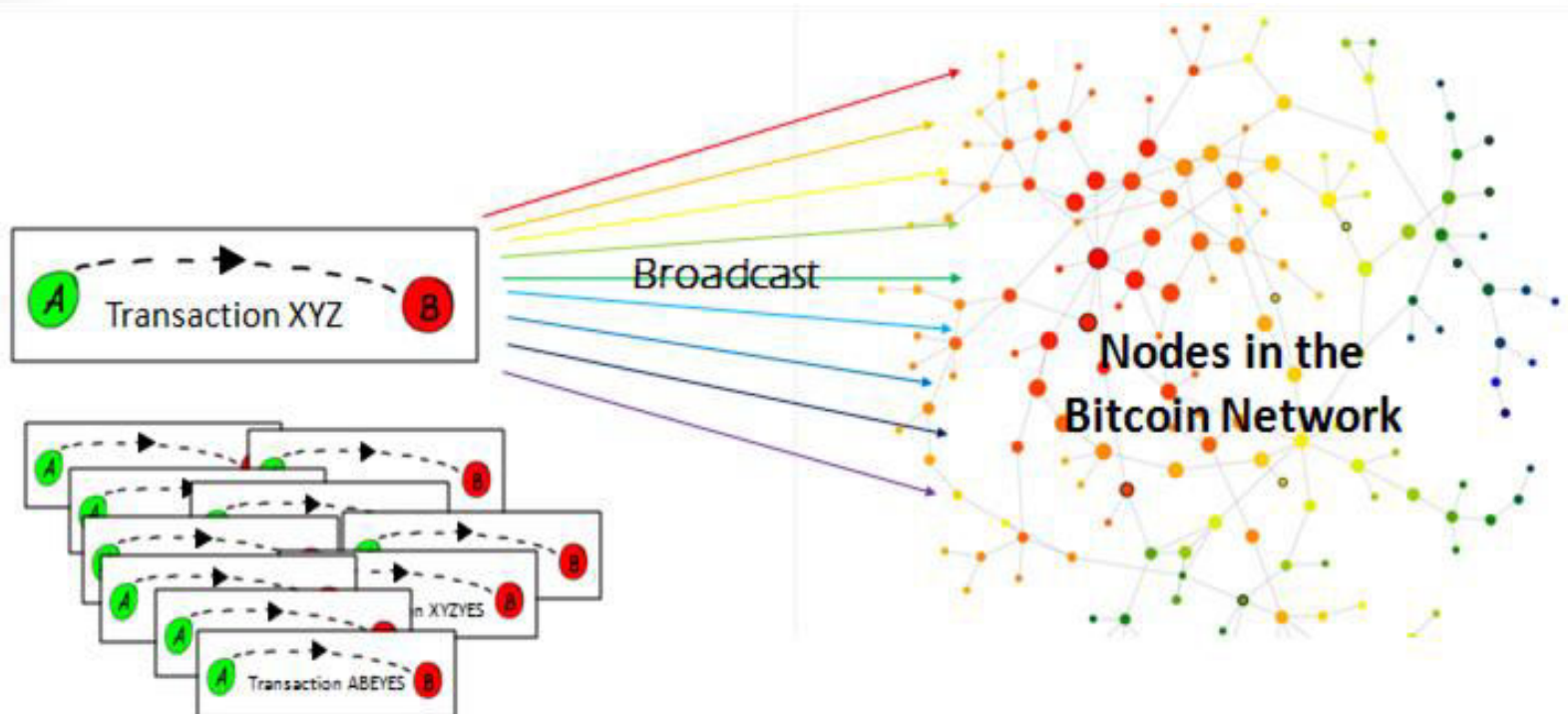


Ethereum Protocol

- This is an open platform that lets anyone build and use decentralized applications that runs on blockchain technology.
- This is an open-source project built by many people around the world.
- Contrary to bitcoin, ethereum was designed to be adaptable and flexible.

Bitcoin Transaction

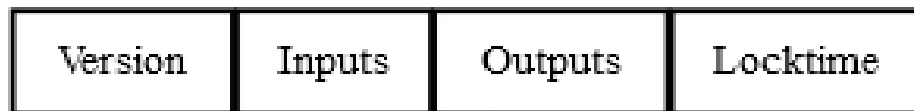
- Transactions let users spend satoshis
- A **Satoshi** is the smallest fraction of a Bitcoin that can currently be sent: 0.00000001 BTC
- There are two types of transactions
 - Coinbase transactions
 - New Bitcoins are introduced into the system
 - In every block as the very first transaction
 - reward for solving a proof-of-work problem
 - Regular transactions
 - Are used to transfer existing Bitcoins amongst different accounts



- Each transaction is prefixed by a four-byte transaction version number
 - Bitcoin peers and miners which set of rules to use to validate it
- Each transaction has at least one input and one output
- Each input spends the satoshis paid to a previous output.
- Each output then waits as an Unspent Transaction Output (UTXO) until a later input spends it

Each input spends a previous output

The Main Parts Of
Transaction 0



The Main Parts Of
Transaction 1



Each output waits as an Unspent TX Output (UTXO) until a later input spends it

- An input uses a transaction identifier (txid)
- And an output index number (often called “vout” for output vector) to identify a particular output to be spent
- It also has a signature script which allows it to provide data parameters that satisfy the conditionals in the pubkey script

- An output has an implied index number based on its location in the transaction
- The output also has an amount in satoshis which it pays to a conditional pubkey script
- Anyone who can satisfy the conditions of that pubkey script can spend up to the amount of satoshis paid to it

Further readings

<https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/>

<https://bitsonblocks.net/2016/05/09/confused-by-blockchains-revolution-vs-evolution/>

<https://bitsonblocks.net/2015/12/01/the-pros-and-cons-of-internal-blockchains/>

Further readings

<https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens/>

<https://bitsonblocks.net/2015/09/21/a-gentle-introduction-to-bitcoin-mining/>

<https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/>