Internet, Principes et Protocoles (IPP)

IPv6 address composition

- An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.
- 0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011
- **2001:0000:3238:DFE1:0063:0000:0000:FEFB**

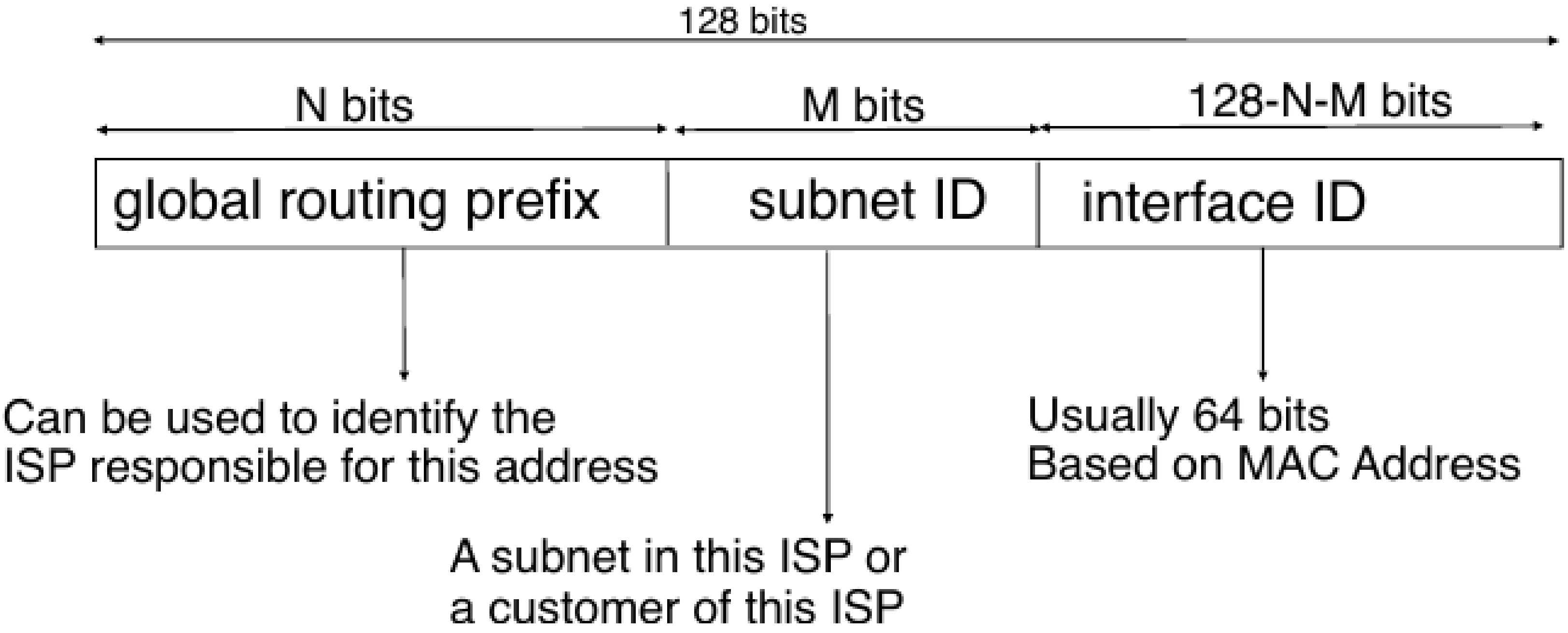
IPv6 Unicast

Special addresses

- Unspecified address : 0:0:0:0:0:0:0:0 (aka *::*)
- Loopback address : 0:0:0:0:0:0:0:1 (aka *::1*)

Global unicast addresses

- Addresses will be allocated hierarchically



128 bits

N bits

M bits

128-N-M bits

global routing prefix

subnet ID

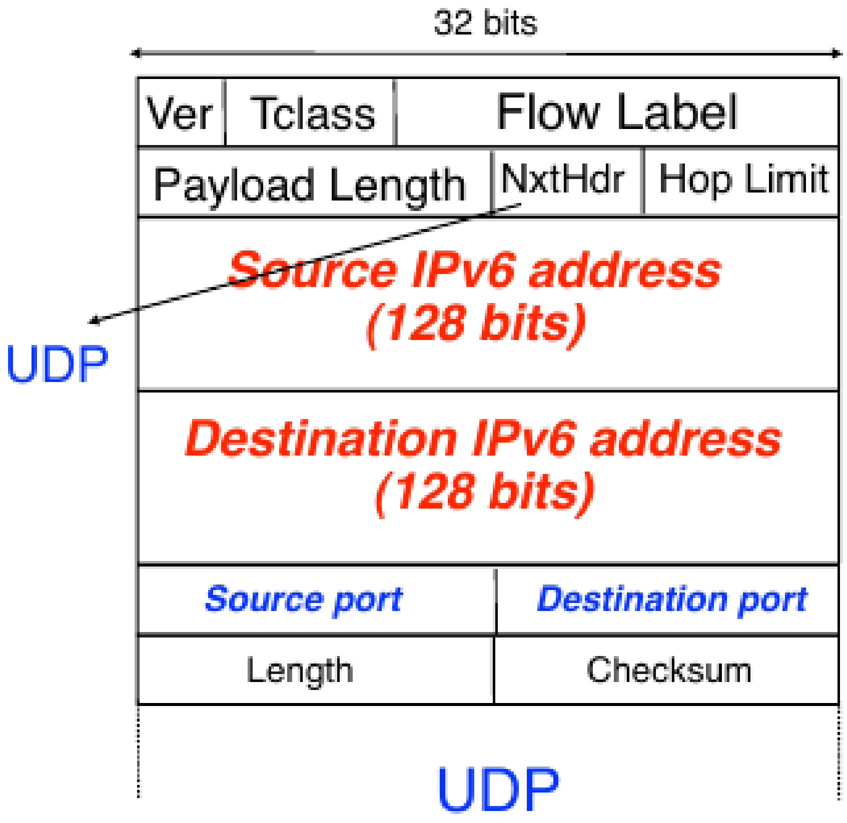
interface ID

Can be used to identify the
ISP responsible for this address

A subnet in this ISP or
a customer of this ISP

Usually 64 bits
Based on MAC Address

IPv6 Paquet example



32 bits

Ver | Tclass | Flow Label

Payload Length | NxtHdr | Hop Limit

Source IPv6 address (128 bits)

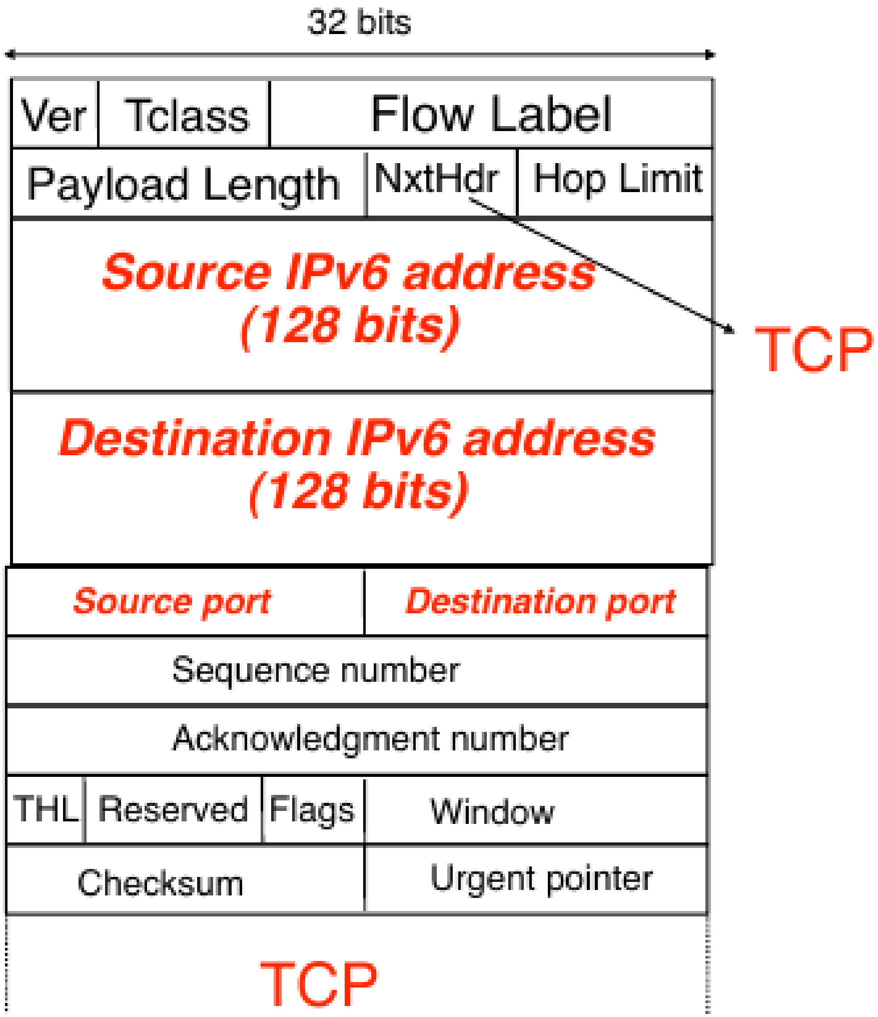
Destination IPv6 address (128 bits)

Source port | *Destination port*

Length | Checksum

UDP

UDP



32 bits

Ver | Tclass | Flow Label

Payload Length | NxtHdr | Hop Limit

Source IPv6 address (128 bits)

Destination IPv6 address (128 bits)

Source port | *Destination port*

Sequence number

Acknowledgment number

THL | Reserved | Flags | Window

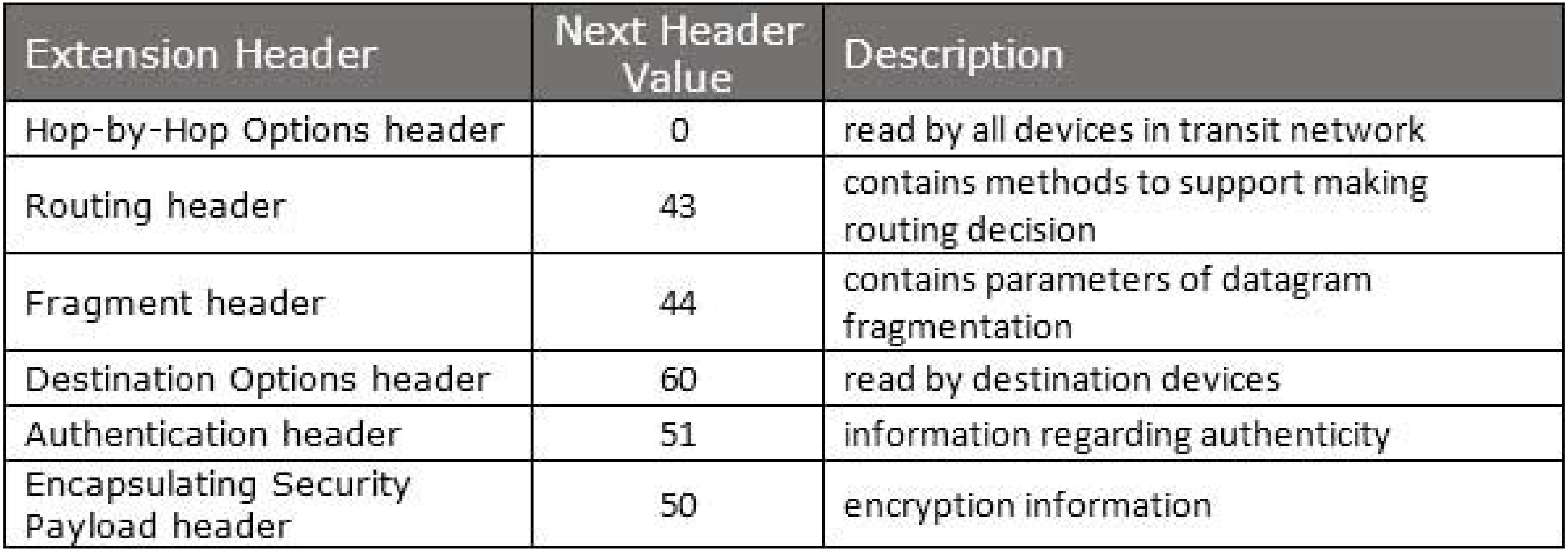
Checksum | Urgent pointer

TCP

TCP

IPv6 Extension Headers

As you can see, The IPv6 fixed header is short. IPv6 supports header extensions, that hold more info.



Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

Neighbor Discovery Protocol

- ARP, translates MAC address to IP address. Uses broadcasts (not possible in IPv6).
- DHCP, gives IP address to the machines on the network that request it.
- Since an IPv6 is composed of the MAC address and subnet, a newly connected machine could auto-configure its IPv6 (network + subnet + MAC).
- Uses ND protocol to advertise/choose an IP

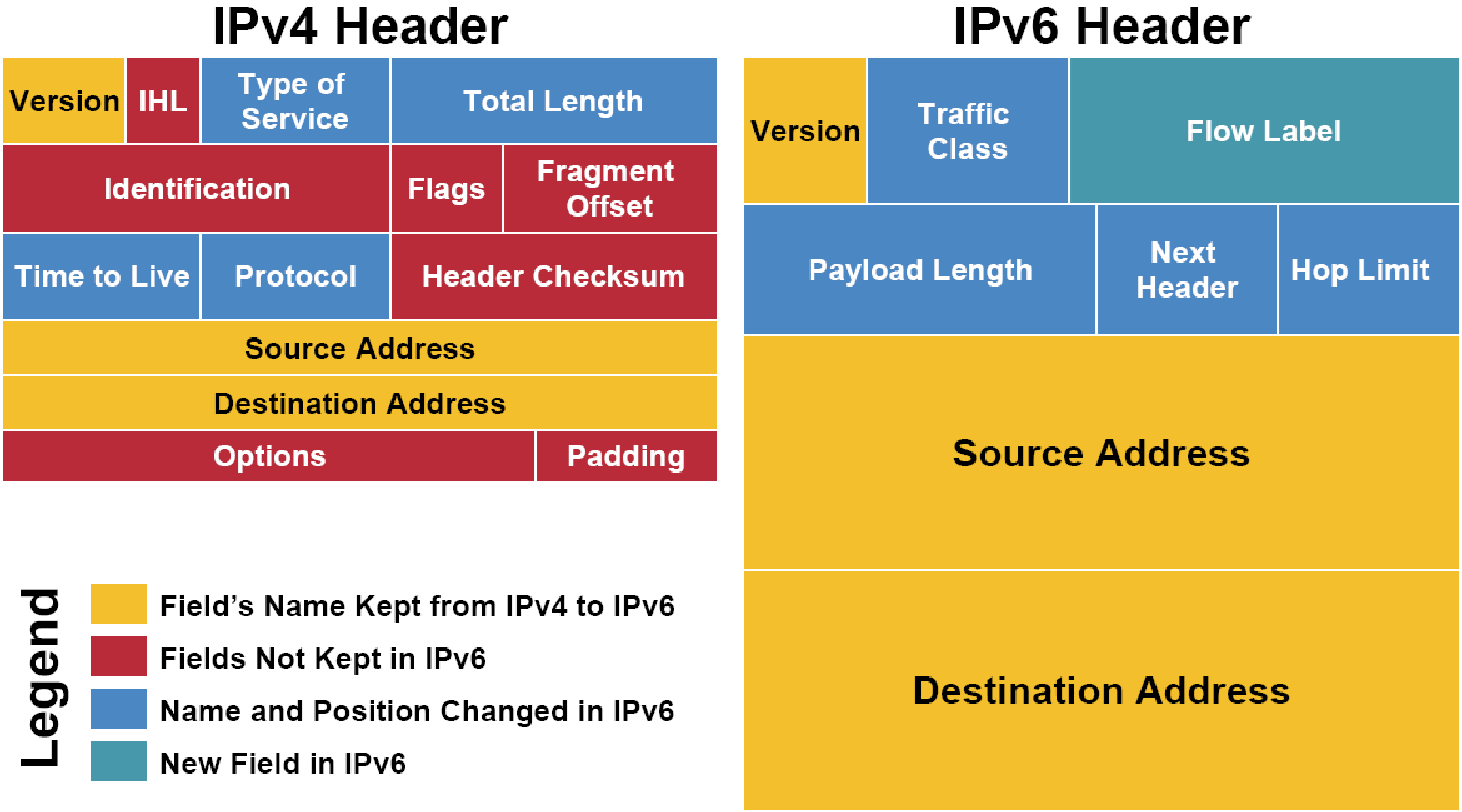
IPv4 to IPv6 Transition

- IPv6 is not backwards compatible. A domain/network either uses one or the other.
- Solutions:
  - Dual-stack routers
  - Tunneling (ISATAP, Teredo, 6over4 or 4over6)
  - NAT-PT (Network Address Translation – Protocol Translation), already obsolete. DSTM is the new sexy.

Food for thought

- Why is the EU/US slower to adopt IPv6 than the rest of the world, for example Asia?
- Compare the ipv6 header and the ipv4 header, and for each field that is different in IPv6 (added, removed, new), explain what is/was it used for.

Header differences



IPv4 Header

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options | Padding

IPv6 Header

Version | Traffic Class | Flow Label

Payload Length | Next Header | Hop Limit

Source Address

Destination Address

Legend

- 🟨 Field's Name Kept from IPv4 to IPv6
- 🟥 Fields Not Kept in IPv6
- 🟦 Name and Position Changed in IPv6
- 🟩 New Field in IPv6

Bitcoin

- Why is this in the networking class?
  - Peer-to-Peer Cryptographic protocol to share information.
  - A payement System
  - Also, a cryptocurrency
  - The blockchain has a big technology impact

- We will not talk about how to buy, sell and secure your cryptomoney!

Bitcoin

- Reminder on Private-Public keys, Hash functions
- Bitcoin, how does it work
  - Basics (goal, problems, solutions)
  - Blockchain (Video)
  - Mining, forks (51% attack)
- Proof of work vs proof of stake (and implications: resources needed, envir,)
- Other currencies
- Other bitcoin applications, is it really anonymous, mixers,.. cryptokittens and eth

Bitcoin Origins

- White paper published November 2008 by Satoshi Nakamoto

  "Bitcoin: A Peer-to-Peer Electronic Cash System"

- Working implementation published 3 months later as an open source project.

Bitcoin Goal

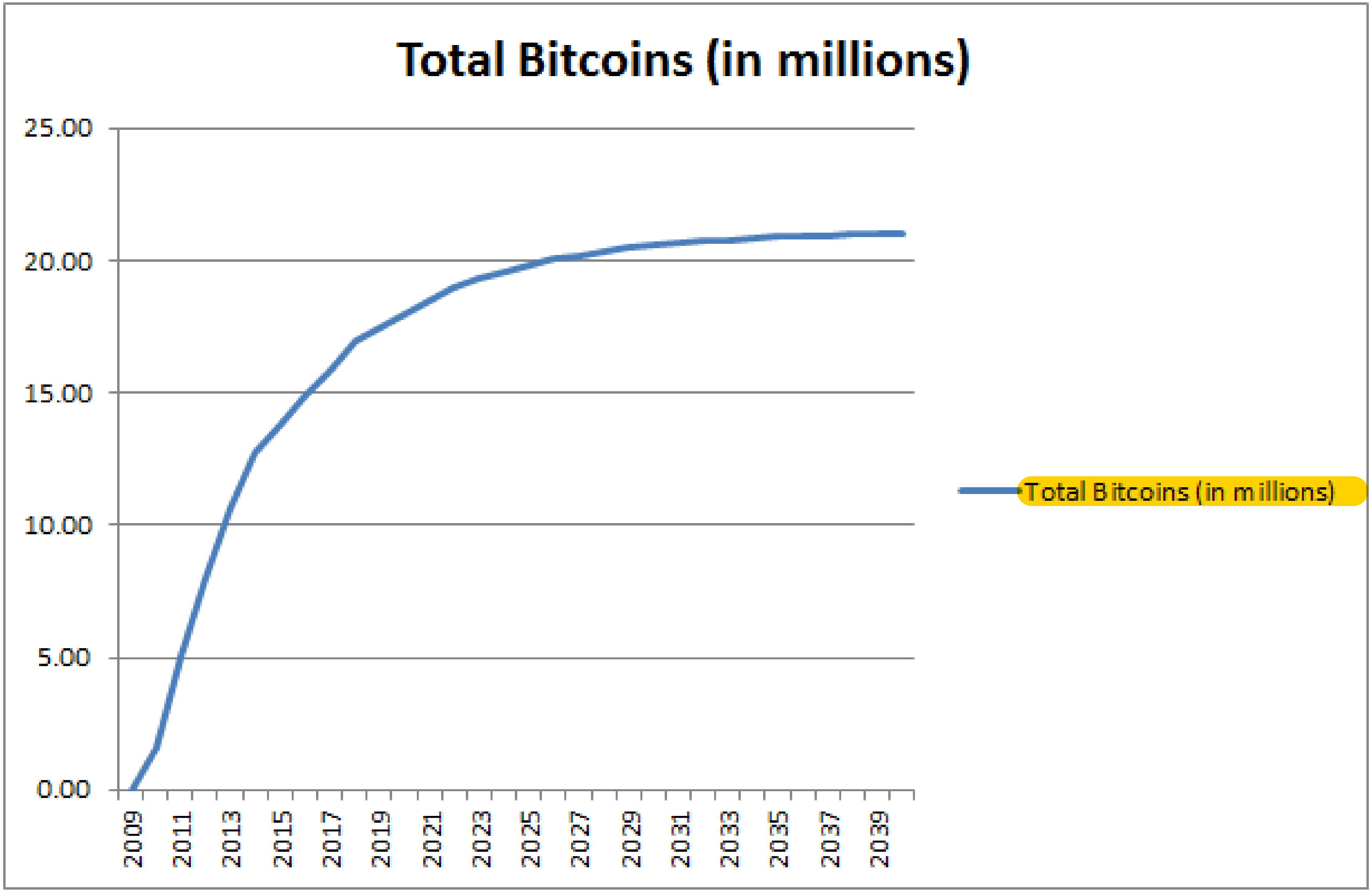
- A new P2P Electronic cash system, designed to avoid a central authority (banks IRL).

- Properties of Digital Payment Systems
  - No counterfeiting: You cant increase money supply at will (create new money)
  - No double spending: You cant spend the same value more than once
  - Transactions are irreversible: You cant undo a transaction

Bitcoin

- 1st things first: how do you distribute the original bitcoins?
- Every 10 minutes, a node in the Bitcoin network receives a reward for its work (mining).
- Reward started at 50 bitcoins, and halves every 4 years.

Maximum Bitcoins possible

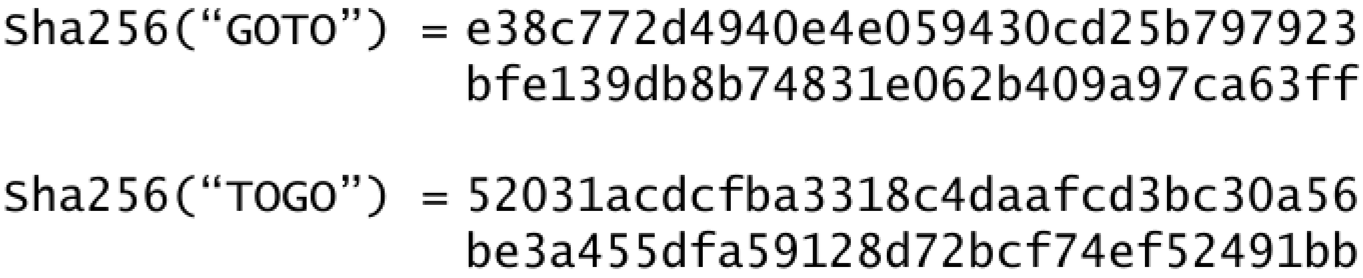


The blockchain

- The big invention that makes the Bitcoin work
- The blockchain is a database containing historical records of all the transactions that ever occurred on the network.
- Every full node in the network has a copy that they keep up-to-date.
- Some nodes extend (add to) the blockchain, they are called miners.
- First feeling for how it works?

Cryptography reminder

- A hashing function takes any input and produces a fixed-length output.
  - *hash_function(input) = fixed_length_output*
- It is theorically not possible to find the input starting from the output, even knowing the hash_function.
- FYI: Also used for passwords storage.



```
Sha256("GOTO")  = e38c772d4940e4e059430cd25b797923
                  bfe139db8b74831e062b409a97ca63ff

Sha256("TOGO")  = 52031acdcfba3318c4daafcd3bc30a56
                  be3a455dfa59128d72bcf74ef52491bb
```

Cryptography Reminder

- Diffie-Hellman - Everyone on the network gets a private(secret)/public key pair.
- To sign a message:
  - Hash the message to be signed
  - Use the senders private key to encrypt the result. Result is a signature.
  - Send **both** the message(unencrypted) and the signature.
- Check for the signature:
  - The receiver decrypts the signature with the sender’s public key. Only the sender’s PK can decrypt the message, thus ensuring the origin.
- Check for message integrity:
  - The receiver re-hashes the message, and compares it with the hash in the signature. If ==, then OK.

Video Time

One transaction

- Sending a bitcoin from wallet A to B, you need to add a transaction fee. The higher the fee, the faster the transaction (miners will pick it up faster).
- Because you are sending a Bitcoin you received, you can follow the blockchain all the way to the origins of the bitcoin you are sending:
- *You can follow a Bitcoin along the blockchain*

Mining and 51% attack

- Mining = Proof of work
- Everyone trusts the longer chain. If someone controls +51% of nodes, he could control the chain
- 2018, Bitcoin mining represents the electricity consumption of Tchequia, at some point same as Danemark.
- 1 transaction represents a USA house’s energy consumption for 21 days.
- Alternatives? (Start from the goal of mining)

Proof of work/Stake

- Proof of work: needs energy, could be positive (usefull CPU calculations, proof of sports – run,..) or not. Cost intensive.
- Proof of stake:
- The creator of the next block is chosen from a pool via various combinations of random selection and wealth or age (node or coin age).
  - Problem: you can ‘work’ on several forks at the same time, since ‘mining’ is almost costless

Other Famous Currencies

- Ethereum: decentralized software platform that enables Smart Contracts and Decentralized Applications Ethereum is a decentralized software platform that enables Smart Contracts and Decentralized Applications
- Ripple is a real-time global settlement network that offers instant, certain and low-cost international payments. Launched in 2012, Ripple "enables banks to settle cross-border payments in real-time, with end-to-end transparency, and at lower costs." Sponsored by banks
- Bitcoin Cash, Litecoin, dodgecoin,...

Misc Discussions

- Is bitcoin really anonymous?
- What is a bitcoin mixer?
- CryptoKittens
- What is the role of a ‘notaire’? Can we use bitcoin in a way to bypass them?
- Other Bitcoin applications
- Money laundering and market manipulation

- We just scratched the surface – plenty of books about the details