BLOCKCHAIN 101

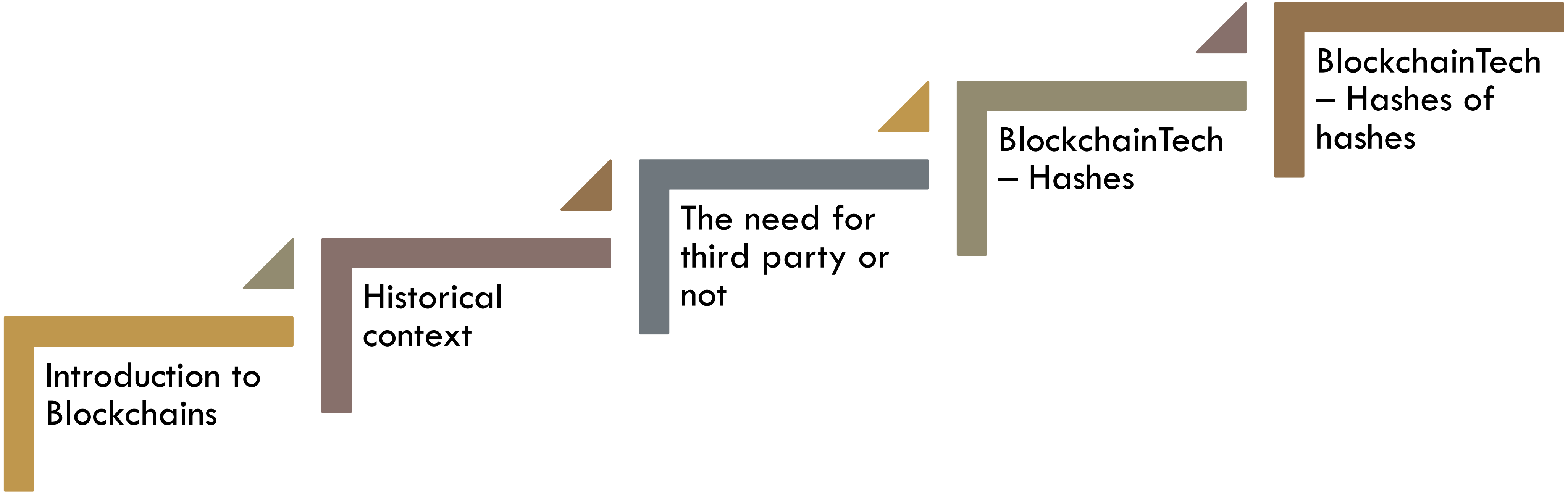
Prassanna Ganesh Ravishankar
github.com/atemysemicolon
prassanna.io (under construction)

INTRODUCTION

Why I like blockchains
Keywords
Let’s introduce ourselves.
Why do we want to do this course.
Choose whatever language is comfortable!

STRUCTURE

TALK



Introduction to Blockchains

Historical context

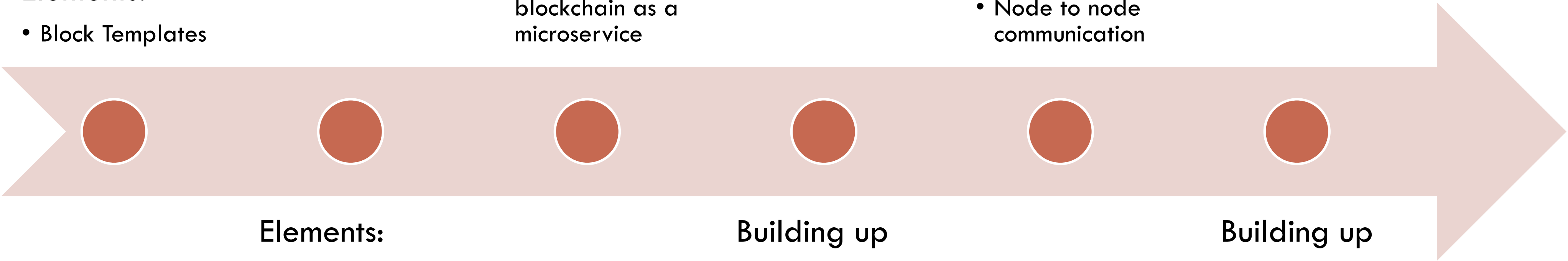
The need for third party or not

BlockchainTech – Hashes

BlockchainTech – Hashes of hashes

STRUCTURE

PROGRAMMING



Elements:

- Block Templates

Elements:

- Synchronization
  - Loading and Saving

Elements:

- Deploy the blockchain as a microservice

Building up

- Blockchain = chain of blocks

Building up

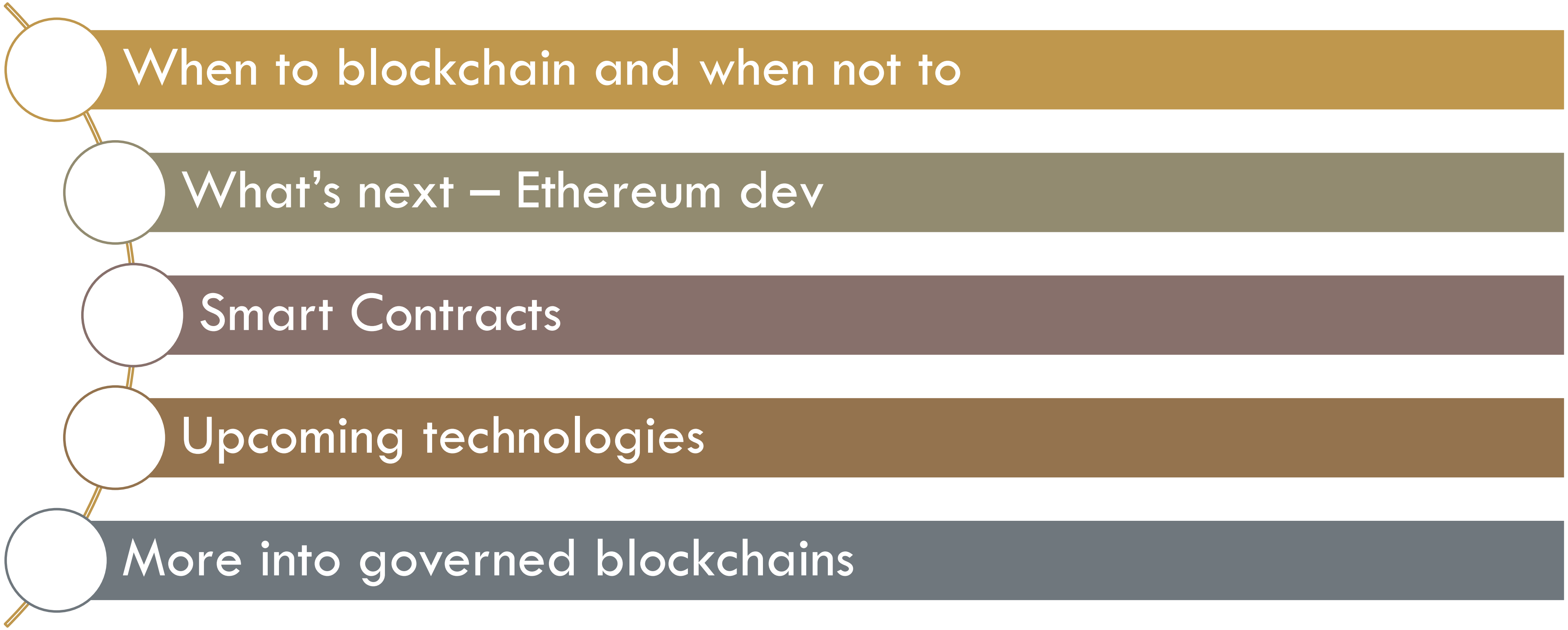
- Creating a node
- Node to node communication

Building up

- Node Transactions

STRUCTURE

PRESENTATION AND OPEN ENDED DISCUSSIONS



- When to blockchain and when not to
- What’s next – Ethereum dev
- Smart Contracts
- Upcoming technologies
- More into governed blockchains

LETS GET IN AND THEN GET OUT
A BRIEF INTRODUCTION BEFORE WE GO IN DEEP

What is a blockchain?

- Not a relational database
- Not a common folder such as dropbox or google drive
- Isn’t contained in one server
- Database is not anonymous

What is a blockchain then?

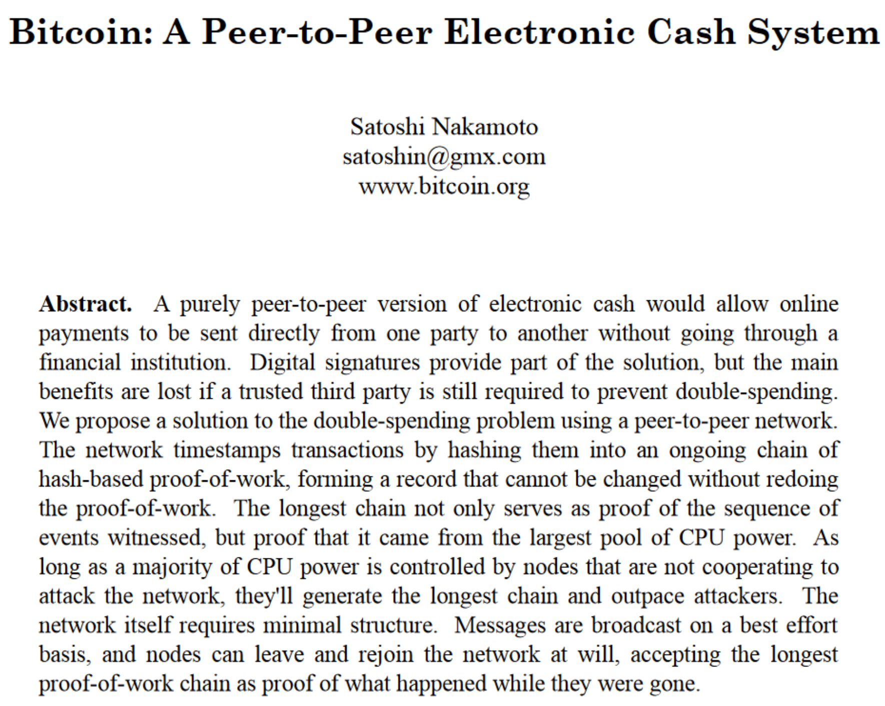
- A collection of serializable data objects, called blocks
- Connected through their hashes
- Linked list : hashes instead of pointers
- Technically, has no limit.
- Represents, almost always a sequence of events
- Transactions are “anonymous” as long as you don’t reveal your public key

BLAST FROM THE PAST

- Some history
- Providing context
- Motivations and inspirations

THE BIRTH OF THE BLOCKCHAIN

WHO IS NAKAMOTO?



Bitcoin: A Peer-to-Peer Electronic Cash System

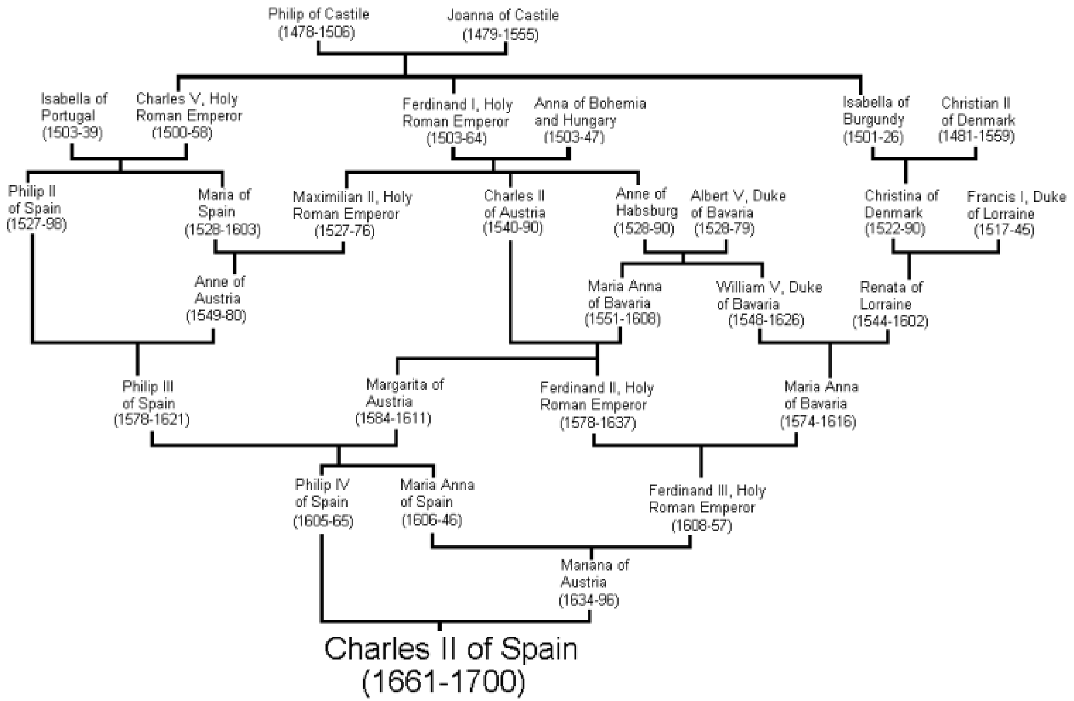
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

- Does it matter who Nakamoto is?
- It is compliant with the blockchain that his name stays public, yet anonymous
- Started of as a currency mechanism
- Possibilities : Cyberphunks
  - John Gilmore : **A guarantee - with physics and mathematics, not with laws - that we can give ourselves real privacy of personal communications.**
- Bitcoin, a direct successor of HashCash

HUMAN REFERENCE TO TECHNOLOGY

The Ancestry of King Charles II of Spain
(1661-1700)


Philip of Castile (1478-1506)
Joanna of Castile (1479-1555)
Isabella of Portugal (1503-39)
Charles V, Holy Roman Emperor (1500-58)
Ferdinand I, Holy Roman Emperor (1503-64)
Anna of Bohemia and Hungary (1503-47)
Isabella of Burgundy (1501-26)
Christian II of Denmark (1481-1559)
Philip II of Spain (1527-98)
Maria of Spain (1528-1603)
Maximilian II, Holy Roman Emperor (1527-76)
Charles II of Austria (1540-90)
Anne of Habsburg (1528-90)
Albert V, Duke of Bavaria (1528-79)
Christina of Denmark (1522-90)
Francis I, Duke of Lorraine (1517-45)
Anne of Austria (1549-80)
Maria Anna of Bavaria (1551-1608)
William V, Duke of Bavaria (1548-1626)
Renata of Lorraine (1544-1602)
Philip III of Spain (1578-1621)
Margarita of Austria (1584-1611)
Ferdinand II, Holy Roman Emperor (1578-1637)
Maria Anna of Bavaria (1574-1616)
Philip IV of Spain (1605-65)
Maria Anna of Spain (1606-46)
Ferdinand III, Holy Roman Emperor (1608-57)
Mariana of Austria (1634-96)
Charles II of Spain (1661-1700)

How are genes transferred? Based on the parents

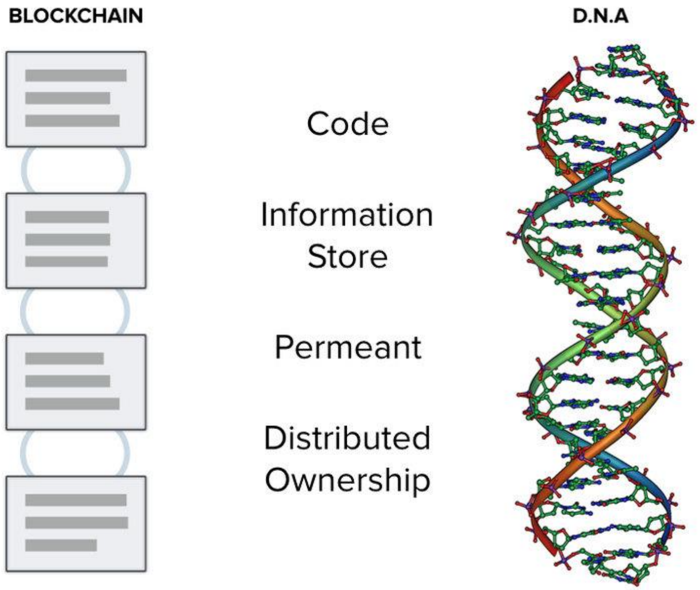
Can we remember our family from the beginning of time?

Making babies – Do we require third parties?

What is the one thing that keeps growing and morphing beyond birth and death?

- Your genes perhaps?

BIOMORPHIC SOFTWARE DESIGN



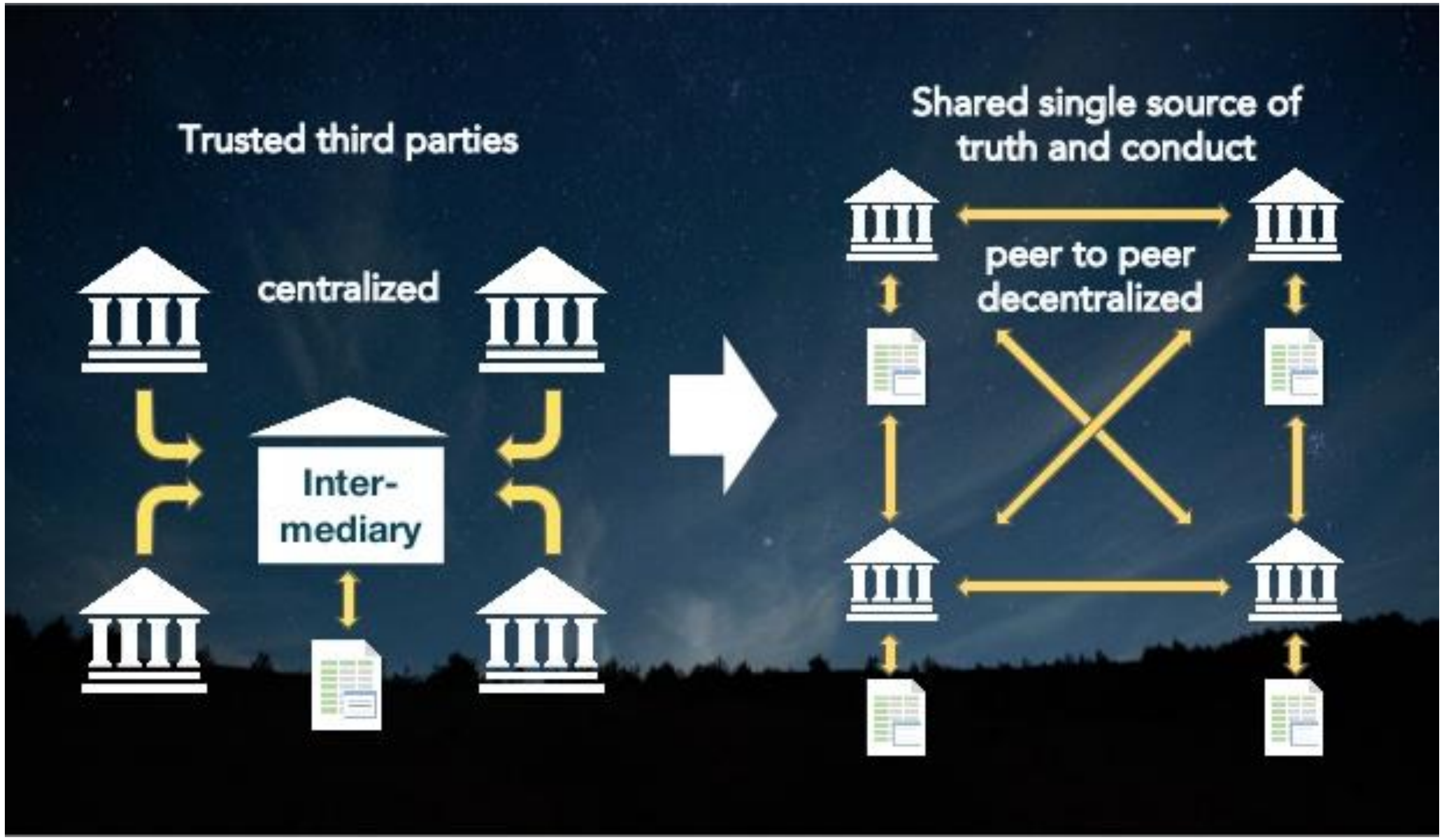
Now you understand why the previous slide!

Organic design of software.

Blockchains are a chain of blocks(i.e information).

A new block is added onto the chain with "energy" being spent based on the "environment" of transactions – The proof of work paradigm

- Don't laugh



THIRD PARTIES

Do we need third parties in transactions between two parties?

- Banking
- Downloading some famous software
- Hosting a social network
- Accessing Email

How does a blockchain replace the third party?

- It uses your peers as the third party

Cryptographic proof instead of trust

- Let’s start trusting people again by removing the need for trusting 3rd parties

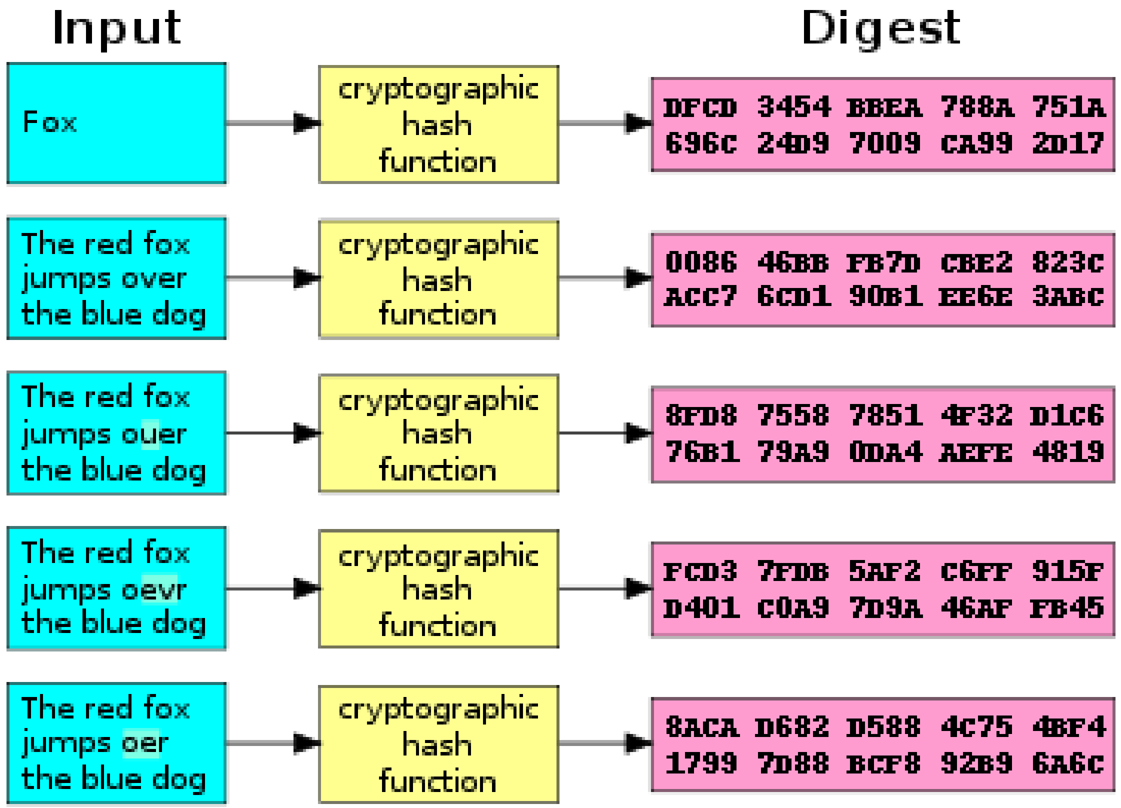
Therefore everyone “owns” the blockchain, but no one can “edit” the past.

HASHES

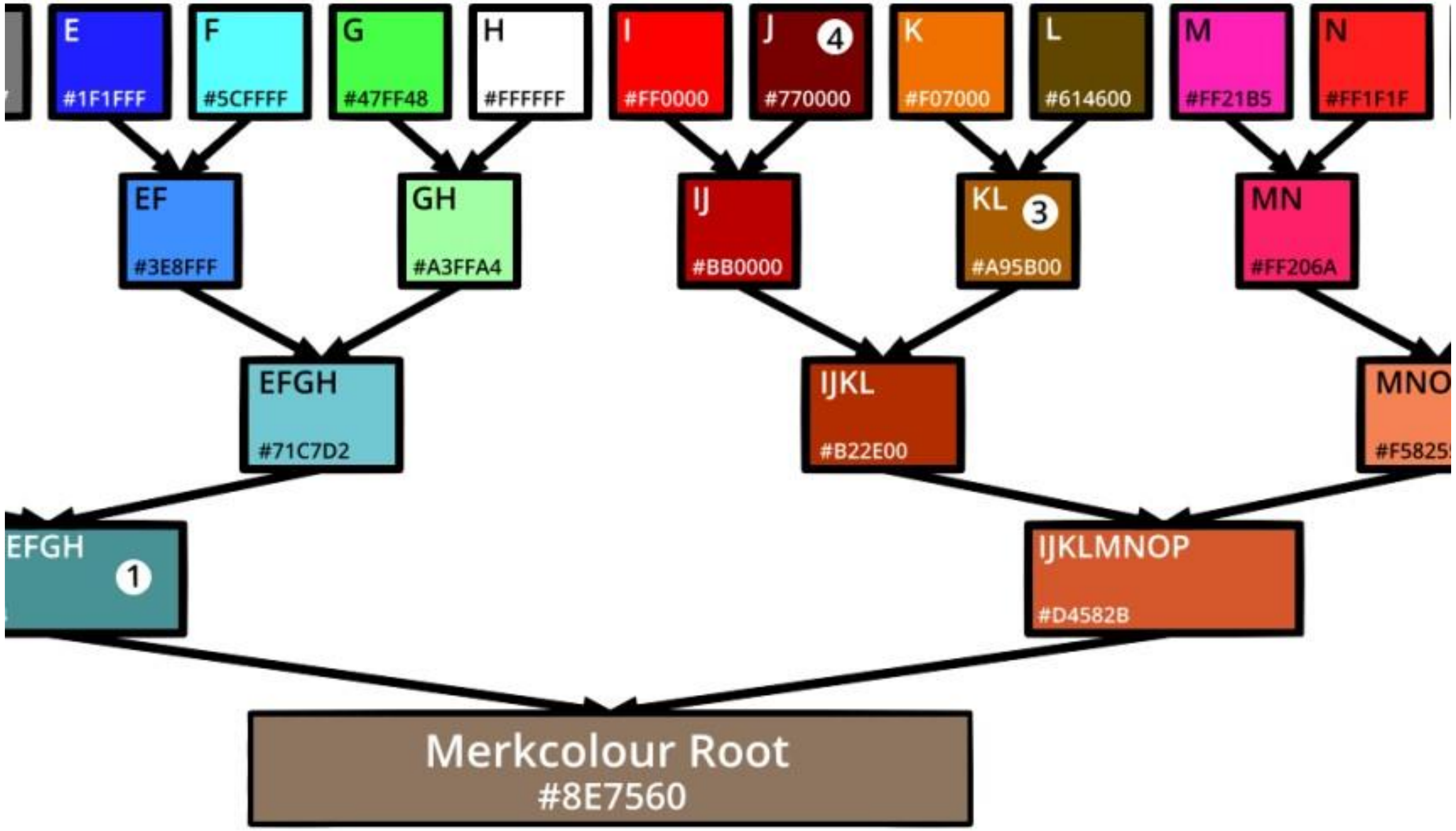
Hashes : are mathematical functions that take string data of fixed length and turn it into numerical data of fixed length

If I send some data and some hash, the receiver can hash the data he receives and verify if that's as expected

Easy way to verify data, not too intensive on the CPU



Input		Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog	cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	cryptographic hash function	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C



WHY ARE HASHES IMPORTANT?

Does it make sense using a hash for the entire blockchain, or using it Little by Little

Can I reverse all the combinations of colours if I reverse from the hash?

A merkle tree, is used in multiple applications

- git to keep track of branches, and from where they branched out of
- Apple has started using it to discover sectors of a corrupted hard disk, by having layers of hashes

Easy way to verify integrity in parts of a large, large structure of data

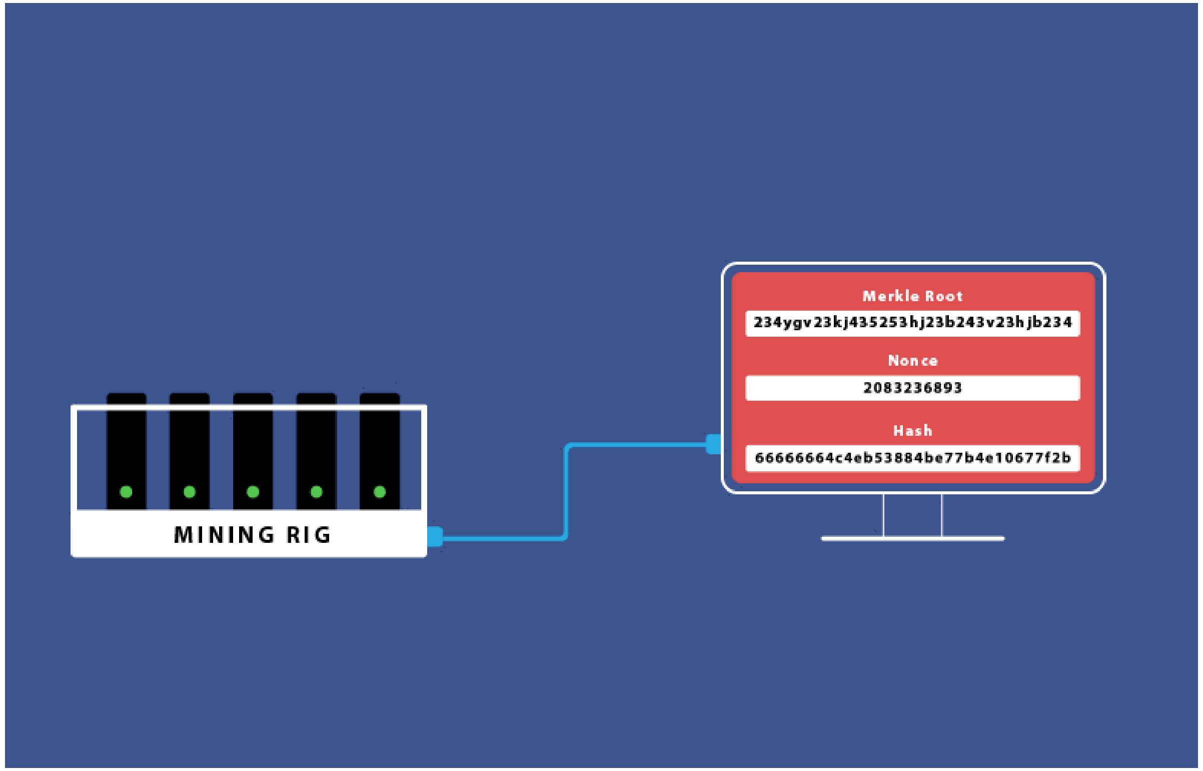
MINING
PROOF OF WORK

What is mining?

- Giving birth
- The creation of a new block from the previously existing block on the chain
- Mined blocks are verified and added to the chain
- In the case of bitcoin, mined blocks are blocks that take a bunch of transactions, and collect them as a block

Proof of work is the Mining technique that Bitcoin uses

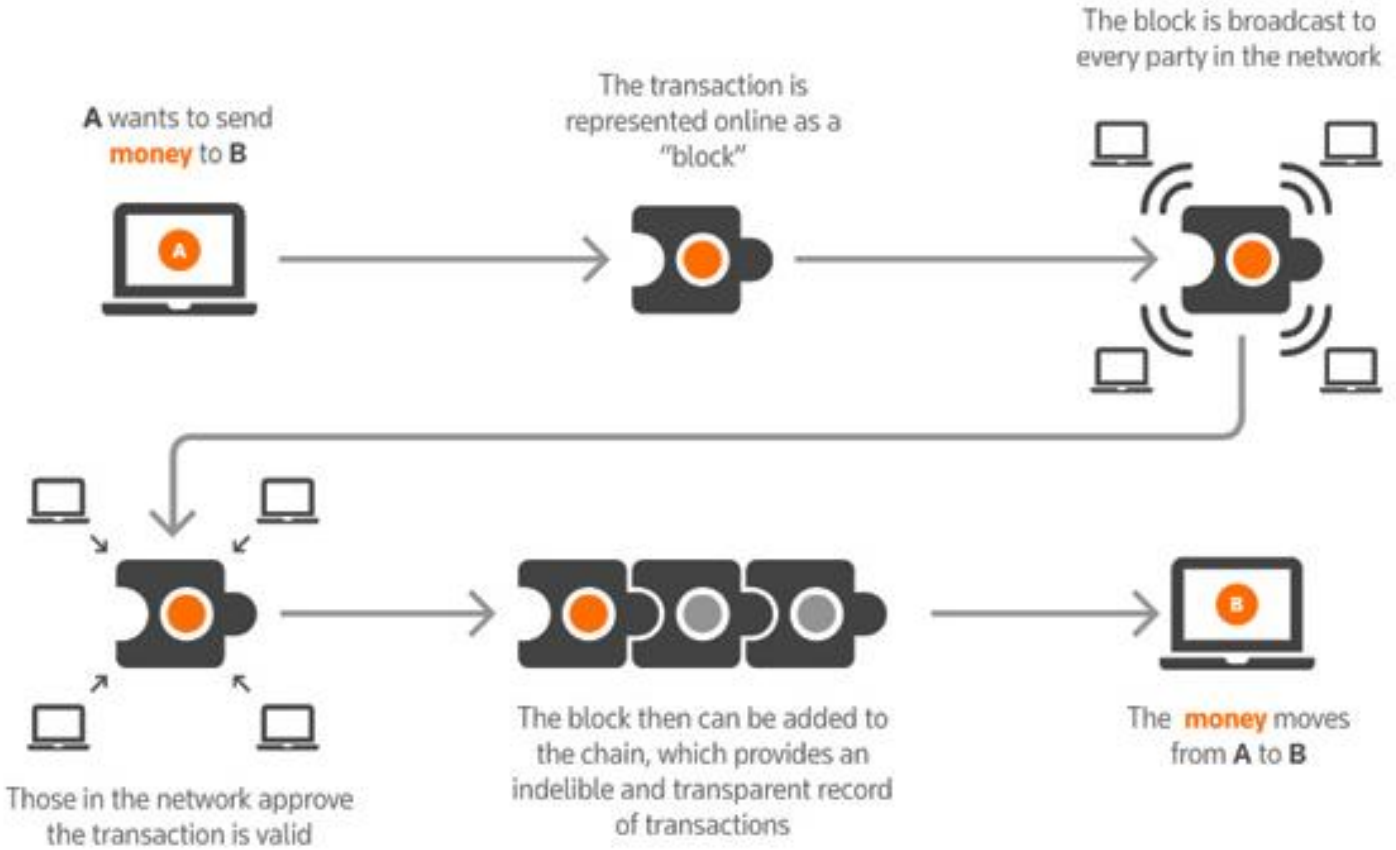
- Idea – Energy spent cannot be reversed.
- Keep adding a counter to your hash, till the hash follows a pattern
- This pattern is defined by the "difficulty" of the network
- Simple : Increment a counter till you get the required number of zeros in your hash



Merkle Root
234ygv23kj435253hj23b243v23hjb234

Nonce
2083236893

Hash
66666664c4eb53884be77b4e10677f2b


A wants to send money to B
A
The transaction is represented online as a "block"
The block is broadcast to every party in the network
Those in the network approve the transaction is valid
The block then can be added to the chain, which provides an indelible and transparent record of transactions
B
The money moves from A to B

WHAT IS A LEDGER?

A place where transactions are stored

- Banks do this (earlier in notebooks, now it computers)
- Mafia dons also do this in notebooks

Let's define the perfect Ledger

- Anyone should be able to access the ledger
- Anyone should be able to write transactions on the ledger
- If the book is over, let's index it and place it on the shelf, not in order
  - So if someone wants to steal it, or change transactions, they have to struggle to change the entries
- Each new book starts with the location of the previous book

BACK TO OUR BELOVED BLOCKCHAINS

To summarize:

- Blockchains are a collection of blocks
- Blocks always have a field pointing to the previous block
- Security comes from mining
  - If you change the content of the block, the hash would change, therefore the same counter will not follow the rule
  - Have to re-do the mining
  - For every block that comes after it
- Where is the block stored?
  - Any one who is a full-node, stores the block
  - A full node may mine, but also can verify a new block
- How do we verify the blockchain?
  - See if hashes computed for every block match the hash that's reported
  - Go back till the first block and see if we get the genesis block

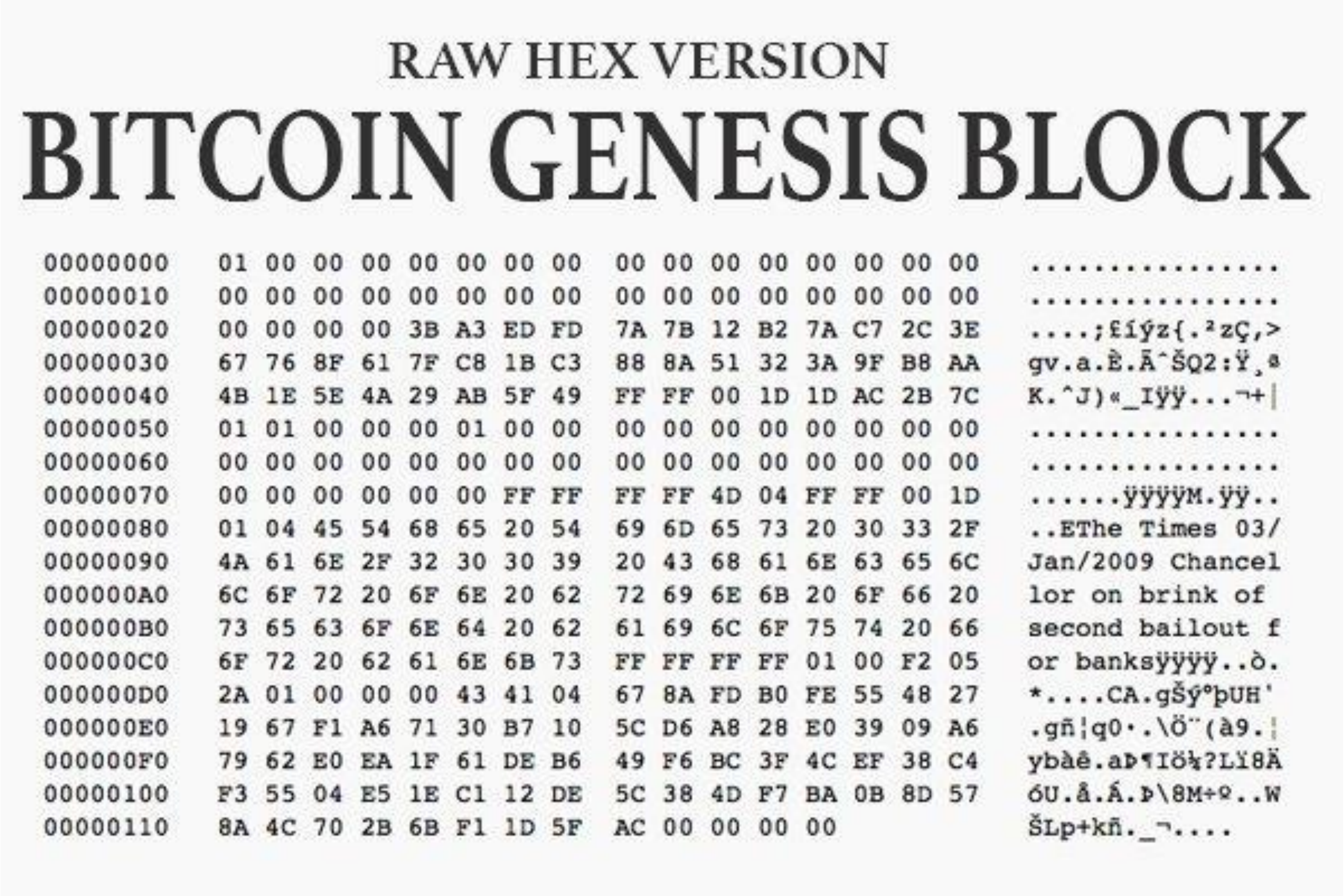
LETS GET OUR HANDS DIRTY

Before we start programming, let's just have a look at the bitcoin genesis block

- Newspaper headline from The guardian on a particular day (don't remember)
- We can always cross reference this, to make sure we don't get an entirely stupid chain

Open up PycharmEdu and open up the course.

- Lets keep this interactive



RAW HEX VERSION

BITCOIN GENESIS BLOCK

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```