THE PHILOSOPHY OF BLOCKCHAINS

A HITCHHIKERS GUIDE

Prassanna Ganesh Ravishankar | The Nomadic Chef | github.com/atemysemicolon | github.com/altran-blockchain

WHO AM I ? (THE BORING STUFF)

- Education
  - BE Electronics and communication from Manipal University
  - Masters in Science in Computer Vision from the University of Sheffield
  - The last couple of years : PhD student in the computer vision centre, Spain in the field of autonomous driving
- Currently : Image Processing consultant working for Altran
  - With HP inc.
  - Working on Image processing problems
  - Providing knowledge base for Machine Learning / Artificial Intelligence
- GOAL : To make the human brain on a silicon chip.

WHO AM I ? (SLIGHTLY MORE INTERESTING STUFF)

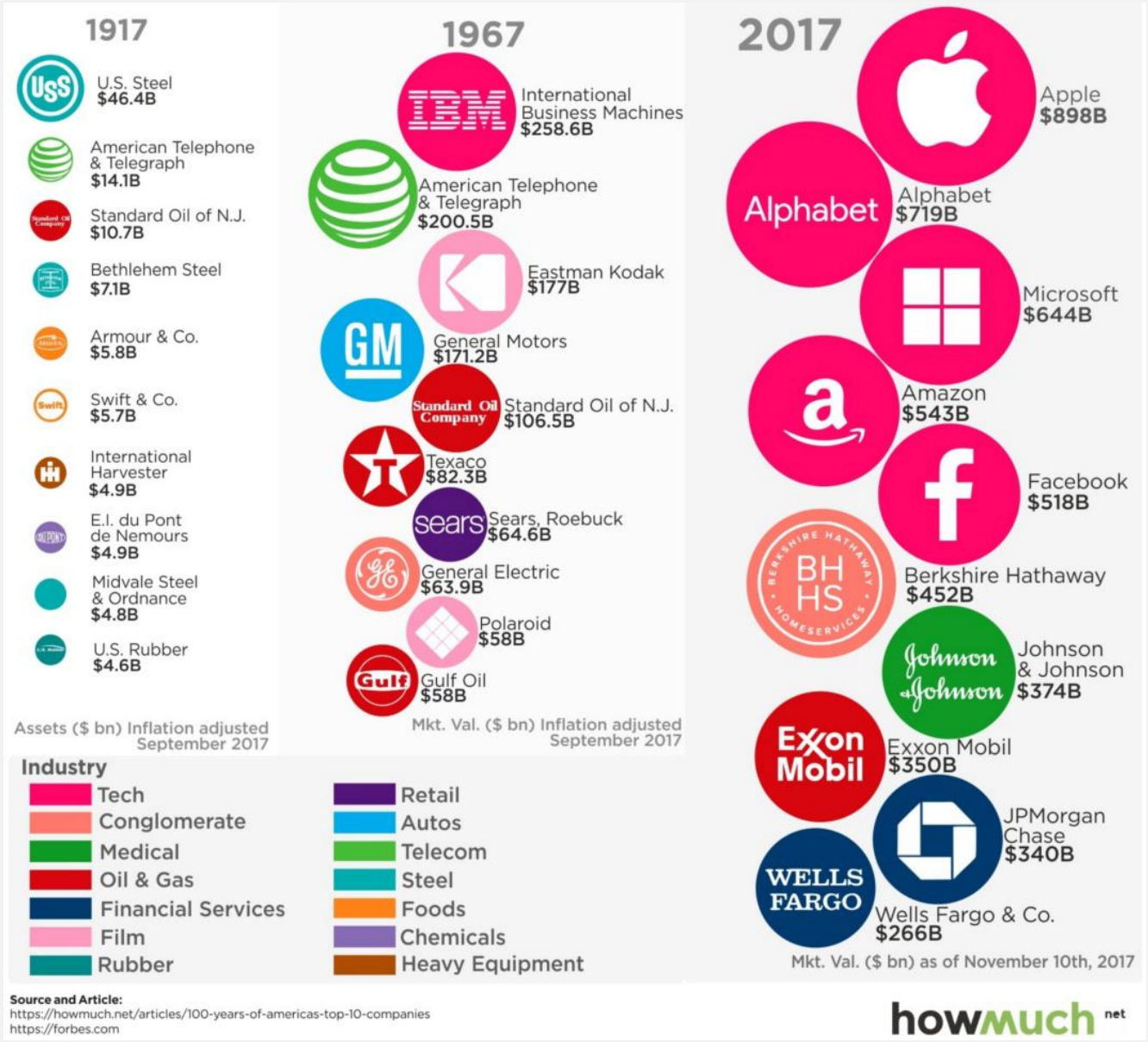
- Primarily - A Programmer by heart
- Age 8-9 : Wrote my first DOS script
- Age 10-11 : Made my first website
- Age 11-12 : National Cyber Olympiad – rank 92, state level 3
- Age 13 - Wrote my first real C++ code
- Fast forward some gaming years
- Web Designer while I entered university, picked up graphic designing
- Got into research in vision algorithms
- Lots of time during my PhD to work on interesting problems.
- Ideals
  - Idealism in life– Most of the time, there's no reason to escape the truth.
  - Internet idealism – The internet offers a level playing field for everyone
  - Crypto Idealist – Firm belief that the socialism that internet offers could provide for "true" capitalism and kick away crony capitalism.

PROLOGUE

- Disclaimer : I have nothing against banks/regulators, but I will point out bottlenecks in the current banking/regulatory system.
- What are we going to cover?
  - A little bit of history
  - A little bit of philosophy
  - A touch of context
  - A lot of concepts
  - A handful of use cases
  - A small warning label
  - An eye on the future
  - Some knowledge of tools to cook ‘em up
  - And hopefully, a bunch of interrupts

THE PRESENT IN THE LIGHT OF THE PAST

- The top 10 companies of the past vs today's top 10


1917
U.S. Steel
$46.4B
American Telephone & Telegraph
$14.1B
Standard Oil of N.J.
$10.7B
Bethlehem Steel
$7.1B
Armour & Co.
$5.8B
Swift & Co.
$5.7B
International Harvester
$4.9B
E.I. du Pont de Nemours
$4.9B
Midvale Steel & Ordnance
$4.8B
U.S. Rubber
$4.6B
Assets ($ bn) Inflation adjusted September 2017
1967
International Business Machines
$258.6B
American Telephone & Telegraph
$200.5B
Eastman Kodak
$177B
General Motors
$171.2B
Standard Oil of N.J.
$106.5B
Texaco
$82.3B
Sears, Roebuck
$64.6B
General Electric
$63.9B
Polaroid
$58B
Gulf Oil
$58B
Mkt. Val. ($ bn) Inflation adjusted September 2017
2017
Apple
$898B
Alphabet
$719B
Microsoft
$644B
Amazon
$543B
Facebook
$518B
Berkshire Hathaway
$452B
Johnson & Johnson
$374B
Exxon Mobil
$350B
JPMorgan Chase
$340B
Wells Fargo & Co.
$266B
Mkt. Val. ($ bn) as of November 10th, 2017
Industry
Tech
Conglomerate
Medical
Oil & Gas
Financial Services
Film
Rubber
Retail
Autos
Telecom
Steel
Foods
Chemicals
Heavy Equipment
Source and Article:
https://howmuch.net/articles/100-years-of-americas-top-10-companies
https://forbes.com
howmuch.net

THE PRESENT IN THE LIGHT OF THE PAST

- The top 10 companies of the past vs today's top 10
- What was done differently?
- What changed?
  - Innovation
  - Technology
  - Interconnectedness – The internet, message boards, social media
  - Speed +++
- **Conclusion** : Need for innovation, need for technology, need for technology innovation to be applied to age old practices and benefit from interconnectedness

AND A LITTLE BIT OF PHILOSOPHY….

- A quick look at humanity from an aliens point of view :-
  - **Interactions**
  - A knowledge base transferred through language
  - Competitive nature
- Do we see this in other animals as well?
  - Bees and ants
- Do we see this in tools and machines we create as well?
  - Emergence! – Moving from unary potential to interaction potential
- Let's just have a broad look at DNA – we will come back to it later

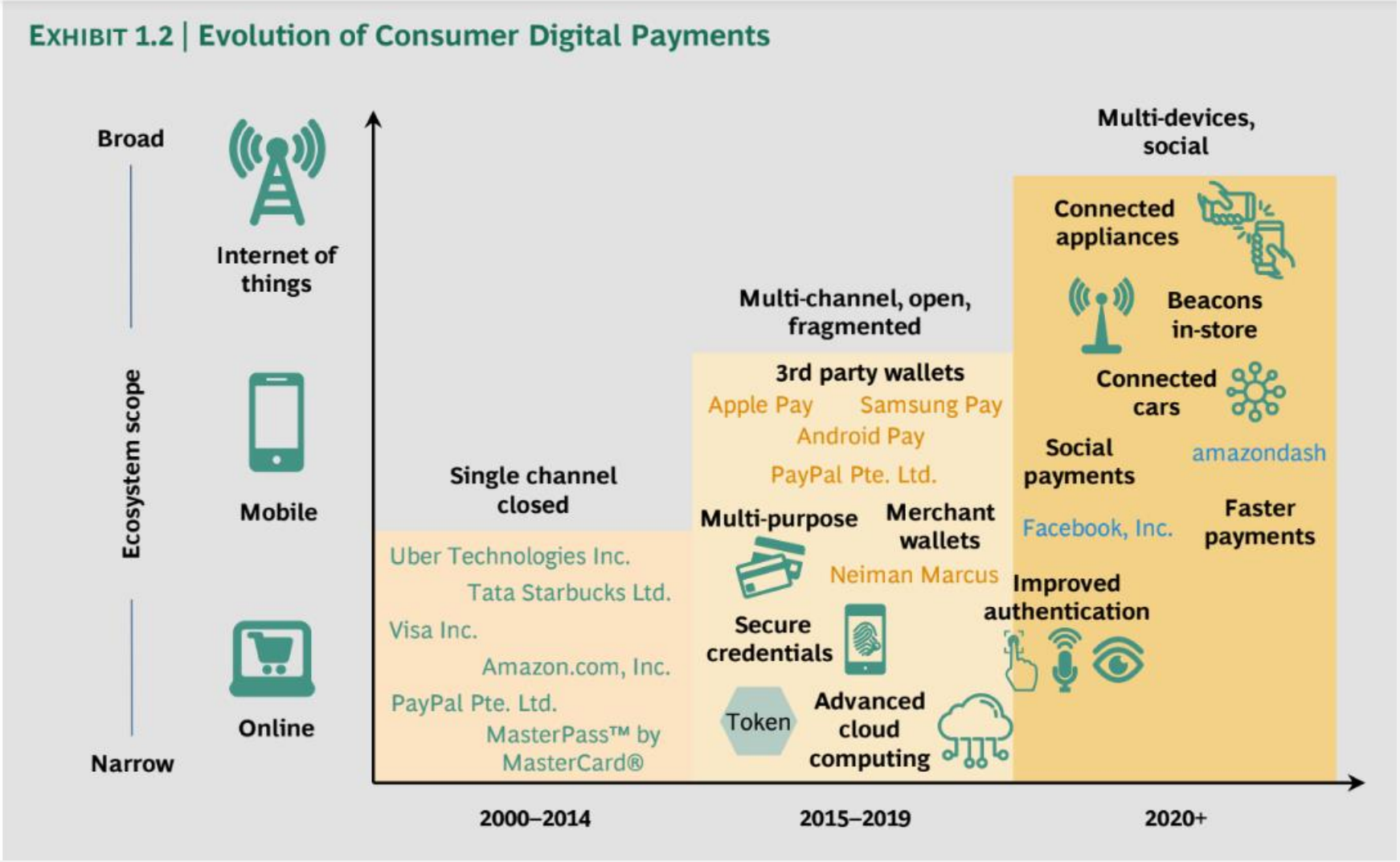
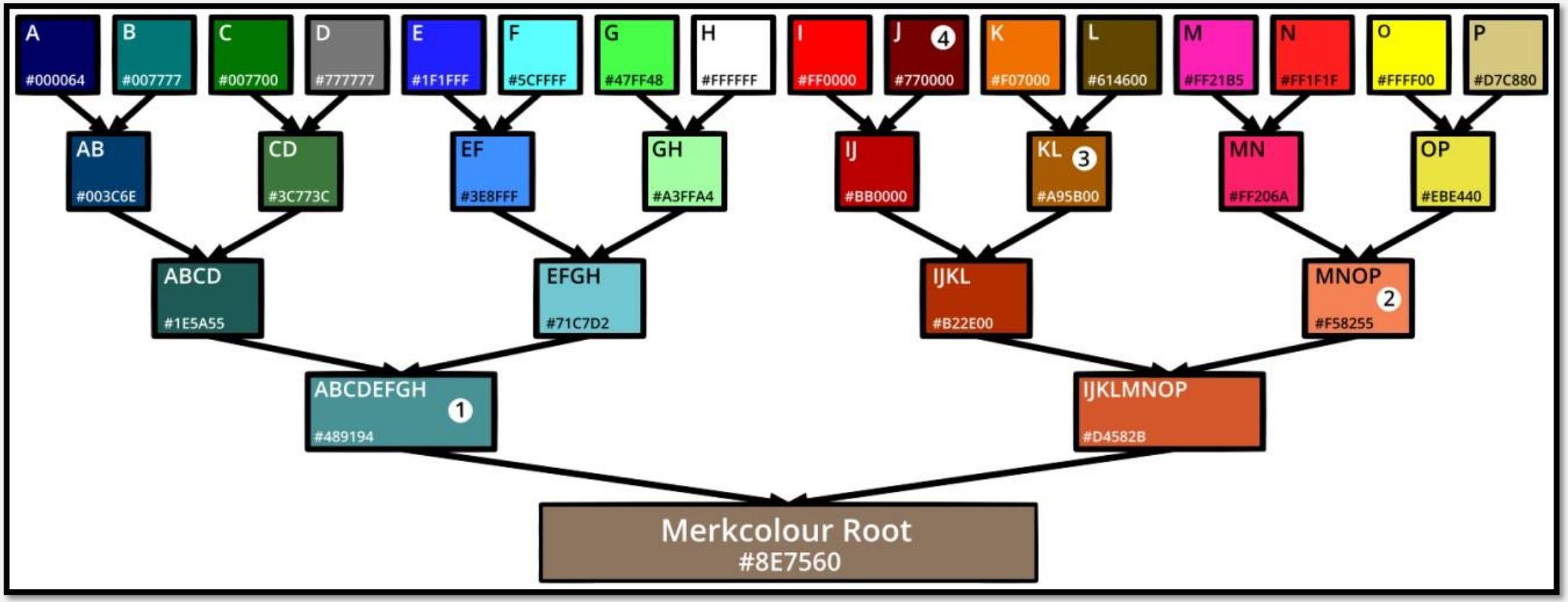


EXHIBIT 1.2 | Evolution of Consumer Digital Payments
Broad
Ecosystem scope
Narrow
Internet of things
Mobile
Online
Multi-devices, social
Connected appliances
Beacons in-store
Connected cars
Social payments
amazondash
Faster payments
Facebook, Inc.
Improved authentication
Multi-channel, open, fragmented
3rd party wallets
Apple Pay
Samsung Pay
Android Pay
PayPal Pte. Ltd.
Multi-purpose
Merchant wallets
Neiman Marcus
Secure credentials
Token
Advanced cloud computing
Single channel closed
Uber Technologies Inc.
Tata Starbucks Ltd.
Visa Inc.
Amazon.com, Inc.
PayPal Pte. Ltd.
MasterPass™ by MasterCard®
2000–2014
2015–2019
2020+

PRE NAKAMOTO

- Broad Context
  - Communication is faster and more affordable (the trajectory of always)
  - More communication > More interaction > More “transactions” > Recurse
  - Moving towards decentralization - The existence of git and wikis (torrents/p2p)
  - Who pays for your data (Facebook/google/MS)
  - Currency – The perfect proof-of-concept
  - Is the internet really decentralized? The realization of the dream of the internet
- Technical context Context
  - Underlying ip layer moved to ipv6 (more node capacity)
  - HD transfer speeds and internet speeds increased
  - Merkel trees everywhere

MERKEL TREES IN ONE PHRASE
CHANGE ONE COLOR AND EVERYTHING CHANGES



WHY FINANCIAL INSTITUTIONS?

- Internet commerce rely on financial institutions
  - Serve as trusted third party to process transactions
- Completely non-reversible transactions not really possible
  - Job of financial institutions is to mediate disputes
- Cost of mediation increases transaction costs
- Limits minimum practical transaction cost
- With possibility of reversal, need for trust spreads
- Certain percentage of fraud unavoidable.
  - Risk gets factored into the transaction cost
- Can be avoided using physical currency
  - No mechanism to avoid trusted party over a communication channel (pre-bitcoin)

SATOSHI'S VISION
ORIGINS OF BITCOIN

- Cryptographic proof instead of trust
- Therefore, no need for trusted third party
- Computationally impractical to reverse transactions
  - Protect sellers from fraud
  - Escrow mechanisms could be implemented to protect buyers
- However, need some verification method
  - Beat the double spending problem
  - Enter blockchains
- System is honest as long as 50% + is with honest nodes

Note: Satoshi is also the smallest unit of BitCoin

NAKAMOTO'S LEDGER

- Nakamoto said – Let there be a ledger! (a ledger a book maintained by a bank in 1800s or a mafia don describing all transactions made)
- Who can write into pages of the ledger
  - Anyone, but before I write, I ask my friends if I am correct.
- Who can collect a lot of pages and make a book
  - Anyone again, but the first one to do it is accepted
- Where can I place the book?
  - A place on the shelf that follows "certain" rules
- How do I prevent the anyone from adding rubbish into the book?
  - Make it difficult to write, but easy to read (prove to me that you did enough work to place the book)
- How do I know the order of books?
  - Every book starts with the index of the previous book

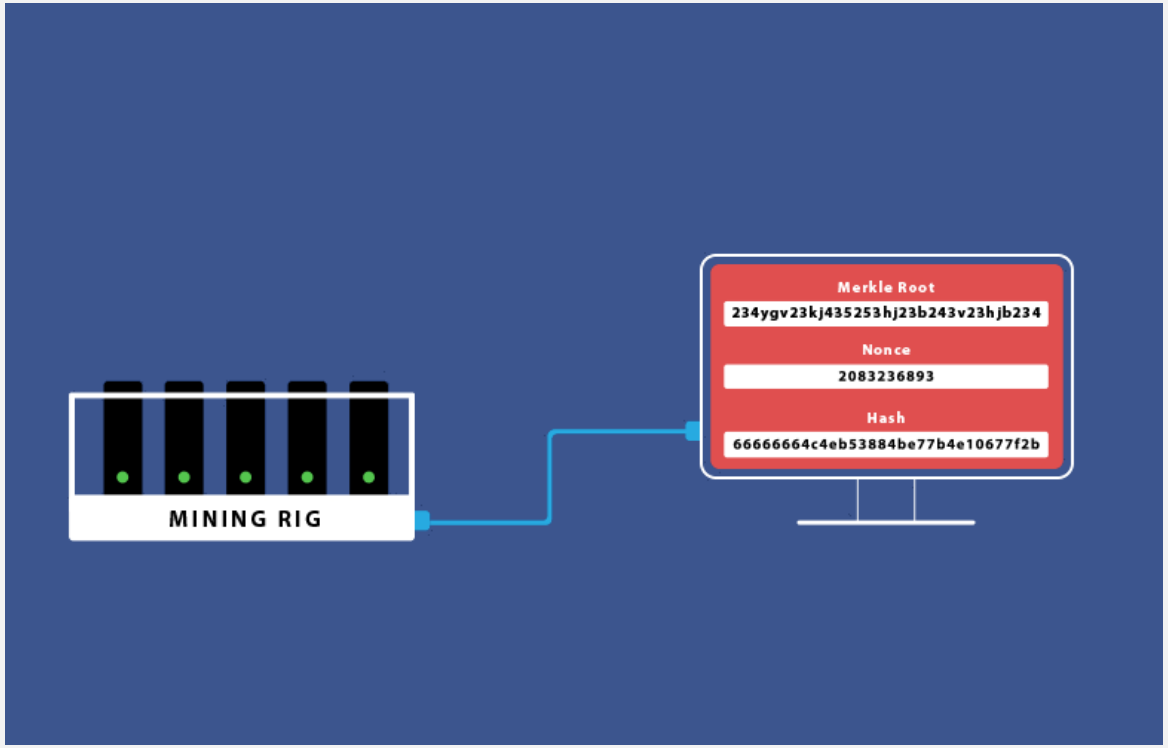
FROM BOOKS TO CHAINS

- This new ledger is our blockchain
- Who can make transactions?
  - Verification : The process of the network accepting a transaction. The nodes have to agree
- Who can combine these transactions, into a **block**?
  - Mining : The process of the collecting transactions. A group of transactions (1M) is a block.
- How I make a block immutable?
  - Proof of work : Prove to the blockchain that sufficient work was done (solve a hard cryptographic problem)
- How do I know the order of books?
  - Link the hash : Each block points to the hash of the previous block. (make a chain!)
  - Also used for verifying if you have the right chain of blocks

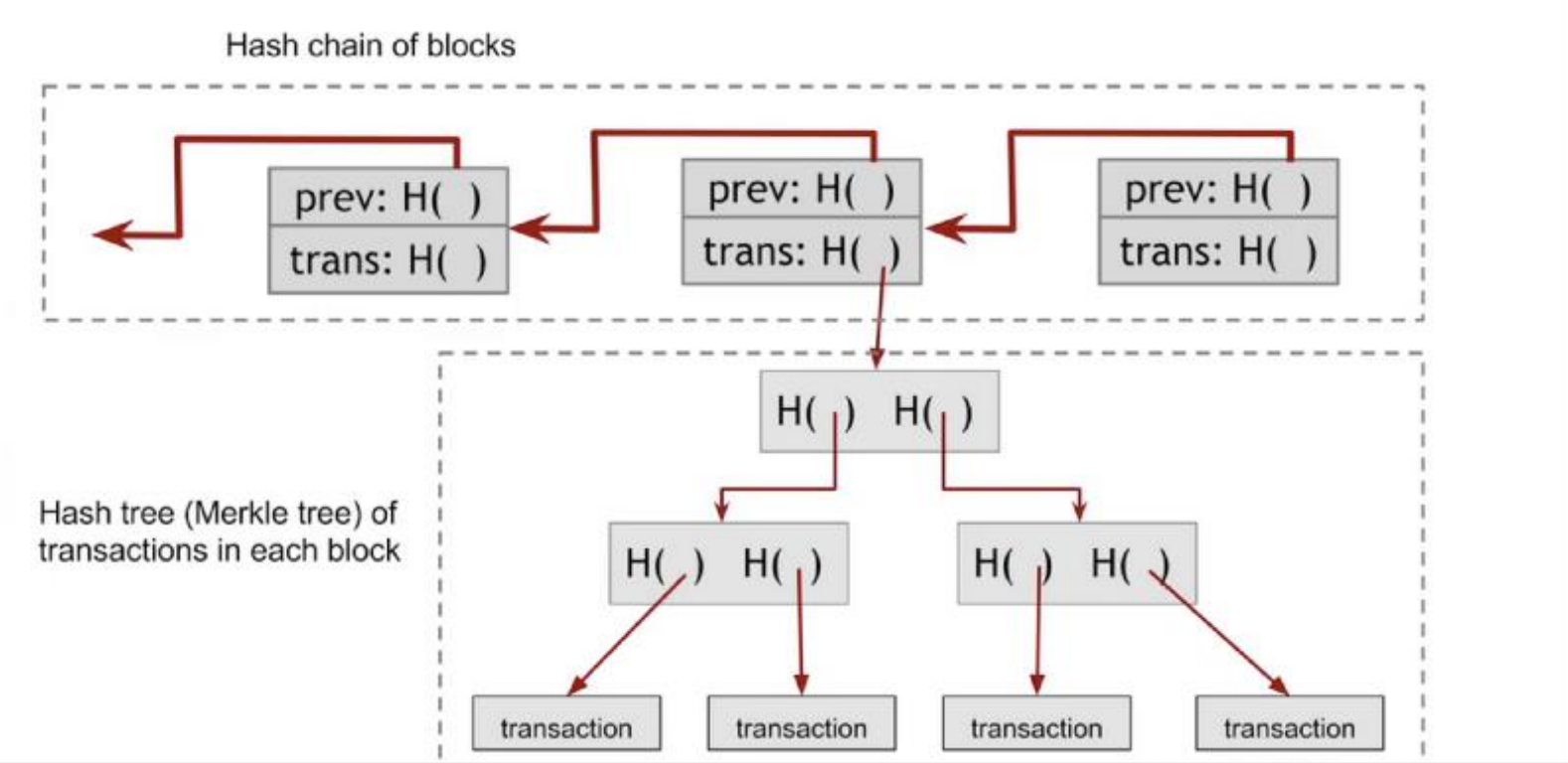
BEAUTY LIES IN THE DETAILS

- Double Spending problem?
  - Solution : TimeStamps
- Why is it called a chain?
  - It's a linked list that of the hash "pointers" point to the previous block
- Who choses the transactions to mine?
  - Verified (by the nodes in the network) transactions are added to the pool
- HASHCASH
  - The concept of nonce and leading zeros
  - The "difficulty"
  - The resultant hash
  - Tries to solve : Immutability of a block and of the chain
- Wallets are just collections of key
  - Give you power to spend, you don't really care about power to receive

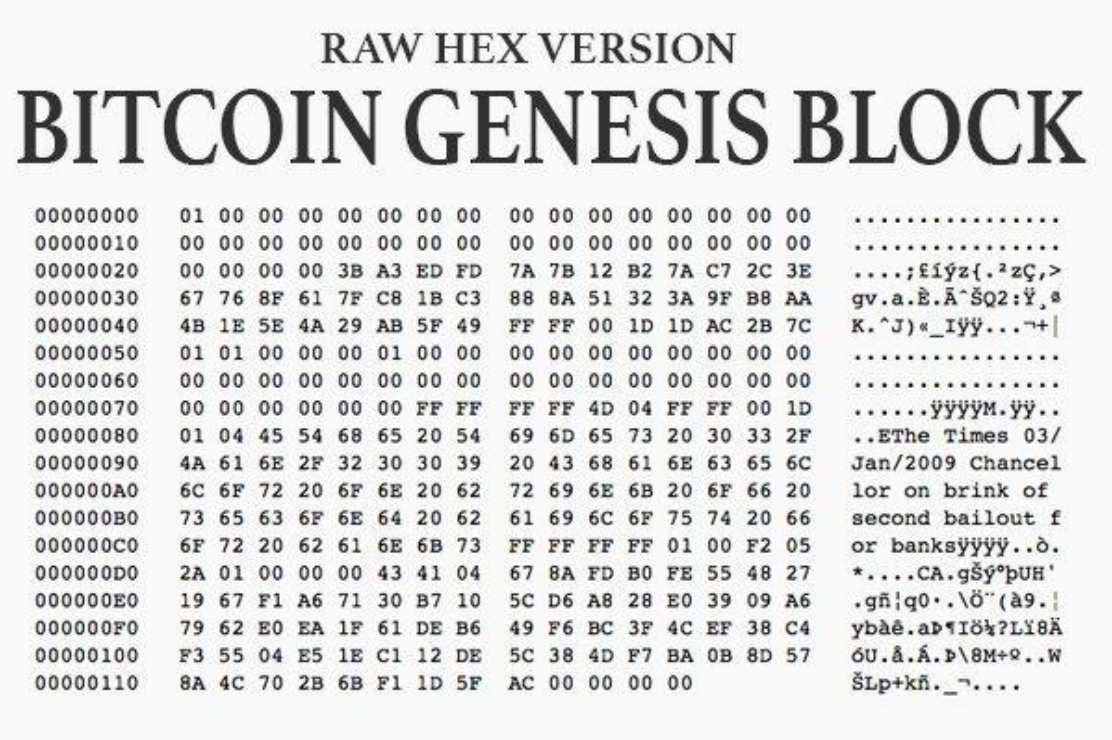
PROOF OF WORK



BITCOIN BLOCK STRUCTURE



REFERENCING THE CREATION

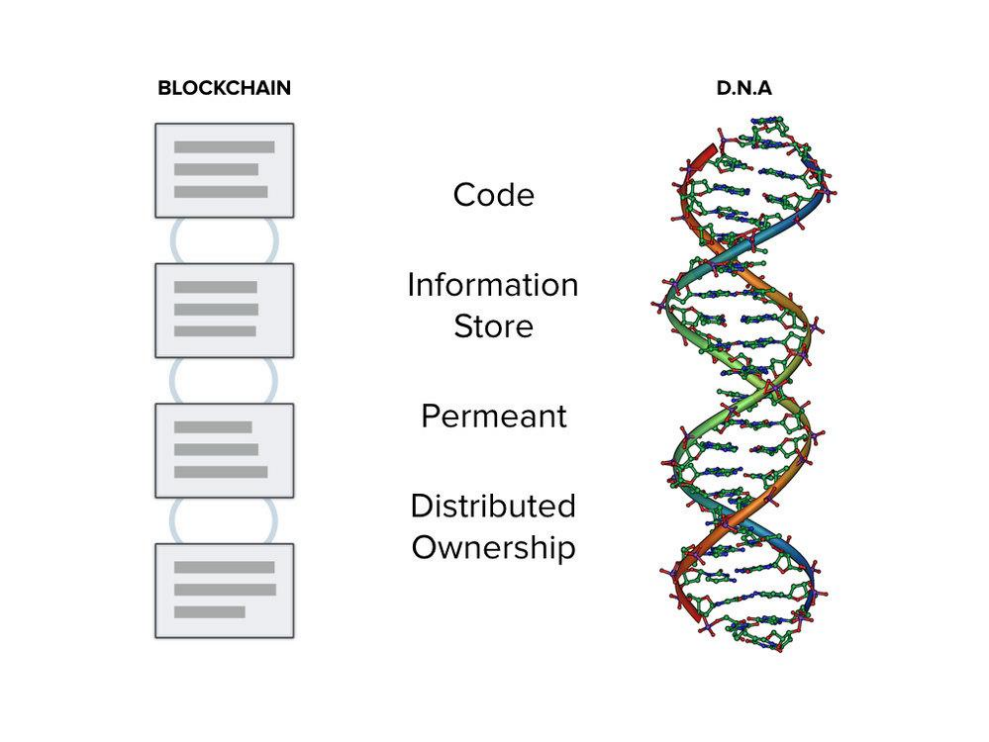


RAW HEX VERSION

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._¬....
```

WHY DID I MENTION DNA EARLIER?



THE ECOSYSTEM

- Reward/Incentive for participation
  - Mining
  - You need a reward to make sure people are paid for their “compute” time
- Value of the Bitcoin :-
  - Does the US Dollar have an inherent value?
  - Who determines the value of a currency – the market!
  - The real value of bitcoin lies in the cost of mining
- Forking
  - The birth of a blockchain (BCH vs BTC)
- Time to think
  - Can I only upload transactions into a block? Or can I add arbitrary code?
  - Mining would then mean executing this code.

ENOUGH OF CURRENCIES

- Execute code on the cloud – Azure/AWS or something different?
  - What if you want anyone to interact with your code?
  - What if you don't want to worry about the security of your servers?
  - Enter : Smart Contracts - Ethereum
- Smart contracts have their issues too! (example Ethereum)
  - I'm a miner. I don't want to run infinite code on my machine
  - Hence the concept of Gas : Each contract is triggered with some ether, which limits the amount of compute cycles per transaction
- Unforseen advantage – can't have special purpose hardware for this kind of mining.

HOLD ON!

- Blockchains lack a bunch of things
- They're suitable for organic crowdsourced applications, not everything in this universe
- Can Blockchains be :-
  - Fast? (Have to wait till a block is built)
  - Cheap to maintain? (Cost - Money+Energy+Storage)
  - Cheap to grow a chain? (Cost - Money+Energy)
- If you have a service/product that is well designed for the client-server model – skip blockchains
  - Example of blockchain done wrong– 4new
- If you have a service that's perfect for anyone to interact with, and roles between the server and the client are blurred - then go for blockchains 100%
  - Example of blockchain done right - WePower

EH. MAYBE IT'S NOT ALL THAT BAD

"The Bitcoin network takes up as much energy as the entire country of Denmark"

- Lightning network to take known verifiable load off the general network
- Proof of stake – to go from everyone mining, to stakeholders mining
- The hybrid model – proof of work vs proof of stake
- Enterprise blockchains – Consensus and permissioned
- dApps – Distributed apps which work on a smart contract protocol
- Tokens – if a code can live on the blockchain, this code can represent a new currency on top of it's platform (Ethereum gives birth to multiple application tokens – like shares in company)
- How can my new "token" company be funded to perform some application? ICOs

LOOKING AHEAD

- The new web
  - What else can we do? (IOT)
- Finance (already happening)
  - How about taking fiat currencies on the blockchain?
- Smart Contracts on property
  - Less potential for banks to cheat you
  - Don't need a bank, for a loan, can be crowdfunded
- Identity
  - Secure your identity on a blockchain
- HealthCare data
  - Estonia
- Businesses
  - Handle Mergers/Transfers
  - Handle Employee identity
  - **HERMES**
- Supply Chains
  - ShipChain
  - SmartAppliances and supply chain sensors
- Decentralized Organizations
  - DAO
- Governments
  - Voting, and a new system of participation

ENOUGH. GET ME STARTED

- Altran Blockchain – github.com/Altran-blockchain
- Development:-
  - Ethereum (or Neo/Cardano/Ark)
    - Remix – An online solidity compiler
    - Tuffle + Ganache + Geth
    - Truffle's pet shop tutorial
    - Metamask extension / Mist browser
  - Enterprise blockchains – IBM's hyperledger (permissioned consensus based mechanism – lighter)
- Learning More :-
  - ICOs – WhitePapers – look for decentralized applications
  - Coindesk
  - Google anything with "<insert distributed idea here> blockchain"

THAT'S ALL FOLKS

- Q & A