# Blockchain & Distributed Ledgers

CorkSec, 2018-04-10

Johannes Ahlmann, CTO @ iLen

johannes.Ahlmann@ilen.io

iLen

iLen.io

# Agenda

1) High-Level Overview

2) Deep Dive

images:
https://www.biggerpockets.com/renewsblog/2014/07/18/high-level-overview-literally-30-unique-real-estate-markets-around-world/
https://codeburst.io/deep-dive-into-electrons-main-and-renderer-processes-7a9599d5c9e2

# 1) High Level Overview

images:
https://www.biggerpockets.com/renewsblog/2014/07/18/high-level-overview-literally-30-unique-real-estate-markets-around-world/

# When we interact/transact with others, we often delegate **Trust** to **Intermediaries**

producer, provider, seller, lender

consumer, recipient, buyer, borrower

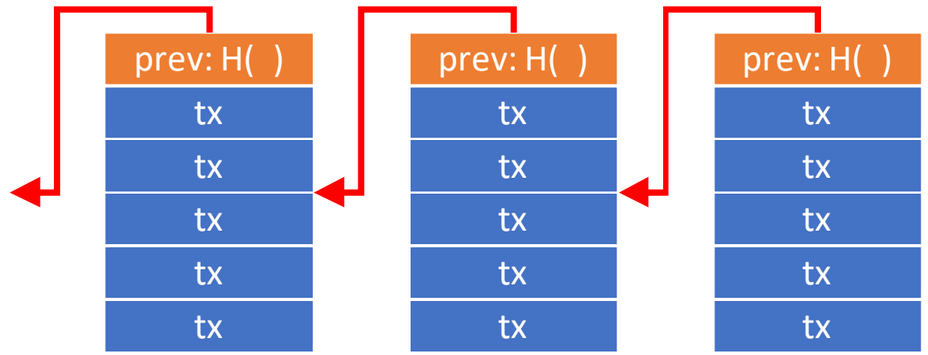
# If we had a trusted **Shared Ledger** many of those Intermediaries would no longer be necessary

1. Shared, distributed **Ledger**
2. Immediate **Consensus** on "State of the World"
3. **Tamper-Proof**
4. **Public**,
   anyone can access, validate
5. **Transactions** change the state

sources:
https://commons.wikimedia.org/wiki/File:Server-based-network.svg
http://www.gjermundbjaanes.com/img/posts/distributed_ledger.png

# How can we achieve a shared, trusted Ledger **without Trust between Parties**?

- Block = List of Transactions
- Blockchain = Chain of Blocks
  - Tamper-Proof
- Consensus (PoW)
  - Miners expend energy to find hash puzzle solution
  - Other nodes accept block if it is valid
- Trustless
  - Nodes assumed to be untrusted
  - Fair Lottery, Cryptography ensure that no one can cheat




source: https://medium.com/@brettking/abc61b2ab49a

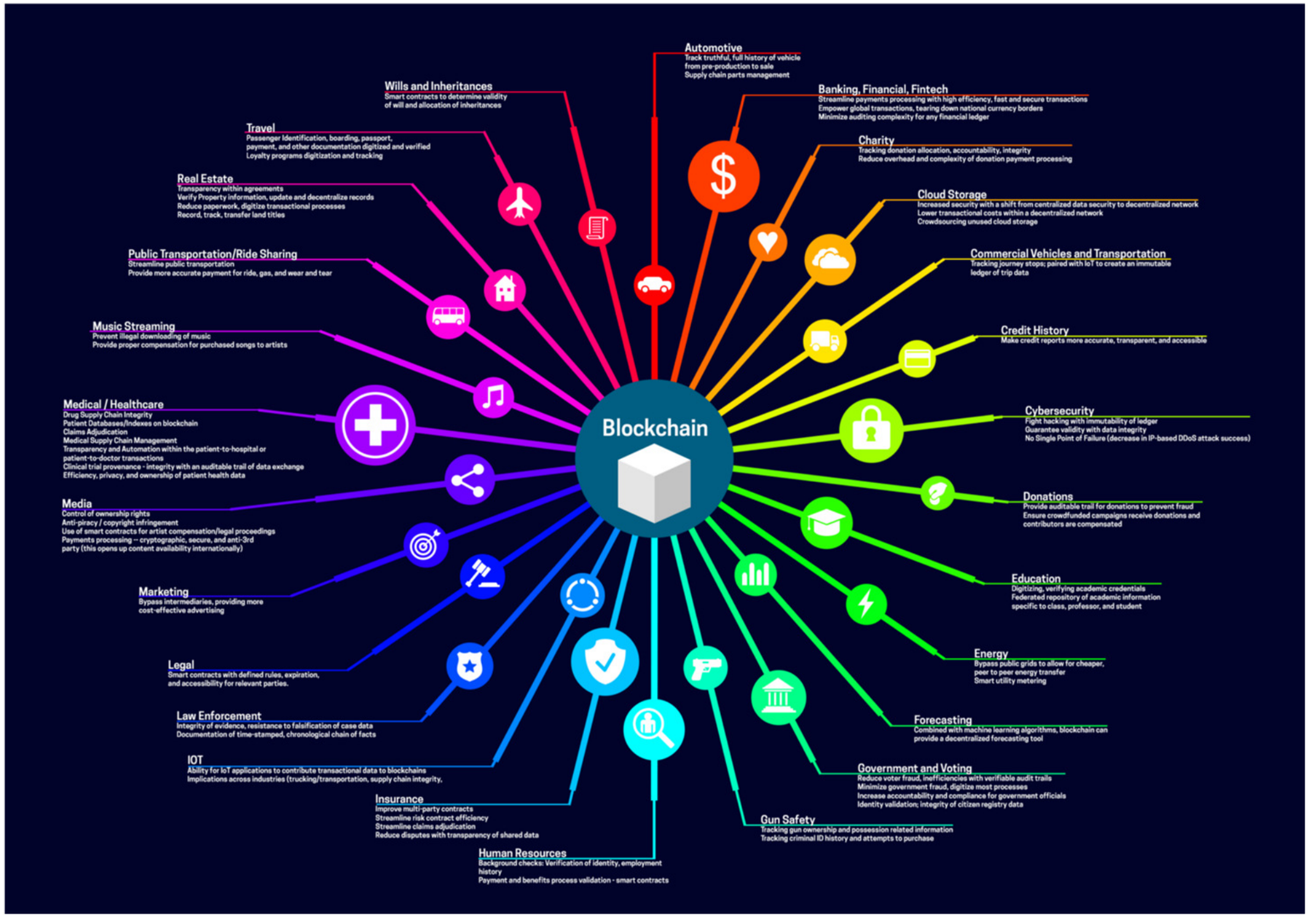
# A **Consortium Blockchain** can address some Challenges Companies may find with Public Blockchains

- Group of known, semi-trusted parties
- Access granted by members
- Consensus ~ majority vote (BFT)
- Consensus can withstand 1/3 of malicious nodes
- Easier Governance

| Public | Consortium |
|---|---|
| Data is Public | Privacy, Confidentiality |
| Transactions are Public | Private Channels |
| Pseudonymous | Known participants |
| Anyone can join | Permissioned |
| Anyone can access | Permissioned |
| Trustless Nodes | Semi-Trusted Nodes |
| Low tx/s | High tx/s |
| | GDPR Compliance |

# What are some of the Blockchain **Use Cases** for Companies?

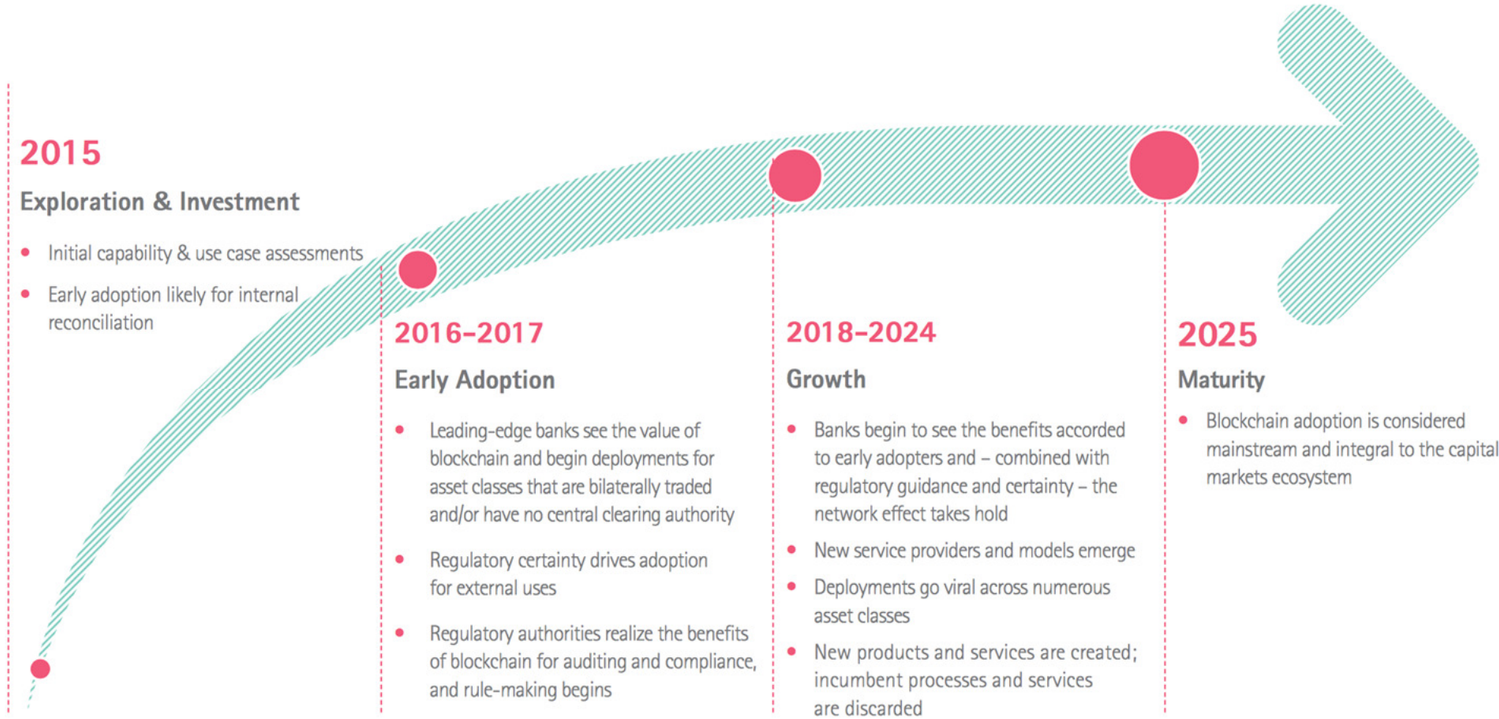
- Data Exchange between multiple parties
- End-to-End Supply Chain Transparency
- Product Traceability
- Marketplaces, Trading
- Clearance & Settlement
- Public Registries




source: https://medium.com/fluree/blockchain-for-2618-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99

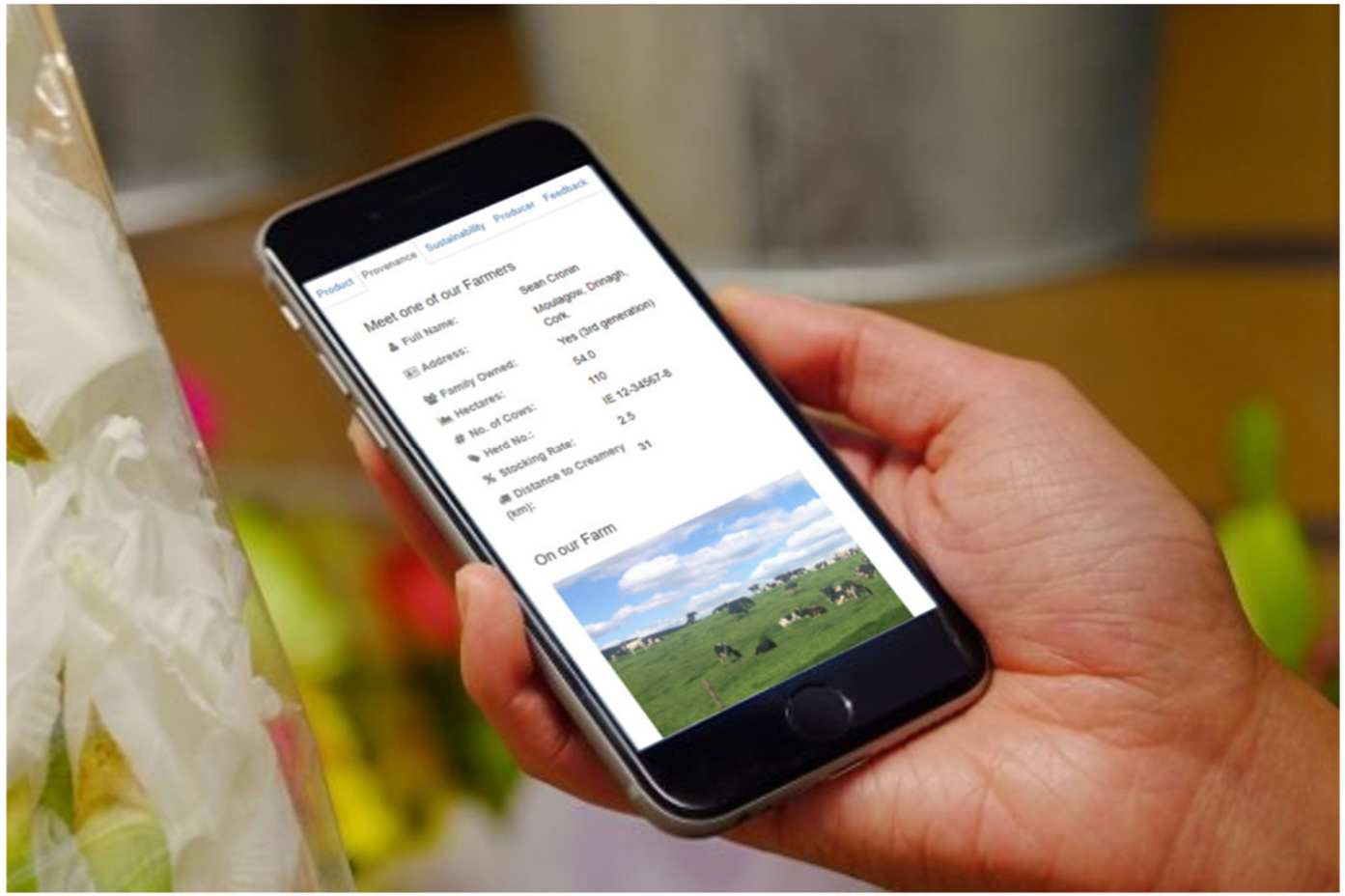
# There is large interest in Blockchain **Adoption**, with many projects underway

| | |
|---|---|
| Maersk | cargo tracking |
| Port of Antwerp | container handling |
| Walmart | supply chain transparency |
| Airbus | jet plane parts tracking |
| UPS | supply chain transparency |
| FedEx | customer dispute resolution |
| Australian Securities Exchange | clearance & settlement |
| Credit Suisse | syndicated loans |
| Dubai Land Dept. | land registry |




Source: Accenture Research

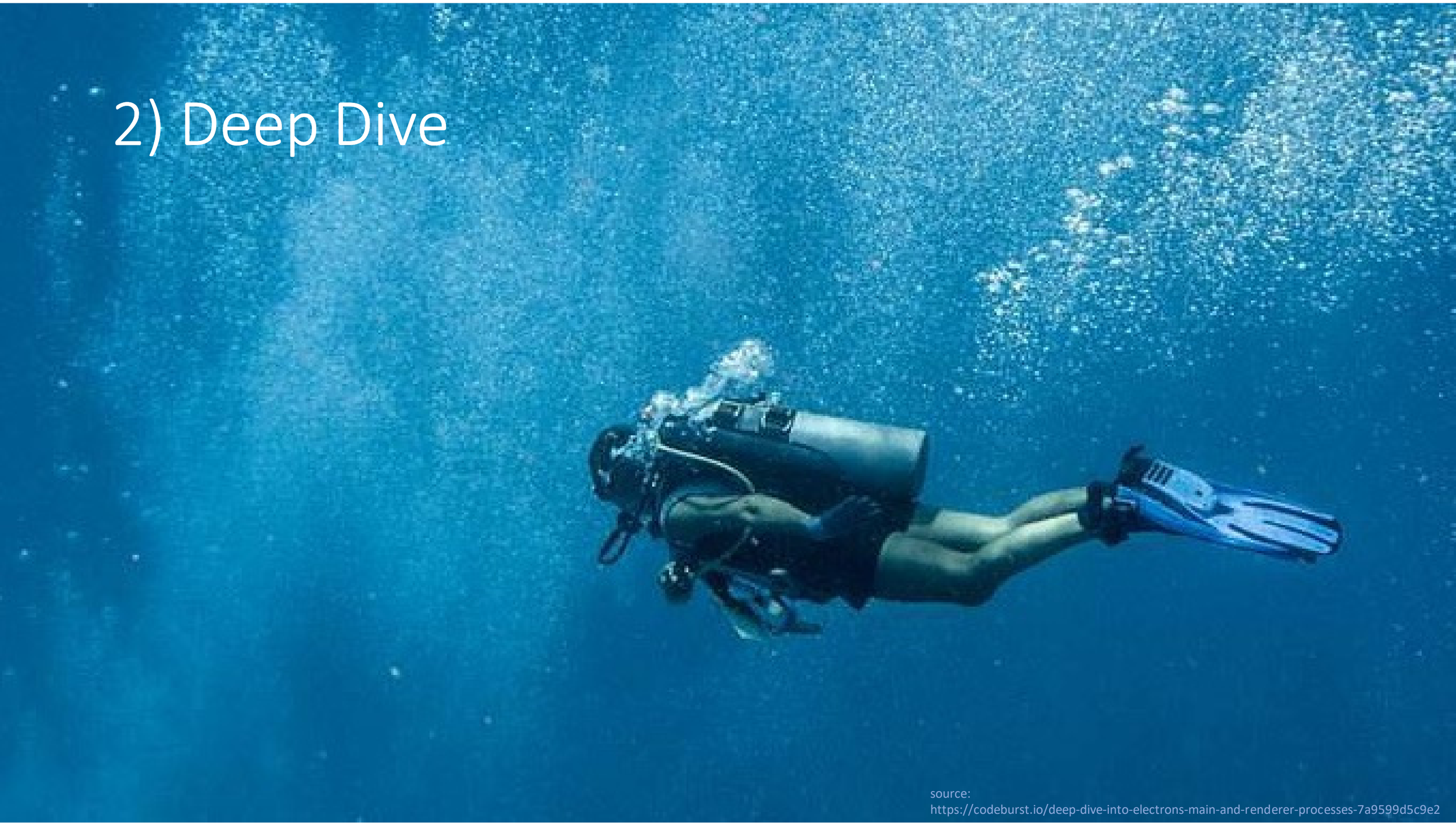
# iLen is bringing **Traceability** to the Irish **Dairy** Sector




iLen

iLen.io

# 2) Deep Dive



source:
https://codeburst.io/deep-dive-into-electrons-main-and-renderer-processes-7a9599d5c9e2

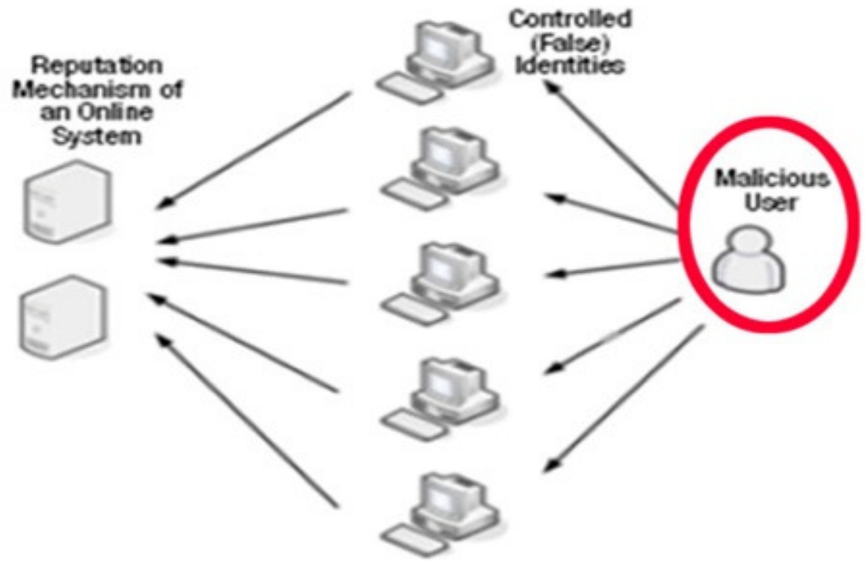
# Overview

1. Why so complicated?
2. Keys, Addresses
3. Transactions
4. Blocks
5. Consensus, Mining


https://melbournepsychooncology.com.au/overview/

# Why so complicated?

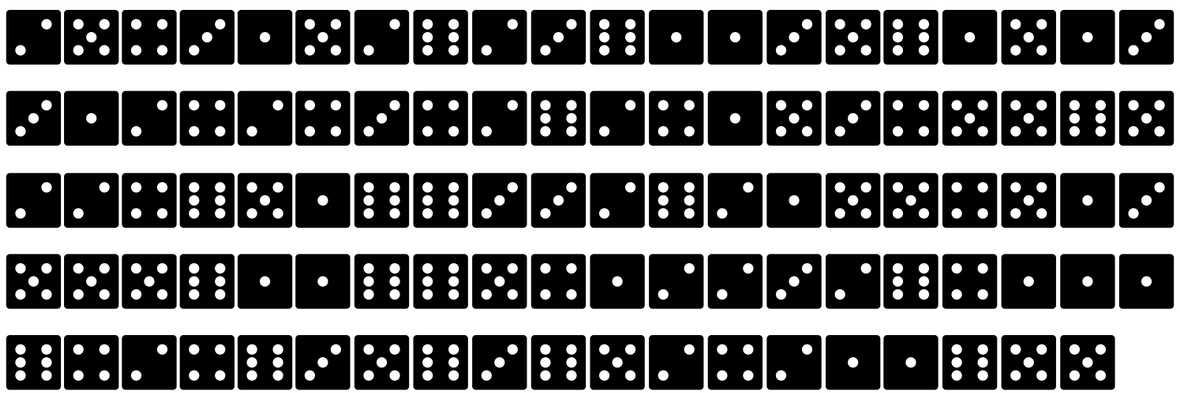
- Distributed Systems are Hard
  - Consensus of Equal Peers
  - Malicious Actors suck!
- Trustlessness
  - No Privileged Nodes to ask!
- Challenges
  - Sybil Attack
  - Double Spend Attack
  - 51% Attack
- Bitcoin Whitepaper:
  - Economic Incentive, Game Theory



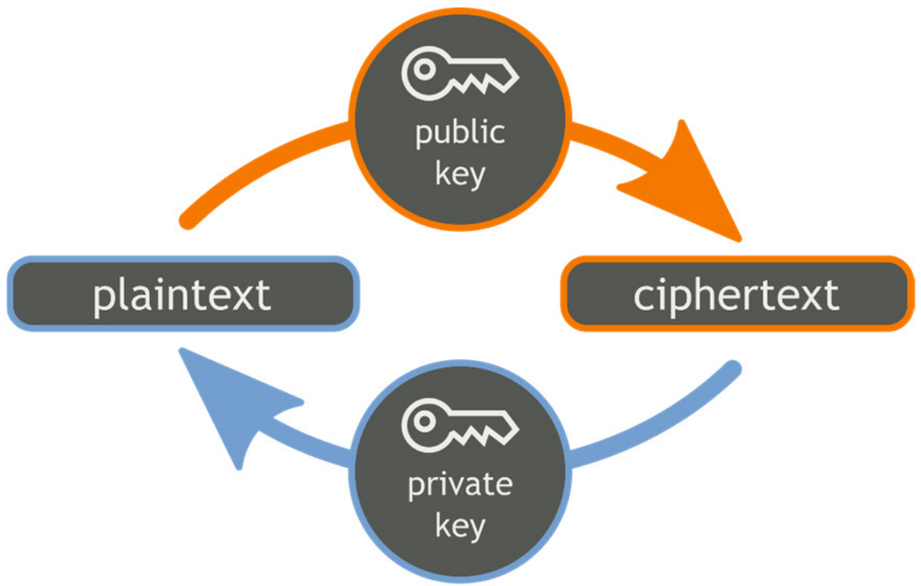

https://www.123rf.com/photo_45705087_genius-aged-teacher-explains-a-complicated-lesson.html
http://ablogaboutnothinginparticular.com/?p=3734

# Keys, Addresses, Wallets

- ECDSA
  - Generate Private Key
  - Private Key => Public Key
  - Public Key => Address
- Key Generation (via casino dice ;)



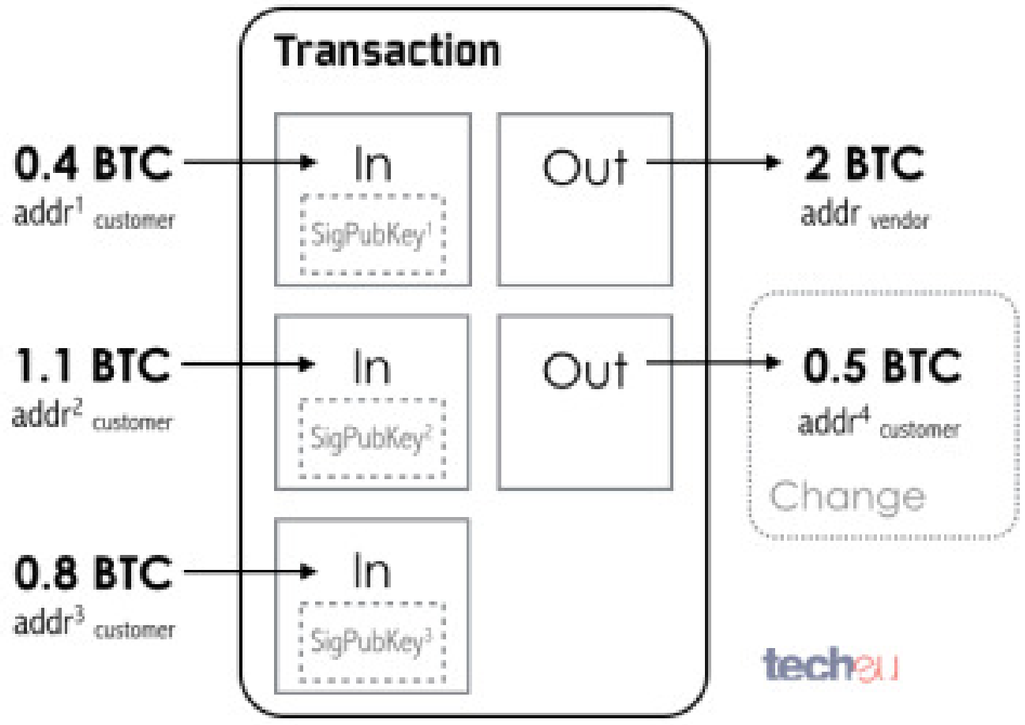
- Wallet




https://commons.wikimedia.org/wiki/File:Orange_blue_public_key_cryptography_en.svg

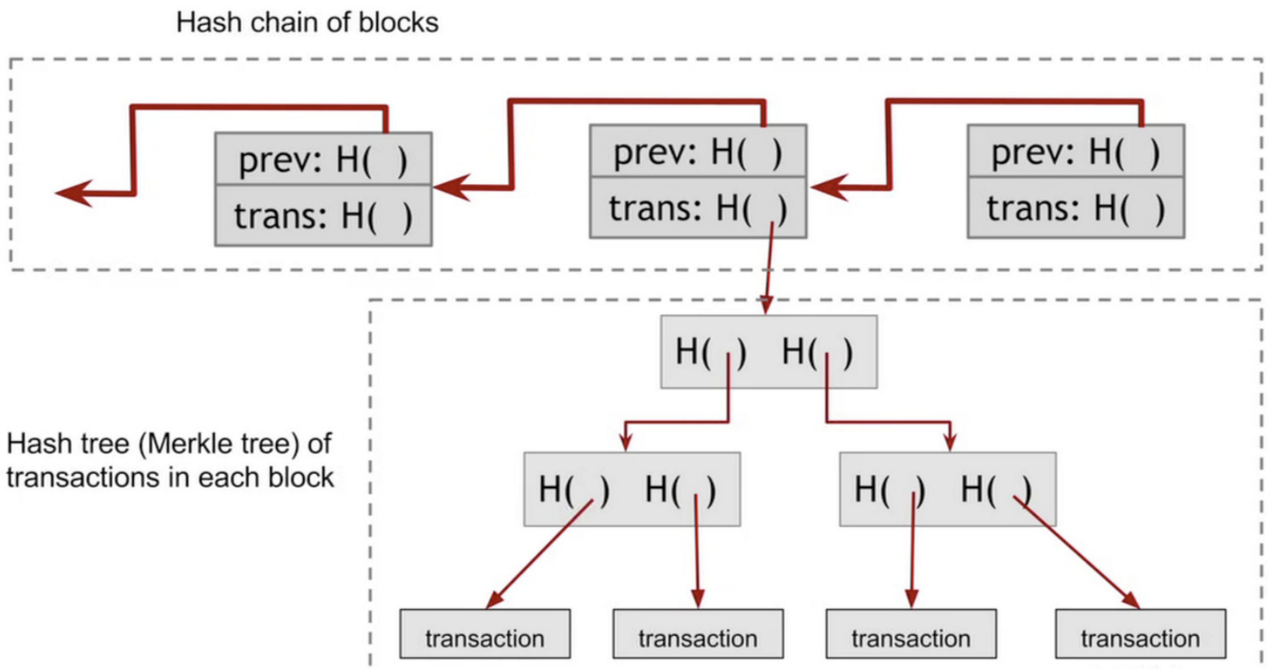
# Transactions

- Unspent Transaction Outputs (UTXO)
- Multiple inputs/outputs
- Inputs
  - Completely consumed
  - Signatures matching address
- Outputs
  - Change Address for excess amount
  - Inputs - Outputs = Implicit Mining Fee



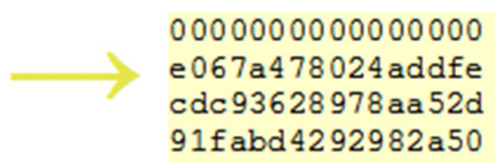

Note: Inputs should be > outputs, and signature is using PrivKey ;)
http://tech.eu/features/808/bitcoin-part-one/

# Blocks




| | |
|---|---|
| version | 02000000 |
| previous block hash (reversed) | 17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000 |
| Merkle root (reversed) | 8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787 |
| timestamp | 358b0553 |
| bits | 535f0119 |
| nonce | 48750833 |
| transaction count | 63 |
| coinbase transaction | |
| transaction | |
| ... | |

Block hash




images:
http://learningspot.altervista.org/bitcoin-blocks/
http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

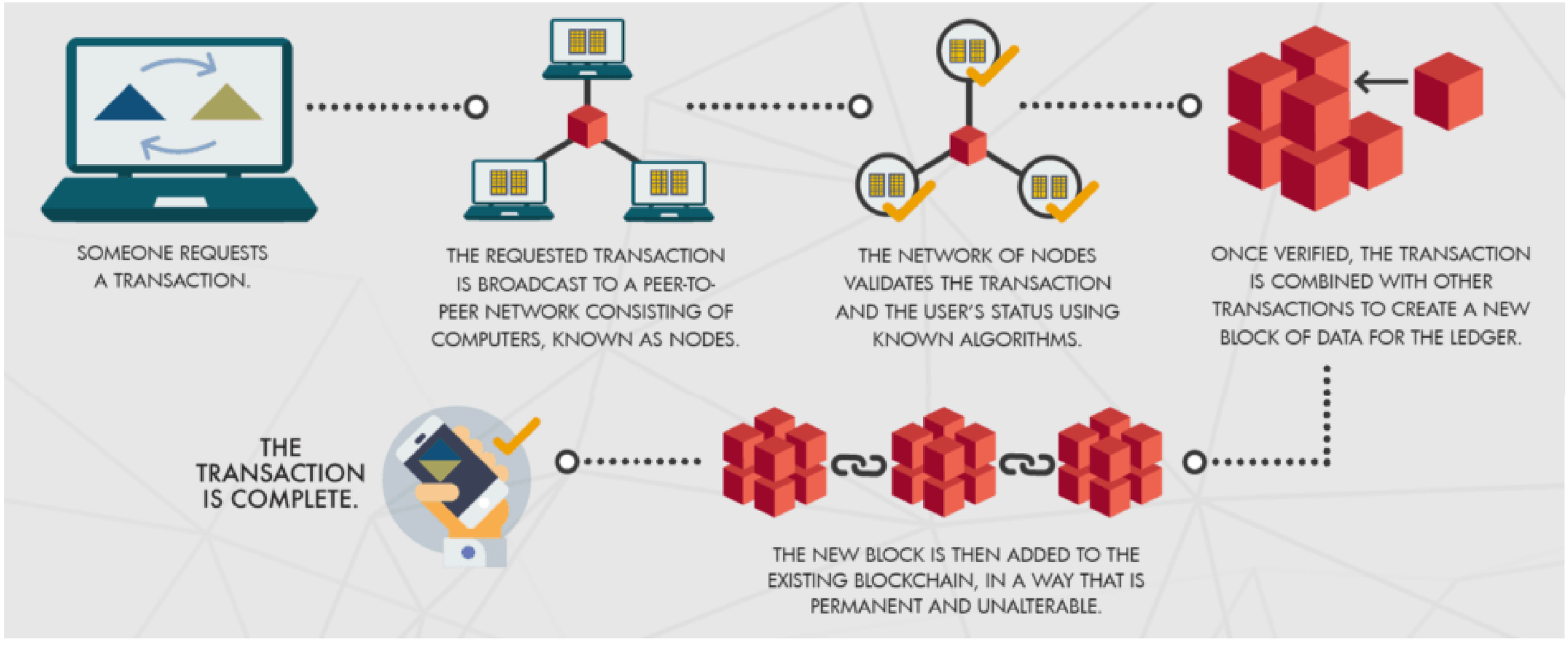
# Mining, Hash Puzzle

- Hash Puzzle: Find Nonce,
  so that Block Hash < Diff. Threshold

  i.e. starting with 0x000000000004
- Race to find solution to Hash Puzzle
- Fair Lottery ~ Node Hashrate
  - Currently total: 25,000,000 TH/s
- Block Reward = 12.5 BTC ~ $85,000
- "Race Condition": Two blocks found within short time
  - Longest Chain wins
  - Wait 6 Confirmations (1h) to be sure

source: https://medium.com/@brettking/abc61b2ab49a

# A day in the life of a Blockchain **Transaction**




source: https://www.burniegroup.com/infographic-a-look-at-blockchain-technology/

# Do you want to know more?

- Meetup: Cork Blockchain
- Slides, Material on corkblockchain.com
- Upcoming "Blockchain in Practice" Event at UCC June 19th => ilen.io
- Good MOOCs
  - Coursera (Bitcoin and Cryptocurrency Technologies)
  - University of Nicosia (DFIN-511 Introduction to Digital Currencies)
    - Also offer MSc Digital Currencies
  - More Courses

# Resources

- Blockchain Explorer - https://blockchain.info/
- Key Generation Toy - https://www.bitaddress.org
  - (obviously don't use a website for real keys)
- Interactive Demo - https://blockchaindemo.io/
  - Another One from Bloomberg
- Bitcoin Hashpower and Difficulty Chart
- Bitcoin Energy Consumption
  - bitcoin ~ 6GW (depending on exchange rate)
  - 1 nuclear power plant ~ 1GW

# Thank you,
# any questions?