# Blockchains and Smart Contracts - marvel, maybe or meh?

**Lee Thomas**

# Contents…

- What is a blockchain?

**Block chain**

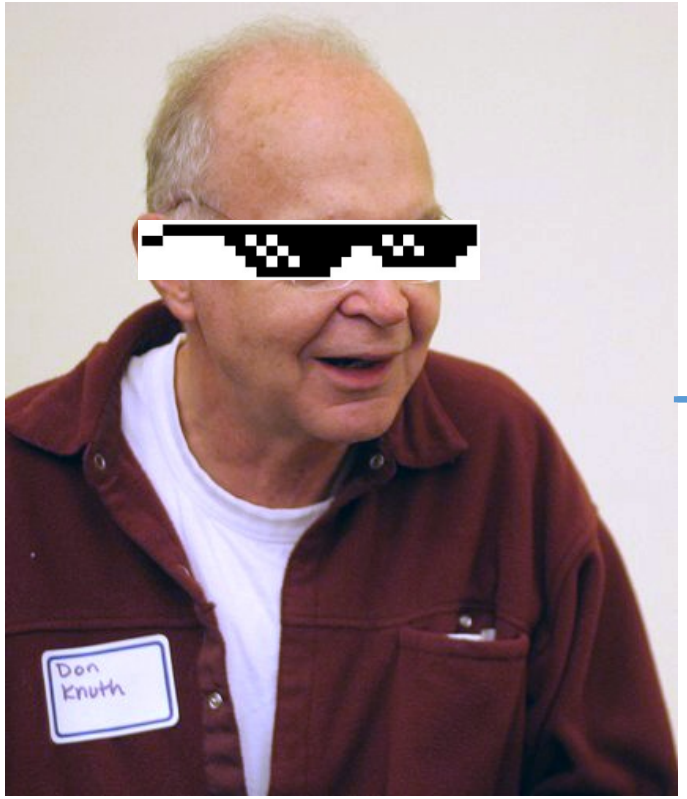
Agreed data structure with agreed rules for change

Versions linked with cryptographic hash function

- **Why….** Smart Contracts
- Classification of blockchain protocols
- Applied to P2P energy trading

# Cryptographic hash function

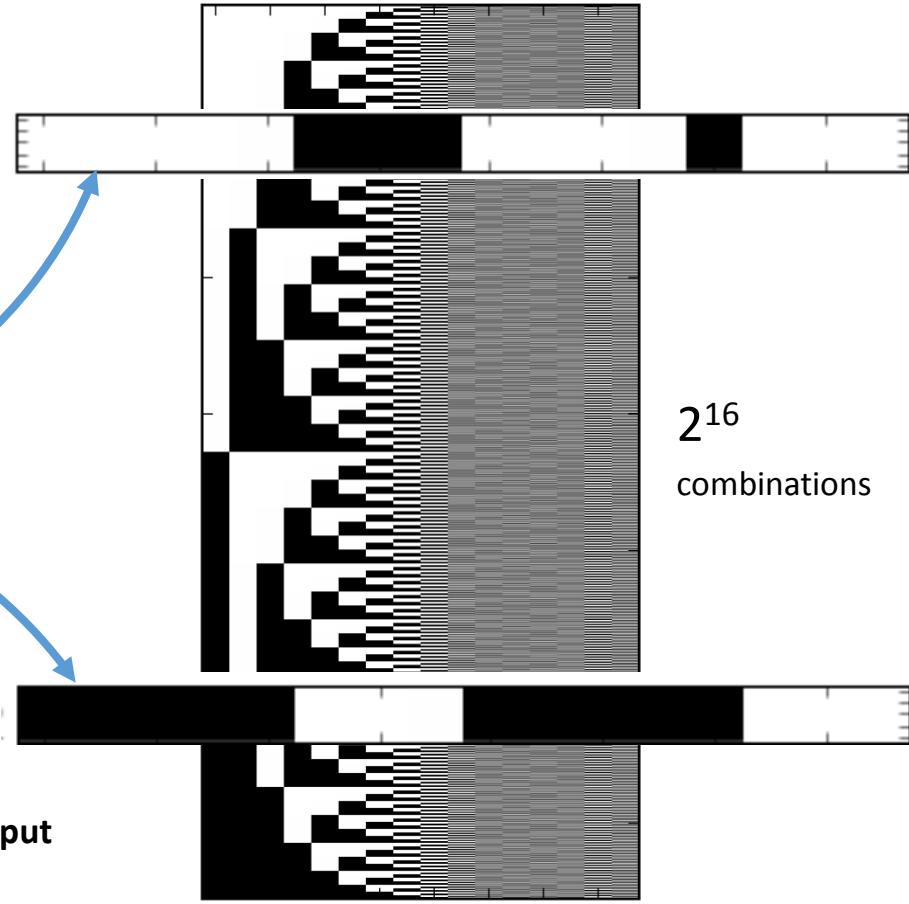
A hash function maps input binary to a hard-to-predict number with a finite range




easy

$HASH_{16}$

hard



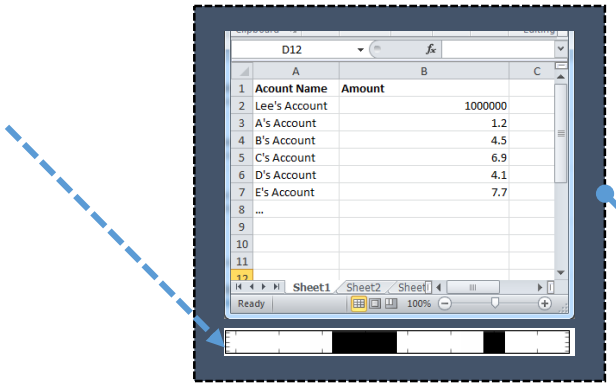
$2^{16}$ combinations

16 bits

**Small change to input -> hard-to-predict change to output**

# Blocks

1. **Block** – An agreed data structure containing a cryptographic hash of its previously agreed state

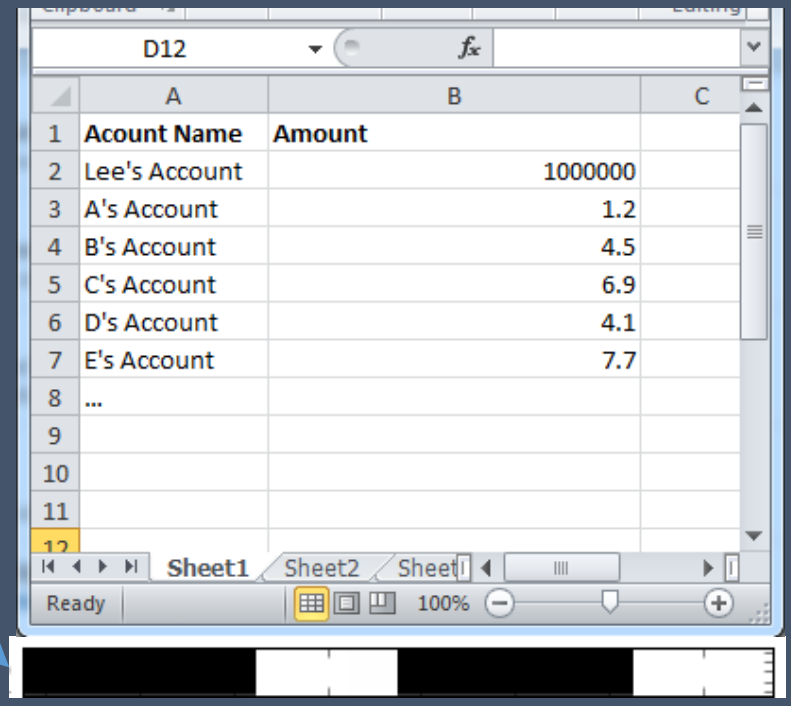



time

$HASH_{256}$

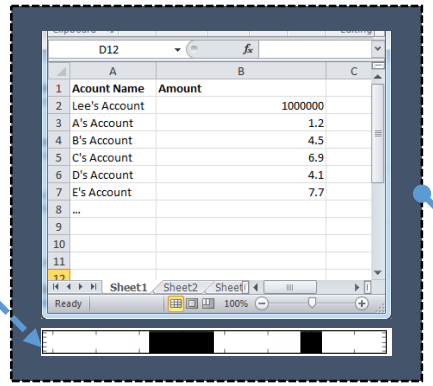
E.g. a spreadsheet

Block



# Transactions – changing blocks

1. **Transaction** – A proposed change – valid if it adheres to agreed rules (broadcast to all computers)

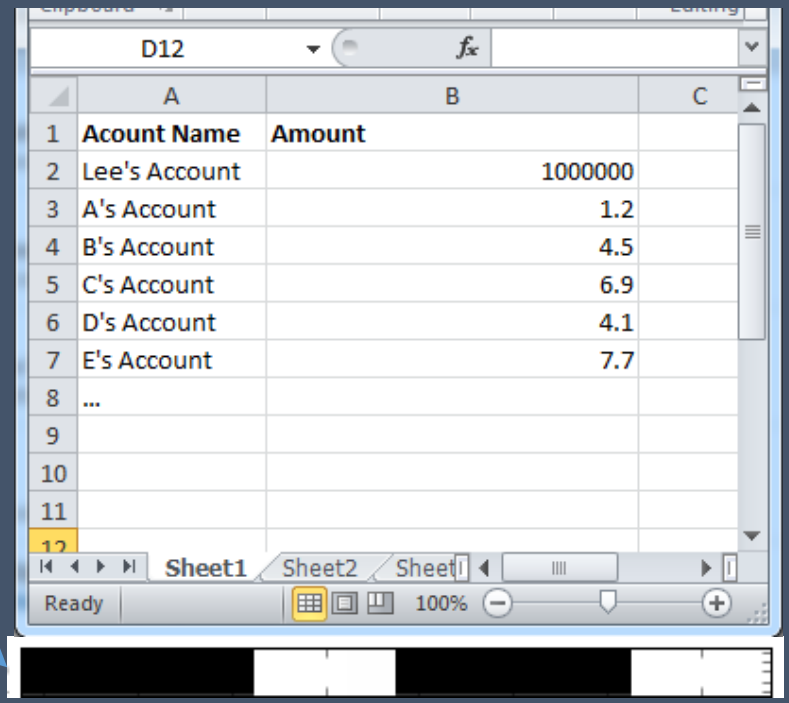



time

HASH256

E.g. a spreadsheet

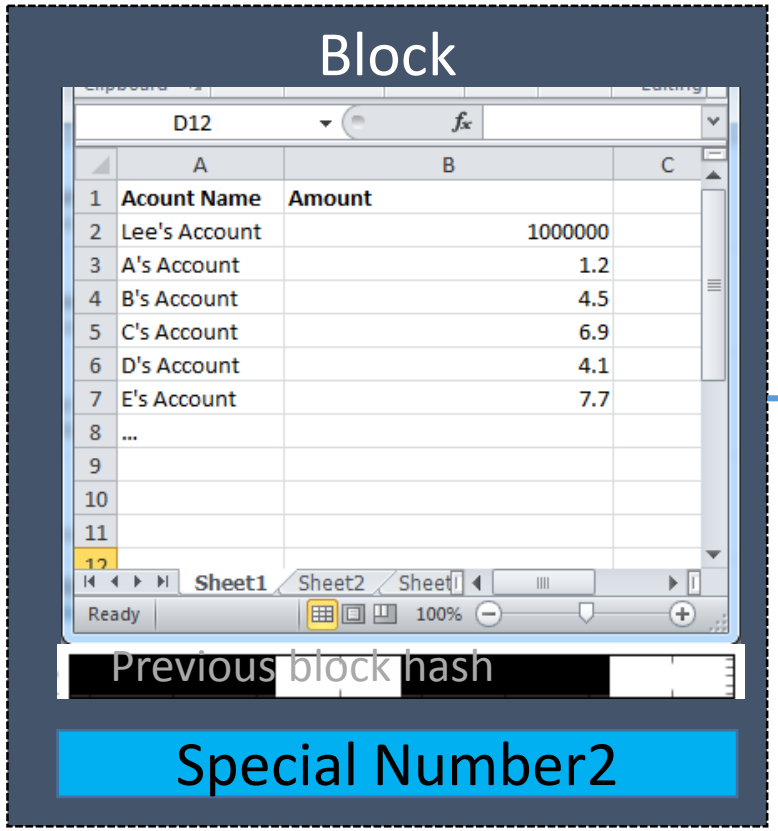
Block

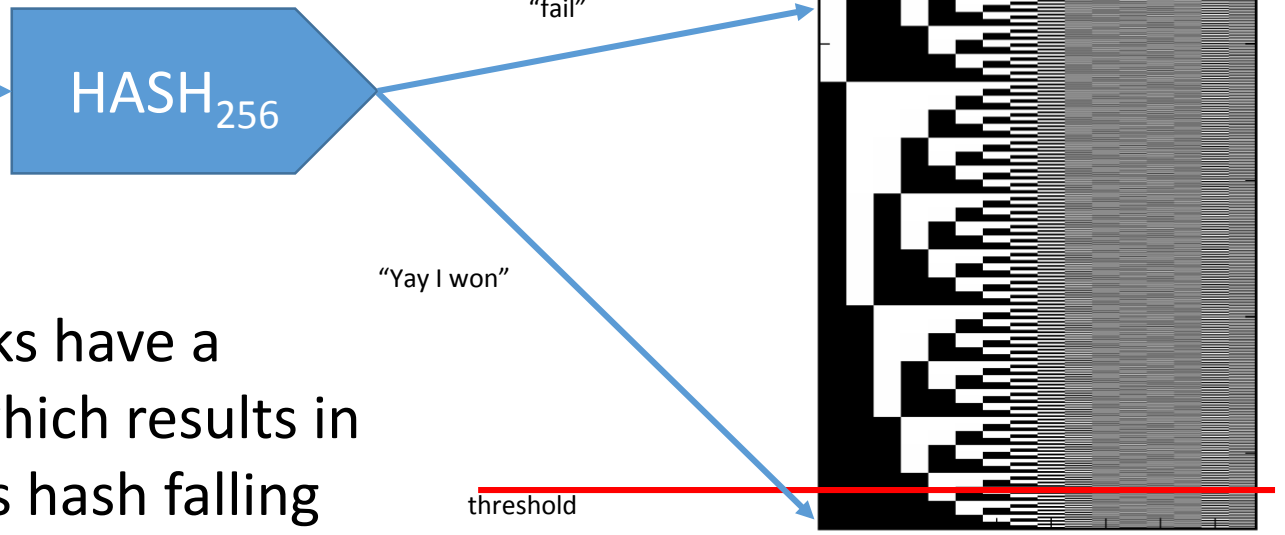



**E.g. "take X from my account and put it in Y's account"**

# Consensus

1. **Proof of Work** – Let's race to see who's computer can find a valid block

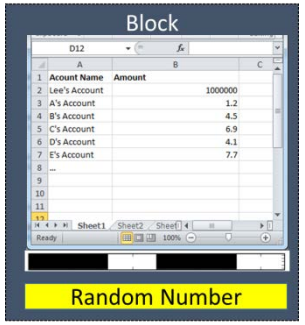


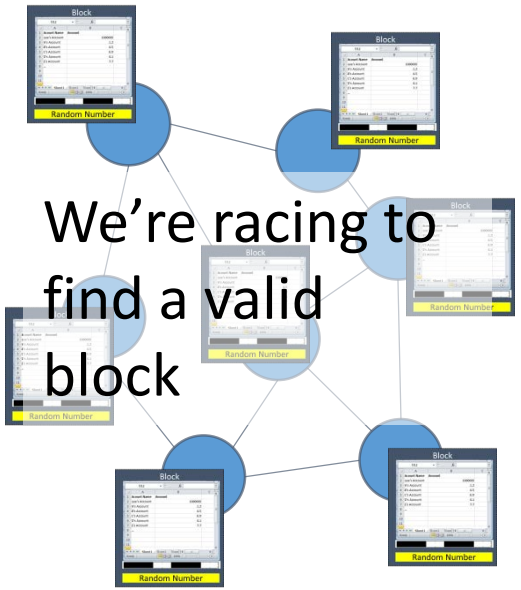




Valid blocks have a number which results in the block's hash falling below a threshold

# Consensus

1. **Proof of Work** – Let's race to see who's computer can find a valid block



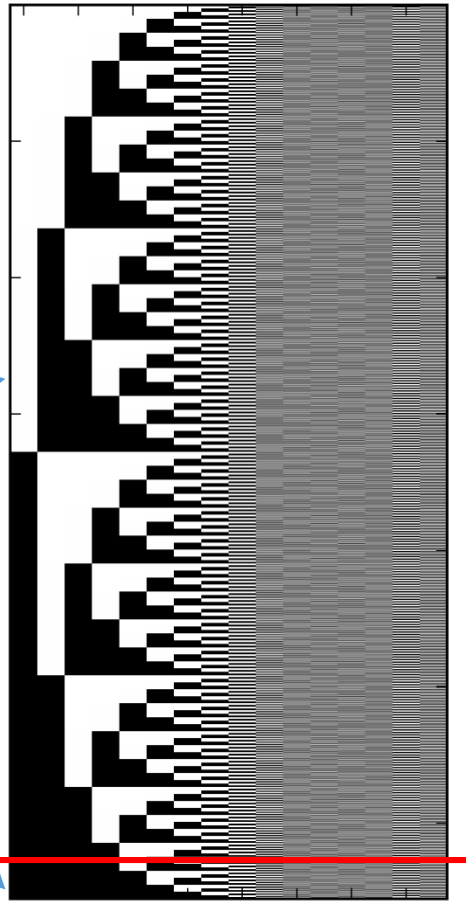

We're racing to find a valid block

BTC: ~500MW
ETH: ~200MW

$HASH_{256}$

"fail"

"Yay I won"



Threshold varied to maintain an agreed time between blocks

threshold

# Consensus Alternatives

**Proof of Stake** – “I bet you that this is a valid future block”

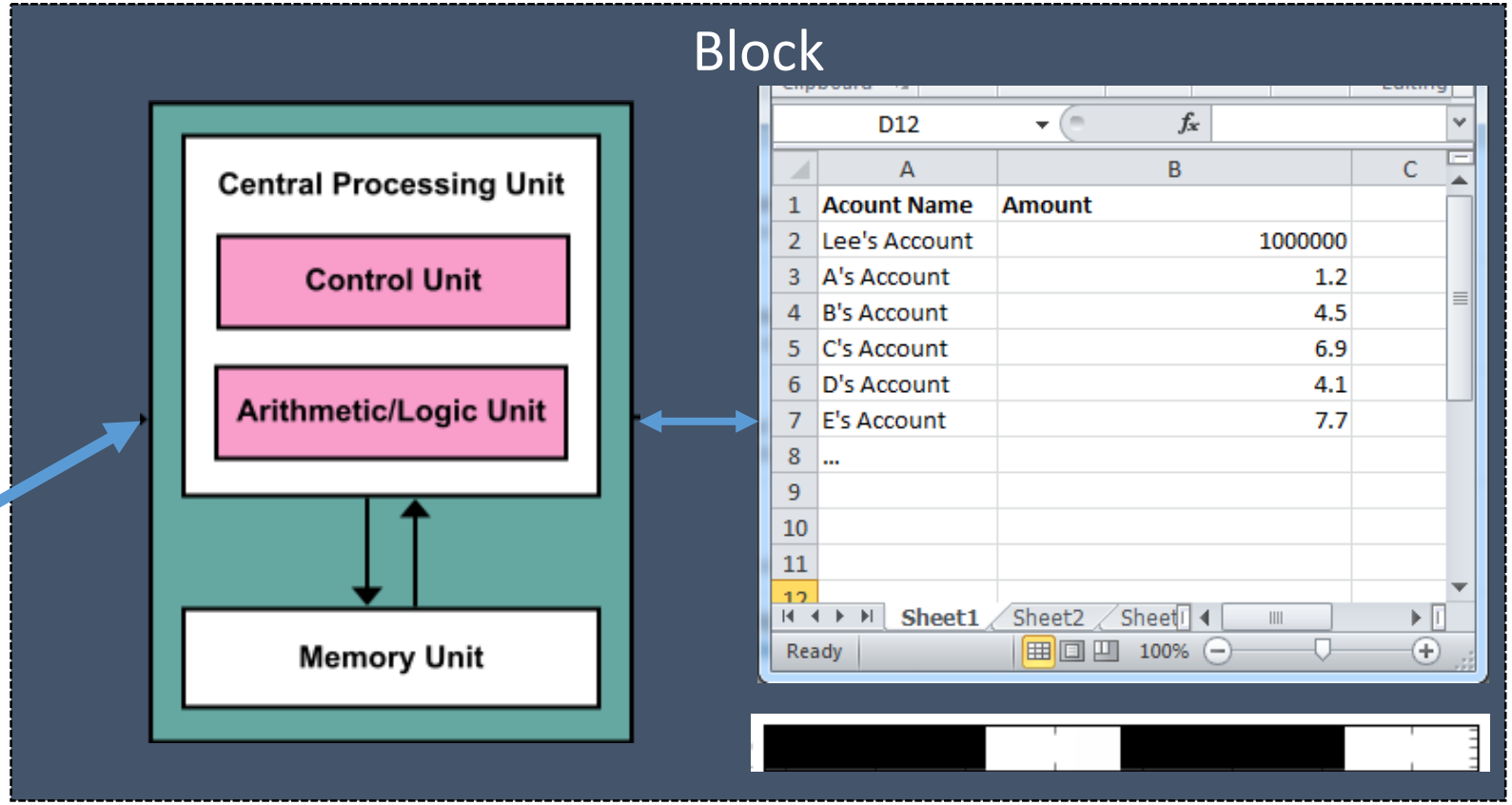
**Proof of Authority –** “I prove that I am a valid authority and hereby pronounce this to a valid future block”

# Smart Contracts

What if we add a virtual computer definition?

This helps us to create smart contracts

**Smart Contracts:**
Decentralised Autonomous Organisations




A transaction might be **"run this code using the agreed instruction set on the agreed virtual machine"**

Examples : Ethereum Platform, Bitcoin Rootstock, Hyperledger

# Smart Contracts – A timeline

**Nick Szabo**

**"I define a smart contract as a computerized transaction protocol that executes terms of a contract. …"**

- replicable,
- secure,
- verifiable,
- translucent
- immutable

**1994AD**

**Gavin Wood**

**Readable and Executable by computers**
**Unambiguous** *unless designed in*
**Autonomous** *merging of agreement and enactment*
**Enforced**

**2015AD**

**Brennan and Lunn – Credit Swisse**

**" Smart Contracts are Self-executing commitments, fulfilment of which can be trusted. "**

**2016AD**

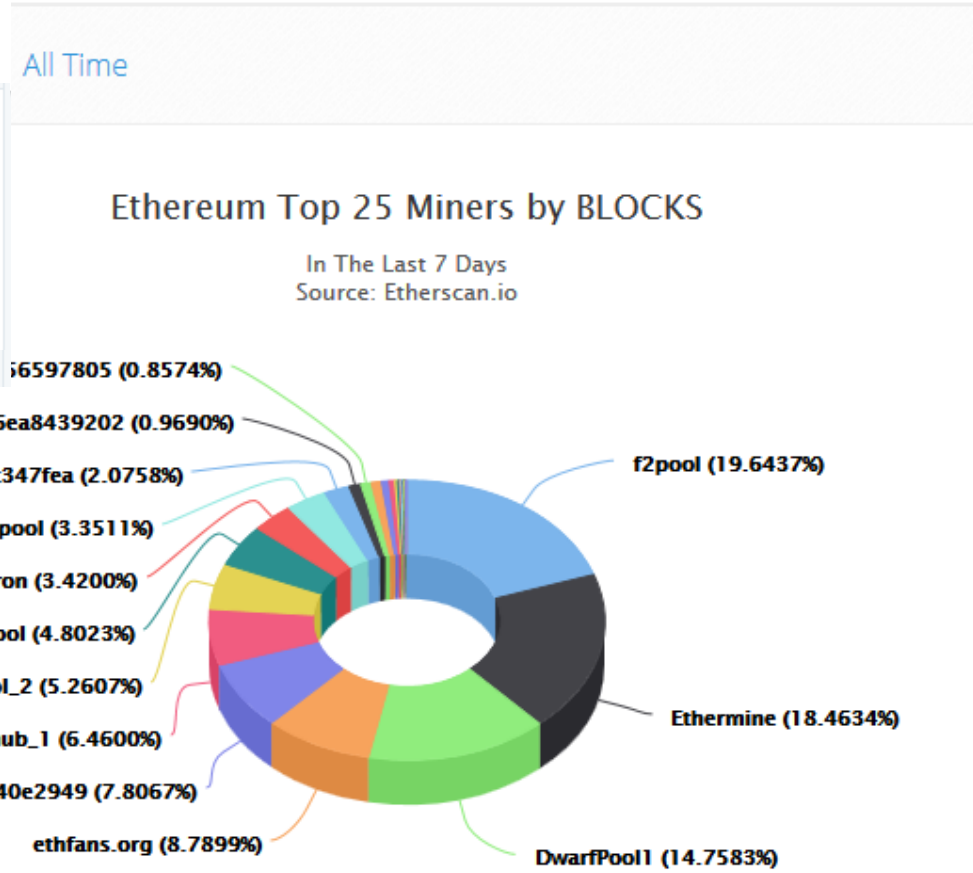
# Classification of Blockchain Protocols

| | Layer | Protocol (e.g. Ethereum) | |
|---|---|---|---|
| Blockchain Protocols | **Governance** | EIP process, influencer announcements and social consensus | Protocol change decisions made here |
| | **Social** | Github, Reddit, SE, Slack, Word of Mouth etc | |
| | **UX/UI** | Geth, Parity, PyEthApp, Mist | |
| | **Consensus** | Block derivation rules and PoW (Yellow Paper) – PoS in future | |
| OSI stack | **Application** | Kademlia, RPC, IPC | |
| | **Presentation** | AES, ECDSA | |
| | **Session** | | |
| | **Transport** | DevP2P, RLPx, TCP | |
| | **Network, Data-link and Physical** | As public Internet | |

# Attack vector – security of end-points


Picture - An Intertec Superbrain microcomputer (Tom Murphy VII)

# Attack vector – miners

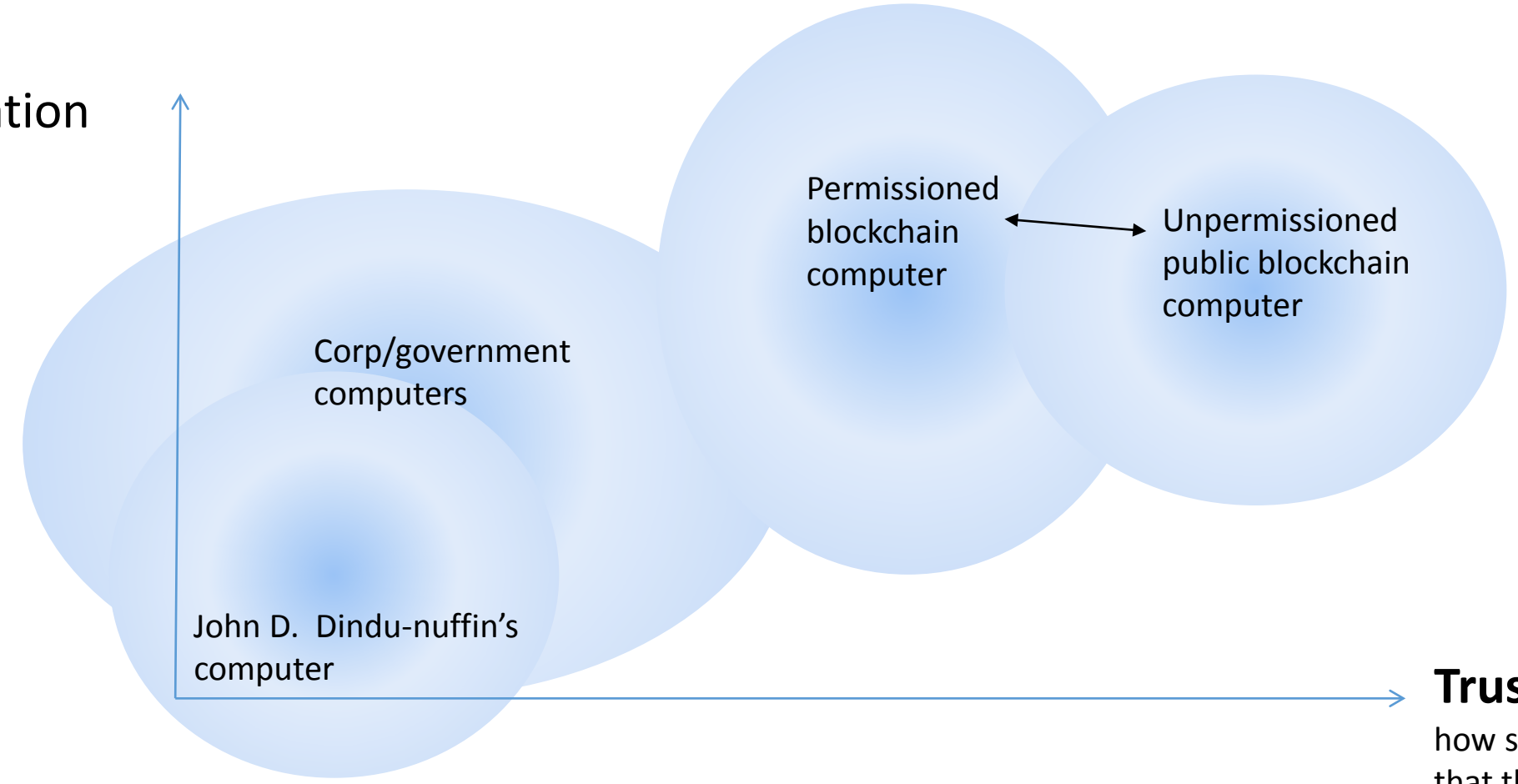




(A Total 42105 Blocks Mined by 66 miners In The Last 7 Days)

**From Etherscan.io**

# Computation cost vs Trust?

**Cost** per computation




?

**Trust**,
how sure can I be that the code will run as defined?

# Grid in a box….


**What is paid for?**

**Energy –** imported or exported energy

**Power –** some maximum import and export capacity

**Security of supply –** the continued reliable existence of voltage across my metered terminals.

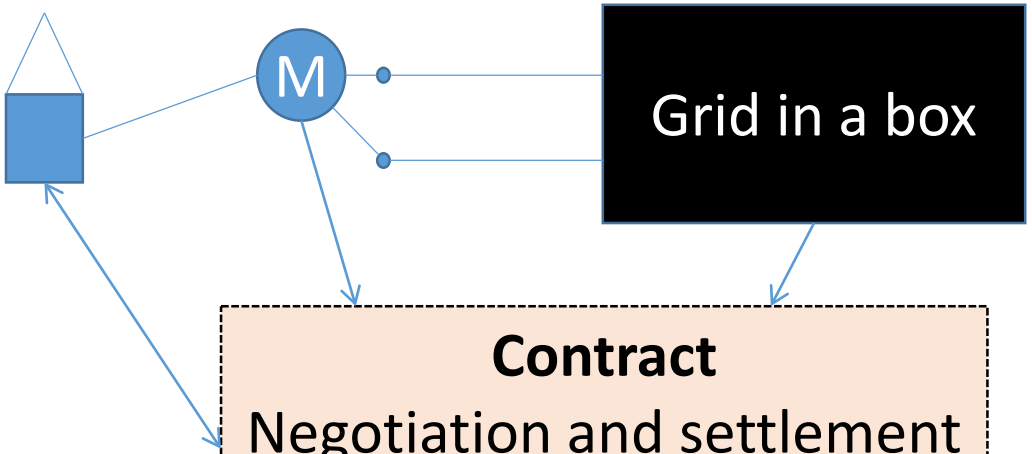
**Safety** – sufficient fault level to operate my protection, not too much

**What lowers cost?**

**Certainty** of future usage

**Compromise** on service quality

# What could a smart contract look like to user?




**Reward/penalty based on quality of prediction**

**Contract**
Negotiation and settlement of Energy, Power and Security of Supply

**Constraints set by:**
Regulator, Network Operators
**Service offers by:**
Demand, Generators, Network Operators, Storage

# Example: Automation of supplier role

Users either **critical** or **non-critical**

Accept market price

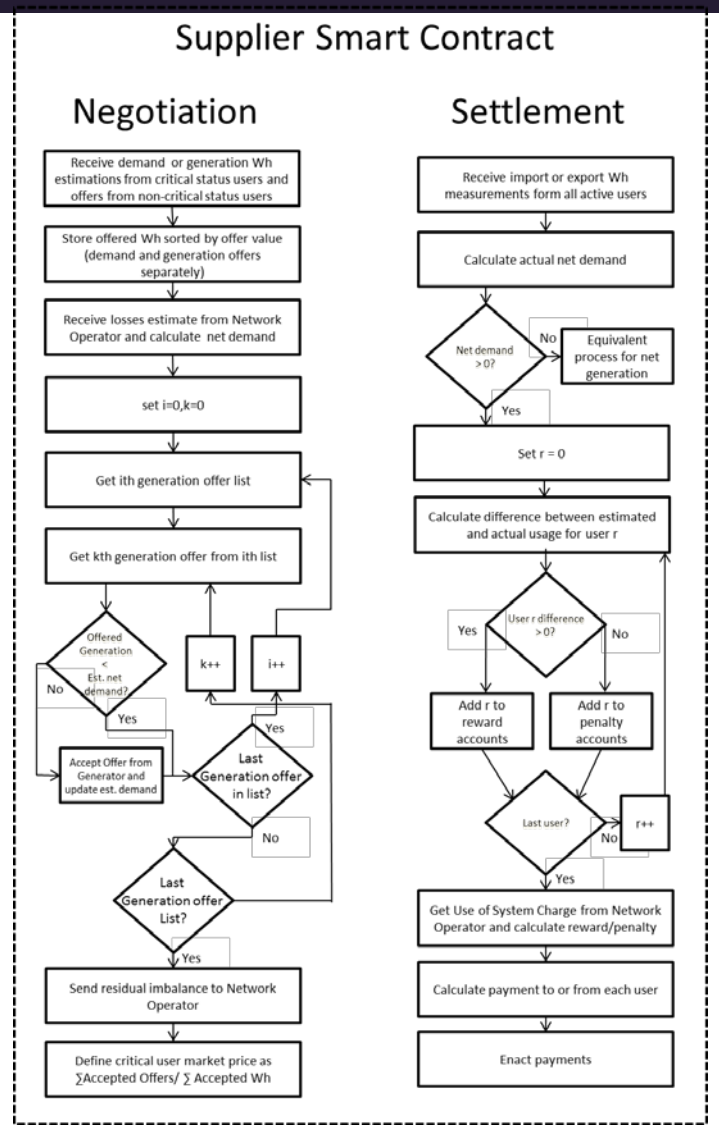
Prepared to not participate – make offers

1. Critical **users estimate usage**
2. Offers accepted until little/no imbalance – defines market price
3. Users rewarded/penalised based on their mis-estimation

$$P_{user} = \frac{|E_{user} - A_{user}| \times \sum_{users}^{U} R_{user}}{|\sum_{users}^{U} E_{user} - \sum_{users}^{U} A_{user}|} \qquad R_{user} = \frac{H_{user} \times |E_{user} - A_{user}| \times \sum_{users}^{U} E_{user}}{\sum_{users}^{U} E_{user} + \sum_{users}^{U} A_{user}}$$

Rewards paid by users tending to unbalance system

Where $R_{user}$ and $P_{user}$ are the calculated reward or penatly for a given user, $H_{user}$ is a historical performance factor between 0 and 1, $A_{user}$ is a users' estimated usage, $E_{user}$ is a users' actual usage and $U$ is the set of all users.



# Automated supplier smart contract

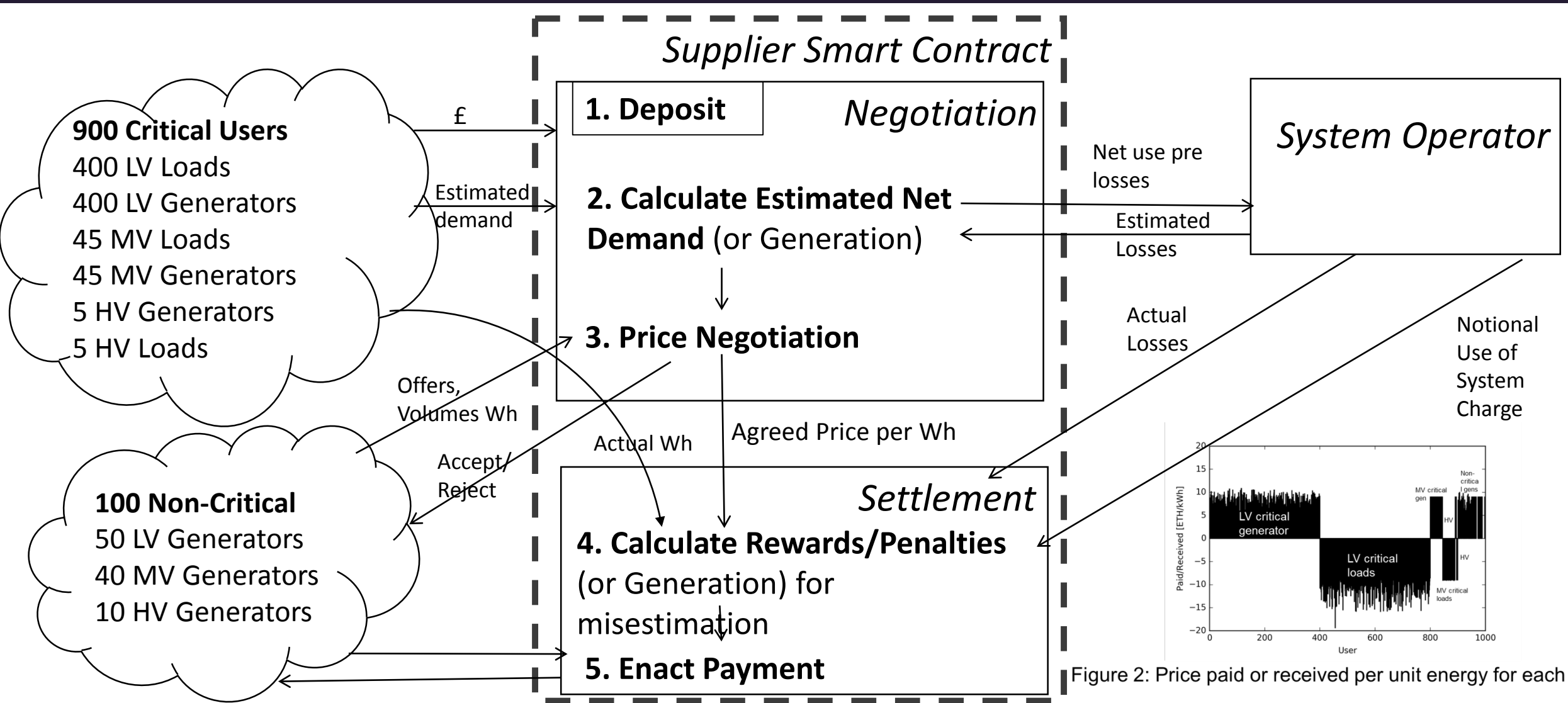



Figure 2: Price paid or received per unit energy for each user

# Conclusions

**Suppliers can be seen as competing negotiation and settlement algorithms**

Scope for the role to be, in part, automated

Open question – is there scope to re-define the playing field to make full use of blockchain platforms

**Off-chain computation?**

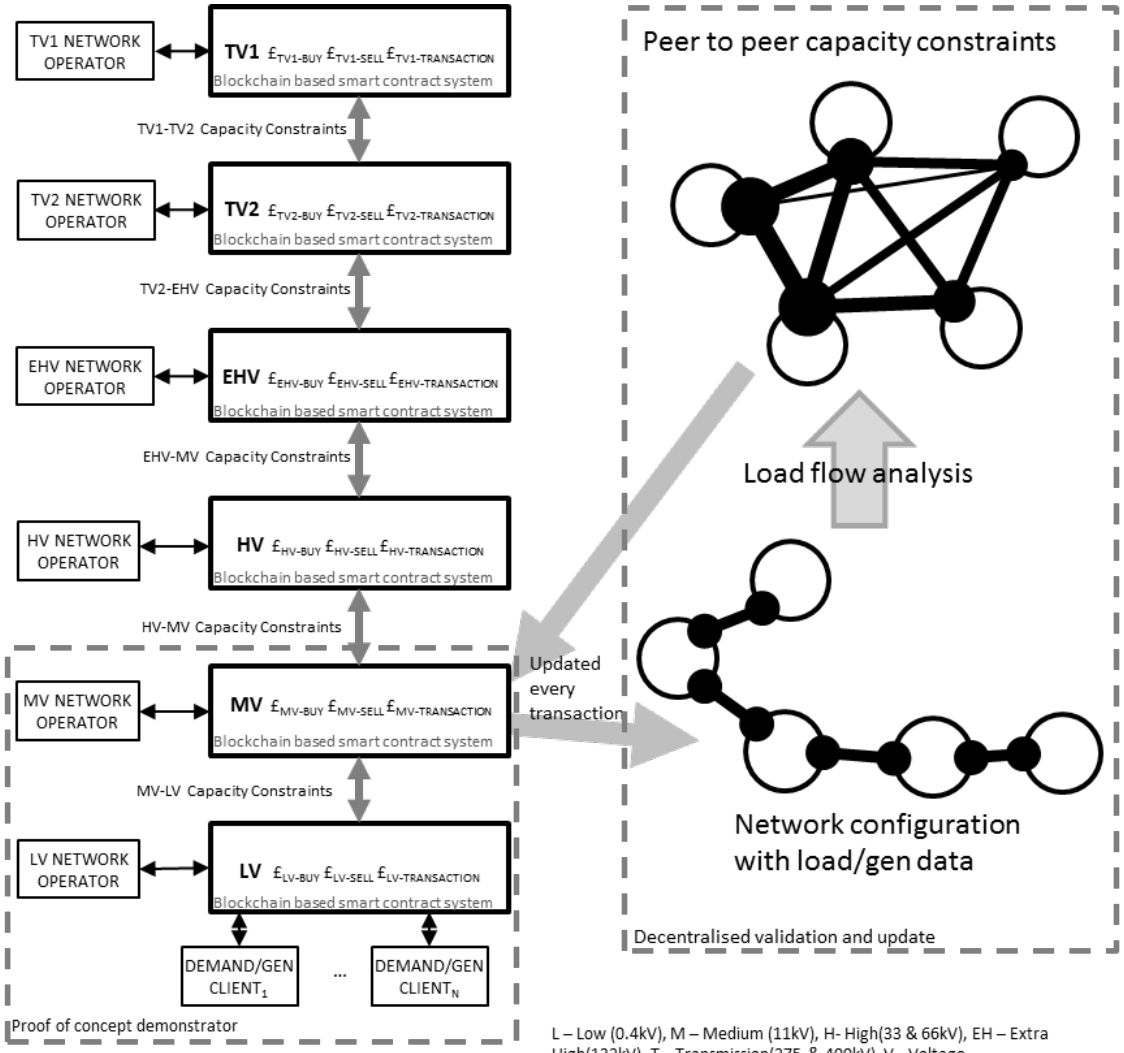
Use blockchain to ensure agreement on the result of computation, rather than to perform the computation

Computation markets…

Co-ordination or permissioned and public blockchains

# Smart Contracts tied to Network Topology

- Demonstrate benefits (and/or drawbacks) of a tiered smart contract philosophy over existing regulatory and control frameworks:
  - Automated supplier role.
  - Enforced consensus on sharing responsibility for system stability.
  - Smart Contracts (relating energy demand/supply balance and Use of System) linked to network topology.
  - Demonstration of clear signaling to potential infrastructure investors.
  - Post-hoc re-distribution of costs




L – Low (0.4kV), M – Medium (11kV), H- High(33 & 66kV), EH – Extra High(132kV), T – Transmission(275 & 400kV), V - Voltage

# Thanks for Listening

Thomas, Lee, Long, Chao, Burnap, Peter, Wu, Jianzhong and Jenkins, Nicholas 2017. Automation of the Supplier Role in the GB Power System using Blockchain Based Smart Contracts. Presented at: *CIRED 2017 - International Conference on Electricity Distribution*, Glasgow, 12-15 June 2017. The IET, pp. 1-5

Hubnet Flexifund Project: Blockchain based smart contracts for peer to peer energy trading using the GB smart metering System