

# NEUROWARE'S GUIDE TO BLOCKCHAINS

— AN EXTREMELY ABBREVIATED VERSION OF OUR TWO DAY BLOCKCHAIN TRAINING —



neuroware

# WE ARE A TECHNOLOGY STARTUP FOUNDED BY TECHNOLOGISTS



## **Mark Smalley - CEO**

Mark's been building distributed applications on the blockchains for over 5 years now from Malaysia, where he's been developing web-applications for 19 years & helping to organize and present at several prominent technology groups and conferences worldwide. He was also the first qualified MongoDB Master in Asia, where he won an award for his open-source NoSQL Content Management System.



## **Ruben Tan - CTO**

Ruben is one of Malaysia's leading NodeJS developers, founding member of the Malaysian JS User-Group, and regular contributor to many open-source projects and communities; having explored distributed consensus technologies and NoSQL data relationships with previous projects such as MyTeksi and OnApp - he has spent a decade mentoring startups and businesses worldwide.

# WE ARE BACKED BY A TRUSTED TEAM OF VESTED ADVISORS



**Colin Charles**  
MariaDB Founder



**Adam Giles**  
Ex Standard Chartered



**Hanson Goh**  
Axiata / Ex Google



**David Barton Grimley**  
Sapient Nitro



**Johnny Mayo**  
Forbes 30 Under 30



**Wu Han Ngeow**  
Maxis



**Gabey Goh**  
Campaign Asia-Pacific



**Gareth Davies**  
Mindvalley

# WE'VE BEEN WORKING WITH AND TRAINING LEADING BRANDS



**Suruhanjaya Sekuriti**  
Securities Commission  
Malaysia



**BANK NEGARA MALAYSIA**  
CENTRAL BANK OF MALAYSIA



# TOPICS TO BE COVERED WITH AS MANY PICTURES AS POSSIBLE

- Section 1 - History of Modern Money - why did Satoshi launch in 2009...?
- Section 2 - Exploring The Technologies Powering Bitcoin Transactions
- Section 3 - Digesting The Distributed Ledger Landscape
- Section 4 - Use-Cases - Hyperlocal Banking & Crowdfunding Equity

## SECTION 01

A BRIEF HISTORY OF MODERN MONEY

WHERE NO IDEA IS A NEW IDEA

**IT ALL STARTS HERE - ON THE ISLAND OF YAP**



# SHOPPING WAS NOT EASY



**SO THEY CREATED A PUBLIC LEDGER**



# UPDATES REQUIRED GROUP CONSENSUS



- Size wasn't everything
- The history of each stone determined it's individual value
- Conducting transactions quite literally involved a song & dance
- This required the majority of people from the village to be present

**BUT IT COULD NOT SCALE - THEY EVENTUALLY SWITCHED TO US\$**



# SETTING THE POST-CIVIL STANDARD



# SETTING THE GOLD STANDARD



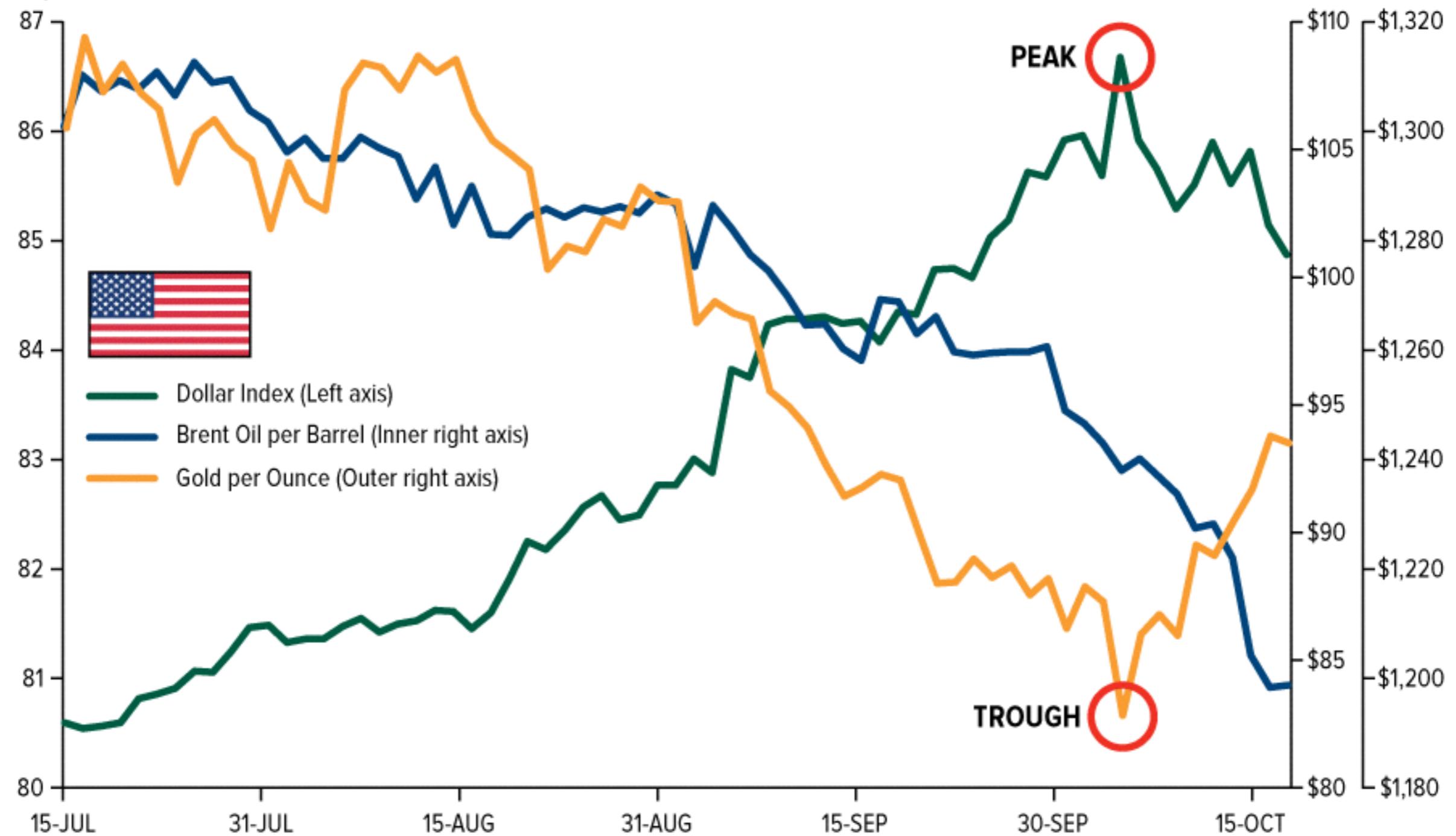
# THE END OF AN ERA

- 1873 to 1914 - All major worldwide currencies were 100% backed by gold
- After WW1 ended the USA switched to Fractional Reserve Banking
  - started by printing US\$50 for every US\$20 deposited in gold
- During WW2 the USA accumulated 2/3rd's of all gold, forcing all currencies to switch to fiat-systems pegged to US\$, which was pegged to gold
- 1971 - Richard Nixon ended the gold standard, introducing **petrodollars**

# GOLD Vs DOLLAR

## A Strong U.S. Dollar Keeps Gold and Oil Prices Low

July 16, 2014 – October 16, 2014



# WHEN YOU THINK ABOUT MONEY - IT'S HARD TO AVOID GOLD



WHEN YOU THINK ABOUT MONEY - IT'S HARD TO AVOID OIL



WHEN YOU THINK ABOUT MONEY - IT'S HARD TO AVOID OIL



WHEN YOU THINK ABOUT MONEY - IT'S HARD TO AVOID POLITICS

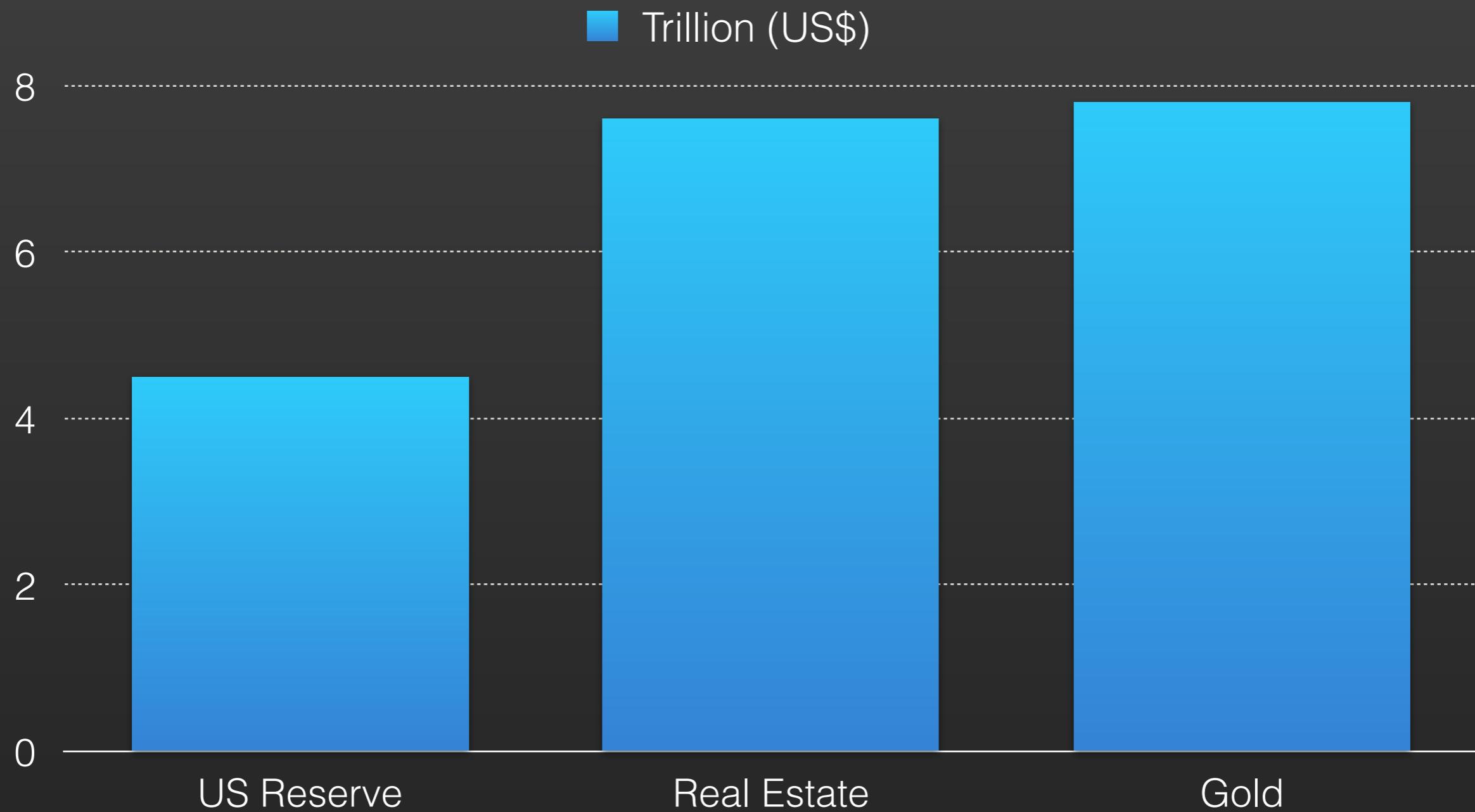


WHEN YOU THINK ABOUT MONEY - IT'S HARD TO AVOID **RELIGION**

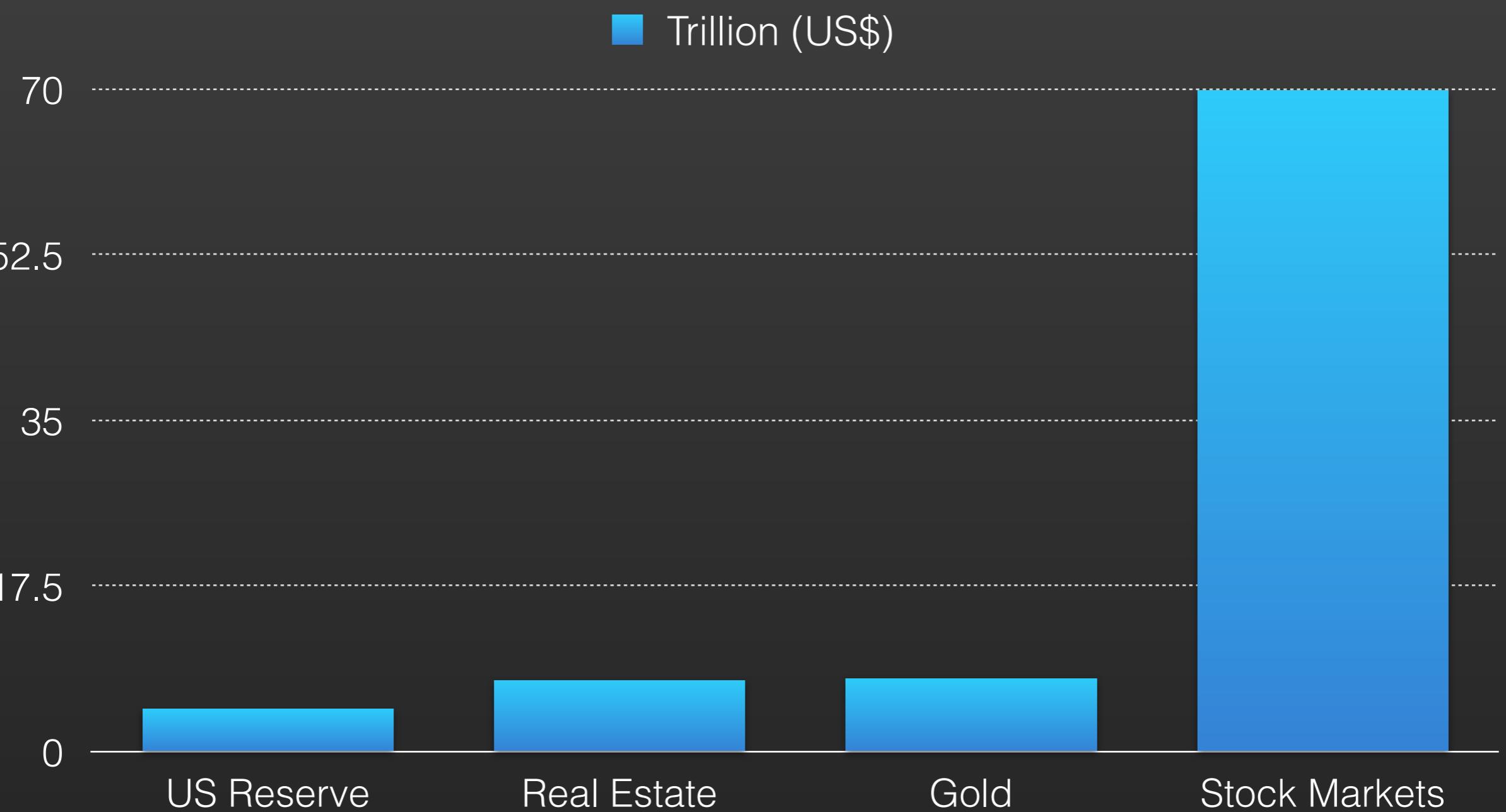
---



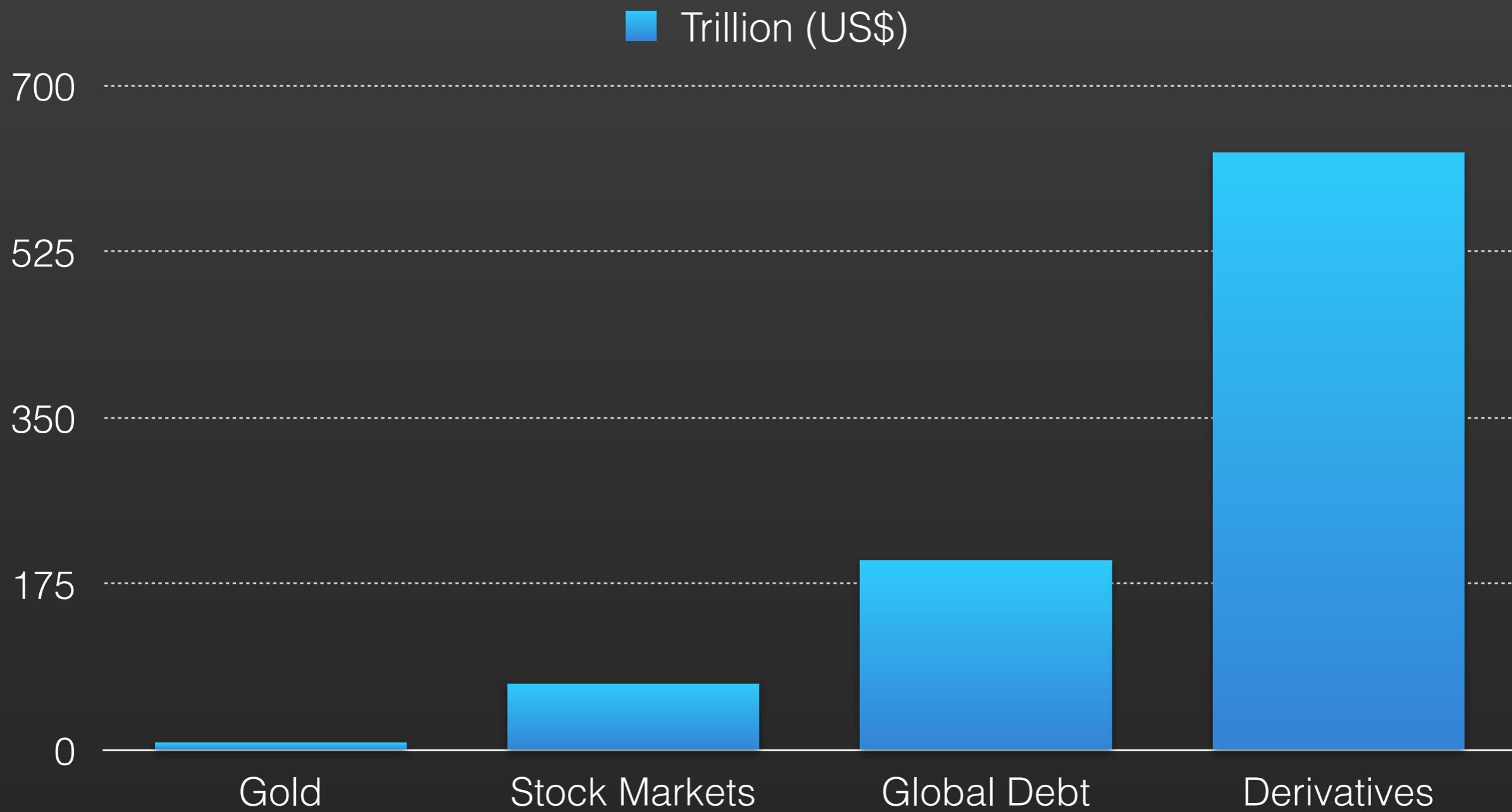
# BEFORE THE US GOVERNMENT LOST CONTROL - **REAL MONEY**



# THEN CAME WALL STREET



# THEN CAME THE INVENTION OF ~~MONEY~~ DEBT



# IT ALL ENDS IN TEARS (512 US BANKS CLOSED SINCE 2008)

World War 2  
US\$3 Trillion

2008 Bailout  
US\$8.5 Trillion

All other US  
Wars Ever



# NOTHING LASTS FOREVER



- Average lifespan of individual currencies is 27 years
- Every 30 or 40 years the reigning monetary system fails
- Over 3,800 fiat currencies worldwide have failed
- 15 of which happened in just the past 25 years

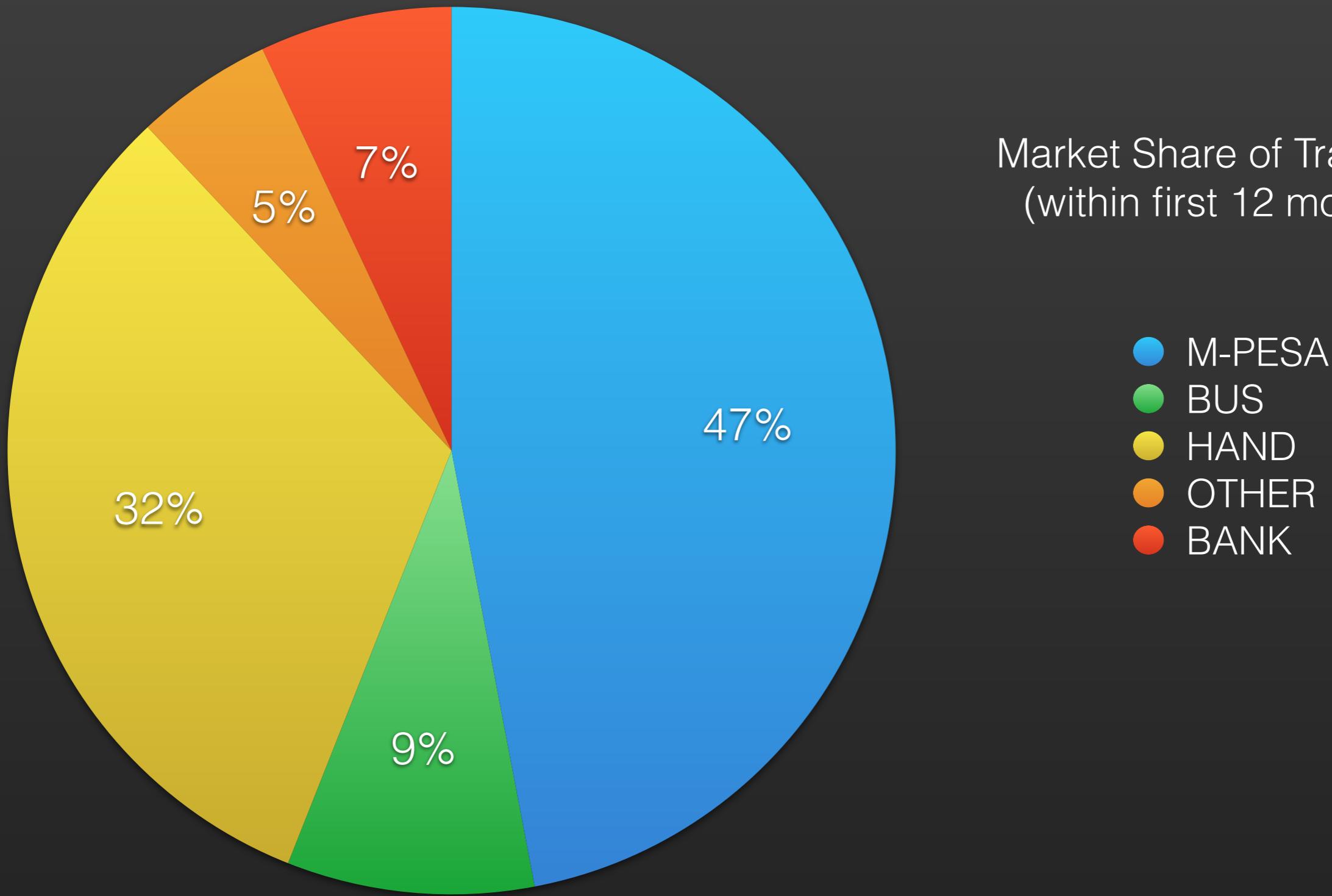
# THE RECENT FAILURE OF FIAT CURRENCIES

COUNTRY	YEAR	PROBLEM
Angola	1991-1999	1 New Kwanza = 1,000,000,000
Belarus	1994-2002	50,000 = 100,000,000 2000 Rublei
Bosnia	1993	Massive hyperinflation
Ecuador	2000	Pegged to USD after 70-80% drop in its dollar
Georgia	1995	1 new lari = 1,000,000 laris
Krajina	1993	Country folded became part of Croatia
Mexico	1993-1994	Defaulted in 1982   1 Nuevo Peso = 1,000 Old Pesos
Poland	1990-1993	1 new Zloty = 10,000 old Zlotych
Romania	2000-2005	1 new Leu = 10,000 old Lei
Russia	1992-1994	100 Rubels = 1 US\$ in 1991   30,000 Rubels = 1 US\$ in 1999
Turkey	1990-2005	1 New Turkish Lira = 1,000,000 Old Lira
Ukraine	1993-1995	1 Hryvnya = 100,000 Karbovantsivi
Zimbabwe	1999 – 2010	Ongoing mess

TECHNOLOGY ALWAYS FINDS A WAY SAVED ZIMBABWE



# WITHIN FIRST 12 MONTHS - 17 MILLION SUBSCRIBERS BY 2011



Market Share of Transfers  
(within first 12 months)

- M-PESA
- BUS
- HAND
- OTHER
- BANK

# ARE BANKS HAVING THEIR ~~KENYAN~~ KODAK MOMENT?



- Founded in 1892
- 90% of film sales in 1976
- 85% of camera sales in 1976
- 4th biggest global brand in 1996
- Removed from S&P 500 in 2010
- Bankrupt in 2012
- **They built 1st digital camera in 1975**

**“ SOFTWARE IS EATING THE WORLD ” - Marc Andreessen**



U B E R



- Uber is the world's largest taxi company, but owns no cars
- AirBnB is the largest accommodation provider, but owns no real estate
- Facebook is the most popular media provider, but creates no content
- Alibaba is the most valuable retailer, but owns no inventory
- **Bitcoin is the most valuable digital currency, but there are no coins**

**SECTION 02**

**DEEP DIVING INTO BITCOIN**

**MAGIC INTERNET MONEY**

BITCOIN

VS

BLOCKCHAINS



**DOGECOIN**

**VS**

**RIPPLE**



ETHEREUM

VS

PRIVATE CHAINS



# WHAT ARE THE BENEFITS OF DISTRIBUTED PUBLIC LEDGERS?

- They provide an immutable tamper-proof audit-trail of the truth
- Data can be easily shared and independently verified by third-parties
- Vastly increased security that is much less vulnerable to attack or outage
- Programmable contracts that can radically reduce human errors and costs



“While Fintech Disrupts Banks,  
the Blockchains Disrupt Fintech”

# WHAT ARE THE BENEFITS OF DISTRIBUTED PUBLIC LEDGERS?

- They provide an immutable tamper-proof audit-trail of the truth
- Data can be easily shared and independently verified by third-parties
- Vastly increased security that is much less vulnerable to attack or outage
- Programmable contracts that can radically reduce human errors and costs



“83% of banks believe they will lose 24% of their revenue to FinTech within 5 Years”

# INTERESTING BITCOIN BLOCKCHAIN FACTS TO REMEMBER

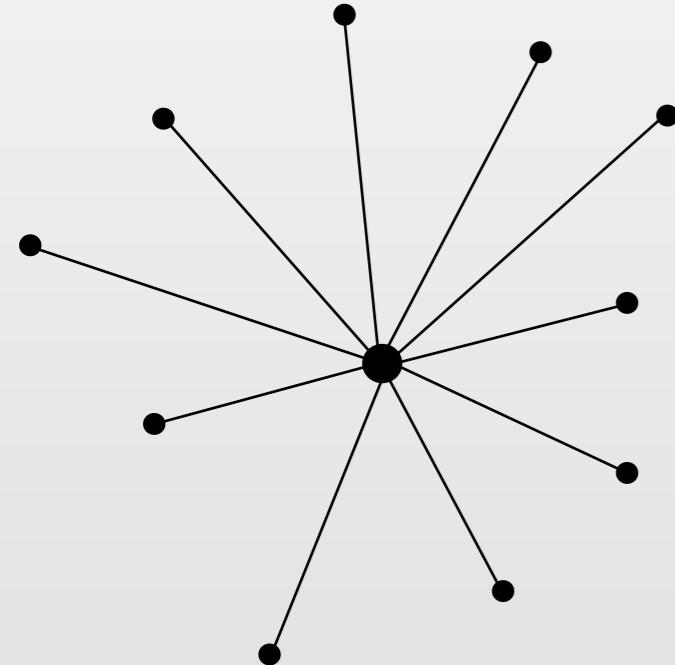
- Bitcoin blockchain released in January 2009 by Satoshi Nakamoto
- We do not know who Satoshi is, or what their religion or political views are
- However, the bailout of 2008 was cited as primary catalyst for its creation
- US\$13 per coin in 2013 (which is when we bought) - now US\$540 per coin
- The Bitcoin network is currently processing over 200,000 daily transactions
- The network's market capitalization is currently around US\$7 billion
- 21 million maximum finite supply, decreasingly dispersed every 10 minutes
- **But most importantly of all is the technology behind it...**

# BITCOIN AND BLOCKCHAINS HAVE NO NEW TECHNOLOGY

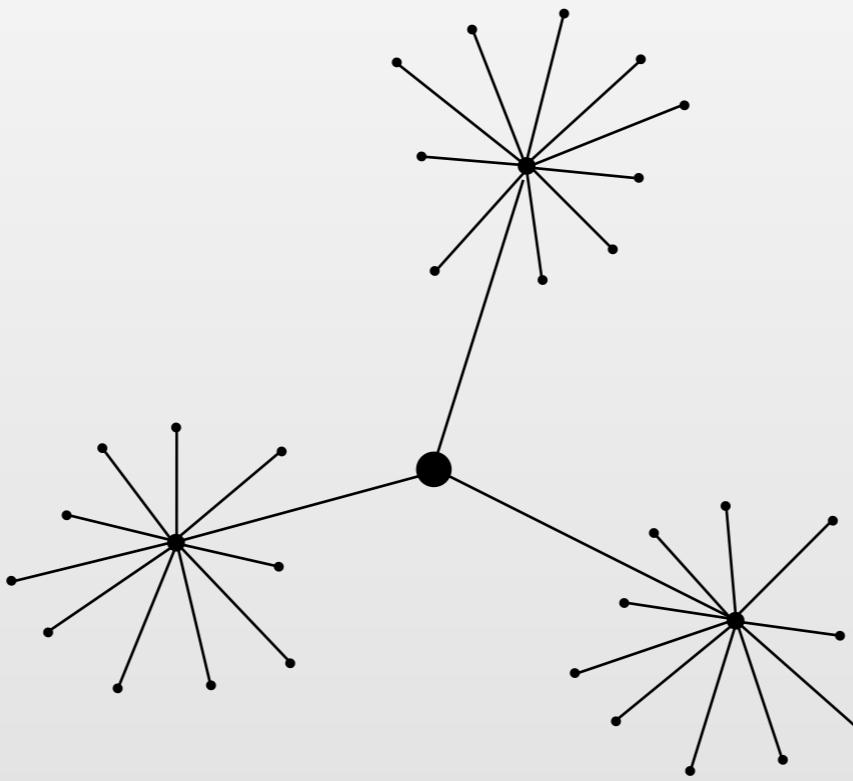


- HASH - Theorized in the 1800s - Coined by IBM in the 1950s
- SHA - Encryption method first introduced by US Navy in 1993
- P2P - Peer to peer protocol popularized by Napster in 1999

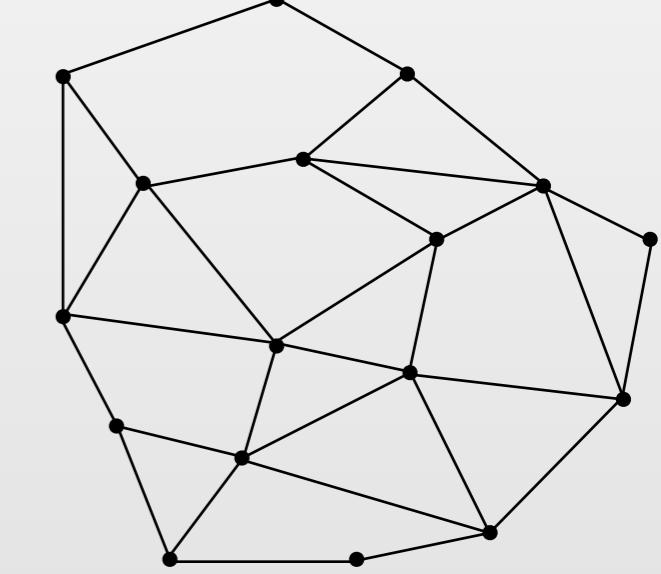
# THE EVOLUTION OF COMPUTER NETWORKS



CENTRALIZATION  
**DATABASE**

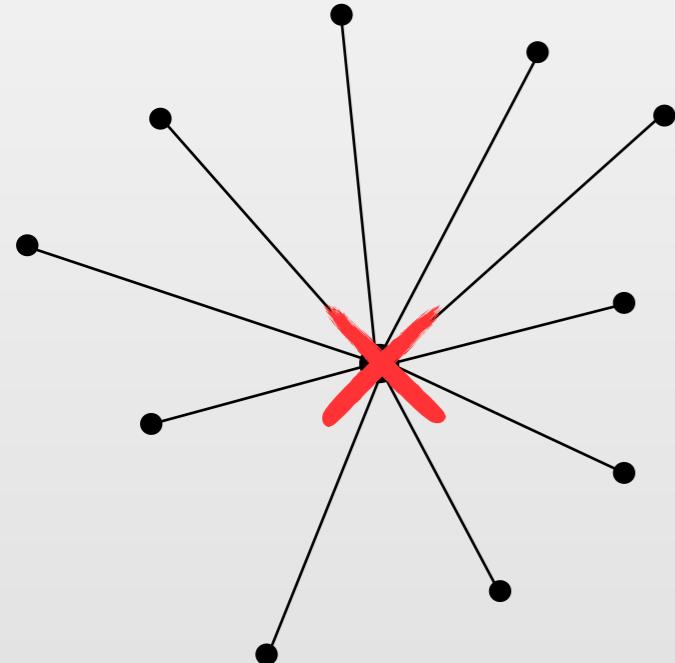


DECENTRALIZATION  
**THE CLOUD**

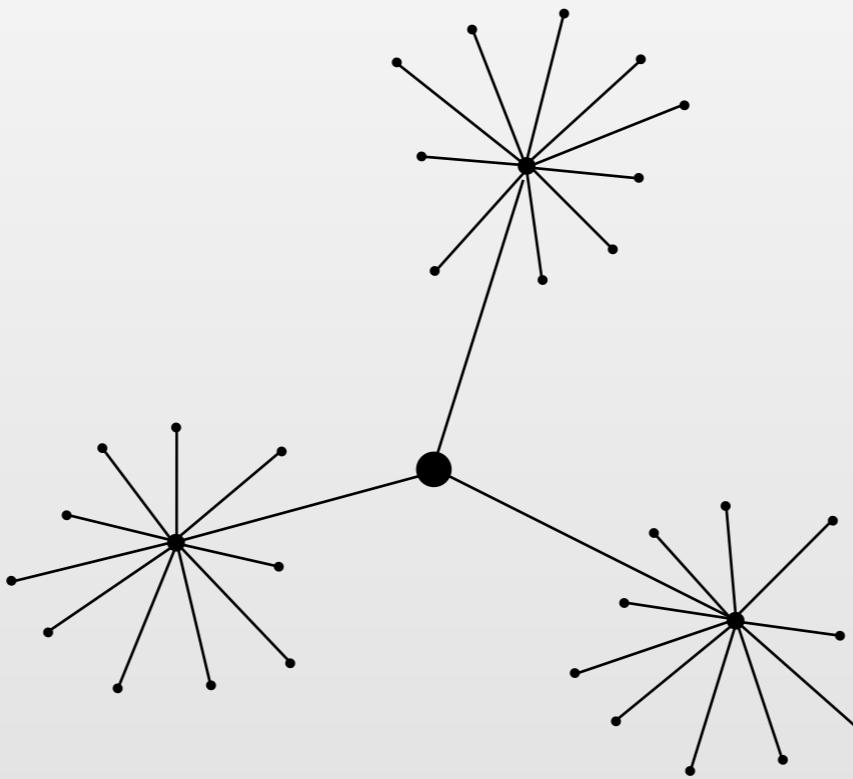


DISTRIBUTION  
**BLOCKCHAINS**

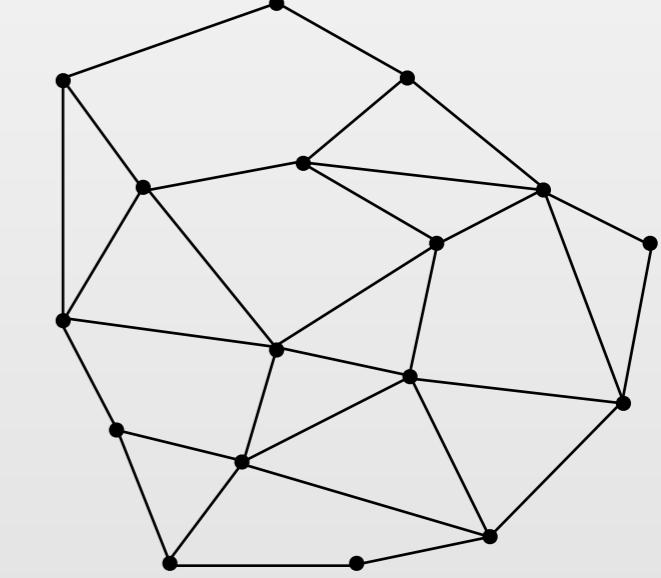
# THE EVOLUTION OF COMPUTER NETWORKS



**CENTRALIZATION**  
**DATABASE**

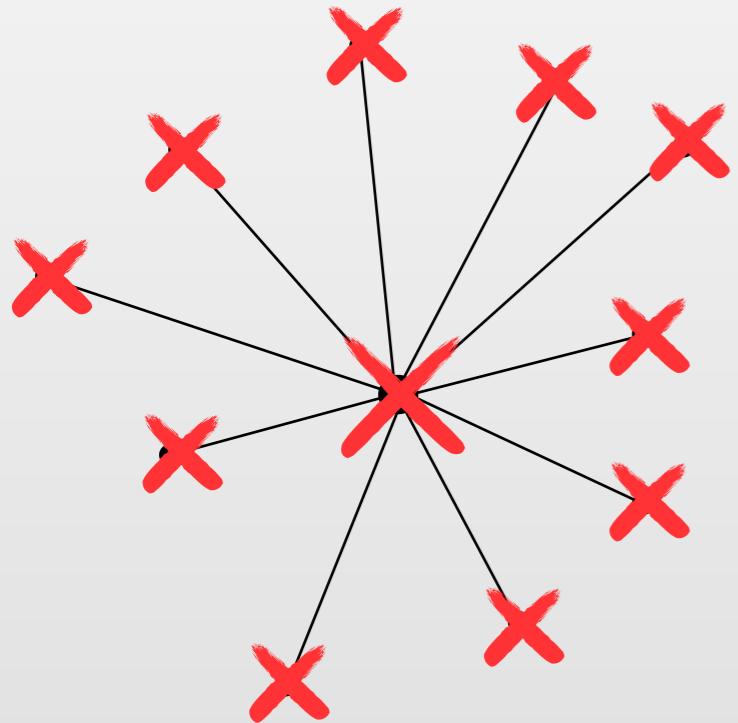


**DECENTRALIZATION**  
**THE CLOUD**

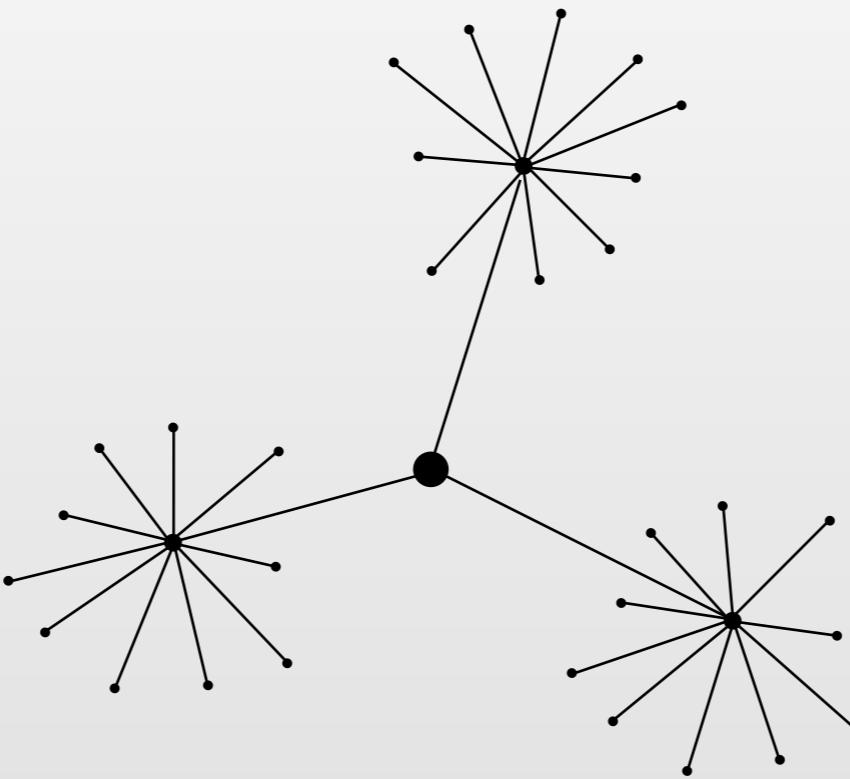


**DISTRIBUTION**  
**BLOCKCHAINS**

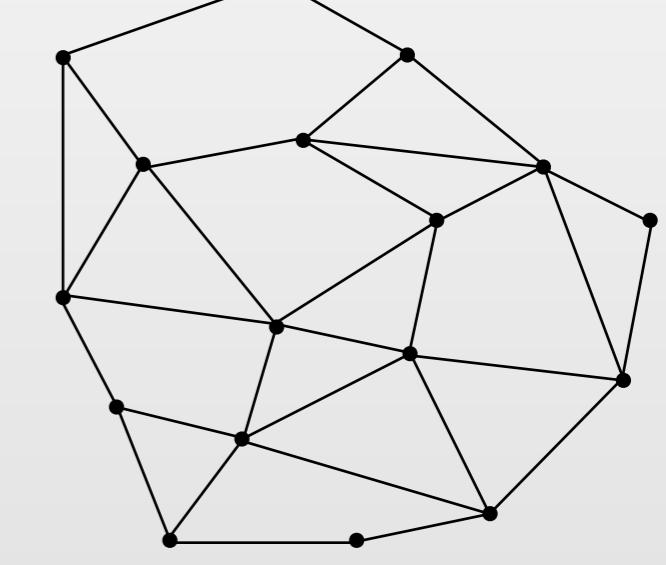
# THE EVOLUTION OF COMPUTER NETWORKS



CENTRALIZATION  
**DATABASE**

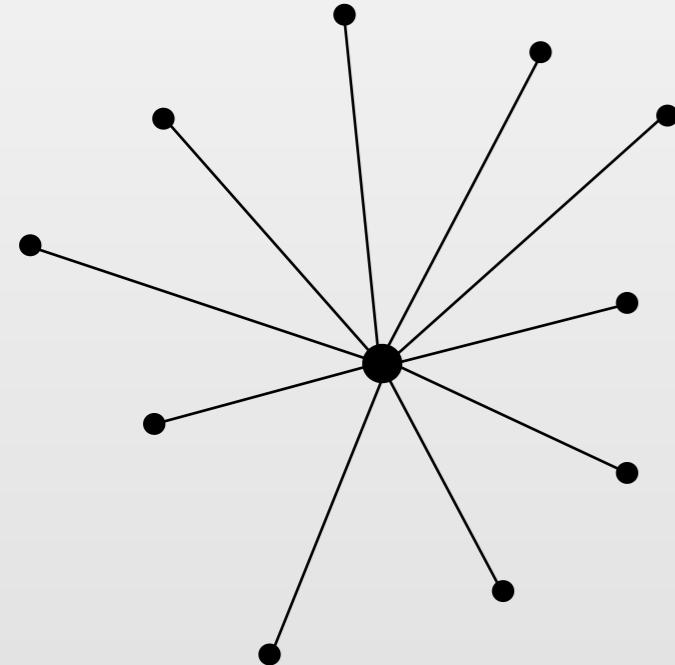


DECENTRALIZATION  
**THE CLOUD**

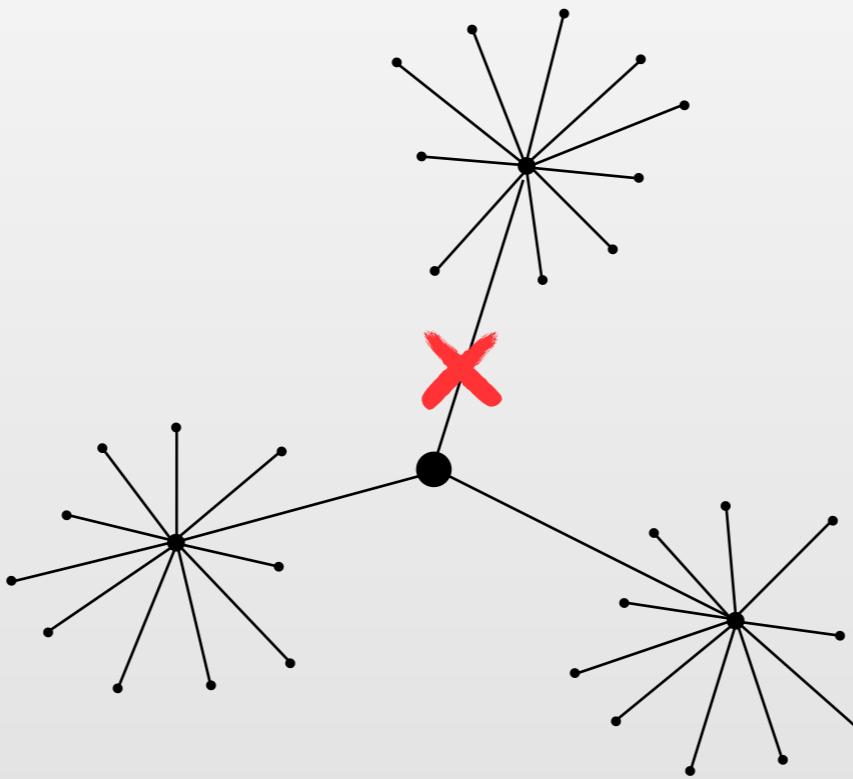


DISTRIBUTION  
**BLOCKCHAINS**

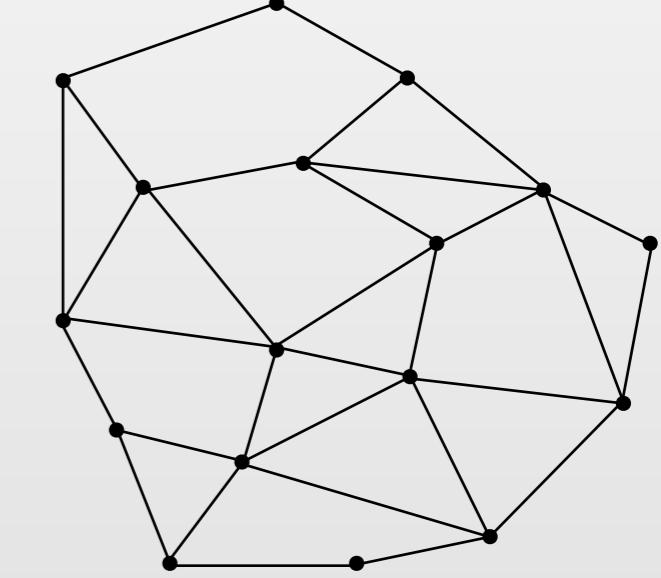
# THE EVOLUTION OF COMPUTER NETWORKS



CENTRALIZATION  
**DATABASE**

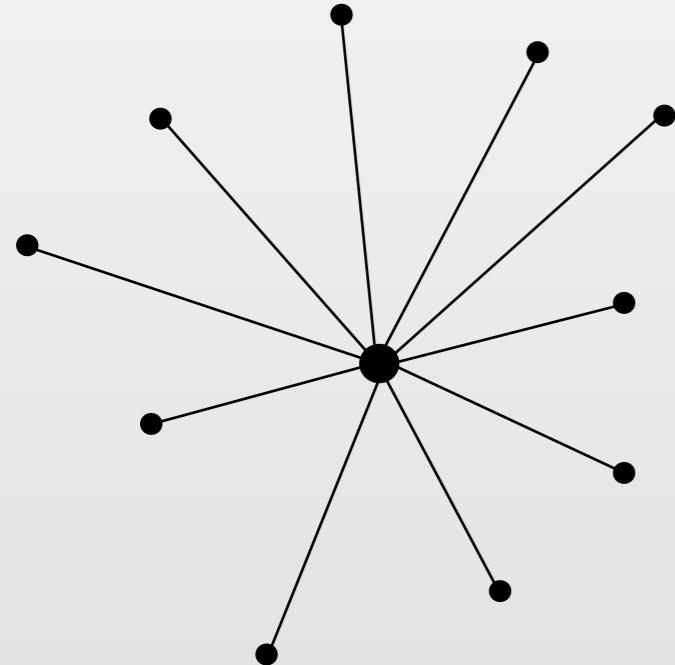


DECENTRALIZATION  
**THE CLOUD**

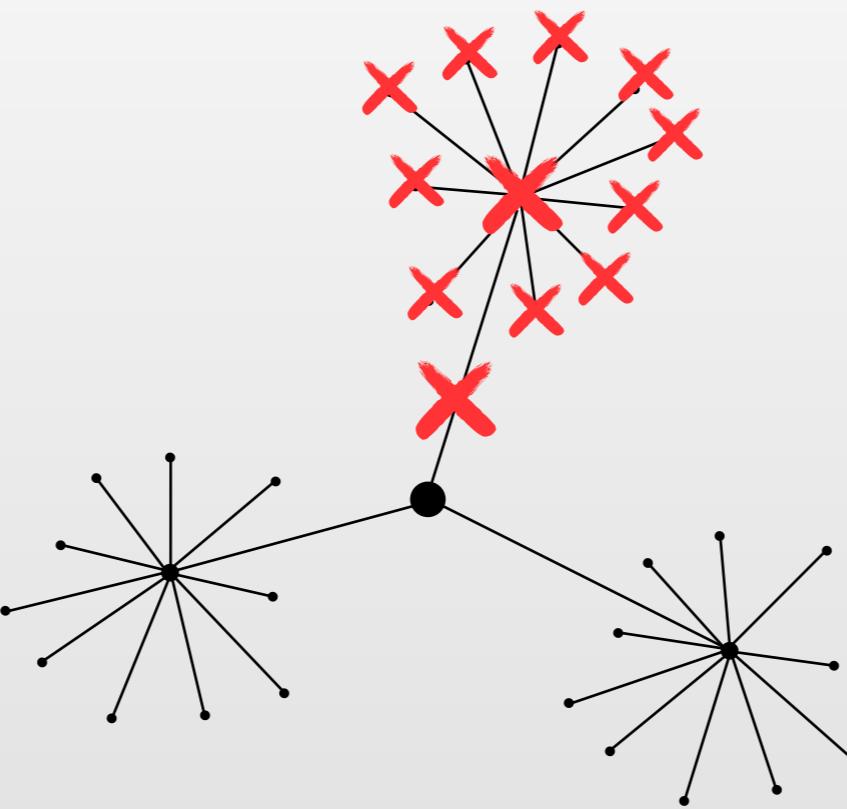


DISTRIBUTION  
**BLOCKCHAINS**

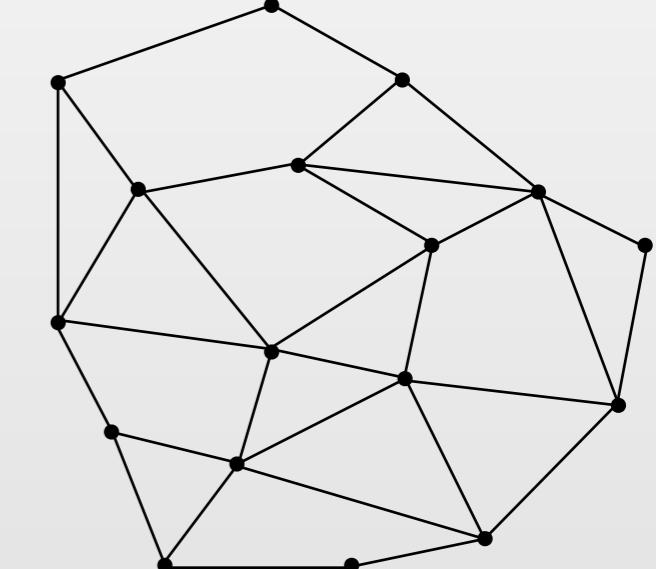
# THE EVOLUTION OF COMPUTER NETWORKS



**CENTRALIZATION**  
**DATABASE**

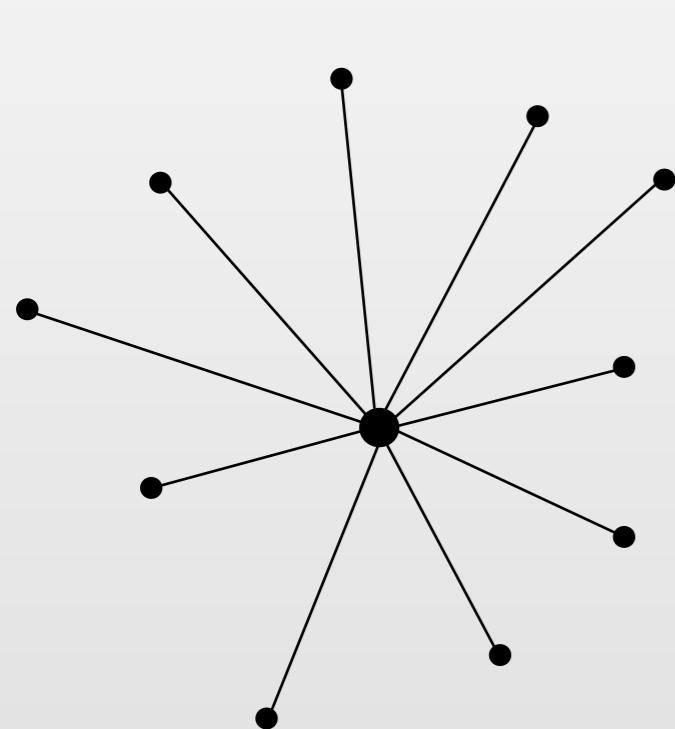


**DECENTRALIZATION**  
**THE CLOUD**

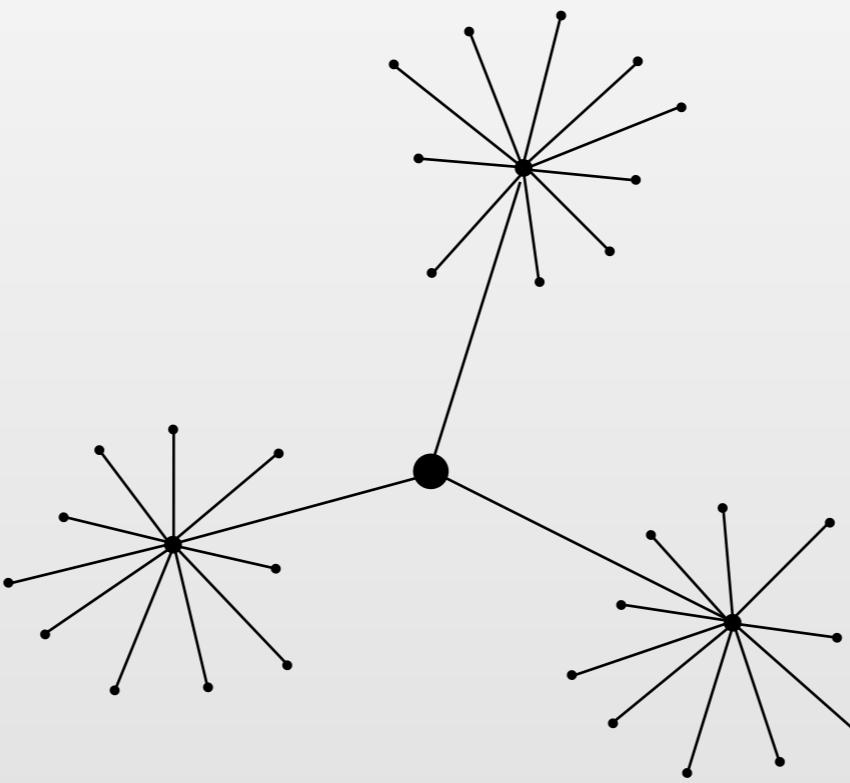


**DISTRIBUTION**  
**BLOCKCHAINS**

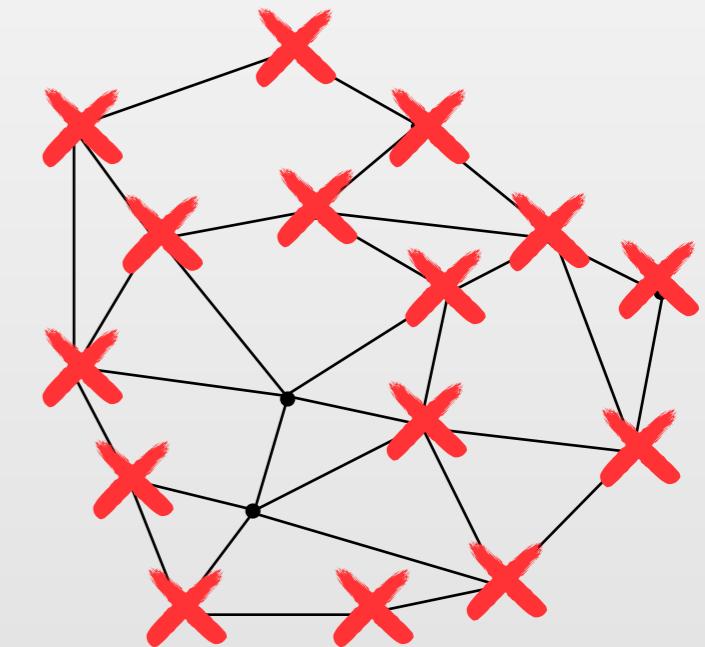
# THE EVOLUTION OF COMPUTER NETWORKS



CENTRALIZATION  
**DATABASE**

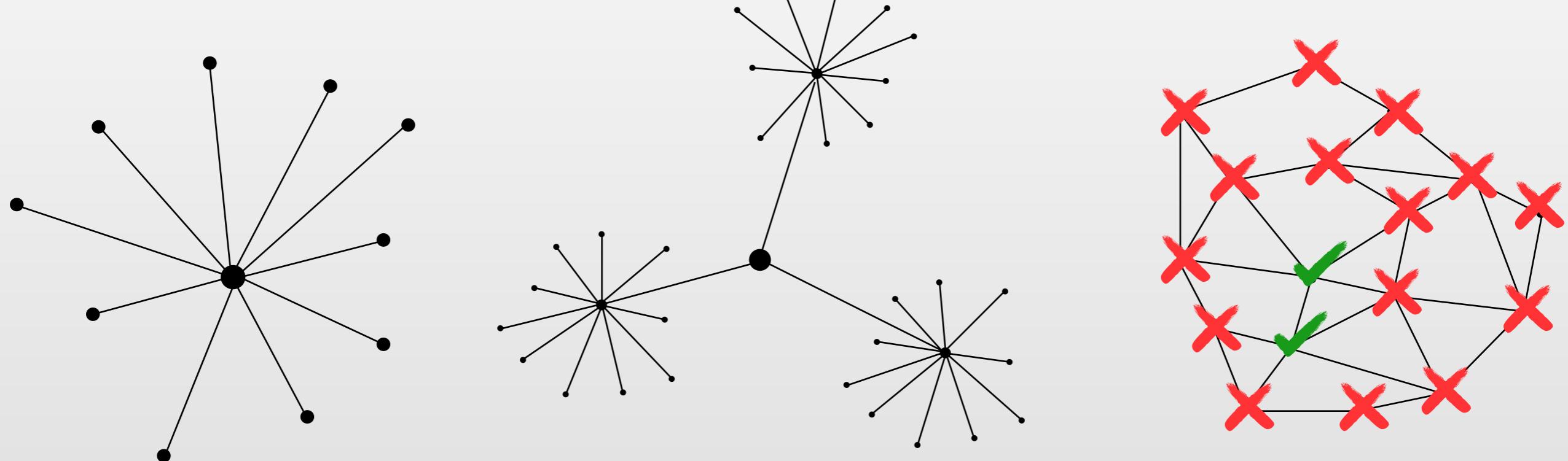


DECENTRALIZATION  
**THE CLOUD**



DISTRIBUTION  
**BLOCKCHAINS**

# THE EVOLUTION OF COMPUTER NETWORKS



**CENTRALIZATION**  
**DATABASE**

**DECENTRALIZATION**  
**THE CLOUD**

**DISTRIBUTION**  
**BLOCKCHAINS**

# BLOCKCHAINS ARE SIMPLY A NETWORK OF NODES

- Each member of the network runs their own node and all nodes are equal
- The blockchain becomes more secure as more nodes join the network
- All transactions across the entire network are tracked by each node
- **There are no actual coins** - there is only a ledger of who owns what
- Cryptographic key-pairs represent accounts and passwords
- On the blockchain - no one knows you're a fridge



**EVERY ACCOUNT IS MERELY A SET OF KEYS**



# EACH “ADDRESS” REQUIRES A PRIVATE KEY TO ACCESS IT



# SOME ADDRESSES EVEN REQUIRE MULTIPLE KEYS



# WHAT'S IN A BITCOIN TRANSACTION?

- Multiple unspent inputs are used in order to form the total value sent
- Cannot send proportions of inputs, must use all and send the change back
- Because a single transaction can send multiple values to multiple outputs
- Fees are based upon the total size (inputs and outputs) rather than value
- Paying these fees is done by forgetting to send some value to someone
- Transaction scripts can contain complex variables (multi-sig & timed locks)



# ALICE CAN'T SEND WHAT SHE DOESN'T HAVE AND BOB WANTS 5

ALICE'S UNSPENT INPUTS

10



3



2



THE TX  
SIGN OUTPUTS

5

4

RELAY HEX TO NETWORK

BOB GETS 5

5

CHANGE MINUS FEE

4

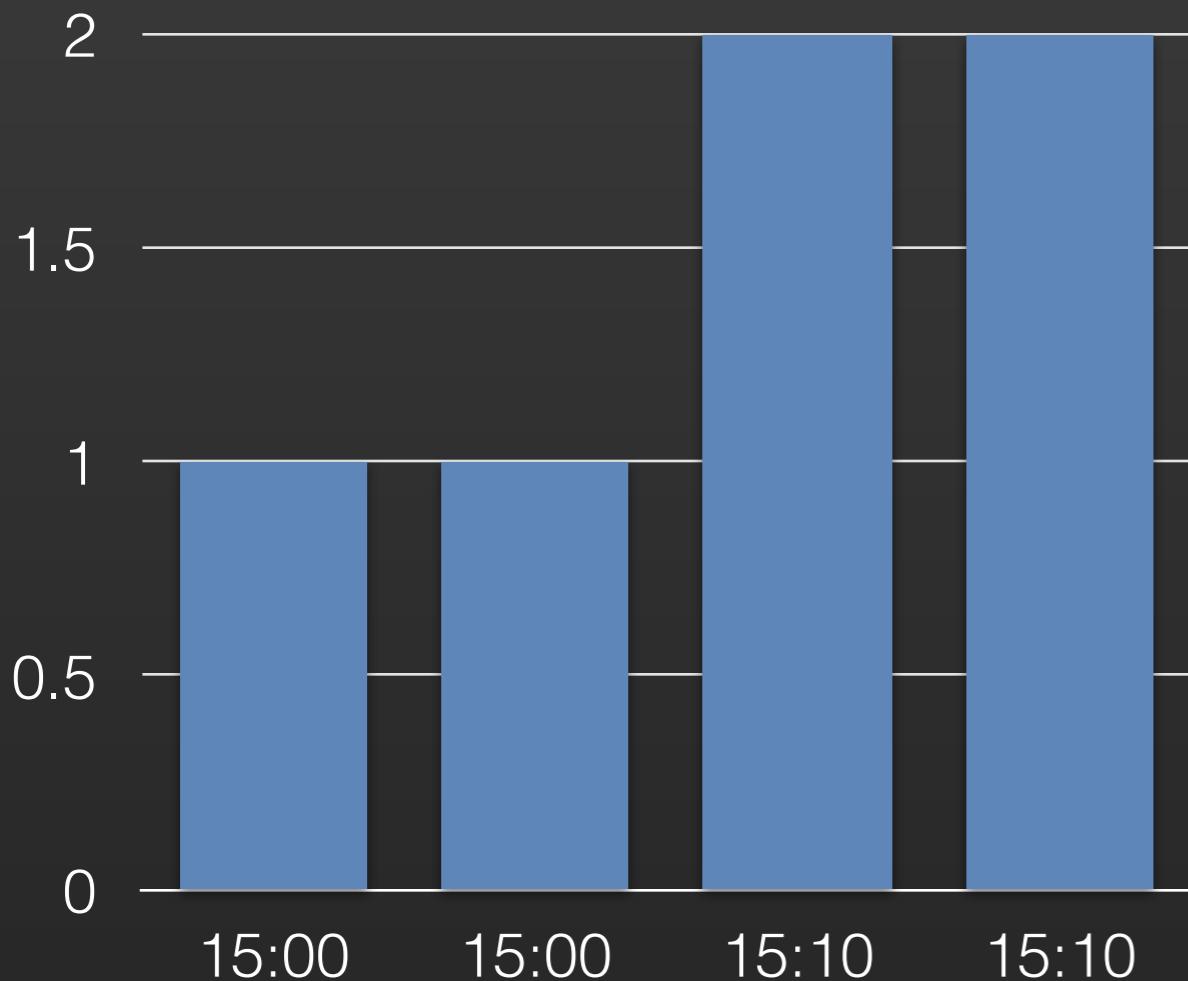
# PUTTING THE BLOCK INTO BLOCKCHAINS

- Transactions are batched into blocks every ten minutes (with Bitcoin)
- The block is added to the chain with a link to the previous block
- With the block added to the chain, its transactions are then confirmed
- As soon as a new block has been added linking to that original block, the transactions from the first block then have 2 confirmations
- It is recommended that large physical transactions wait for 6 confirmations
- Whereas digital downloads may require no confirmations at all

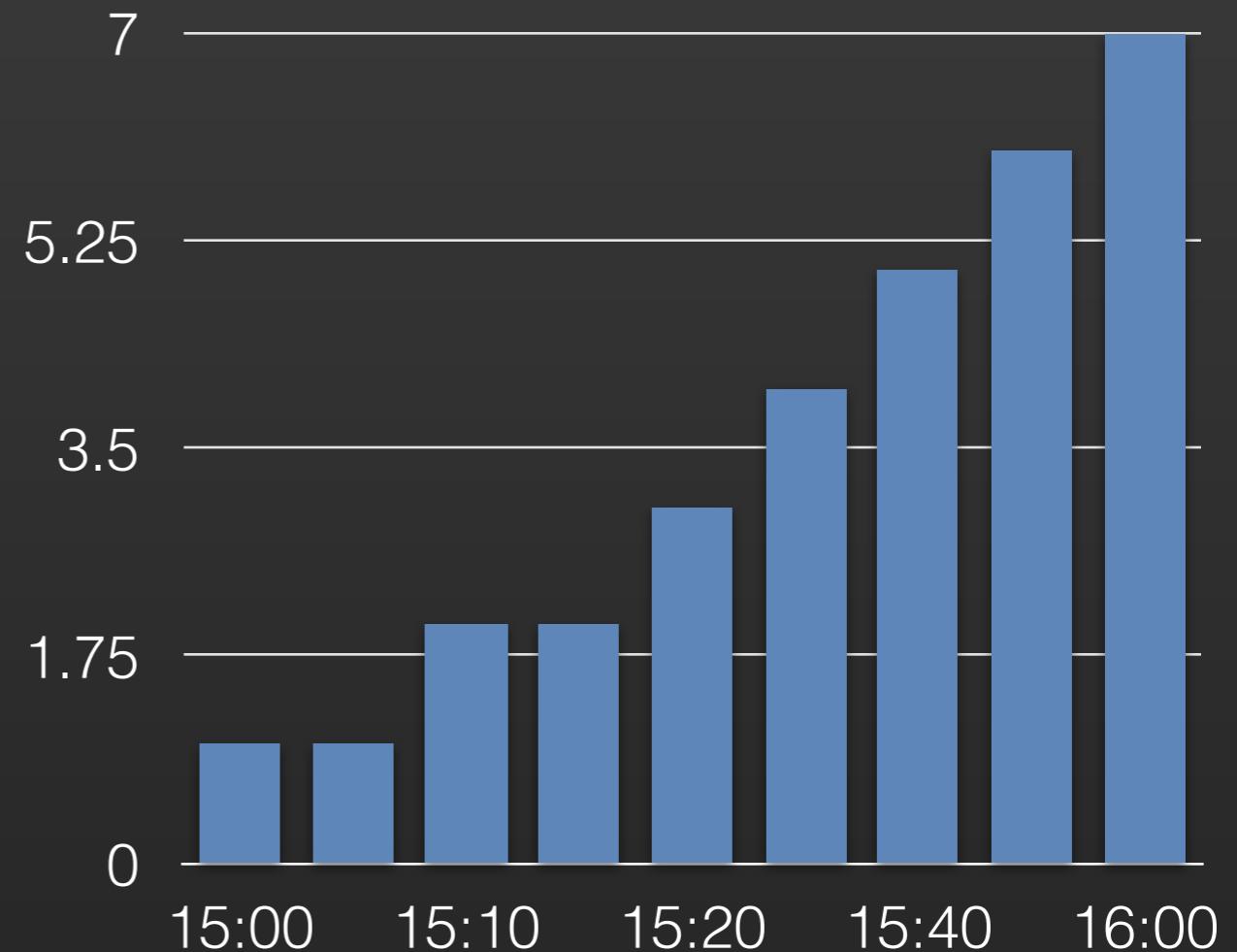


# REALTIME VS TRUTH

Block Heights



Block Heights

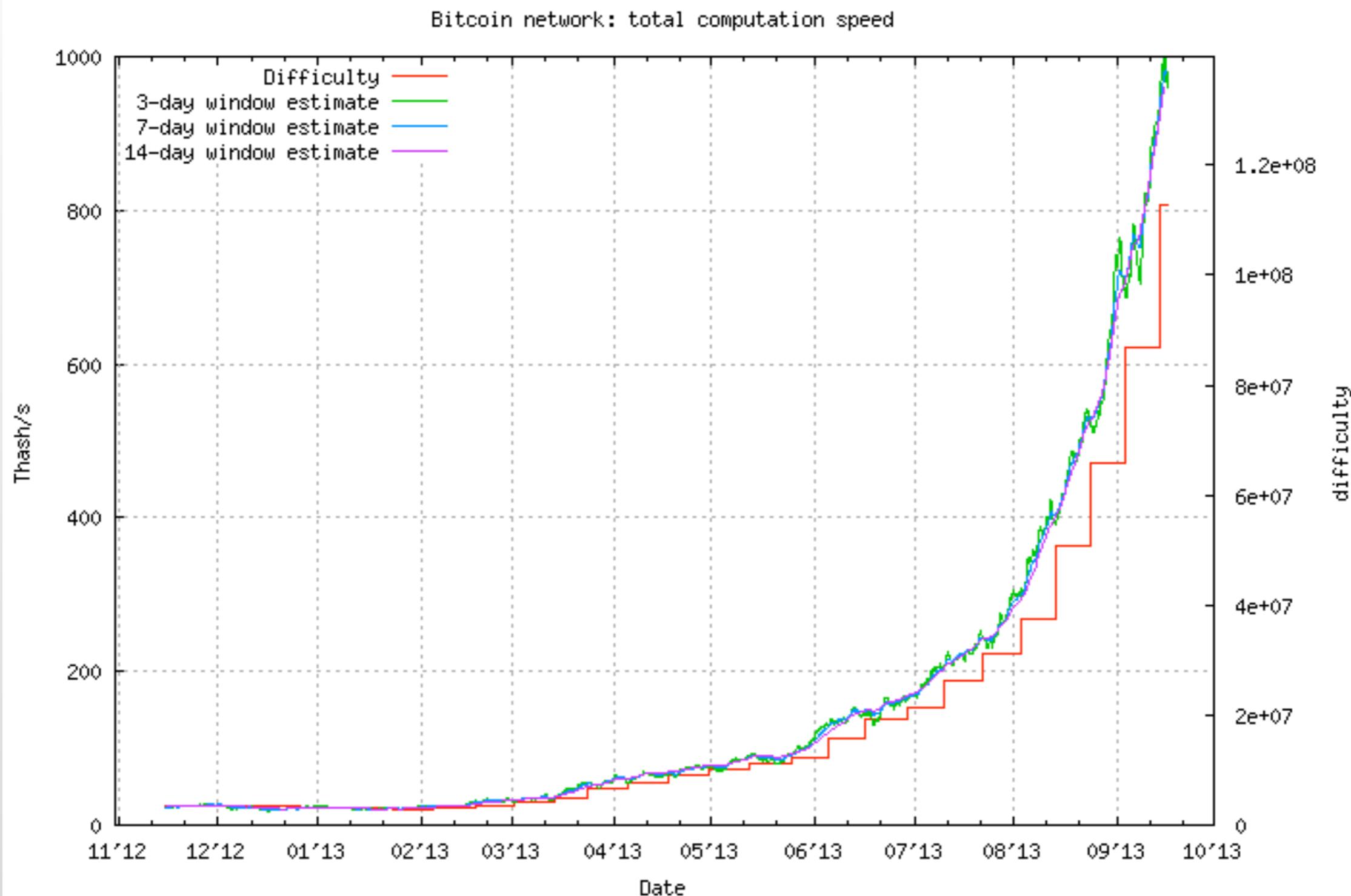


# MINING FOR NUMBERS

- To reach **consensus** as to which node has the right to add the next block to the chain, miners compete in a race to solve cryptographic equations
- Miners gather and in-turn verify unconfirmed transactions into blocks
- They then add a nonce (one use number) to the block and hash it
- If the hash has X number of zeros at the beginning it becomes a valid block
- Otherwise the miners increase the nonce and they hash the block again
- Solving these cryptographic equations is becoming increasingly difficult



# THIS IS THE HASHING POWER OF THE NETWORK IN 2013



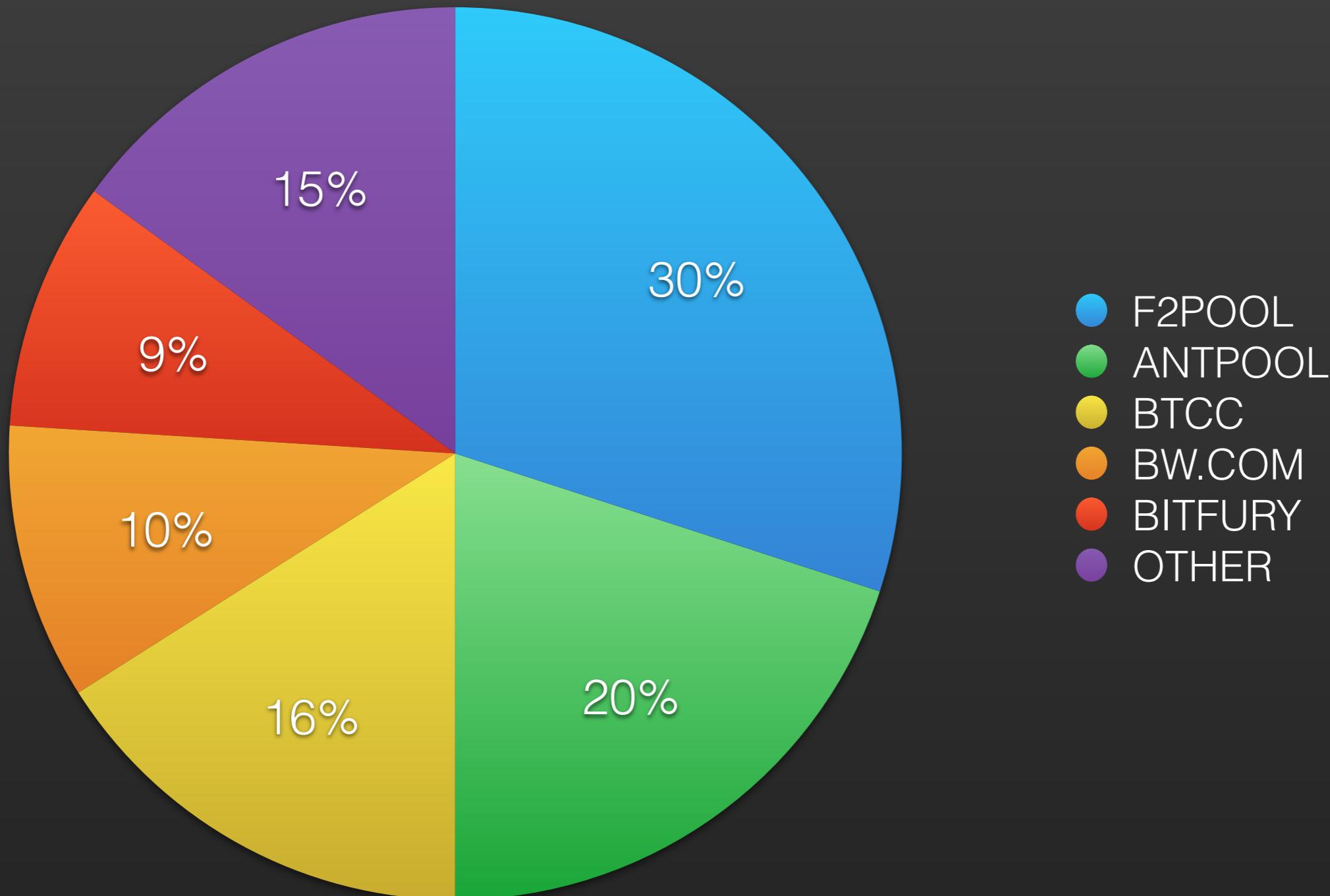


# MINING IS NOW A BILLION DOLLAR BUSINESS

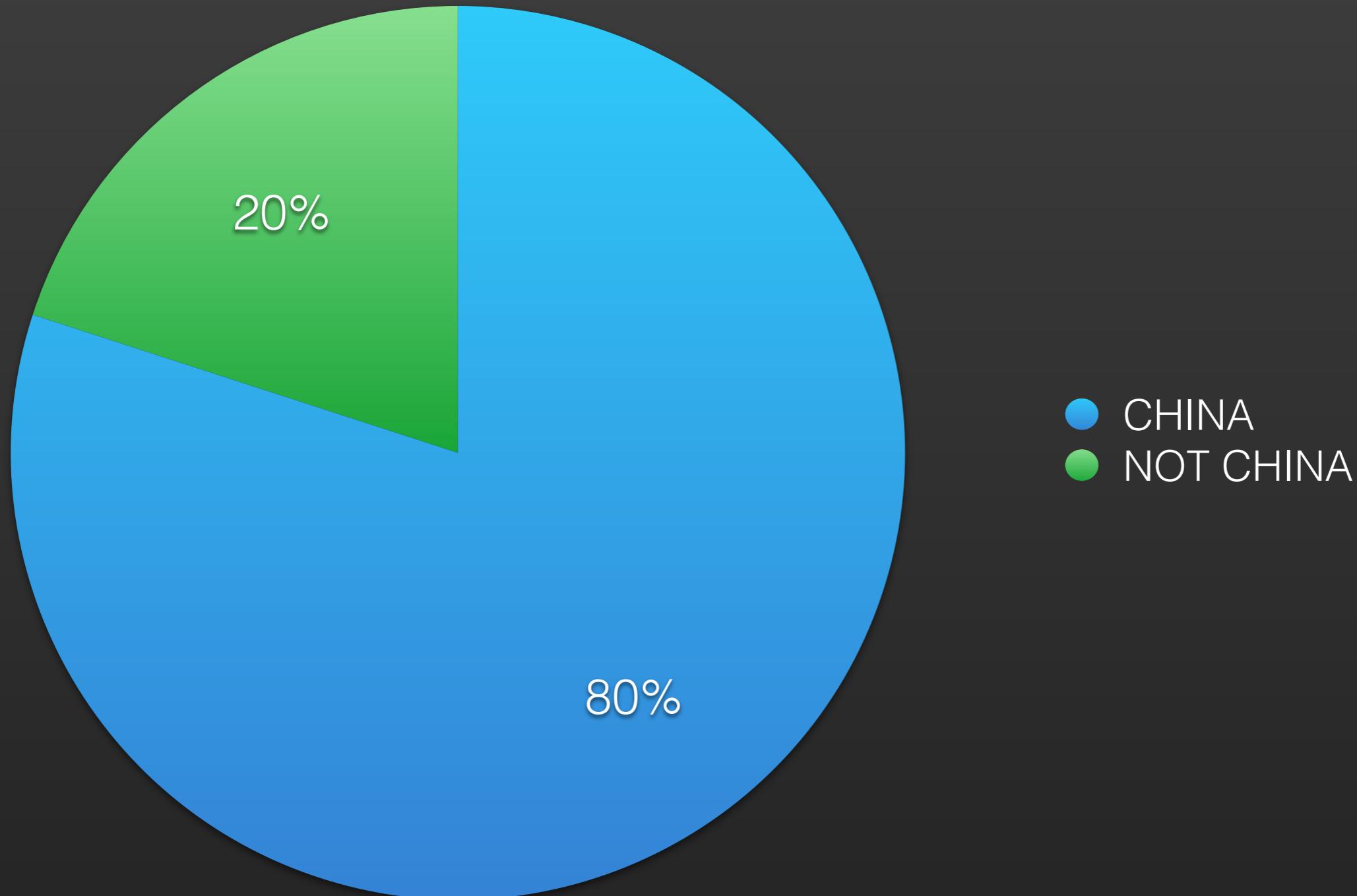




# THE NOT SO DISTRIBUTED ECONOMICS OF MINING



# THE EVEN LESS DISTRIBUTED ECONOMICS OF MINING

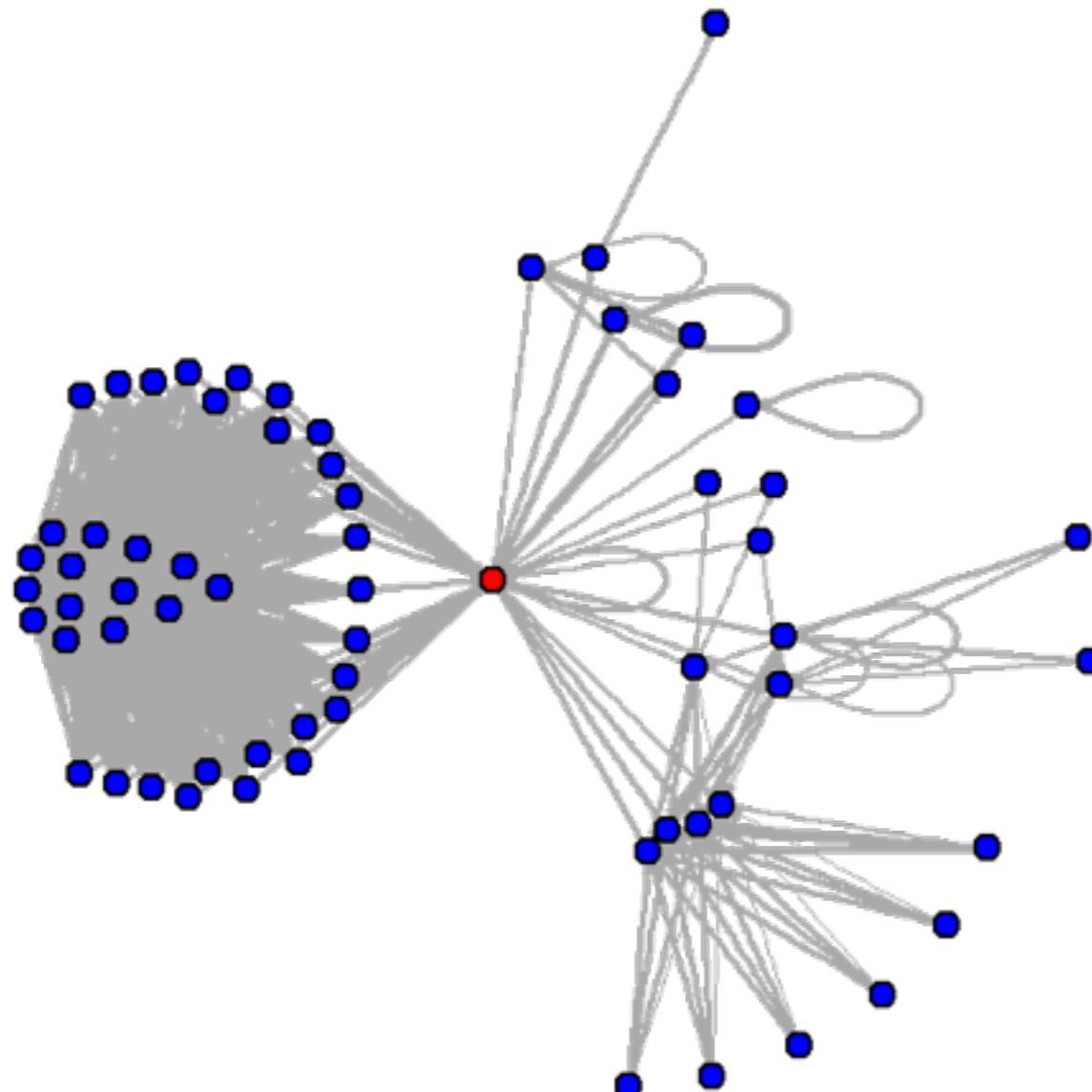


**TRUST IS SOLVED VIA TRANSPARENCY - IT'S OPEN TO ALL**

```
{
  "address": "DEHfgFYKL97gFFoYHM7UejXBGKjLFzD4za",
  "total_received": 1000000000,
  "total_sent": 800000000,
  "balance": 200000000,
  "unconfirmed_balance": 0,
  "final_balance": 200000000,
  "n_tx": 4,
  "unconfirmed_n_tx": 0,
  "final_n_tx": 4,
  "txs": [
    {
      "block_hash": "e9a38d8fa6b7abc1a35a2fad93bfa52e3eb9b1ca5cb2825692db0a3c2f054354",
      "block_height": 1213596,
      "block_index": 35,
      "hash": "3ebaecf042e0dbe20a35c0dd2700c83b13a5a1764e1882c2cc39e4bd81c326cf",
      "addresses": [
        "DEHfgFYKL97gFFoYHM7UejXBGKjLFzD4za",
        "DJHXpkQGcRydRvocWaeUtZir6c2pXHkUn4"
      ],
      "total": 400000000,
      "fees": 100000000,
      "size": 225,
      "preference": "high",
      "relayed_by": "",
      "confirmed": "2016-05-16T14:13:56Z",
      "received": "2016-05-16T14:13:56Z",
      "ver": 1,
      "lock_time": 0,
      "double_spend": false,
      "vin_sz": 1,
      "vout_sz": 2,
      "confirmations": 6935,
      "confidence": 1,
      "inputs": [
        {
          "prev_hash": "1d651b5efc33ff6d7f3b8ba32ce7260a631b0506d13f760753b6528de7091486"
        }
      ]
    }
  ]
}
```

**EVERYONE HAS A RECORD OF EVERYTHING - SO BE CAREFUL**

BTC transaction network for  
**1NfRMkhm5vjizzqkp2Qb28N7geRQCa4XqC**



## REGULATION - THE SIMPLE VERSION

---

BITCOIN IS BAD  
BLOCKCHAINS ARE GOOD

# REGULATION - THE COMPLEX VERSION

- Primary place for regulation is when exchanging cash for crypto-currency
- No regulation published regarding the underlying blockchain technologies
- Bank Negara have stated it is not legal tender and used at consumer's risk
- The same can be said of US Dollars, Gold, Silver, Diamonds and Plutonium
- The US court recently labelled it property in context of a divorce settlement
- In China, individuals can hold and trade Bitcoin but banks and FIs cannot
- In Germany, Bitcoin are legally binding financial instruments
- The Australian Securities Exchange have heavily invested in blockchains
- Japan have recently legalized and begun adopting at banks & exchanges

### SECTION 03

BITCOIN ISN'T EVERYTHING

BILLIONS INVESTED IN BLOCKCHAINS

# BANKS ARE MOVING FAST DUE TO ECOSYSTEM MATURITY

As of January 2016, more than 60 banks and leading financial institutions have made statements confirming that they are actively working on blockchain projects.



# BLOCKTECH in FINANCIAL SERVICES Landscape

## APPLICATIONS & SOLUTIONS



## MIDDLEWARE & SERVICES



## INFRASTRUCTURE & BASE PROTOCOLS



# SOME OF THE INSTITUTIONS LEADING THE WAY



Custom blockchain  
for settlements



Standard  
Chartered



Blockchain based  
trade finance platform

Blockchain based  
loyalty platform

Blockchain based  
remittance platform



multiple blockchains for cross-  
border payments and loyalty

Deutsche Bank



Exploring KYC and AML  
via the blockchains



Patented a blockchain  
based wire transfer system



NASDAQ®

IBM

# STOCK EXCHANGES ARE QUICKLY CATCHING-ON TOO

## Australian Stock Exchange Confirms Upcoming Blockchain For Settlements

© 22/01/2016     Samburaj Das     0

 Bitcoin Technology, Blockchain News, FinTech News, News

# KOREA ARE BUILDING PROTOTYPES TOO



**Korean Securities Exchange is Building Blockchain Trading Platform**

⌚ 01/03/2016 💬 0

≡ Bitcoin & Blockchain Investments, Bitcoin Technology, Blockchain News, News

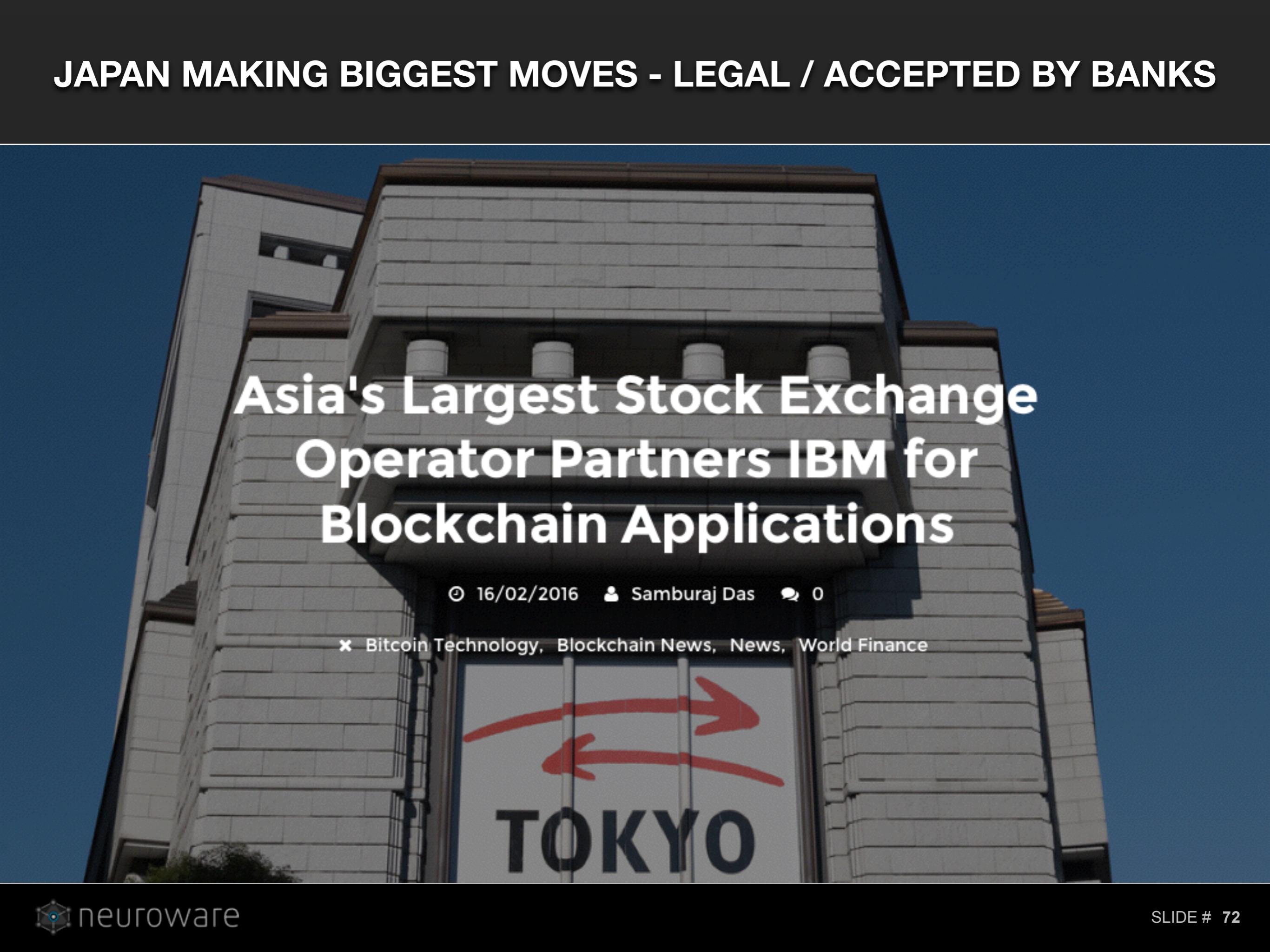
# HONG KONG WERE QUICK TO FOLLOW

## Hong Kong Bitcoin Exchange ANX Touts ‘Easy As Email’ Blockchain Service

© 17/05/2016 • Elliot Maras • 0

≡ Blockchain News, FinTech News, News

# JAPAN MAKING BIGGEST MOVES - LEGAL / ACCEPTED BY BANKS



**Asia's Largest Stock Exchange  
Operator Partners IBM for  
Blockchain Applications**

⌚ 16/02/2016 🚩 Samburaj Das 💬 0

✖ Bitcoin Technology, Blockchain News, News, World Finance



# IMITATION IS THE BEST FORM OF FLATTERY



- 1st Generation of Alt-Coins forked each other with minor tweaks
- Basic breakout alt-coin successes included Litecoin and Dogecoin
- Dash (previously known as DarkCoin) worth noting due to governance
- See the Malaysian-Based **CoinGecko** for a better list!

# BLOCKCHAIN 2.0 - BUILT FROM SCRATCH

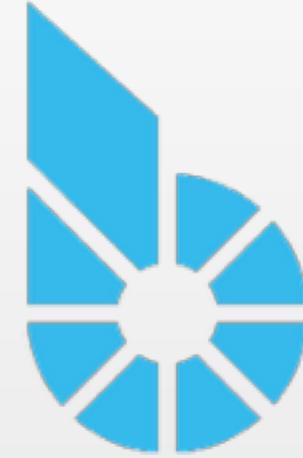


**RIPPLE\***



NXT GENERATION  
OF CRYPTOCURRENCY

**NXT**



**BITSHARES**

- Ripple has most interest from banks due to their pre-mined walled-garden
- NXT is the most realized (fully-featured) of all the ambitious projects
- Bitshares coined the phrase DACs (distributed autonomous corporations)
- We now have a blockchain for everything from songs to logistics & coffee

\* Not an actual blockchain

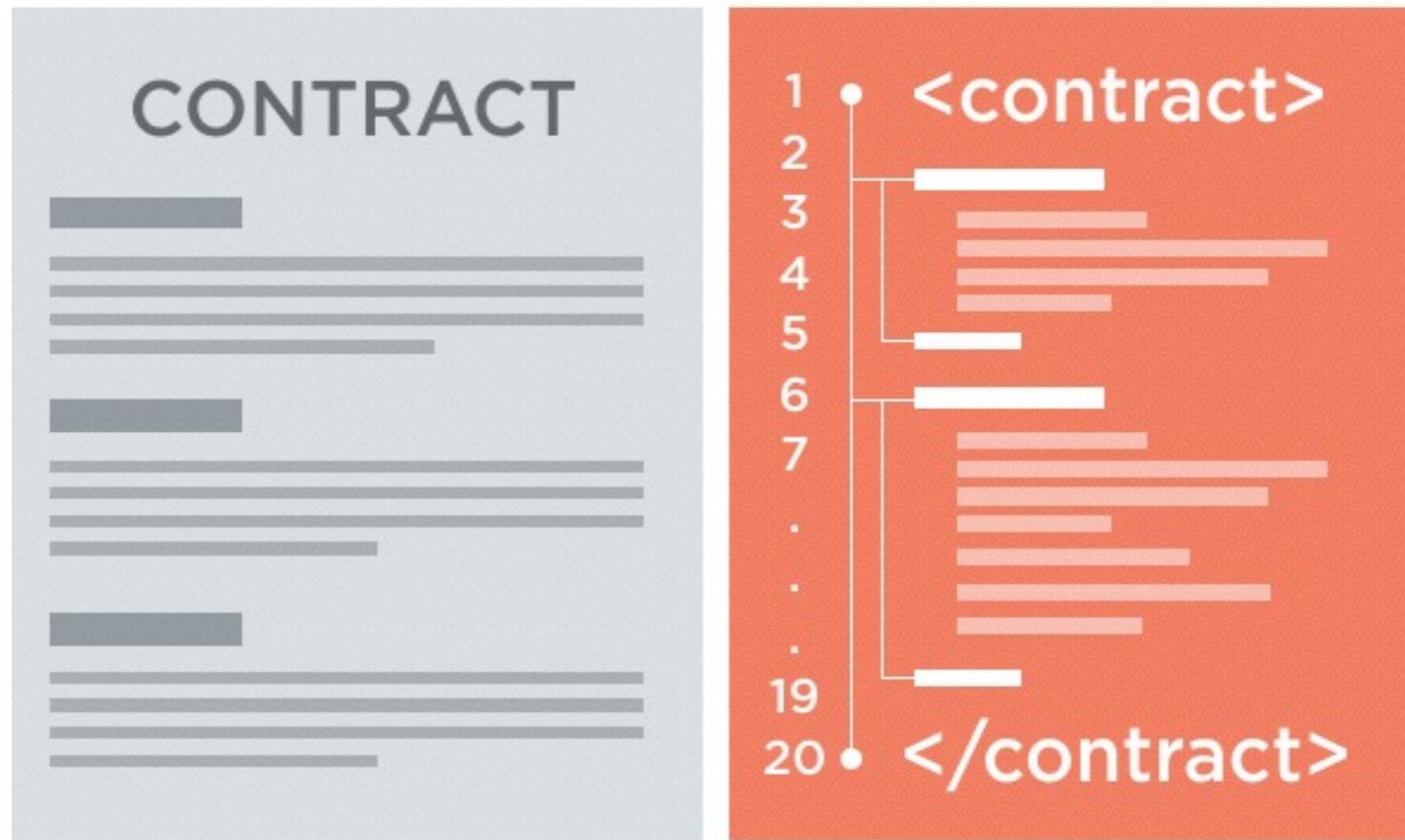
# ETHEREUM TAKES THINGS ONE STEP FURTHER



## THE WORLD'S SUPER COMPUTER...?

- Raised US\$15 Million in crowd-funding when launching their Ether currency
- Aiming to be the first turing complete blockchain, they have almost achieved it
- Heavily supported by Microsoft & also being used by IBM for their IoT platform
- Recently raised US\$150 Million in crowd-funding their own venture fund
- However, the more moving parts a system has - the more likely it is to break

# SMART CONTRACTS ARE EVERYWHERE



- Even Bitcoin utilizes basic smart contracts (with over 100 script functions)
- Smart contracts are snippets of code stored and executed by the network
- They can perform transactional based events if defined conditions are met

# WHAT'S REALLY IN A TRANSACTION?

CO-FOUND... BLOCKSTR... Blockstrap msmalley/f... Everstore ATA-Plus A... Legality of ... bitcoin tran... mining bitc... Mining Bitcoin i... BlockAuth http://...0fd21

api.blockcypher.com/v1/btc/test3/txs/235a88e9853c1c116ef47f795f13ce200c2e1bf37667e99973e1c829f95t

bitcoin transaction script

```
{ "block_hash": "00000000009f30c59abf2f8556c0949c79b54764f4cbb223ca43527394d3ee2f", "block_height": 847281, "block_index": 24, "hash": "235a88e9853c1c116ef47f795f13ce200c2e1bf37667e99973e1c829f95b95f7", "addresses": [ "mpNENnsFcL8a5hPxwfPrYPkZqAkbbFpxLF", "mq7tNFrbi3E3fsuUbsTsA7keoeYL6gYzv2" ], "total": 86124000, "fees": 10000, "size": 339, "preference": "medium", "relayed_by": "", "confirmed": "2016-05-16T07:51:20Z", "received": "2016-05-16T07:51:20Z", "ver": 1, "lock_time": 0, "double_spend": false, "vin_sz": 2, "vout_sz": 1, "confirmations": 19557, "confidence": 1, "inputs": [ { "prev_hash": "bb4cef4d48dba1916c73552342b660be00535c43ad47462abf43a402cc2a61a1", "script": "4730440220618bd76a683d2603edb570e66b851f85dd594abd7a3c25a2b29064b01695907502201edeac4cd777e04a393cf1bca0d7ba5916e3fc8c67efa33268a936bf96b9a7e012103530d0cbdfcd448b8d96ac9c1cbdc88a2f60e05a7f16e7ab321185afb0523e9fc", "sequence": 4294967295, "addresses": [ "mpNENnsFcL8a5hPxwfPrYPkZqAkbbFpxLF" ], "script_type": "pay-to-pubkey-hash" }, { "prev_hash": "42662b2544a7f59a1abd004a8e15c714f108f553f1dd3f0617982eb5b8ac468c", "script": "483045022100f7ab281bcb605550098f62a097b6dbef79a9f35261aae9dc01aec54a08e8212b02201261b2d0f44545a551fe54f1777597e747523f0a66b7cf74521828c67f23887012103530d0cbdfcd448b8d96ac9c1cbdc88a2f60e05a7f16e7ab321185afb0523e9fc", "output_value": 7555000, "sequence": 4294967295, "addresses": [ "mpNENnsFcL8a5hPxwfPrYPkZqAkbbFpxLF" ], "script_type": "pay-to-pubkey-hash" } ], "outputs": [ { "value": 86124000, "script": "76a914695469844938fd58e5cf59987f4cc063d4d657a788ac", "addresses": [ "mq7tNFrbi3E3fsuUbsTsA7keoeYL6gYzv2" ] } ] }
```

# DECODING SCRIPT HEXES

- 80% of transactions are known as **standard transactions**
  - OP\_DUP OP\_HASH160 <pubKeyHash> OP\_EQUALVERIFY OP\_CHECKSIG
- Approximately 1% of transactions contain **OP>Returns**
  - OP\_RETURN <hexedData> - can you find Gandhi?
- There are even a few hidden puzzles on the blockchain...

OP\_HASH256

6fe28c0ab6f1b372c1a6a246ae63f74f931e8365e15a089c68d6190000000000

OP\_EQUAL

# ETHEREUM TAKES THINGS ONE STEP FURTHER

```
contract MyToken {
```

```
    /* Public variables of the token */
    string public standard = 'Token 0.1';
    string public name;
    string public symbol;
    uint8 public decimals;
    uint256 public totalSupply;
```

```
    /* Allow interface to create tokens */
    function MyToken( ... )
```

```
    /* Send coins */
    function transfer( ... )
```

```
    /* Allow another contract to spend some tokens in your behalf */
    function approveAndCall( ... )
```

```
    /* A contract attempts to get the coins */
    function transferFrom( ... )
```

```
}
```

# CURRENCIES CAN BE MANY THINGS - EVEN VOTING RIGHTS

- Symbol = %
- Decimals = 2
- Name = Equity

Contracts can also be linked, which allows governance contracts (DAOs) to then be able to vote and control upon custom currency transfers...

# THE DAO - LARGEST CROWDFUNDING INITIATIVE EVER

The time has come to breathe life into The DAO  
A One Time Only Event

1123.85 M

DAO TOKENS CREATED

11.35 M

TOTAL ETH

151.67 M

USD EQUIVALENT

1.30

CURRENT RATE  
ETH / 100 DAO TOKENS

5 hours

NEXT PRICE PHASE

7 days

LEFT  
ENDS 28 MAY 09:00 GMT



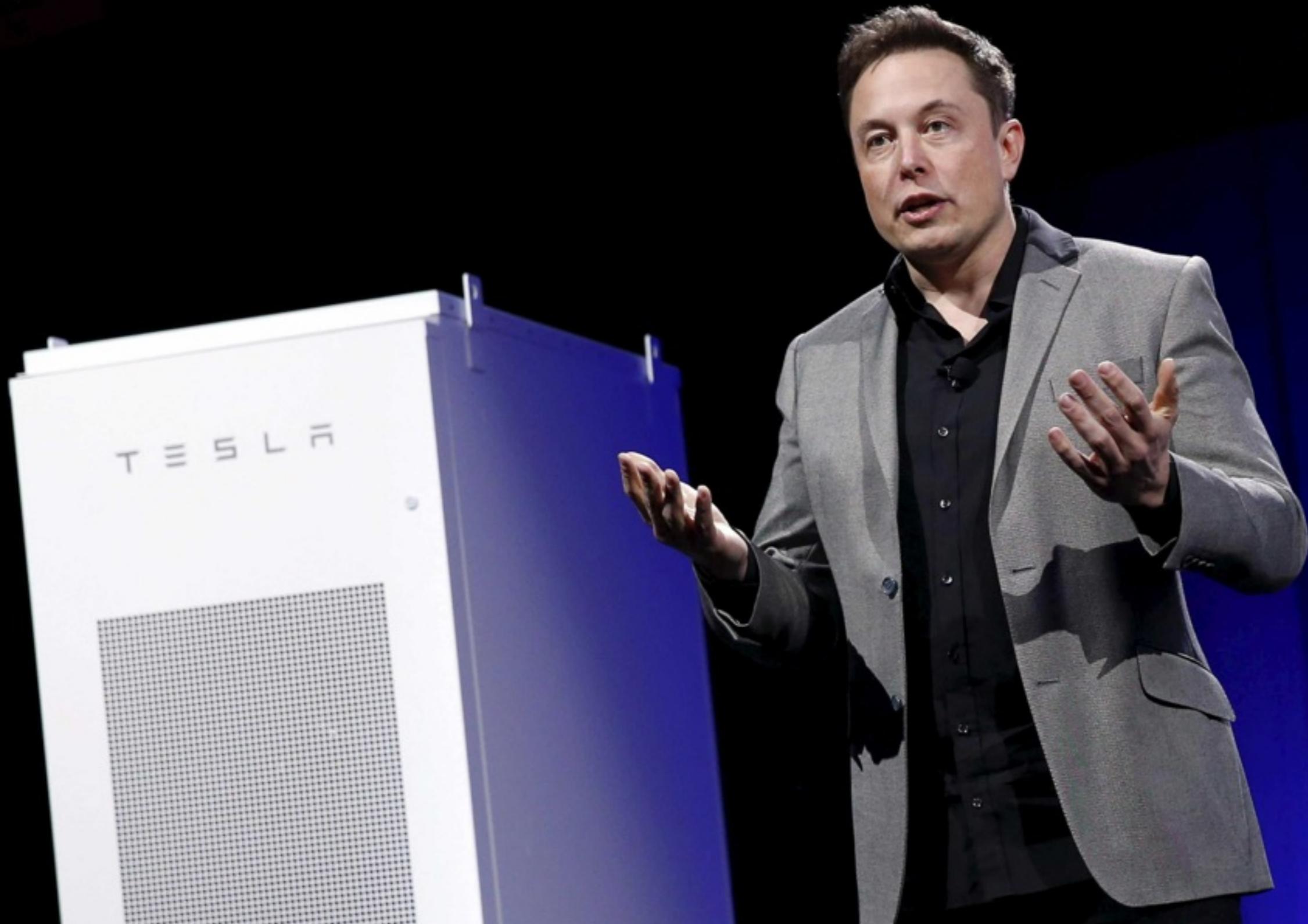
# WHAT'S THE DIFFERENCE BETWEEN PUBLIC & PRIVATE CHAINS?



# COULD ENERGY BE THE GLOBAL RESERVE OF THE FUTURE?



# COULD ENERGY BE THE GLOBAL RESERVE OF THE FUTURE?



# COULD ENERGY BE THE GLOBAL RESERVE OF THE FUTURE?



# COULD ENERGY BE THE GLOBAL RESERVE OF THE FUTURE?



## **SECTION 04**

# **THE BANKS OF THE FUTURE HAVE ZERO EMPLOYEES**

# BANKING ON THE FUTURE OF BLOCKCHAINS

- With banks already KYC and AWL compliant, there are no entities more suited to be offering digital currency brokerage and key management
- With the advent of smart-contracts, banking becomes a sequence of code
- Regulation and compliance would be designed as part of the protocol
- If retail and commercial banking processes were 100% based upon blockchains, staffing requirements could be reduced by at least 90%
- Existing internal infrastructure can be replaced by distributed protocols



# 2ND PLACE WINNER OF THE DBS BLOCKCHAIN HACKATHON

The image shows a hand holding a white smartphone displaying the HyperBank mobile application. The app's interface includes a header with the 'hyperbank' logo and a user profile for 'Tristan Gomez'. Below this are two main sections: 'Monthly Accounts' (12) and 'Monthly Transactions' (128) on top, and 'Total Accounts' (28) and 'Total Transactions' (1,286) on the bottom. A transaction history section follows, showing three entries: '2 Hours Ago - New Account Manuel Rigardo', '18 Hours Ago - TX Jarvis Silo to Manuel Rigardo', and '1 Day Ago - New Account Jarvis Silo'. At the bottom are five navigation icons. To the right of the phone is a laptop screen displaying the HyperBank website with the tagline 'hyperlocal banking for the unbanked'. It features a text input field for 'enter your email for updates or application for beta access' and a yellow 'APPLY' button. The background of the slide is a blue textured pattern.

The application that was previously known as NuBank won 2nd place at the recent [DBS Hackathon](#) in Singapore and is now HyperBank.

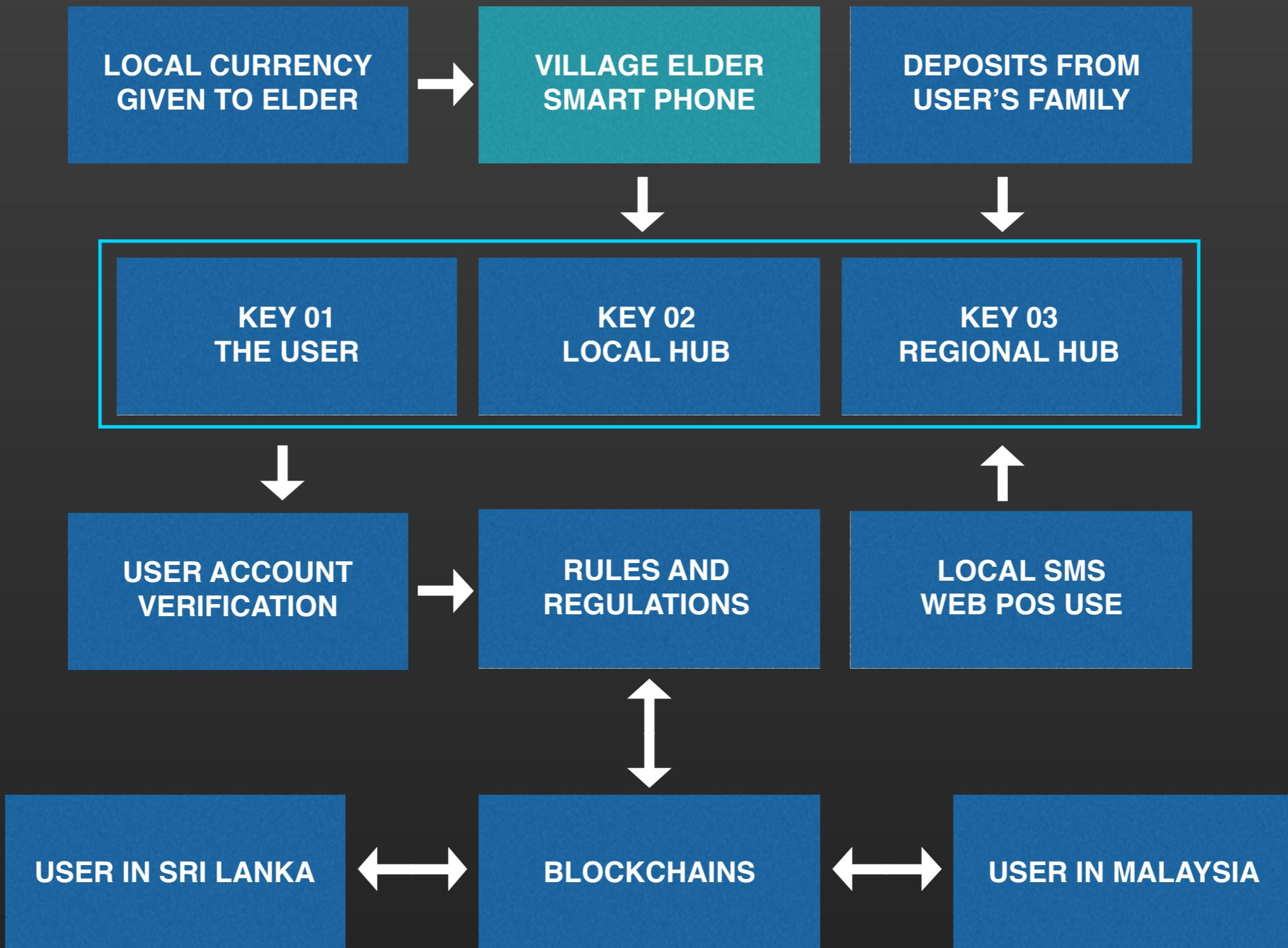
We utilize the blockchains in order to provide a secure and fully auditable digital trail of transactions but avoid volatility by keeping transfers at fixed local currencies with multi-signature signing from top-tier institutional financial partners.

Consumers communicate using standard SMS functionality directly with their village elders who then use their smartphones to record and relay transactions to the blockchain - providing fully distributed M-Pesa functionality.

# PROVIDING HYPERLOCAL BANKING TO THE UNBANKED

- One village elder with smart-phone creates and verifies accounts locally
- Multi-signature keys provided to elder, account owner and regional hub
- Regional hubs could be traditional banks - acting as arbitrators for disputes
- Deposits can be made in any currency accepted both locally or regionally
- Local users transfer directly via local hubs or internationally via regional hub
- Standard SMS can be used to transfer funds and make direct payments
- Web-based technology can be utilized by other inter-network participants

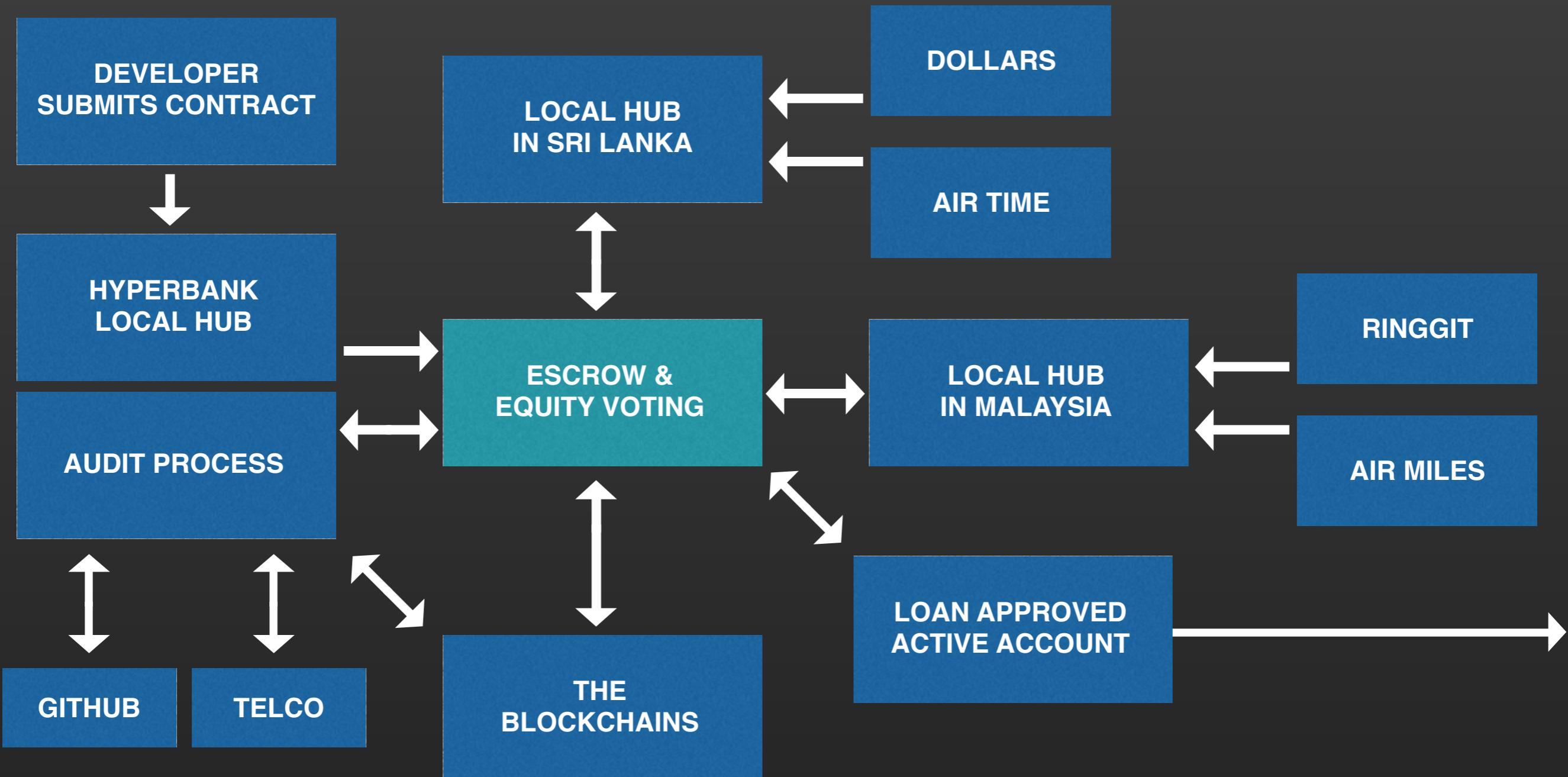
# USE CASE 01 - HYPERLOCAL BANKING IN A GLOBAL WORLD



# DEVELOPER APPLIES FOR A LOAN TO START A BUSINESS

- The developer applies for a business loan via his local HyperBank hub
- His past personal banking and app development history is auto-assessed
- His application process creates temporary contract for global review
- Global hubs review and auto-invest from their regional deposits
- Deposits can be made with any interconnected network currency or service
- New distributed organization created with all shares belonging to developer
- Deposited funds are then allocated to the specific vendor escrow accounts

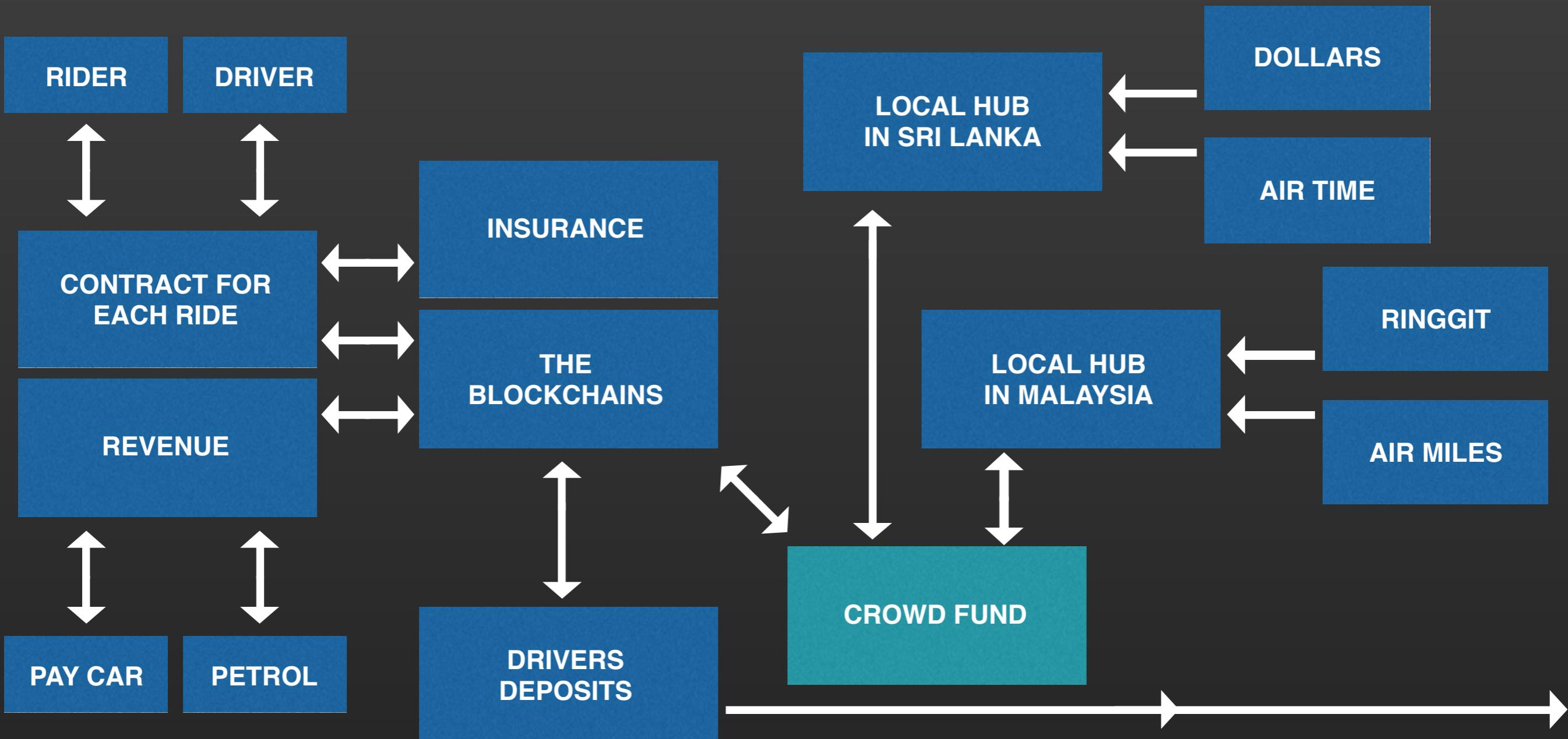
# USE CASE 02 - GLOBAL LOANS VIA LOCAL HYPERBANK HUBS



# FUNDING A SELF-MANAGED UBER-LIKE SERVICE

- After building the prototype, developer and team start equity crowd-fund
- Investments can be made with any network currency - even air miles work
- Investment received and equity now allocated between partners & team
- Audited code and configured contracts are then added to blockchains
- Changes require majority of votes and profits are automatically allocated
- Passengers pay drivers directly, with insurance & tax payments automated
- Car repayments & pre-paid petrol are automatically funded per passenger

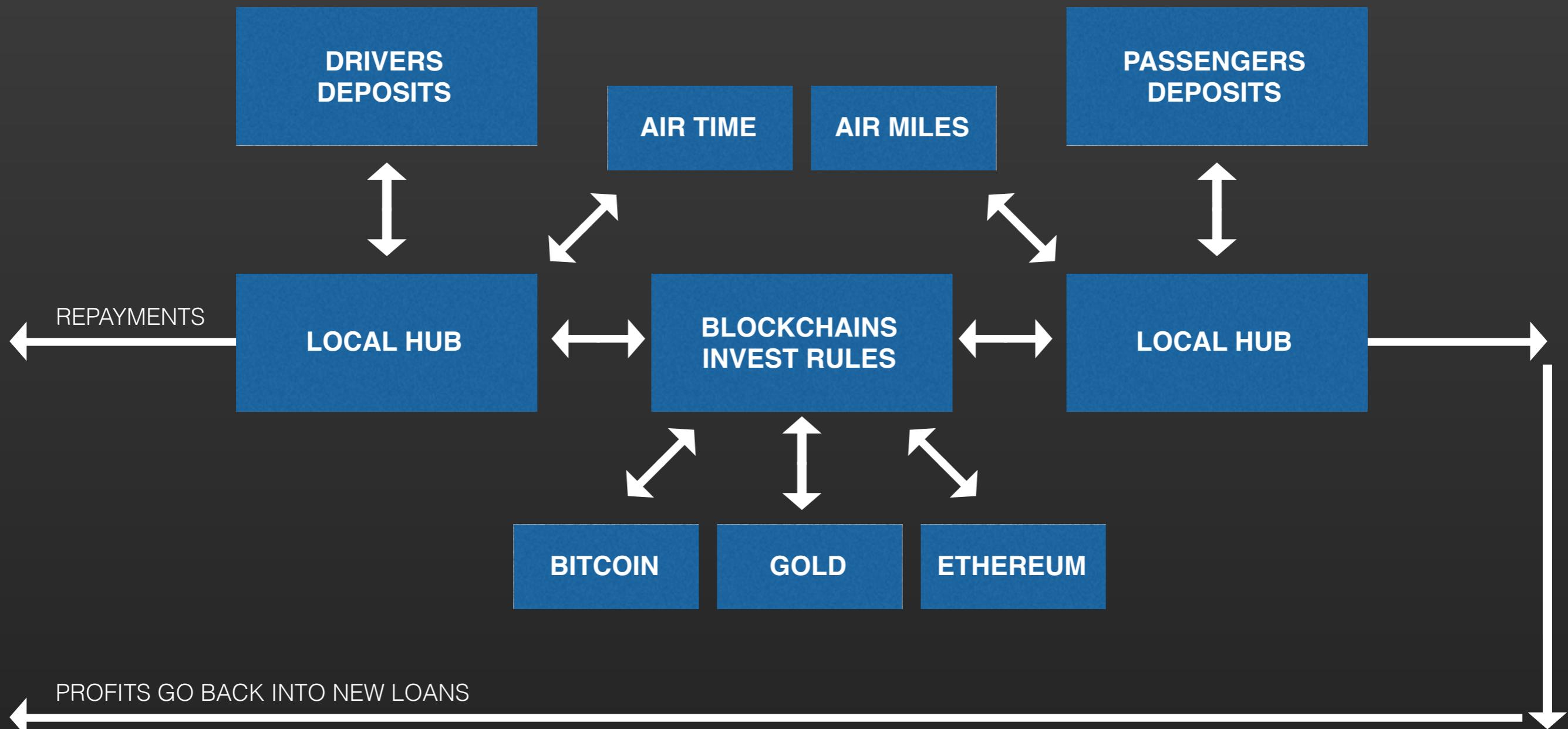
# USE CASE 03 - CROWD-FUNDING AUTOMATED ACCOUNTING



# EARNINGS INCREASED BY DISTRIBUTED INVESTMENT ACCOUNTS

- Drivers can increase earnings by leaving deposits to auto-invest themselves
- Passengers can earn free rides by pre-paying and auto-investing deposits
- Passengers can pay using any currencies or value from investment portfolio
- HyperBank network is automatically re-paid via incoming company revenue
- Equity owners are automatically paid dividends based on company profits
- Both passengers and drivers are part of the same global reputation system
- Inescapable audit trail of every aspect of every component of the business

# USE CASE 04 - AUTO-INVESTING INTO GLOBAL ARBITRAGE



# REASONS TO USE BLOCKCHAINS FOR EQUITY CROWDFUNDING

- Introduce programmable contracts for equity ownership and transfer
- Multi-signature arbitration and escrow with every transactional record
- Instant authorized settlement of deposits & withdrawals in digital currencies
- Optional introduction of localized dollar-to-digital token or national reserve
- Interconnect with other networks to develop a global secondary market
- **Create a tamper-proof audit-trail of every event within the network**



# INTRODUCING THE NOTION OF NODE TYPES

## PARTNER NODES

THESE DO THE HEAVY LIFTING

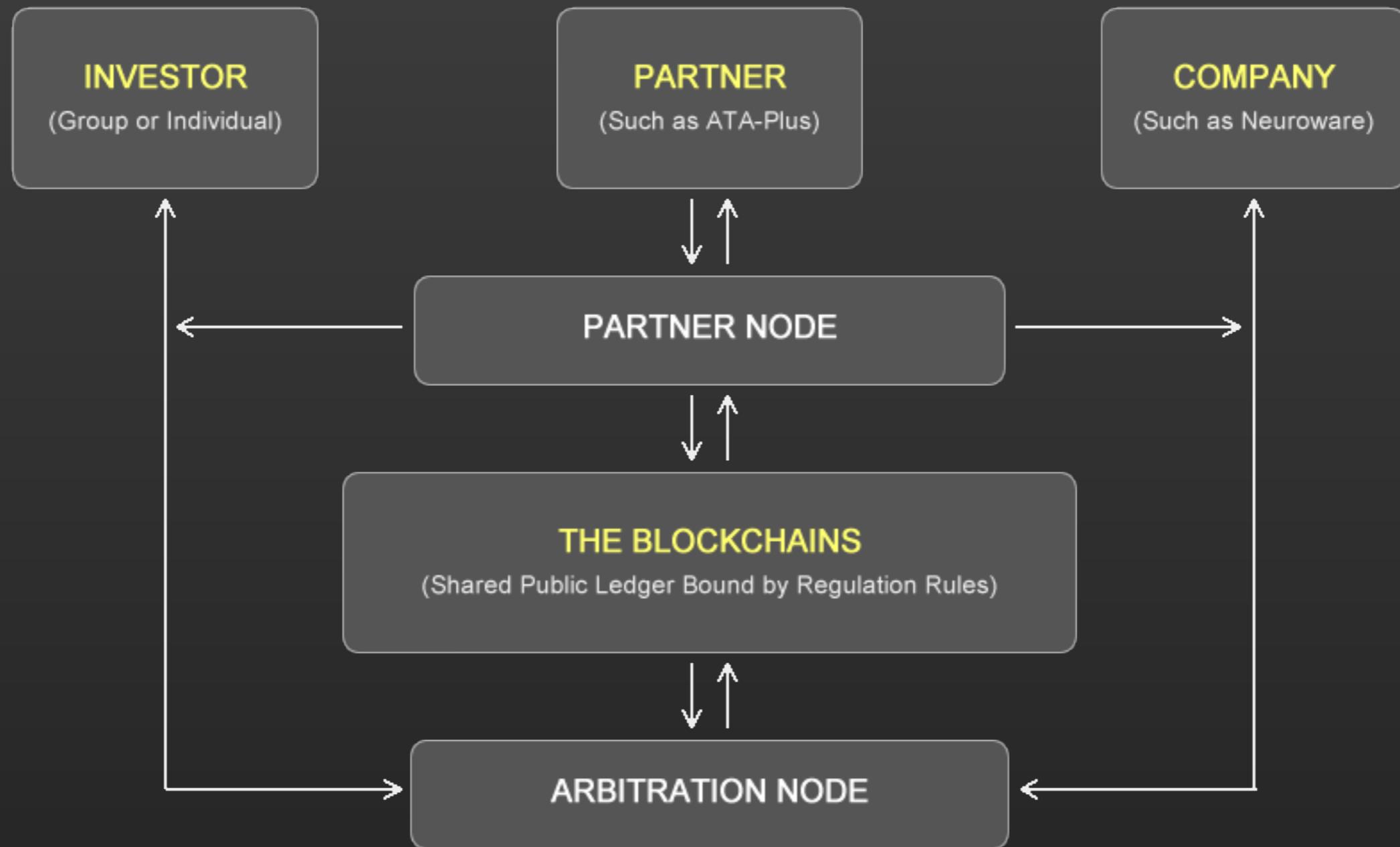
( hosted by licensed partners )

## ARBITRATION NODES

THESE SIMPLY SET AND GOVERN RULES

( hosted by national regulators )

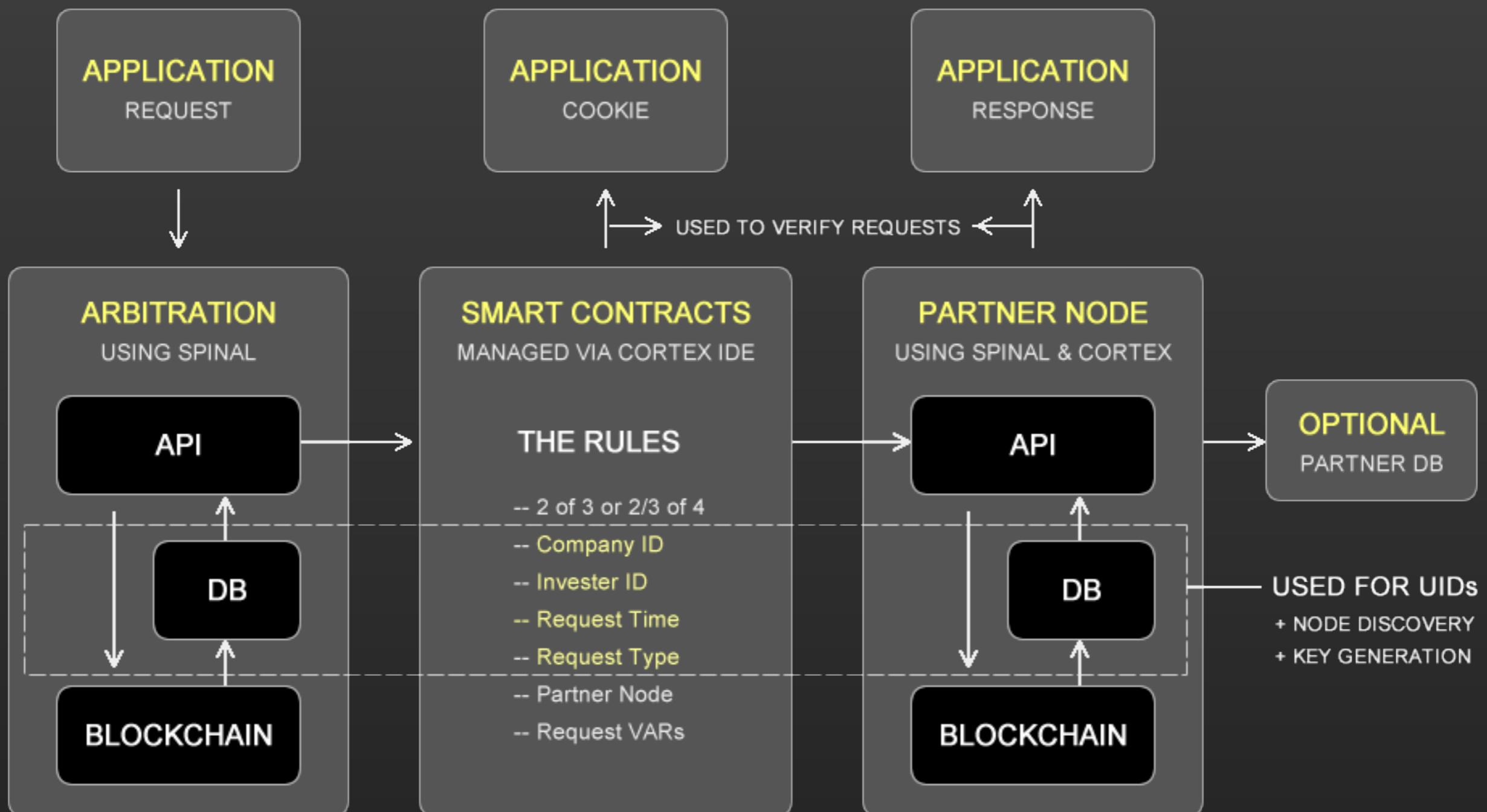
# USING THE BLOCKCHAINS TO OUTSOURCE TRUST



# THE RESPONSIBILITIES OF THE ARBITRATION NODES

- Arbitrators receive and relay requests for each contractual addition or edit
- It issues 2 of 3 multi-signature escrow smart contracts to each investor
- These contracts can also allow for optional deposits within digital currencies such as Bitcoin & Ether, and are relayed via the partner nodes
- Upon successful relay and fulfillment, contracts can then be settled directly
- Upon settlement, the creation of optional tokens representing one of the three keys can then be issued to and traded within secondary markets
- By controlling one of three keys where two keys are required for transfers allows for regulatory nodes to provide judgment in disputes, and also the ability to recover all transactions and control with approval from either side

# CREATING GLOBAL ARBITRATION CONTRACTS

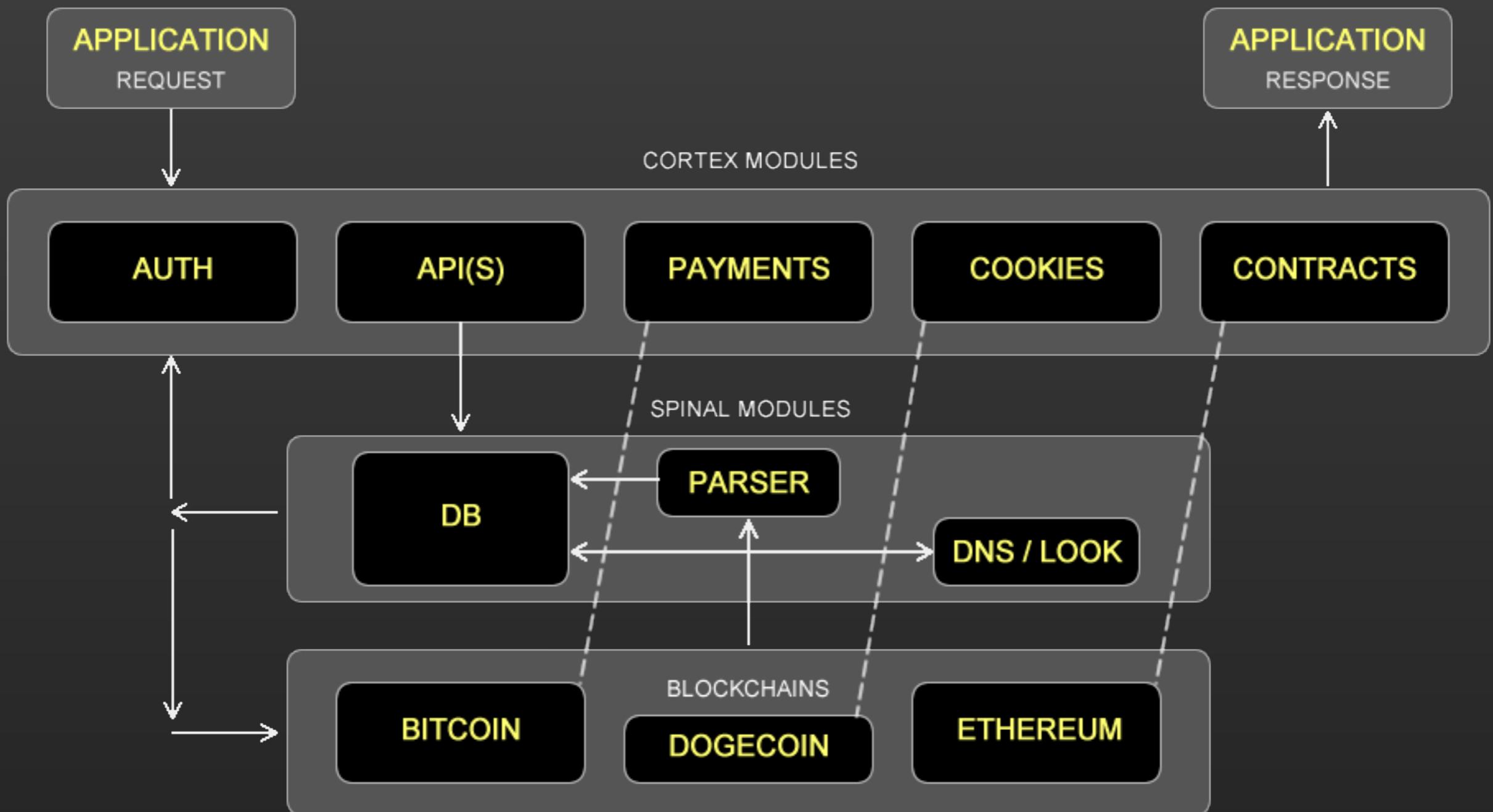


# THE RESPONSIBILITIES OF THE PARTNER NODES

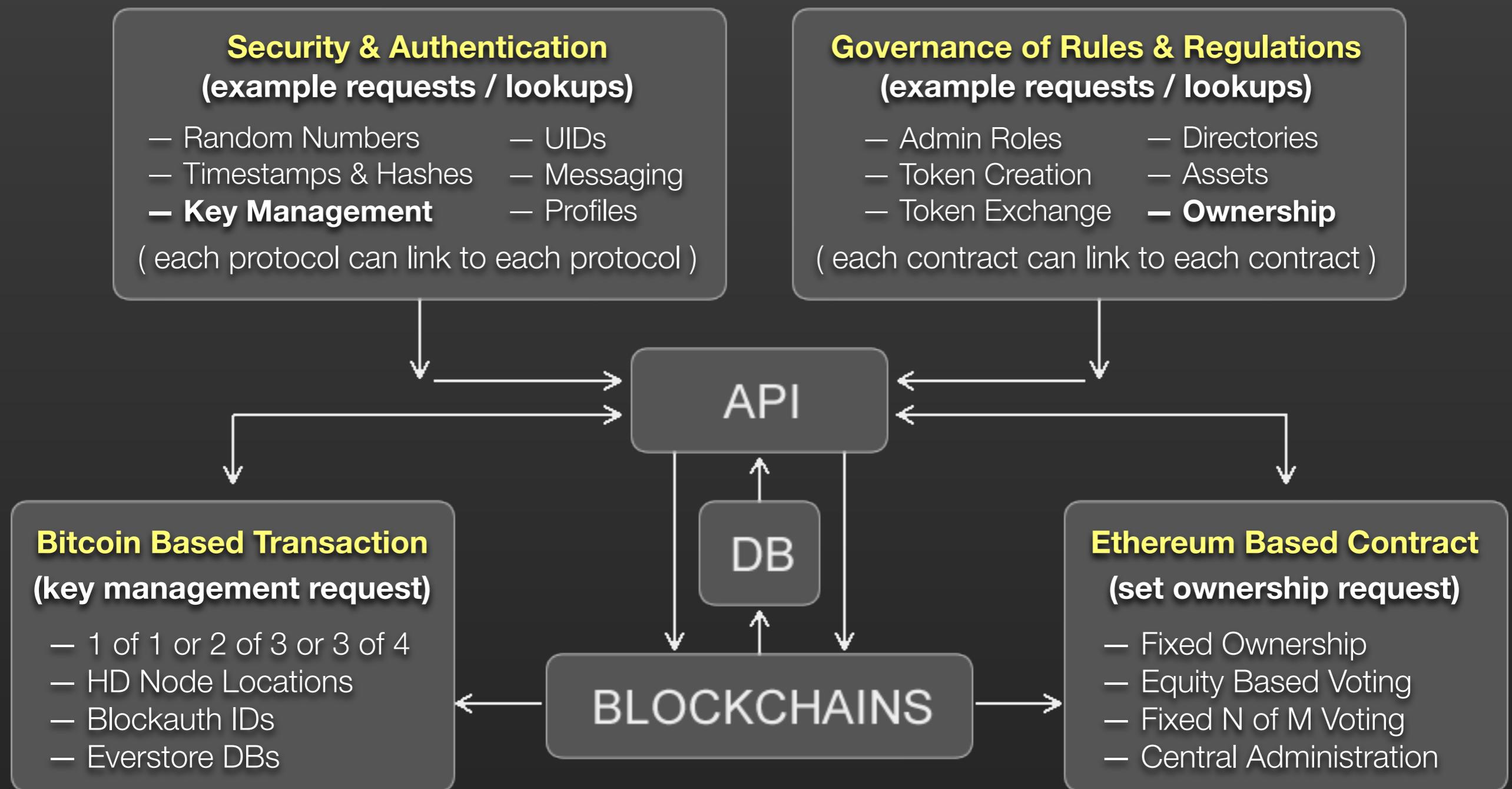
- Designed to conduct the most work and have the biggest and most accessed databases (from all of the application polling & final settlements)
- Licensed partners provide their users with branded customized experiences governed by network rules, regulations and automatically audited accounts
- Approved partners could issue their own tokens pegged to national reserve
- Approved investors could trade directly, or issue approved equity funds
- Partners can then choose to create local secondary markets directly with each other and their respective users (based upon their approved features)



# THE ANATOMY OF A PARTNER NODE



# MULTI-SIGNATURE PROCESSING PER FUNCTION PER PARTNER

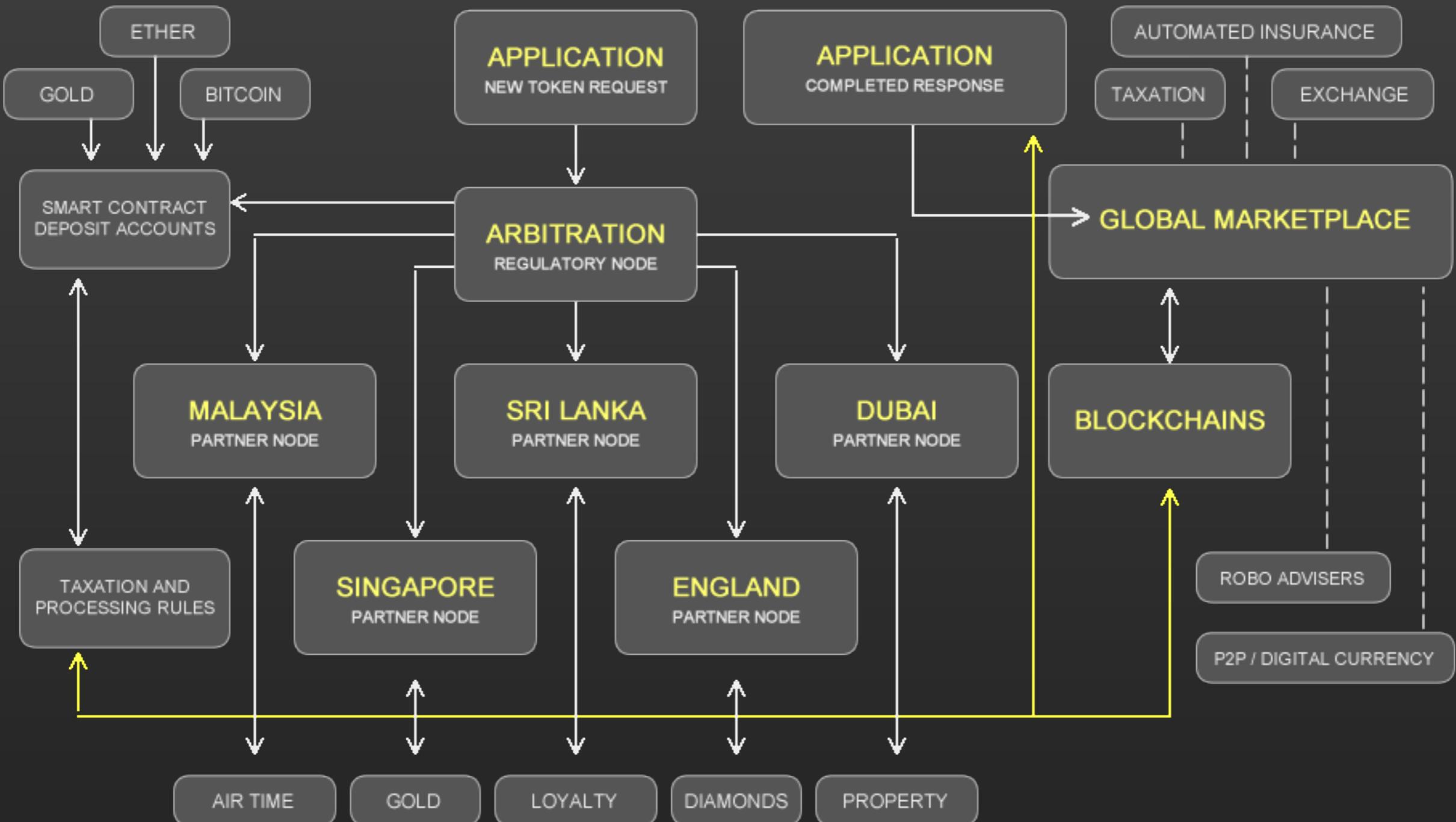


# CREATING A GLOBAL NETWORK OF SECONDARY MARKETS

- With each regional market connected to locally regulated digital securities, this could enable global participants to deposit, withdraw or transfer value and (or) ownership within any approved currency and (or) global location
- Regulatory nodes would automatically receive and relay the appropriate regional and global taxation and processing fees by controlling reserves
- Partner nodes provide the consumer applications, solutions and services
- As new digital-licenses emerge (such as P2P, Digital Currencies, etc) the broader the interconnected marketplace and ecosystem becomes...



# REGULATING A GLOBAL NETWORK OF SECONDARY MARKETS



## TO SUMMARIZE

- The next IT revolution is already underway and finance is only its first target
- Although the future of Bitcoin is uncertain - blockchains are here to stay
- Distributed ledger technology will continue growing at an increasing pace
- **Like databases, there is no blockchain suitable for every use-case**
- Remember to keep a blockchain-agnostic view when developing solutions
- Don't forget that whatever is controlling the private keys **owns** the money

# EVERY USE-CASE FOR BLOCKCHAINS REVOLVES AROUND TRUST

TRUSTING MATHEMATICS *Vs* QUANTITATIVE EASING

TRUST GAINED BY ALGORITHMIC CONFIGURATIONS



# THESE ARE SOME OF THE SERVICES NEUROWARE PROVIDE

- We provide company-wide education, training and blockchain workshops
- We provide self-hosted blockchain agnostic parsers, developer APIs & tools
- We provide consultancy and implementation services utilizing blockchains
- We've developed several open-source blockchain-based applications
- We've worked with banks and other financial institutions and regulators
- We've built platforms combining Ethereum contracts with Bitcoin security
- We've developed the following non-financial blockchain agnostic protocols

# BLOCKCHAIN-AGNOSTIC PROTOCOLS WORK ON ANY LEDGER

**EVERSTORE**

## DISTRIBUTED STRUCTURED DATA

By using a combination of Hierarchical Key Generation and standardized OP\_Return methodology, we are able to store an almost unlimited amount of structured data on any blockchains or ledgers that support OP\_Returns or an equivalent API accessible arbitrary data-storage field within their HD-compatible transaction streams.

 **blockauth**

## DECENTRALIZED ID AND AUTHENTICATION

By introducing Hierarchical roles and privileges using a similar methodology to Everstore, BlockAuth is able to verify and transmit secure messages and independent authorization to and from other BlockAuth enabled individuals and services. Store avatars and social media profiles to remove the need for repetitive form filling & choose who gets what.

 **dnkey**

## KEY LOGISTICS & BROADCASTING

DNKey not only enables basic key-aliasing, which allows other systems, services and users to replace long complicated public keys with memorable domain based identities, which in-turn allows for easier key sharing, it can also enable revocation abstraction layers - but also provides advanced methods for generating vast amounts of secure deterministic key-pairs.

# THANK YOU

NOW IS THE TIME TO QUESTION THINGS

LEARN MORE ABOUT



neuroware

<http://neuroware.io>