BANKING ON
THE FUTURE
(of blockchains)

PRESENTED BY

neuroware

INTRODUCING NEUROWARE

Mark Smalley - CEO

Living in Malaysia for the past 19 Years

Building Web Applications for 15 Years

Spent 10 Years Building Tech Communities

Developing Blockchains Apps for 5 Years

Ruben Tan - CTO

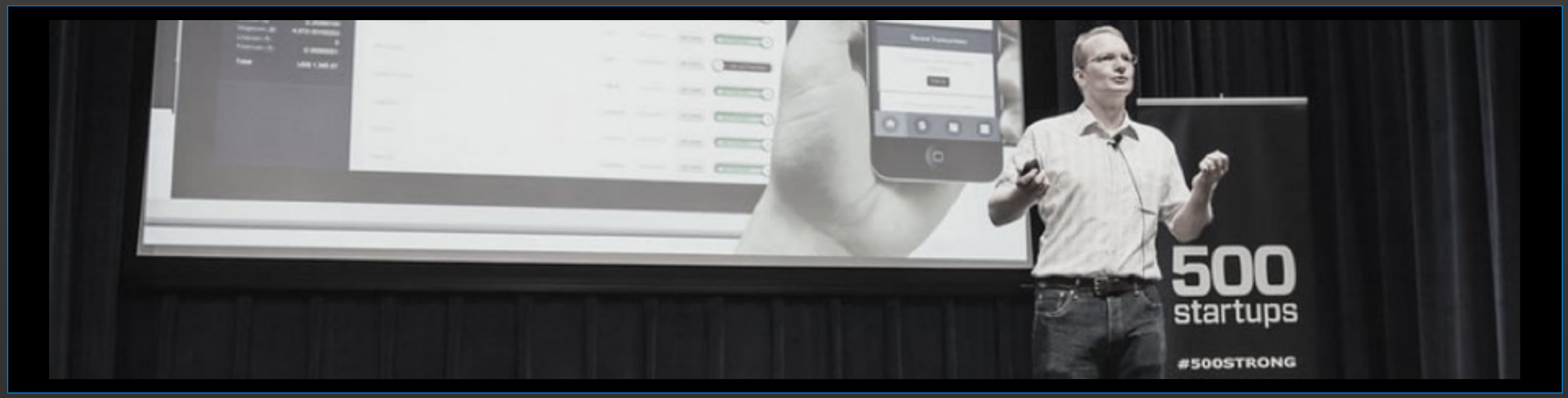
Building Web Applications for 10 Years

Active Community Evangelist & Presenter

Early Developer at MyTeksi and OnApp

Studying Distributed Consensus for 5 Years

EXPERIENCED INNOVATORS IN AN EARLY ECOSYSTEM



- **1st Malaysian Company** to Graduate from 500 Startups in Silicon Valley
- **1st Company in Asia** Providing Public Blockchain APIs & Developer Toolkits
- **1st in The World** to Develop Non-Financial Blockchain Agnostic Protocols
- Helped Organize World's 1st Bank-Backed Blockchain Hackathon (DBS)
- Over 15 Years of Collective Blockchain Development Experience

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

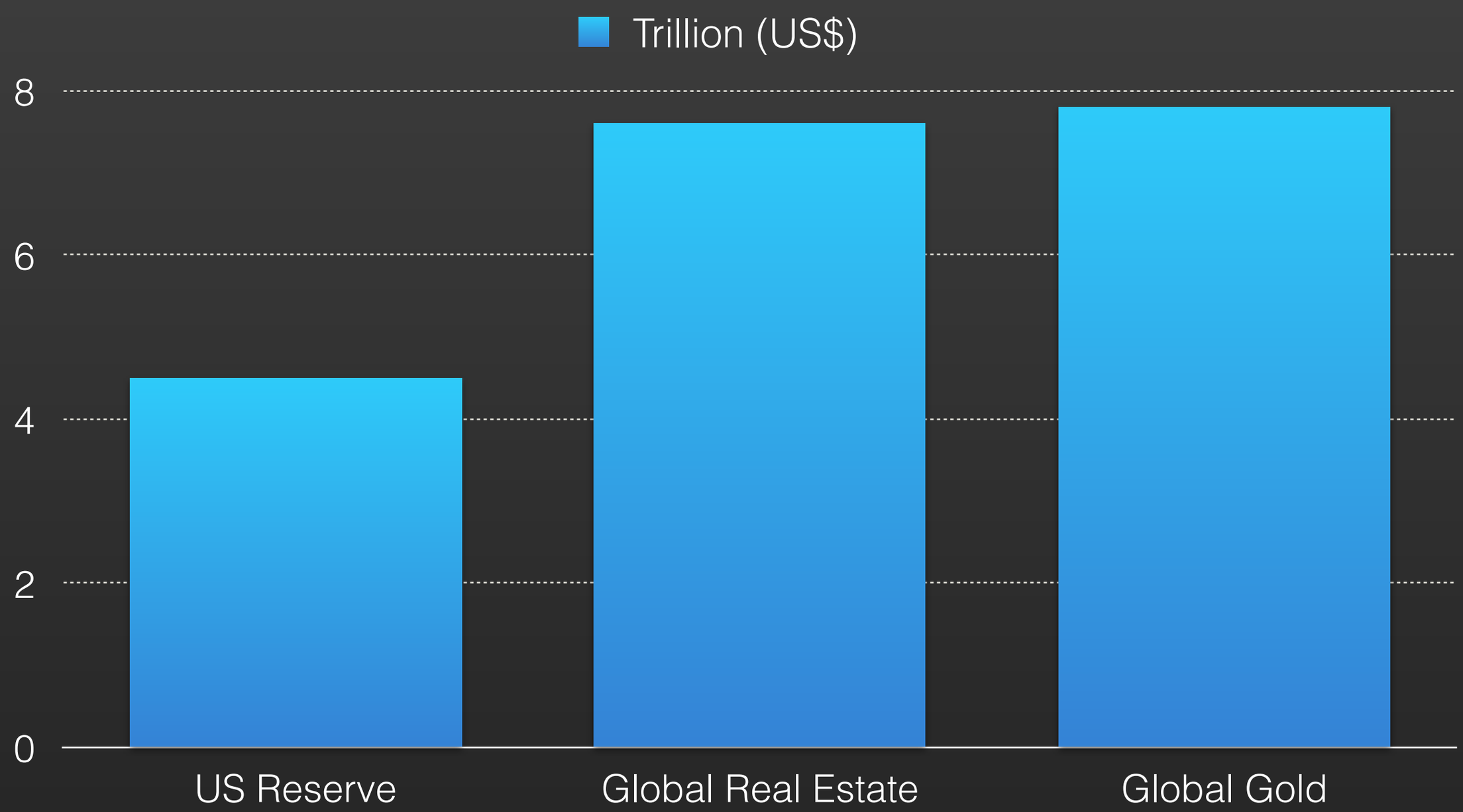
SO THEY CREATED THE WORLD'S FIRST PUBLIC LEDGER

WHERE UPDATES REQUIRED GROUP CONSENSUS

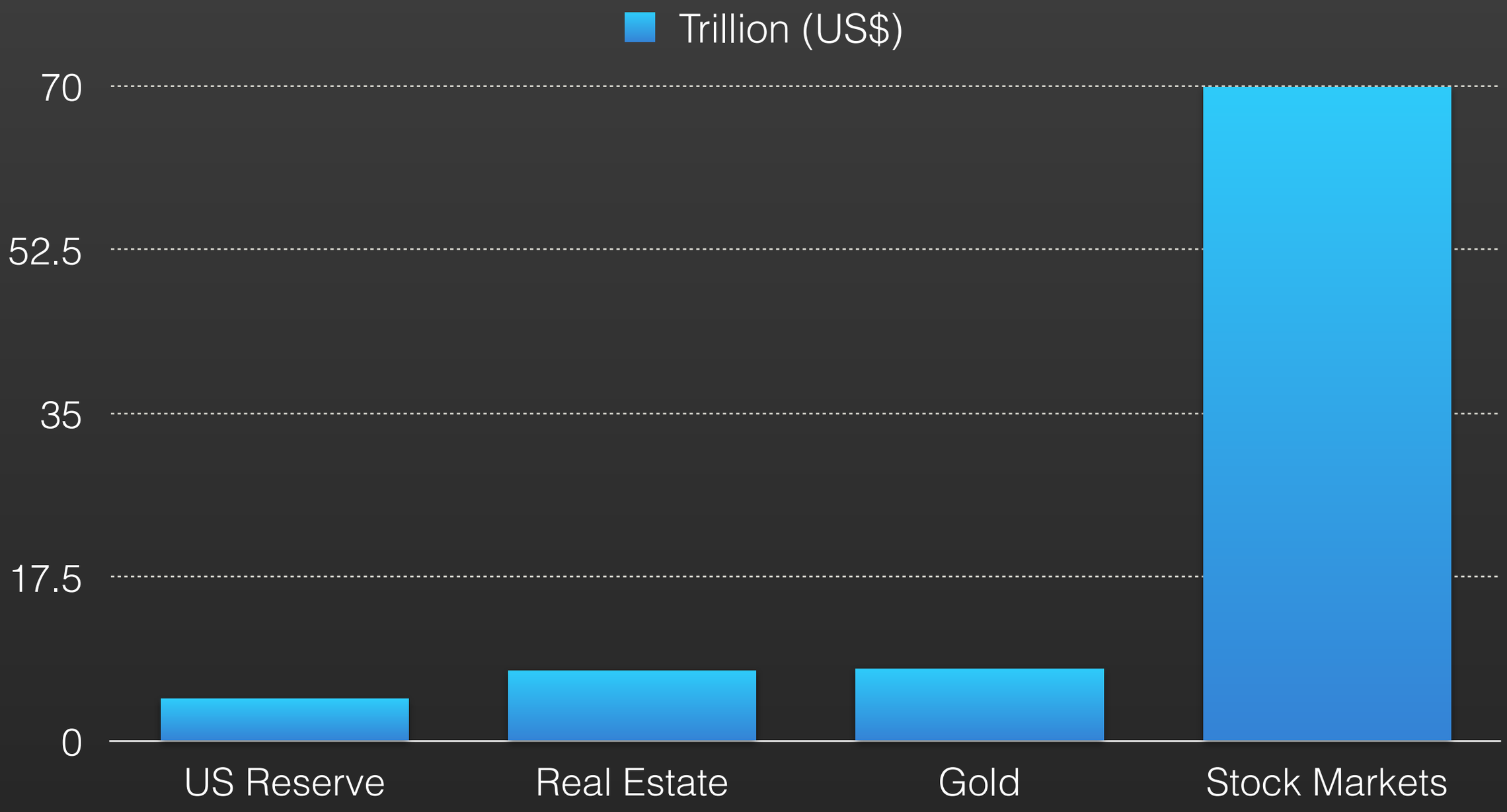
- Size wasn’t everything
- The history of each stone determined it’s individual value
- Conducting transactions quite literally involved a song & dance
- This required the majority of people from the village to be present

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

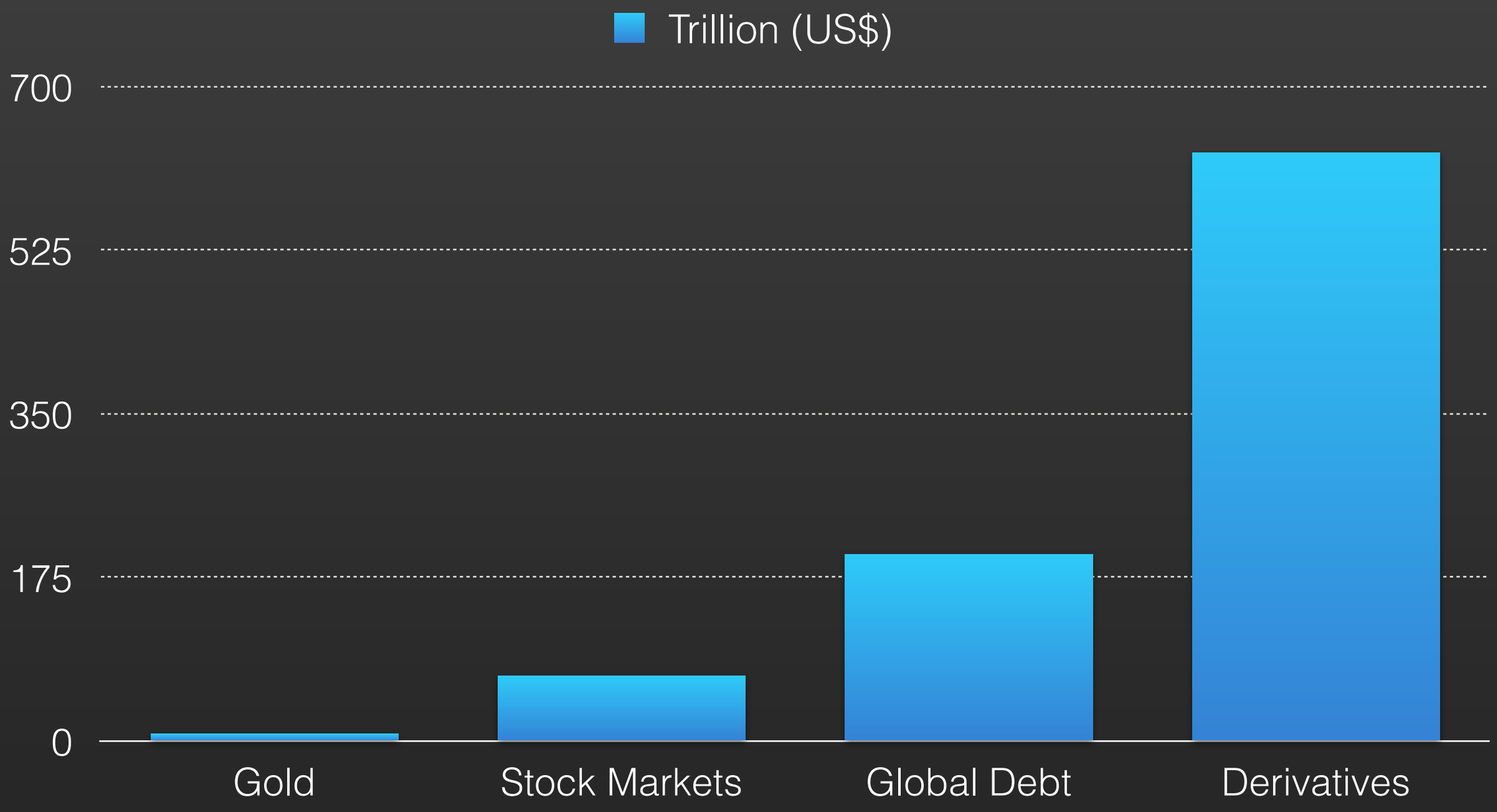
WHEN WE THINK OF THE US DOLLAR WE THINK OF REAL MONEY



AND THEN CAME THE ERA OF DIGITAL CENTRALIZED LEDGERS



AND WITH IT ALSO CAME THE RE-CREATION OF ~~MONEY~~ DEBT



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

World War 2
US$3 Trillion

All other US
Wars Ever

2008 Bailout
US$8.5 Trillion

This really annoyed
Satoshi Nakamoto

NOTHING LASTS FOREVER

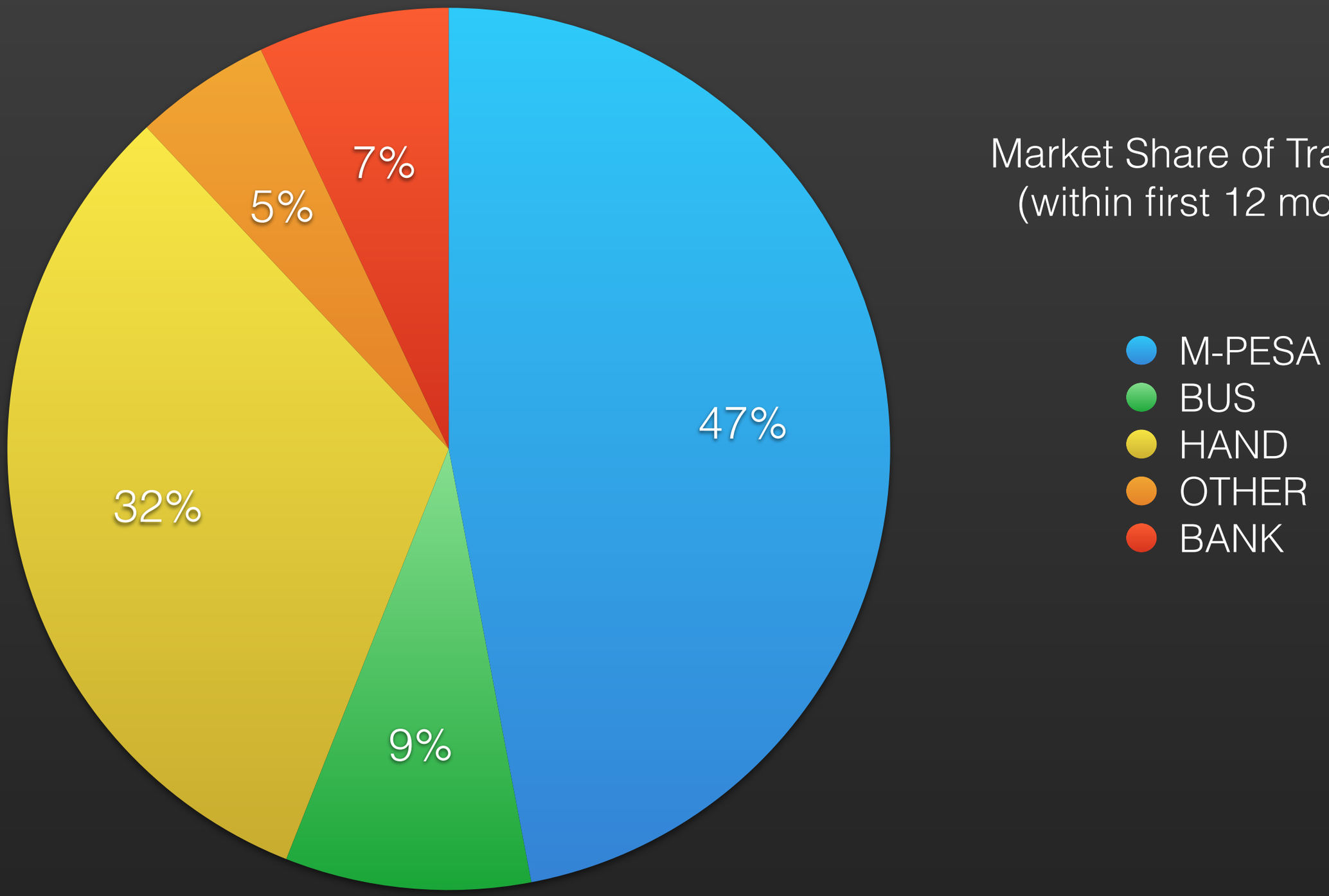
- Average lifespan of individual currencies is 27 years
- Every 30 or 40 years the reigning monetary system fails
- Over 3,800 fiat currencies worldwide have failed
- 15 of which happened in just the past 25 years

THE RECENT FAILURE OF FIAT

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

WHAT HAPPENS WHEN THE BANKS FAIL TO INNOVATE …?

WITHIN FIRST 12 MONTHS - 17 MILLION SUBSCRIBERS BY 2011



“ SOFTWARE IS EATING THE WORLD ” - Marc Andreessen

UBER

- 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**

A TIP-TOE 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

pwc

"While Fintech Disrupts Banks,
the Blockchains Disrupt Fintech"

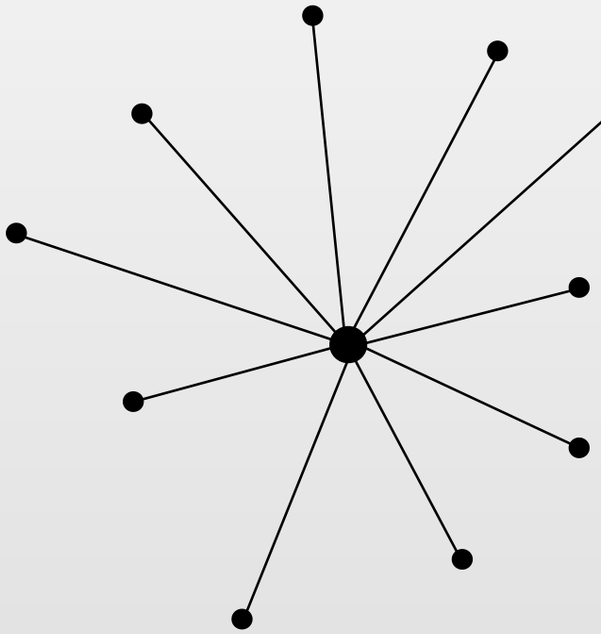
INTERESTING BITCOIN BLOCKCHAIN FACTS TO REMEMBER

- 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 citied 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

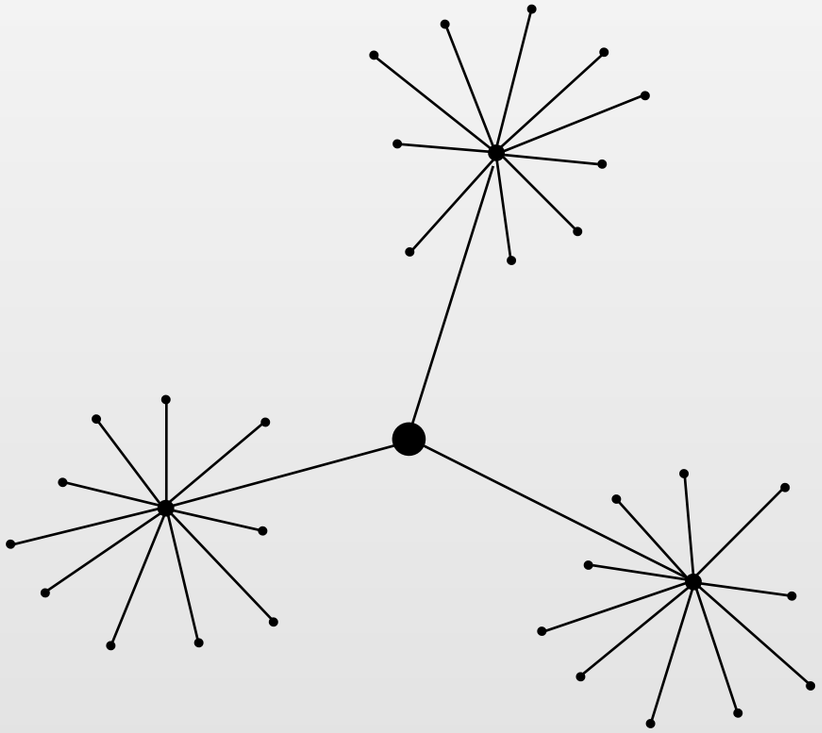
- HASH - Theorized in the 1800s - Coined by IBM in the 1950s
- SHA - Encryption method first introduced by US Navy in 1993
- P2P - Peer to peer protocol popularized by Napster in 1999

THE EVOLUTION OF EVERYTHING …?



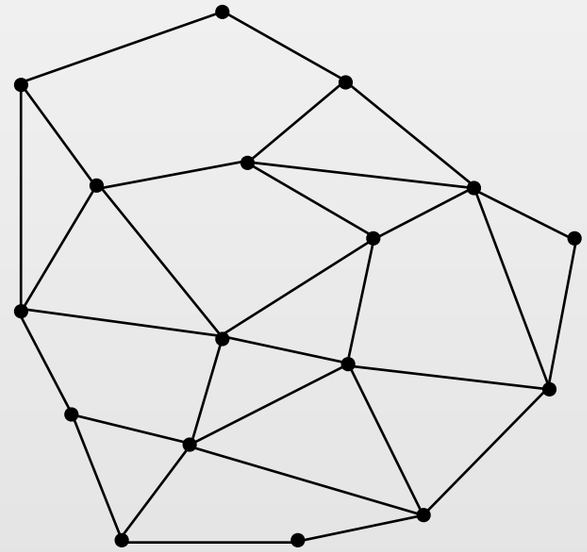
CENTRALIZATION

DATABASE



DECENTRALIZATION

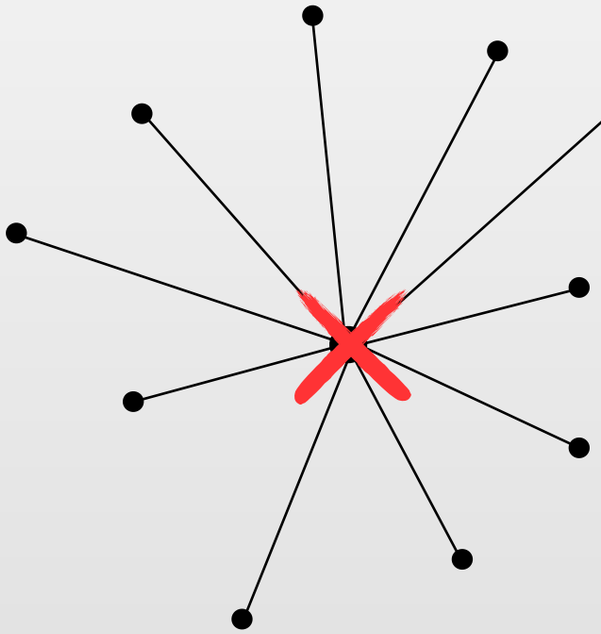
THE CLOUD



DISTRIBUTION

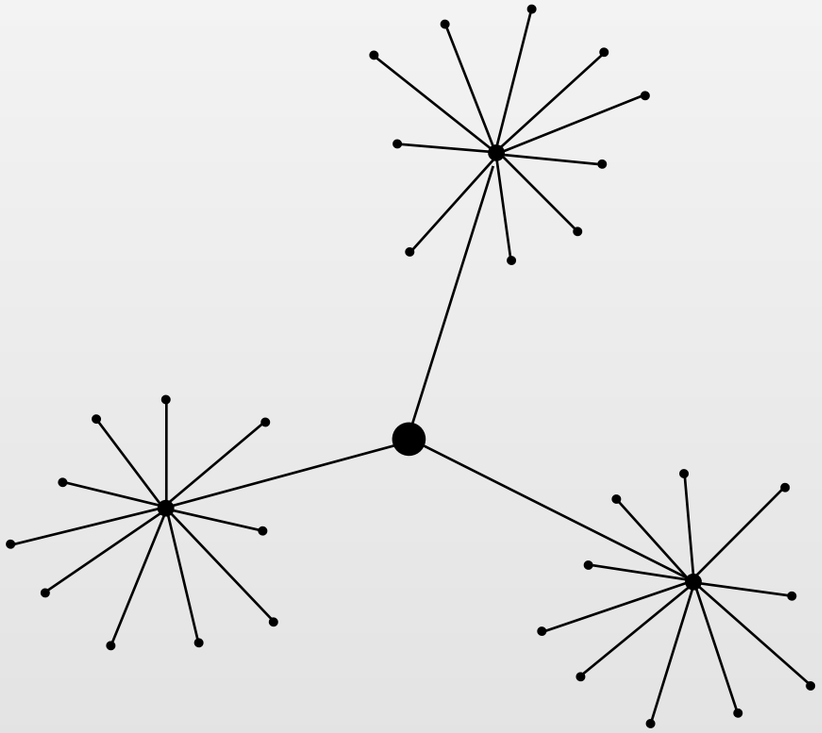
BLOCKCHAINS

THE EVOLUTION OF EVERYTHING …?



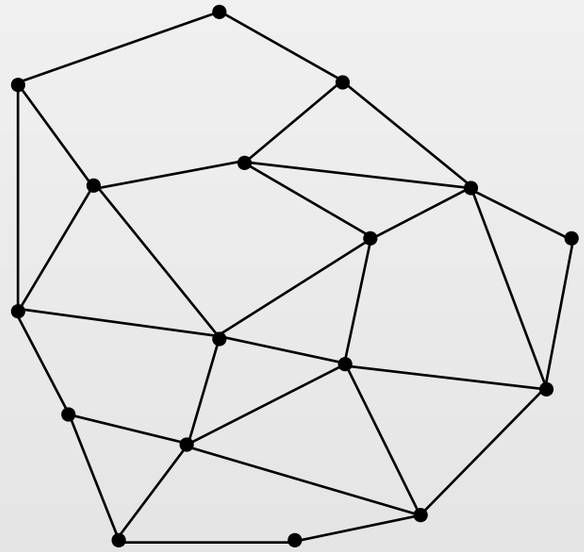
CENTRALIZATION

DATABASE



DECENTRALIZATION

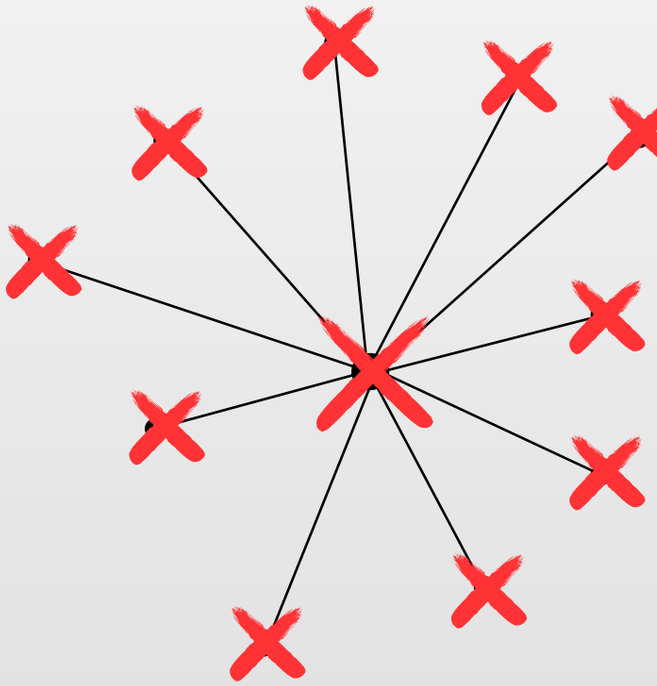
THE CLOUD



DISTRIBUTION

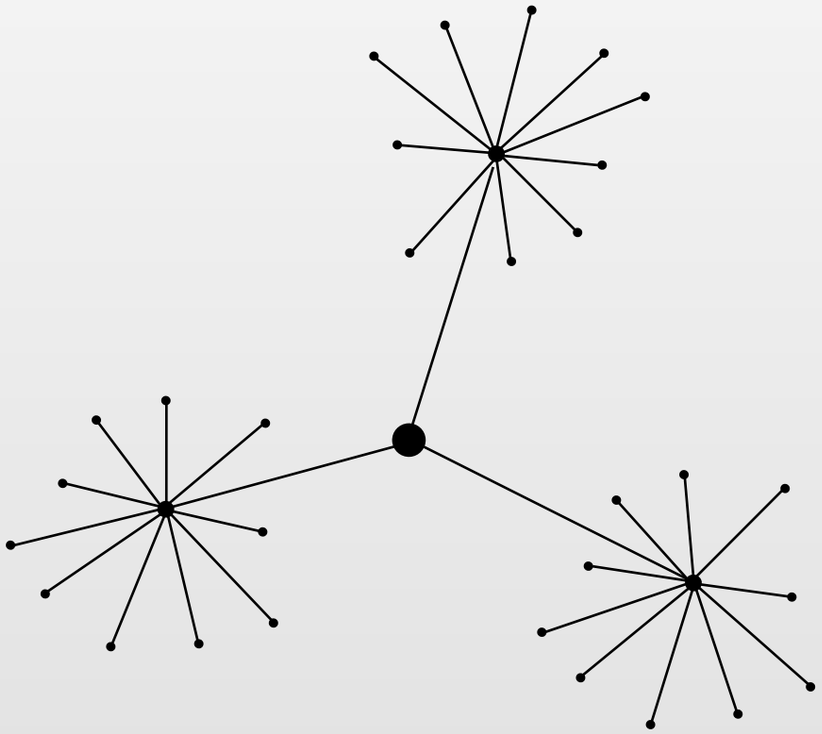
BLOCKCHAINS

THE EVOLUTION OF EVERYTHING ...?



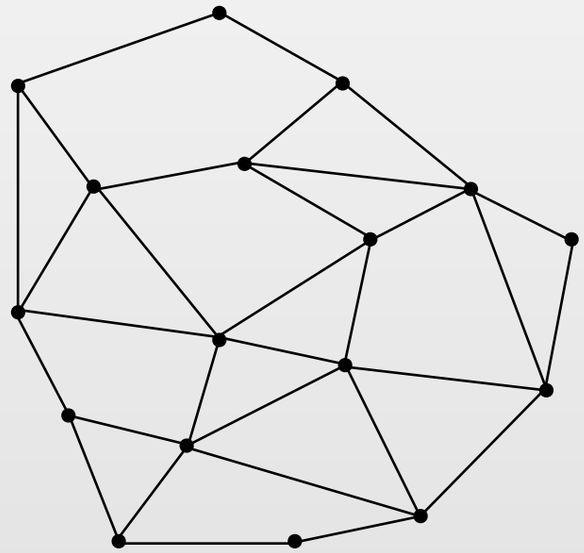
CENTRALIZATION

DATABASE



DECENTRALIZATION

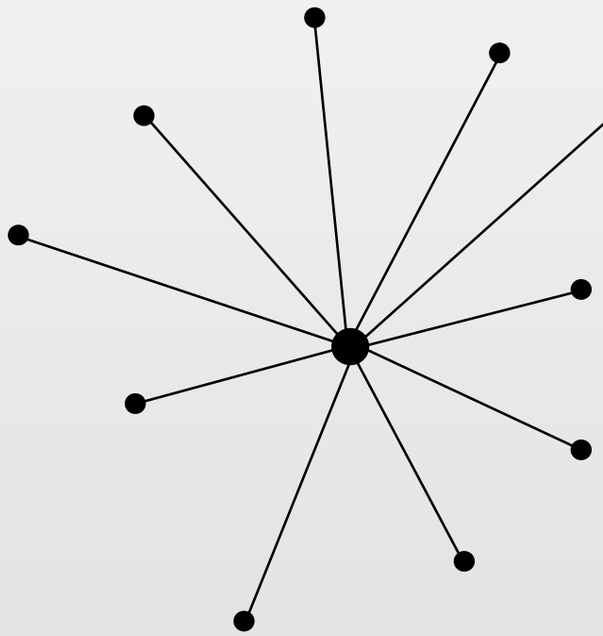
THE CLOUD



DISTRIBUTION

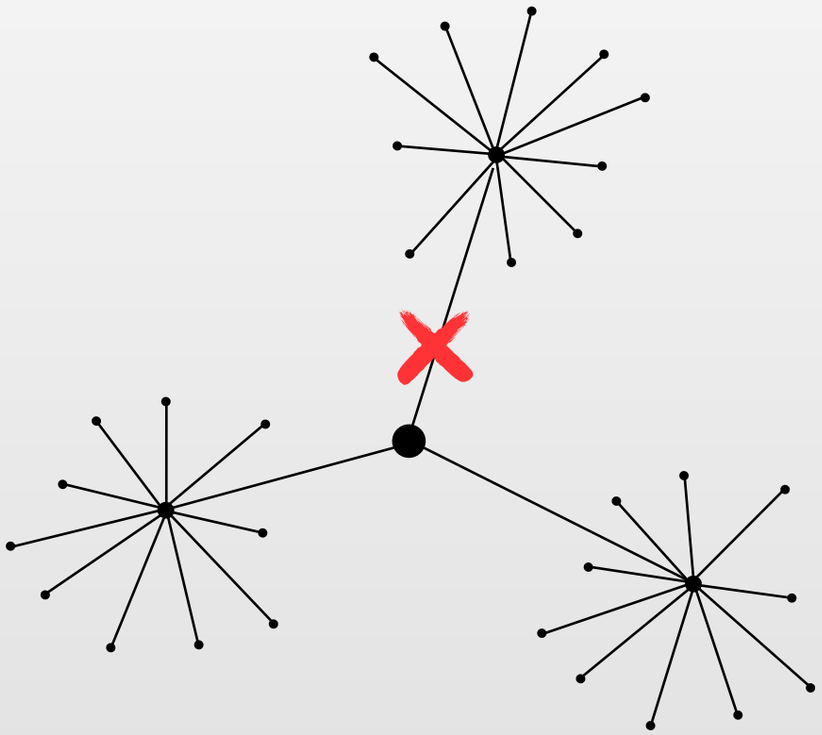
BLOCKCHAINS

THE EVOLUTION OF EVERYTHING ...?



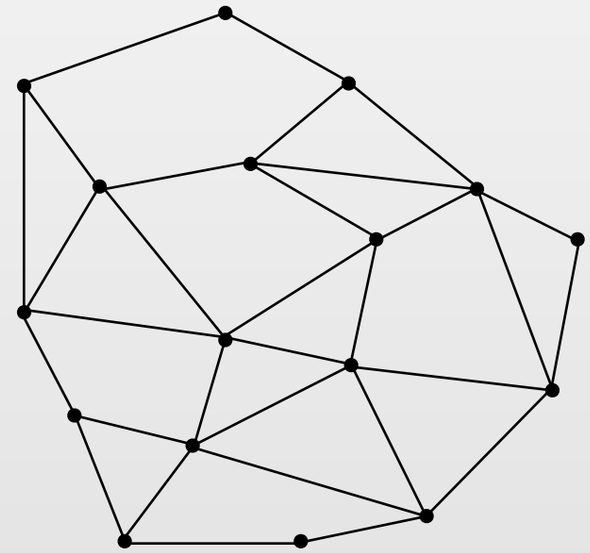
CENTRALIZATION

DATABASE



DECENTRALIZATION

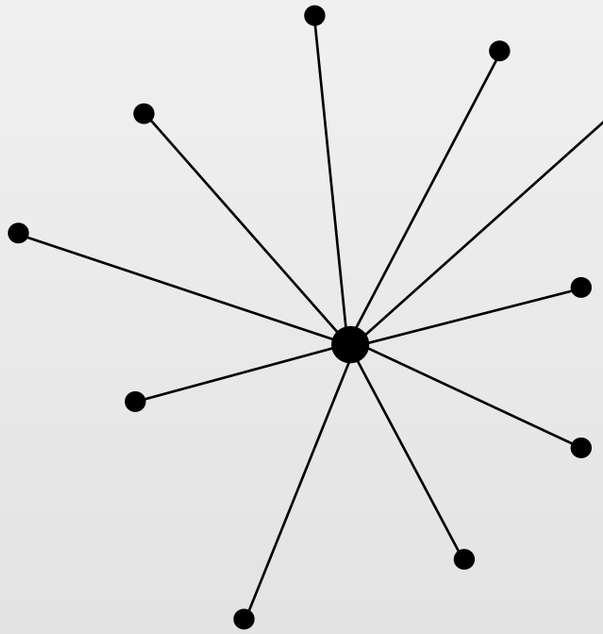
THE CLOUD



DISTRIBUTION

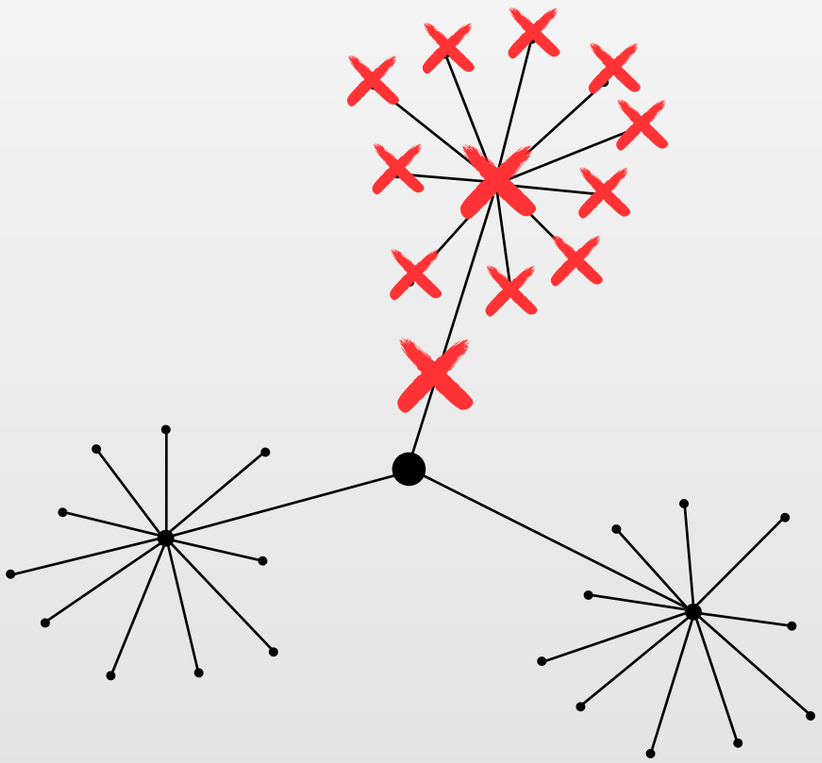
BLOCKCHAINS

THE EVOLUTION OF EVERYTHING ...?



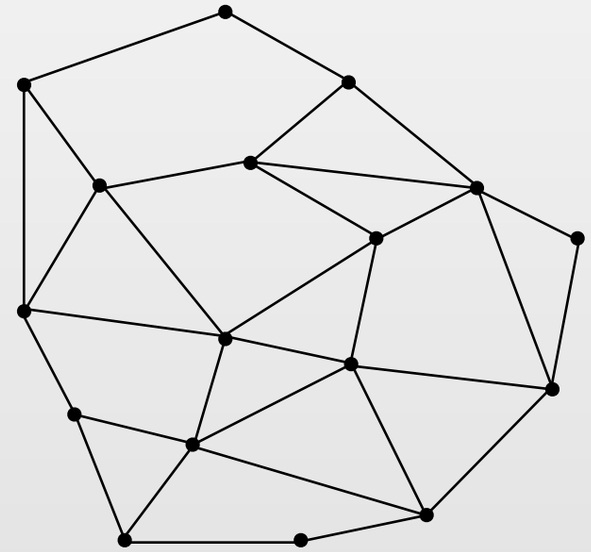
CENTRALIZATION

DATABASE



DECENTRALIZATION

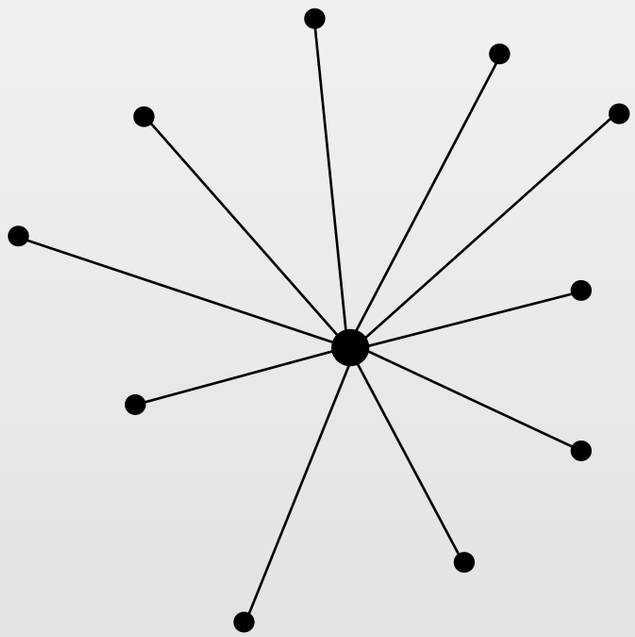
THE CLOUD



DISTRIBUTION

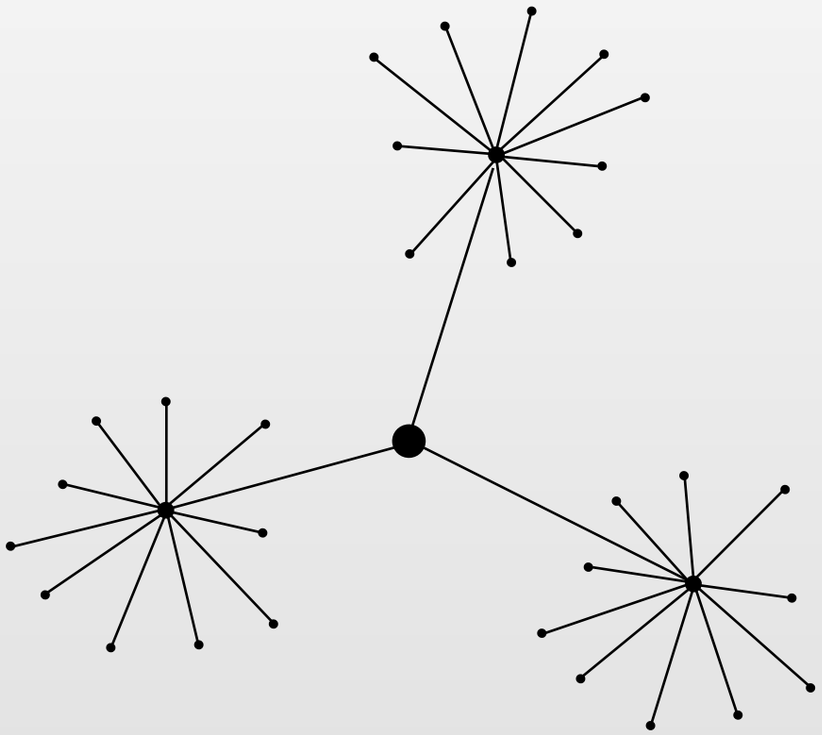
BLOCKCHAINS

THE EVOLUTION OF EVERYTHING ...?



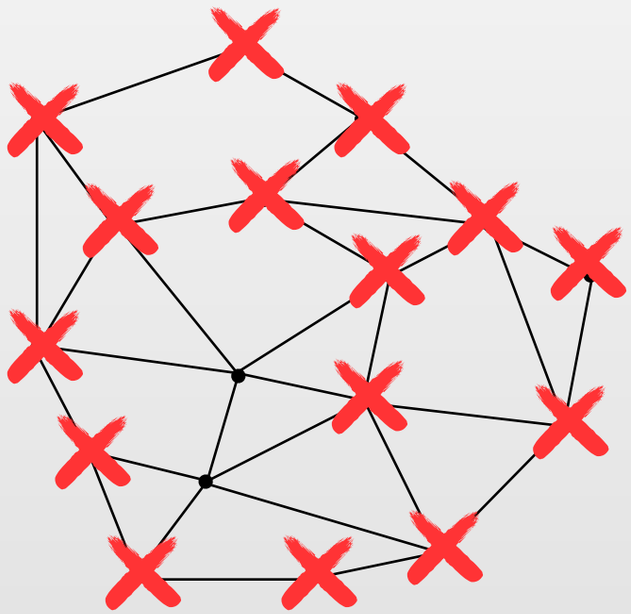
CENTRALIZATION

DATABASE



DECENTRALIZATION

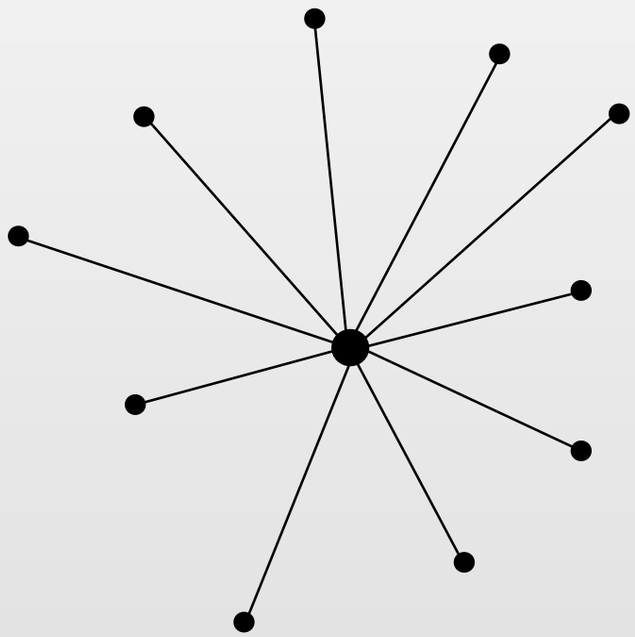
THE CLOUD



DISTRIBUTION

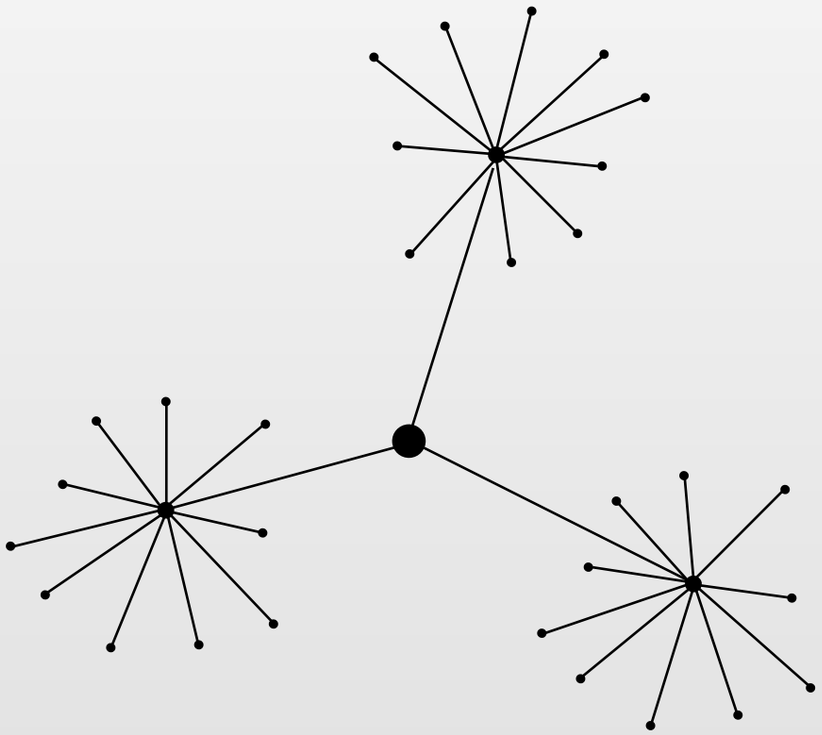
BLOCKCHAINS

THE EVOLUTION OF EVERYTHING ...?



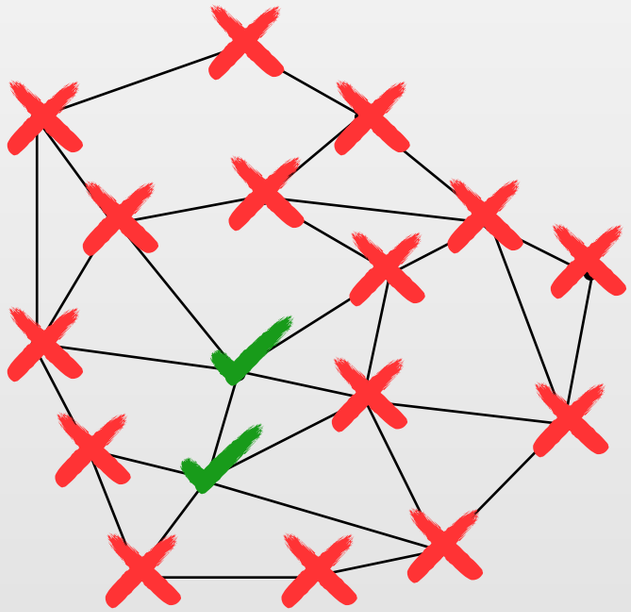
CENTRALIZATION

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

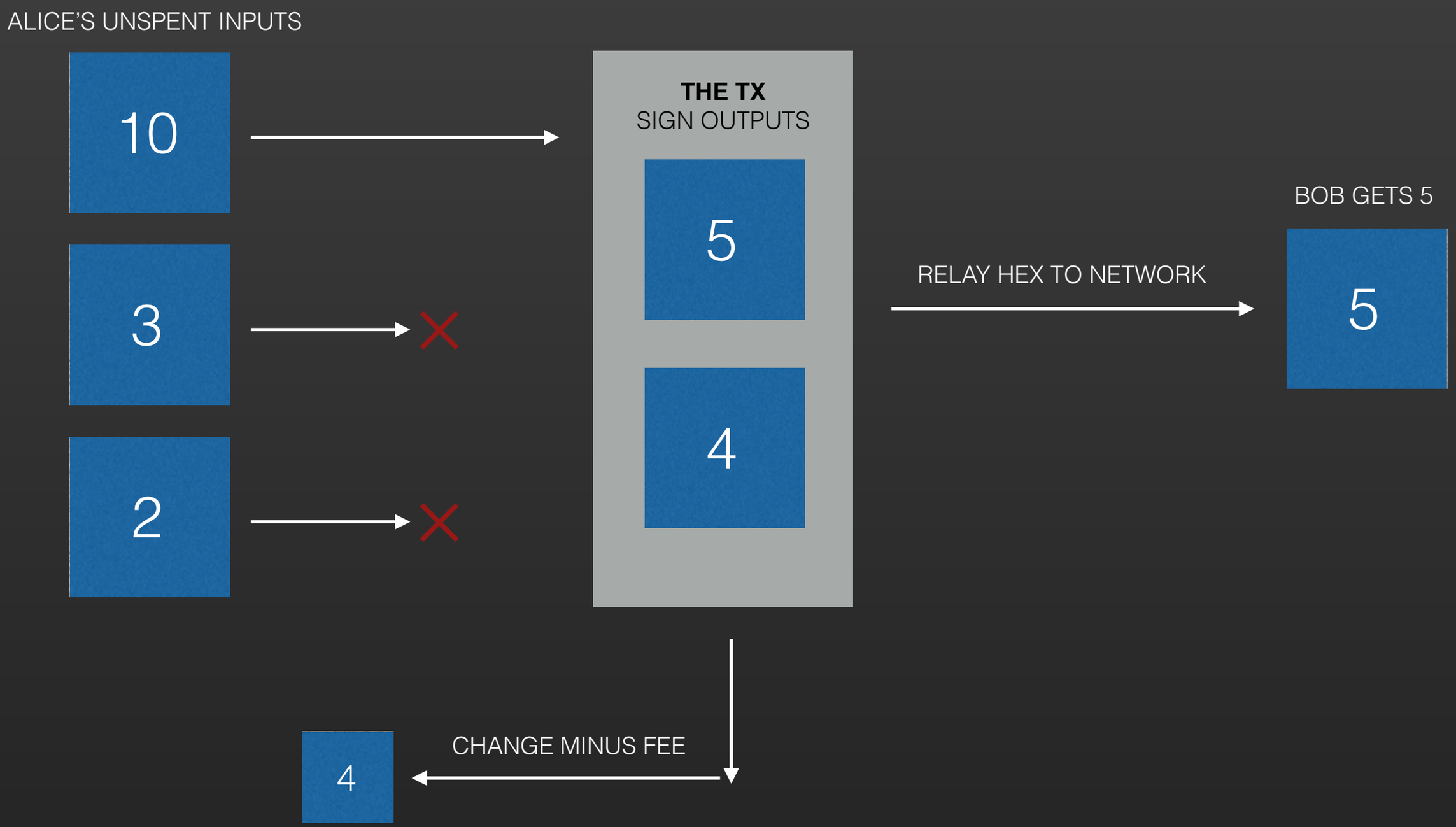
EACH “ADDRESS” REQUIRES A PRIVATE KEY TO ACCESS IT

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)

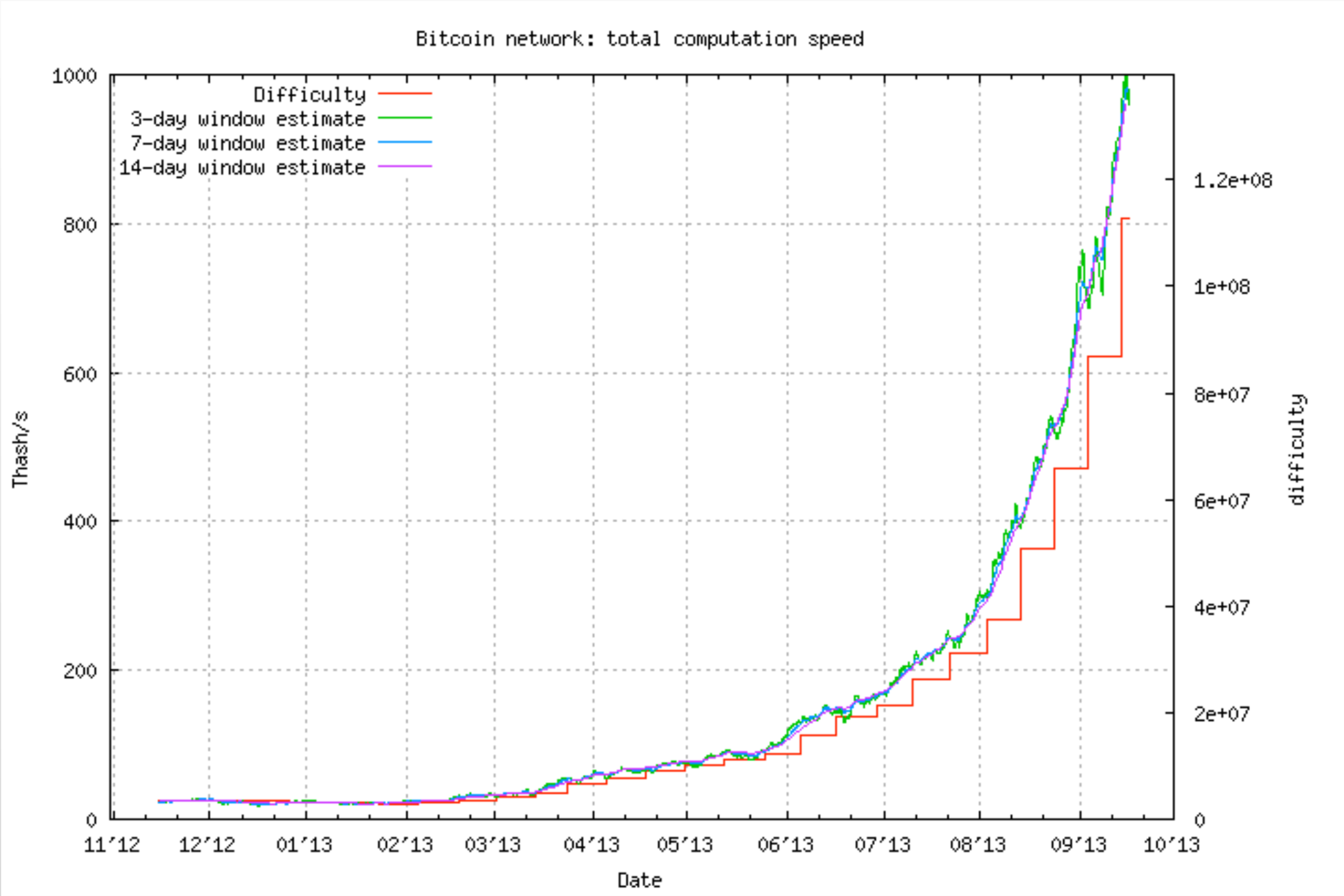
ALICE CAN'T SEND WHAT SHE DOESN'T HAVE AND BOB WANTS 5



PUTTING THE BLOCKS INTO THE BLOCKCHAINS

- Transactions are batched into blocks every ten minutes (with Bitcoin)
- 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
- 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

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

Exchanges
kraken, BTer.com, BITSTAMP, POLONIEX, coinbase, bitcoin.de, BTC-e, GEMINI, mexbt, CAMP BX, PAYMIUM, BITSO, BitOasis, SHAPESHIFT, CAMP BX, COINIGY, coinsetter

Brokerage
BITPagos, coinbase, Unocoin, BTCC, BITFINEX, COINJAR, safello, QUADRIGACX, bitFlyer, NOBLE MARKETS, volabit, coinfloor, coins.ph

Soft Wallets
BLOCKCHAIN, airBitz, ARMORY, coinbase, xapo, ELECTRUM, Mycelium, bread wallet, Coinkite, Darkwallet, coinprism

Hard Wallets
TREZOR, case, π WALLET, keepkey, Ledger Wallet

Investments
Grayscale, loanbase, KOIBANX, Bitbond, WeiFund, BSAVE.IO, Etherplan, BTCjam, dangpu.com, WEALTHCOIN, Yuanbao, lighthouse

Merchants
bitpay, Coinkite, Bitnet, coinbase, PEX, Coinify

Compliance
ELLIPTIC, thirdkey solutions, Sig3, CHAINALYSIS, CryptoCorp, IdentityMind GLOBAL, vogogo, COINALYTICS

ATMs
LocalBitcoins.com, Robocoin, bitxatm, bitaccess, COINOUTLET, PLANETCAPITAL, btcpoint, Project Skyhook, LAMASSU BITCOIN VENTURES, genesiscoin, GB

Capital Markets
symbiont, Digital Asset Holdings, clearmatics, TradeBlock, t0, epiphyte, itBit, R

Money Services
ChangeTip, BITX, ABRA, coinx, uphold, CoinPip, COINAPULT, BitPesa, BlinkTrade, BITNEXO, MELOTIC

Financial Data
bitcoinity., CoinMarketCap, CryptoCoin, BlockJockey, BRAVE NEWCOIN, BitcoinWisdom, CRYPTRADER, CoinGecko, TradeBlock

Payments
Align Commerce, BLADE, GOCOIN, GAZEBO.IO, GemPay, cuber, SETL.io, safecash

Trading
HEDGY, BitMEX, COINUT, Mirror, tradewave, CRYEX, BITNOMIAL, TERA EXCHANGE, TABTRADER

Banks
secco, LHV, fidor BANK, moni

Supply Chain
CHRONICLED, VAVE, skuchain, PROVENANCE

Payroll
paybits, bitWAGE

MIDDLEWARE & SERVICES

Services
CRYPTONOMEX, B9, CONSENSYS, SolidX, Chain, RUBIX

Software Development
chainscript, eris INDUSTRIES, openchain, Blockstream, MultiChain, Blockstack.io, PEERNOVA

General APIs
bitcore, coinbase, BitGo, Gem, neuroware, Coinkite, BLOCKCYPHER

Special APIs
TIERION, Open Assets, COLOREDCOINS, ChromaWay, colu

Platforms
Counterparty, HYPERLEDGER, erocoin, ethereum, blockstack

Smart Contracts
SmartContract, CoinSpark, bitShares, ROOTSTOCK

INFRASTRUCTURE & BASE PROTOCOLS

Public
bitcoin, ethereum

Special
ripple, stellar

Payment
Amiko Pay, Lightning Network

Miners
ANTPOOL, BitFury, 21 INC, BTCC, BTC Guild, KnC, BITCOINCZ

Source: http://startupmanagement.org/2015/10/22/the-global-landscape-of-blockchain-companies-in-financial-services/

SOME OF THE INSTITUTIONS LEADING THE WAY

Custom blockchain for settlements

Blockchain based trade finance platform

Blockchain based loyalty platform

Blockchain based remittance platform

multiple blockchains for cross-boarder payments and loyalty

Exploring KYC and AML via the blockchains

Patented a blockchain based wire transfer system

IMITATION IS THE BEST FORM OF FLATTERY

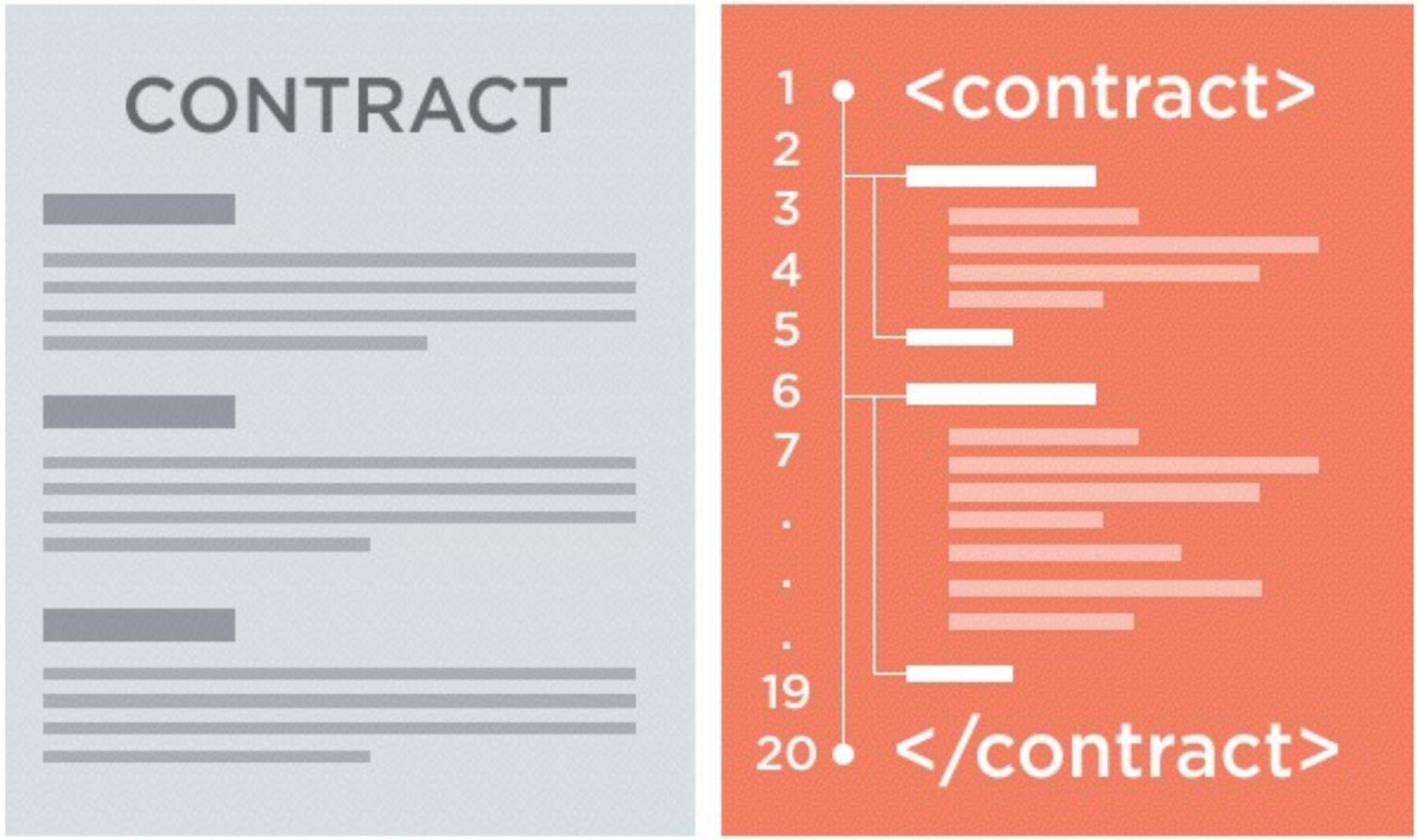
- 1st Generation of Alt-Coins forked each other with minor tweaks
- Basic breakout alt-coin successes included Litecoin and Dogecoin
- Dash (previously known as DarkCoin) worth noting due to governance
- See the Malaysian-Based **CoinGecko** for a better list!

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?

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…

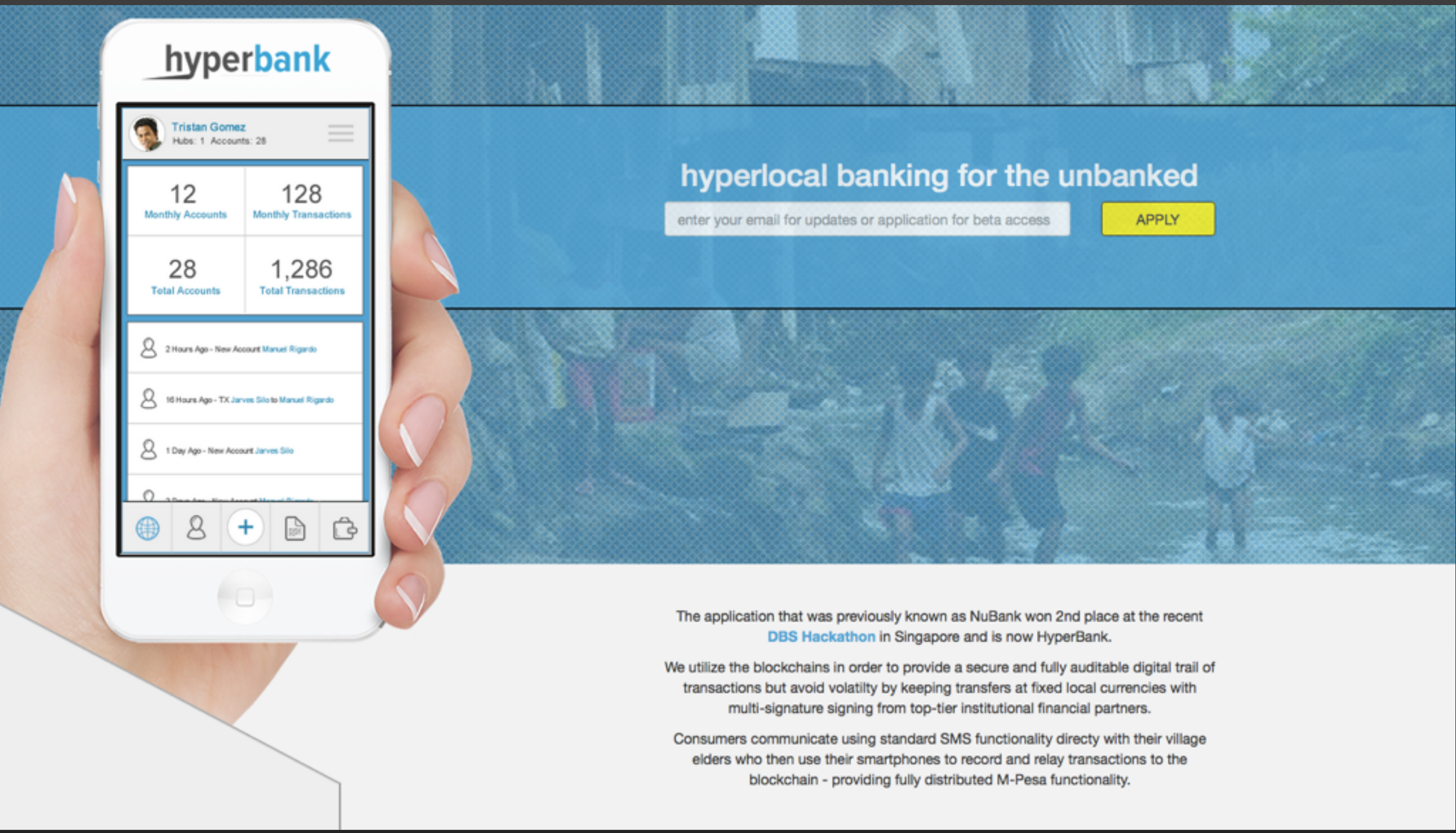
THE BANKS OF THE FUTURE

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 application that was previously known as NuBank won 2nd place at the recent DBS Hackathon in Singapore and is now HyperBank.

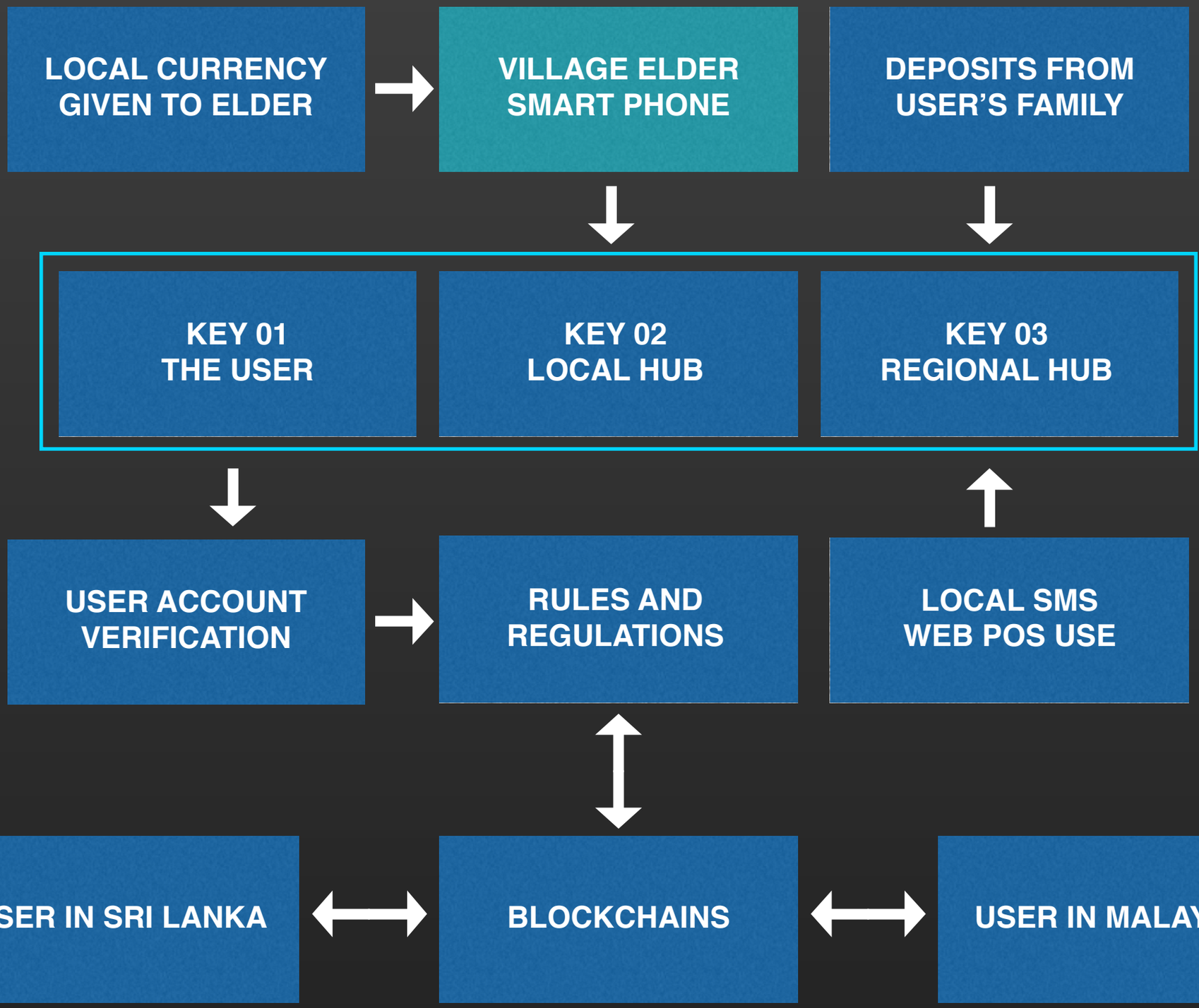
We utilize the blockchains in order to provide a secure and fully auditable digital trail of transactions but avoid volatilty by keeping transfers at fixed local currencies with multi-signature signing from top-tier institutional financial partners.

Consumers communicate using standard SMS functionality directy 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

HYPERLOCAL BANKING IN A GLOBAL WORLD



THANK YOU

NOW IS THE TIME TO QUESTION THINGS

LEARN MORE ABOUT

neuroware

http://neuroware.io