

# Blockchain MasterClass

(2017 - Q4)

presented by



# DISCLAIMER - I BOUGHT BITCOINS WHEN THEY WERE US\$10



**Mark Smalley - CEO ( [Neuroware.io](#) )**

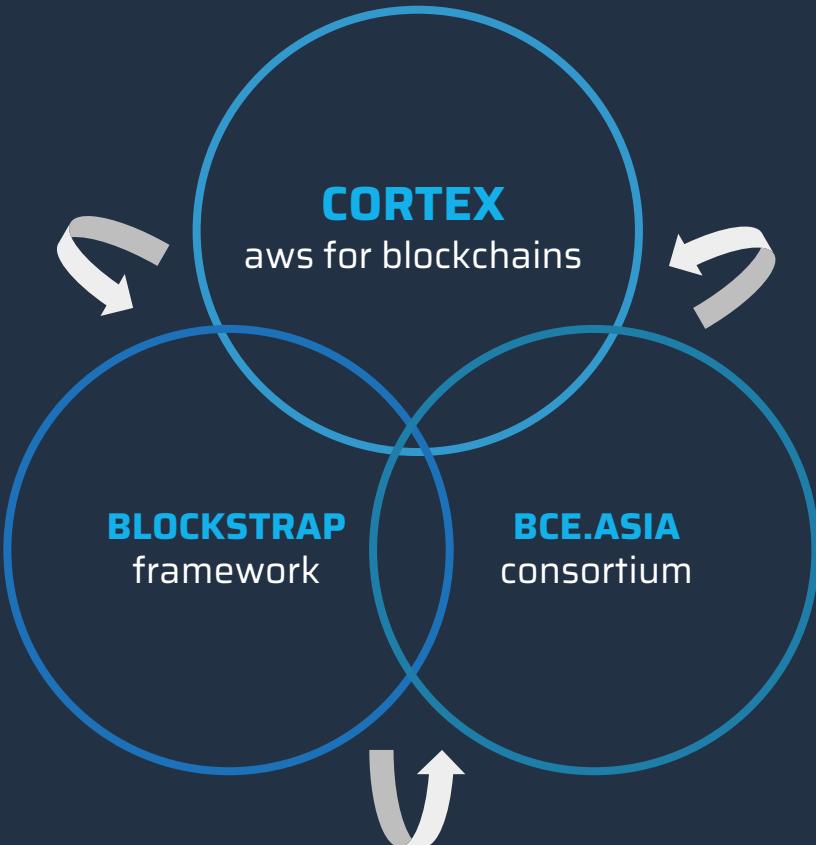
Living in Malaysia for the past 20 Years

Building FinTech Applications for 15 Years

Building Blockchain Apps for 5 Years

Despite a Family of Financial Advisors,  
I've only ever made one investment ...

# INTRODUCING NEUROWARE



## GLOBAL FUNDING

Only Malaysian company to graduate from 500 Startups Accelerator in Silicon Valley, with funding from Coinsilium too

## BUSINESS FOCUS

With DBS, Axiata, Maybank and Securities Commission as clients, we cover a broad spectrum of industries

## FULL-STACK SERVICES

We provide corporate blockchain training and workshops along with consulting on solutions utilizing Cortex

# BLOCKCHAIN TECHNOLOGY IS COMPLICATED

## Blockchains

difficult to choose between a thousand chains with hundreds of different consensus methods and protocols

### Massive Data Sets

TeraBytes of data with billions of records requires a lot technical resources, talent and time

### Disrupting Businesses

Current tools & services designed for individuals and developers; to replace businesses

### Financial Focus

Although crypto-currencies now account for over US\$140 billion, they are merely the fuel for data storage

# WE SIMPLIFY THINGS

## Cortex

we've used decades of distributed ledger developer experience to build a platform that supports the best of the blockchains

### Private APIs

We process multiple blockchains and provide dedicated APIs built for individual businesses

### Enterprise Solutions

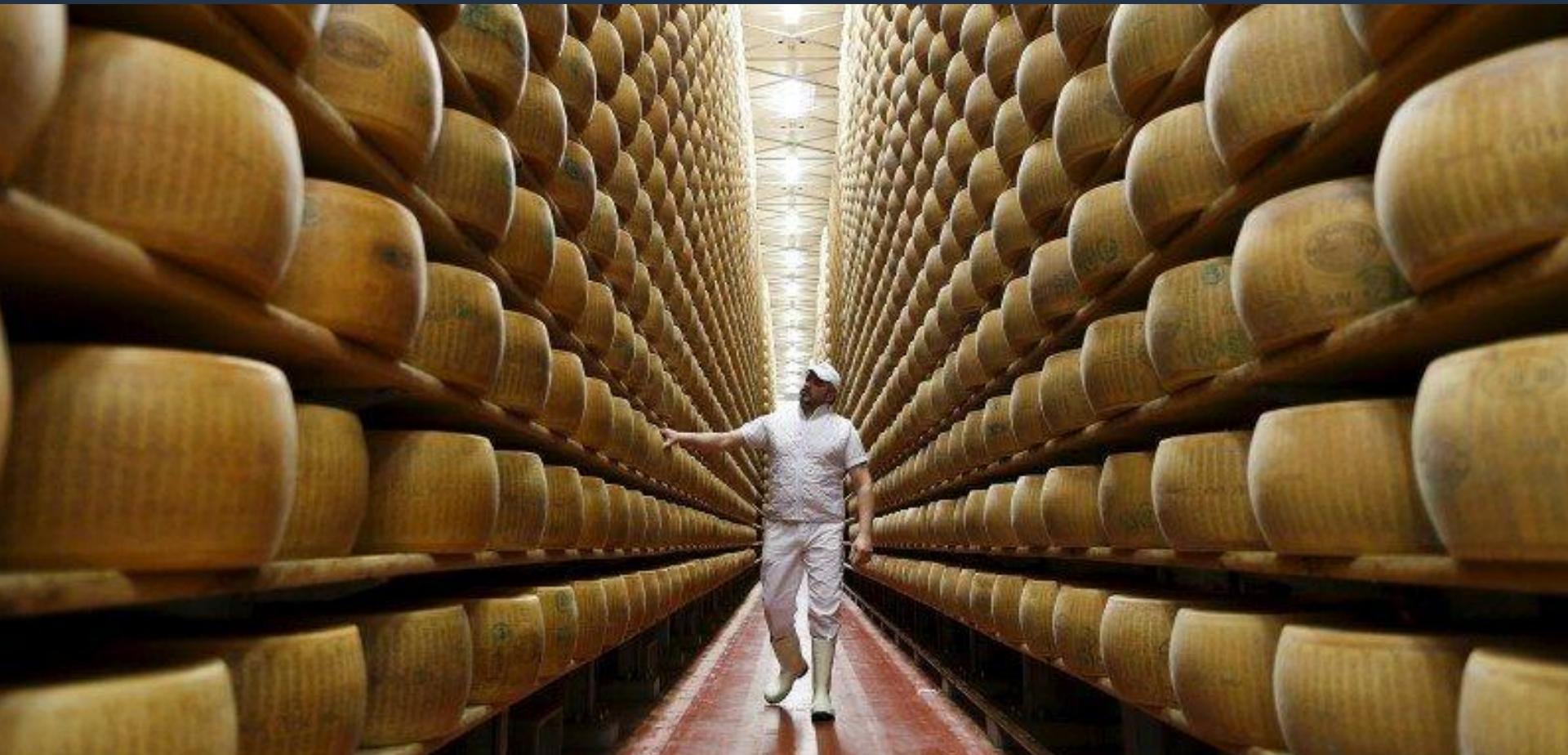
Our products and services have specifically been designed for organizations and businesses

### Agnostic Protocols

We have developed non-financial protocols for data and identity that work across multiple blockchains

A BRIEF HISTORY OF MODERN MONEY  
**( FROM CHEESE TO CRYPTO )**

# EDIBLE CURRENCIES STILL EXIST IN EUROPE TODAY



IN ASIA - YOU COULD AT ONE STAGE DRINK CURRENCY TOO



THE ISLANDS OF YAP HAVE THE MOST RELEVANT EXAMPLE



# SHOPPING WAS ALMOST AS CHALLENGING AS BANKING



SO THEY INVENTED THE WORLD'S FIRST PUBLIC LEDGER



# THEY USED GROUP CONSENSUS - SAME AS BITCOIN



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

THEIR IDEAS COULDN'T SCALE - SO THEY SWITCHED TO US\$



# AMERICA SET THE GOLD STANDARD FOR ECONOMICS



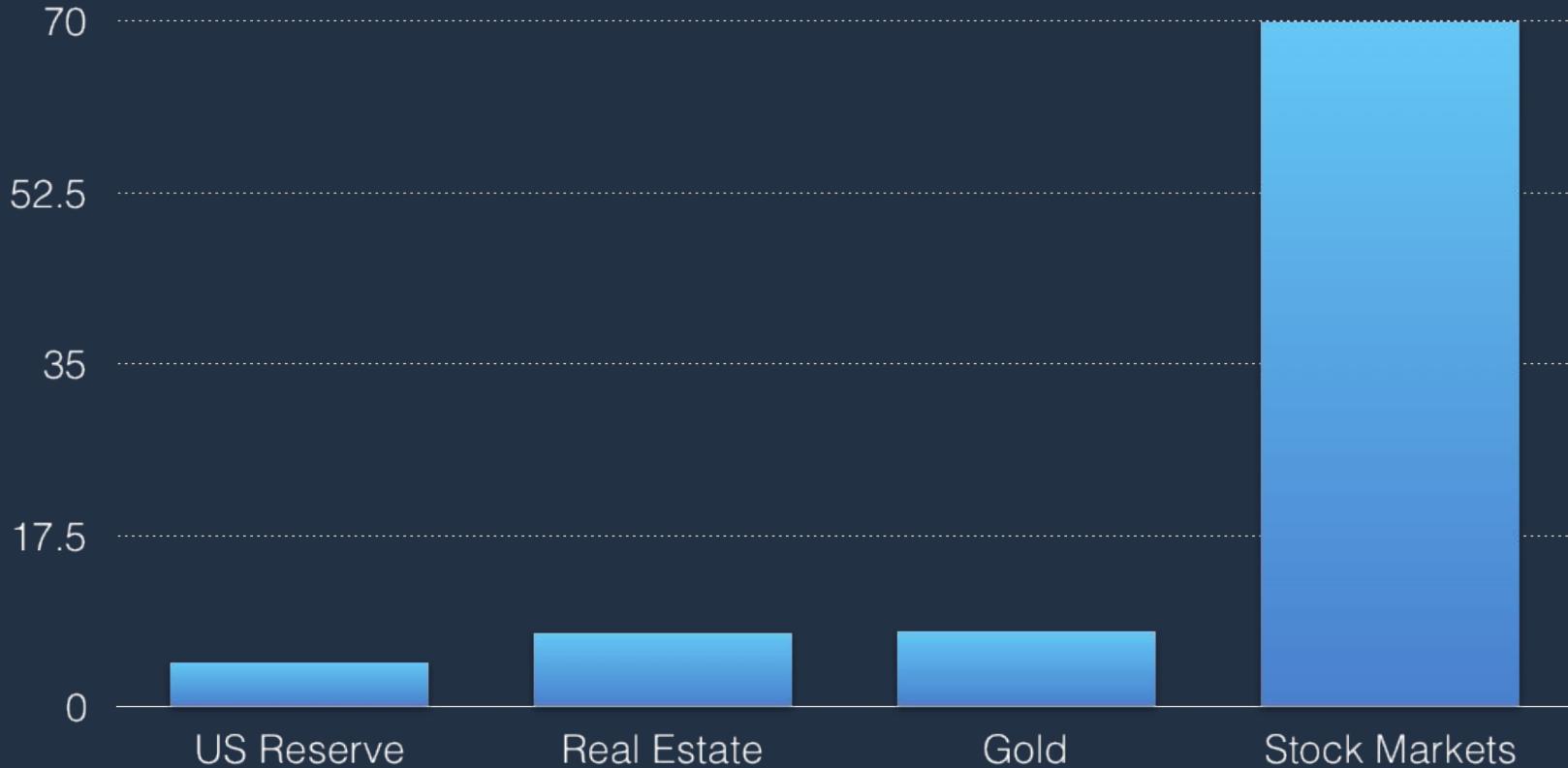
# THE END OF AN ERA

- 1873 to 1914 - All major worldwide currencies were 100% backed by gold
- After WW1 ended the USA switched to Fractional Reserve Banking  
They Printed 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

# US\$20 TRILLION OF PHYSICAL ASSETS WITHOUT LEDGERS



# THEN CAME WALL STREET & CENTRALIZED DIGITAL ASSETS



# AND WITH IT - THE RE-INVENTION OF DEBT



# IT ALL ENDS IN TEARS IN 2008 WITH 500+ BANKS CLOSING



# NOTHING LASTS FOREVER



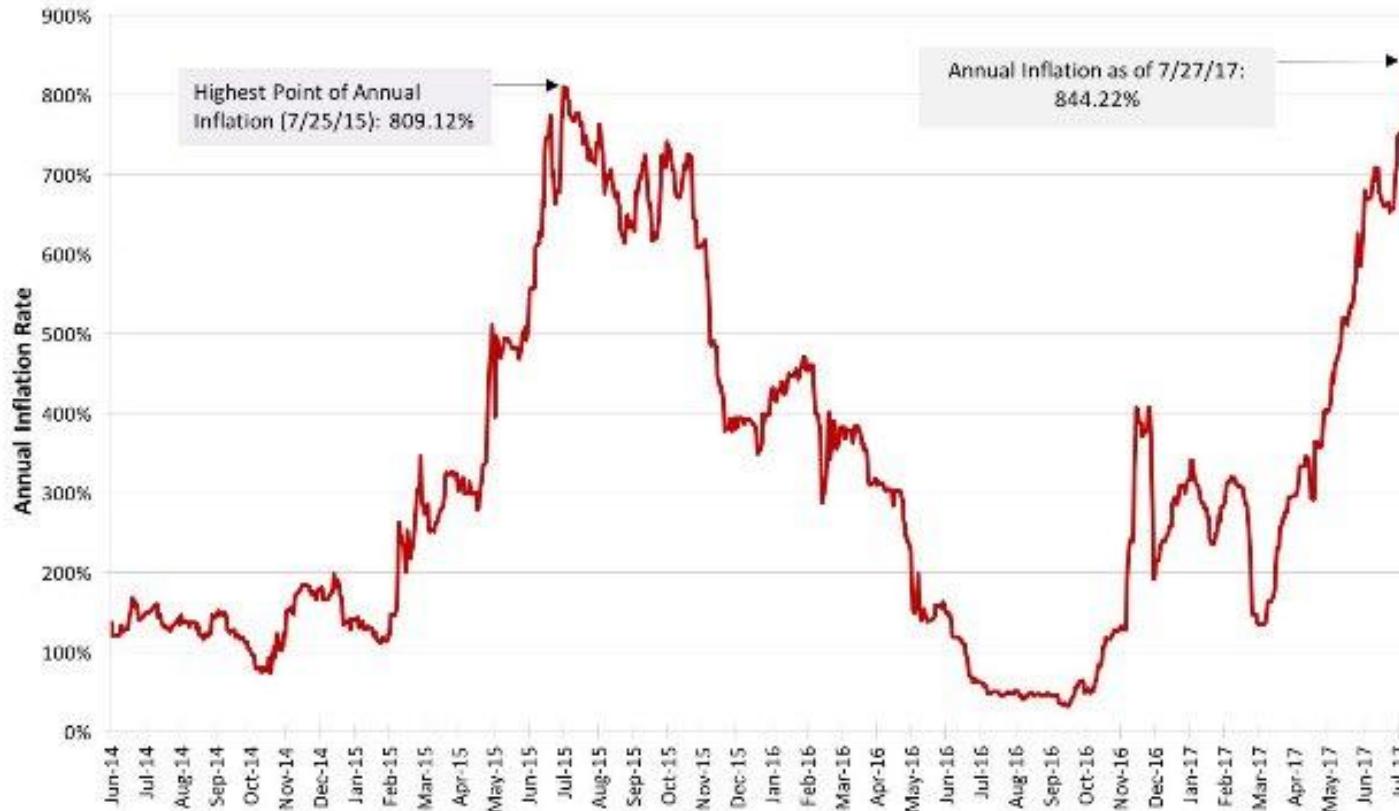
- Average lifespan of individual currencies is 27 years
- Every 30 or 40 years the reigning monetary system fails
- Over 3,800 fiat currencies worldwide have failed
- 15 of which happened in just the past 25 years

# 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

# THE CURRENT FAILURE OF FIAT

## Venezuela's Annual Inflation Rate



# TELECOMMUNICATIONS SAVED ZIMBABWE



# “ SOFTWARE IS EATING THE WORLD ”



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

# DOES ANYONE REMEMBER KODAK ...?



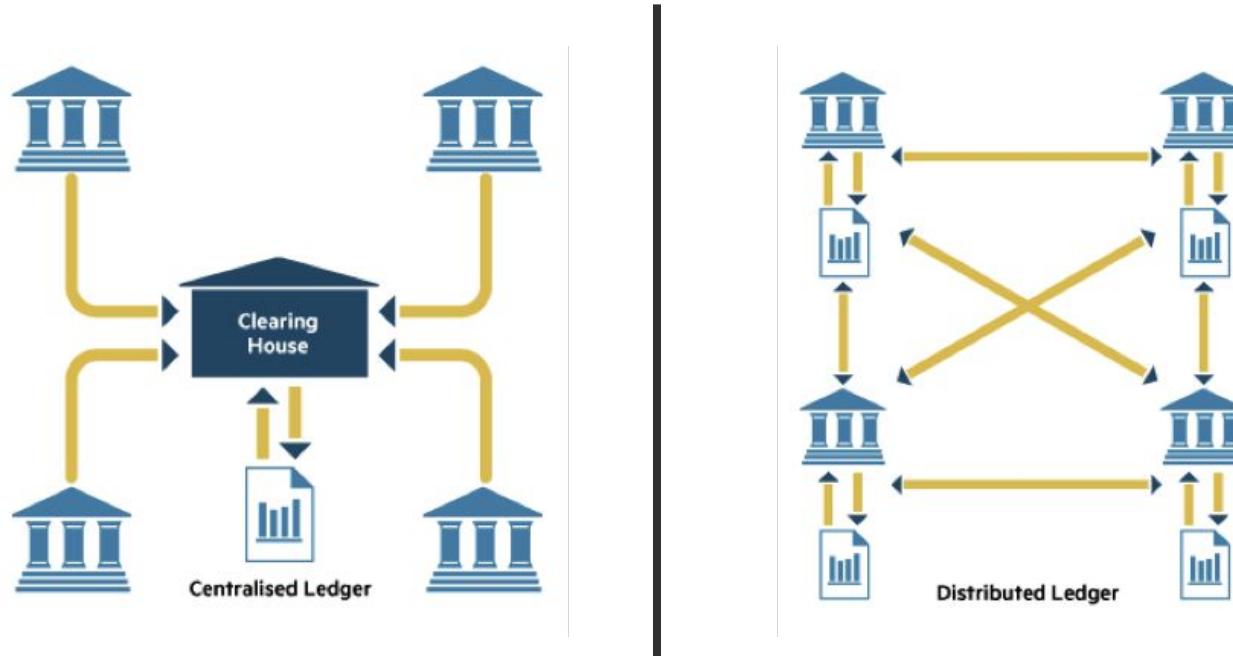
- Founded in 1892
- 90% of film sales in 1976
- 85% of camera sales in 1976
- 4th biggest global brand in 1996
- Removed from S&P 500 in 2010
- Bankrupt in 2012
- And yet...

# ARE BANKS HAVING THEIR 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**

# SANTANDER BANK - 1st TO ADMIT US\$20B ANNUAL SAVINGS



- Reconciling Multiple Central Ledgers Vs Auto-Audited Distributed Ledgers?
- Batch Processing CSVs every 24 Hours Vs Really Real-Time Settlement?

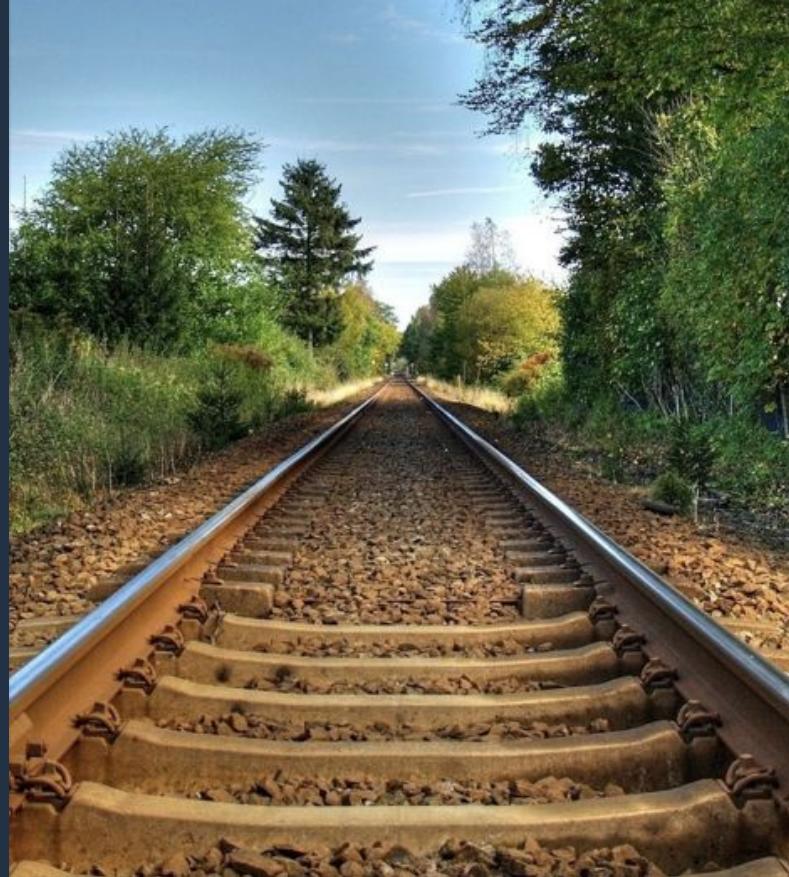
# **BITCOIN**

( the first application / popular digital asset )

Vs

# **BLOCKCHAINS**

( underlying tech / shared public ledger )



# ETHEREUM

( open network for building anything )

Vs

# PRIVATE NETWORKS

( very similar to traditional database )



# **PUBLIC BLOCKCHAINS**

( enables permissionless innovation )

Vs

# **PERMISSIONED LEDGERS**

( puts new central controllers into authority )

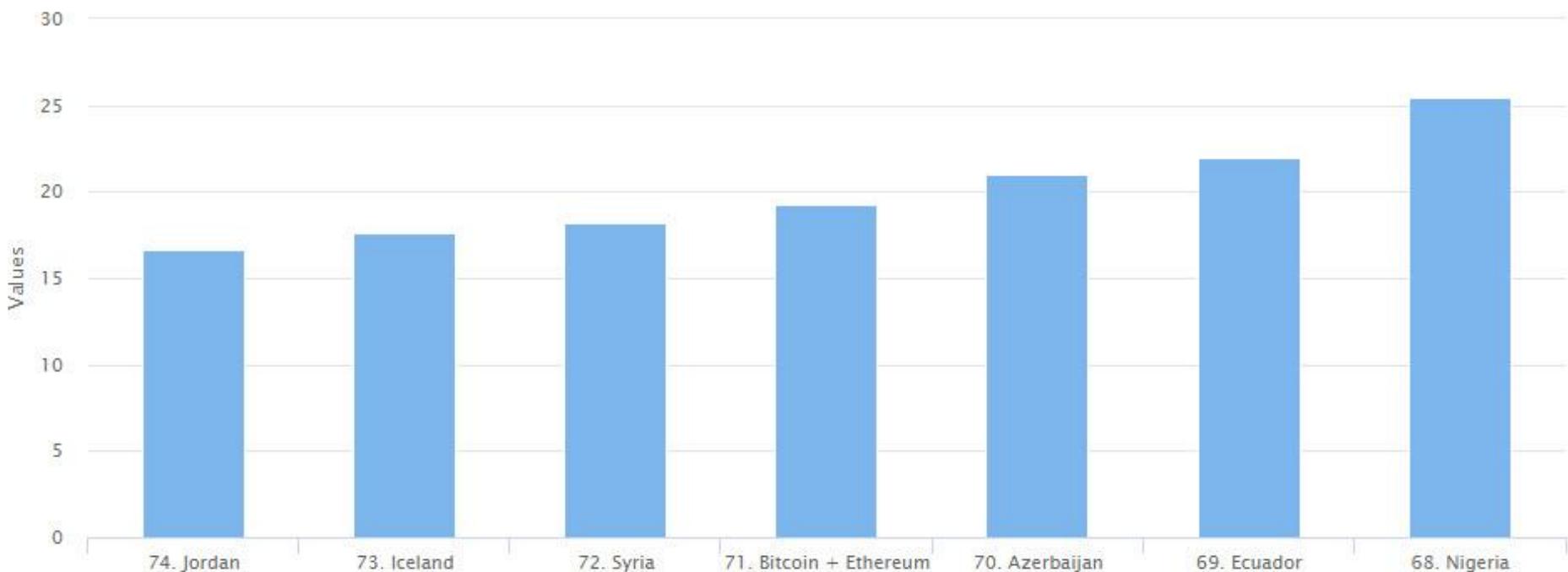


IT'S ALL A QUESTION OF CONSENSUS - AND ENERGY ...?

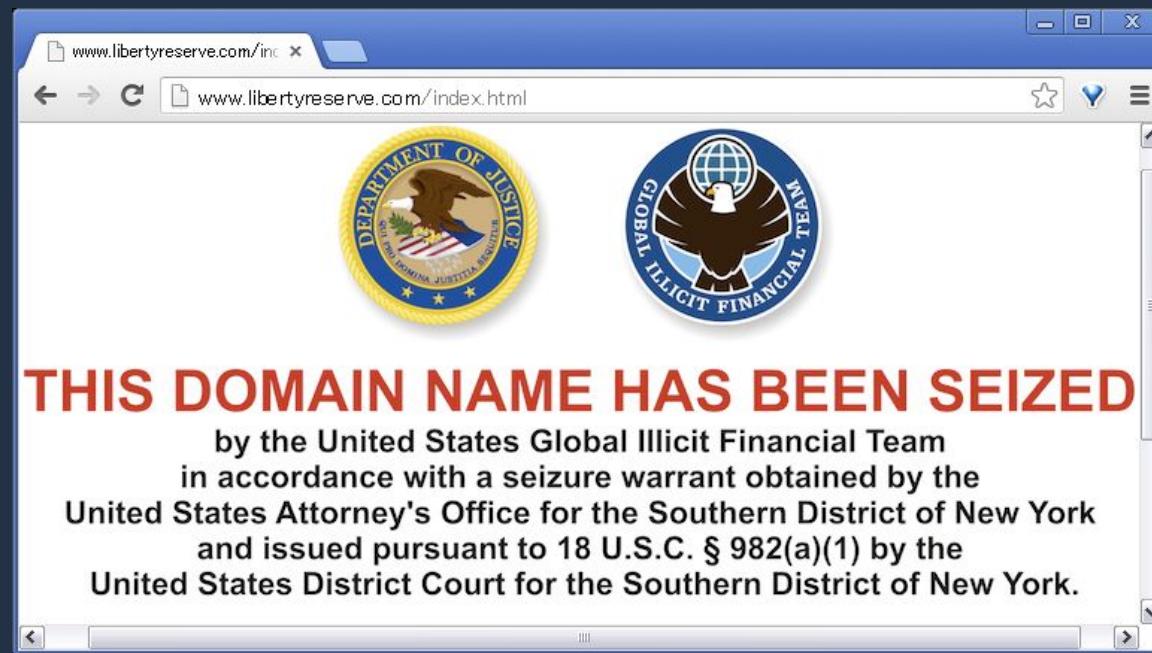


# MORE ENERGY THAN ICELAND, SYRIA, AND JORDAN

Energy Consumption by Country inc. Bitcoin & Ethereum



# BUT WHY ...?



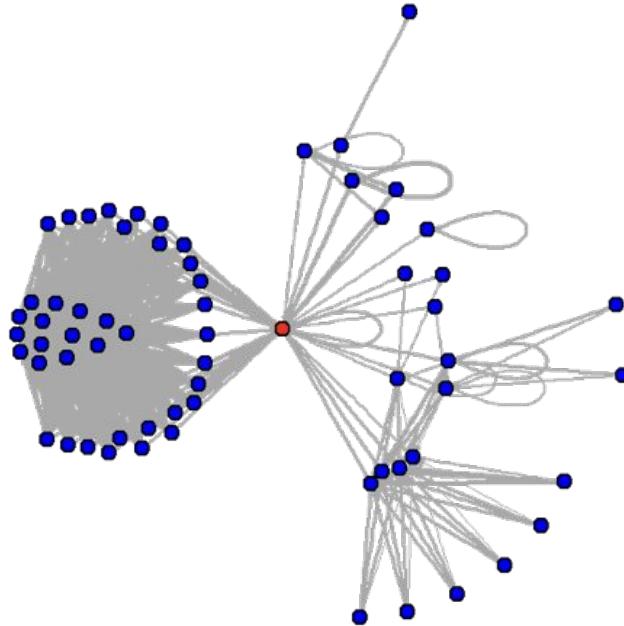
- FLOOZ - Shut down by FED in 2001
- LIBERTY RESERVE - Shut down by FED in 2013

# TRUST IS SOLVED VIA TRANSPARENCY

```
{  
    "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": "e9a38d8fa6b7abcl35a2fad93bfa52e3eb9b1ca5cb2825692db0a3c2f054354",  
            "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,  
            "script": "OP_DUP OP_HASH160 3ebaecf042e0dbe20a35c0dd2700c83b13a5a1764e1882c2cc39e4bd81c326cf OP_EQUALVERIFY OP_RETURN"  
        }  
    ]  
}
```

# EVERYONE HAS A COPY OF EVERYTHING

BTC transaction network for  
1NfRMkhm5vjizzqkp2Qb28N7geRQCa4XqC



# WHAT ARE THE BENEFITS OF A PUBLIC BLOCKCHAIN ...?

- 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 costs and errors

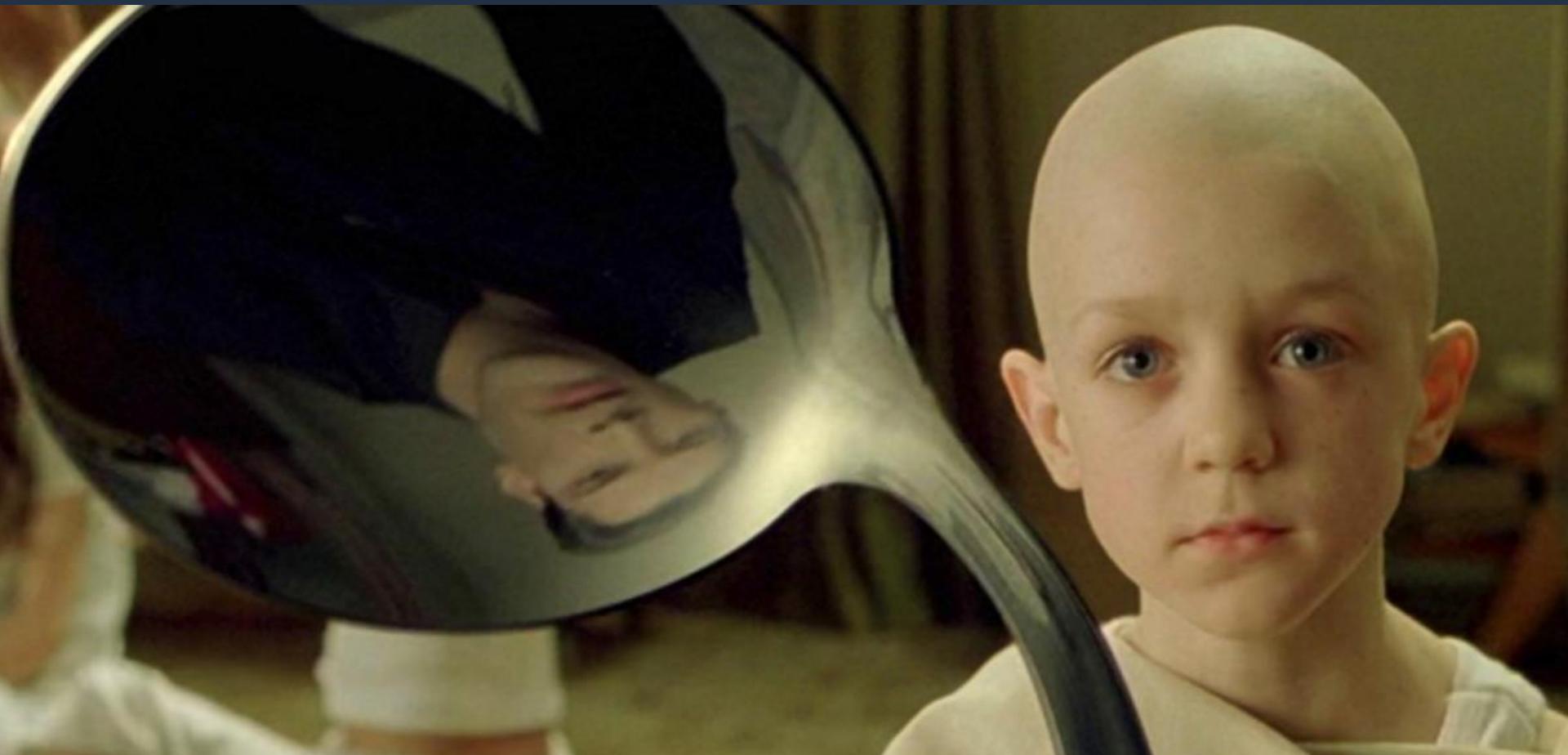


“While Fintech Disrupts Banks,  
the Blockchains Disrupt Fintech”

# GIVING THE BITCOIN CURRENCY SOME UNIQUE PROPERTIES

Traits of Good Money	Gold	\$\$\$	Private DLTs	Bitcoin
Durability		fragile		
Portability	heavy			
Divisibility	difficult	limited		
Uniformity	if processed		censored	
Limited Supply	theoretically	printed at will	central mint	
Sunnah Money	Commodities	\$\$\$		Bitcoin
Intrinsic Value		representation	none	
Inflation Proof	unknown	debt based	no	
Acceptability	limited		unknown	growing daily
Decentralized		man made	unregulated	

LET'S NOT FORGET THAT THERE ARE NO BITCOINS



WHAT COULD REPLACE THE US\$ AS A WORLD RESERVE ...?



NOW POSSIBLE THANKS TO THIS MAN



# BIG PLANS FOR THE FUTURE - HOW FAR IN THE FUTURE ...?



# SOLAR POWERED ROBOTS BUILDING AUTONOMOUS CARS



TESLA

# DRIVING THEMSELVES TO A SELF-CHARGING HOME



EXPLORING THE TECHNOLOGY

**HOW AND WHY DO BLOCKCHAINS WORK ...?**

# INTERESTING BITCOIN FACTS TO REMEMBER

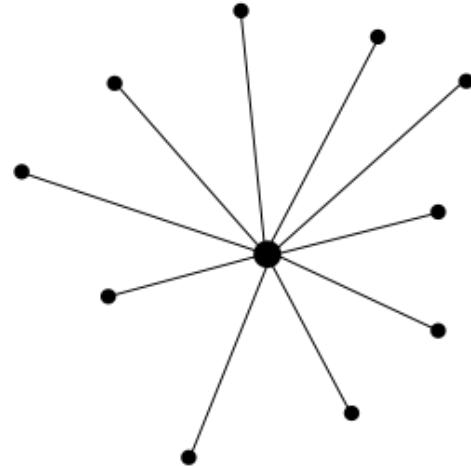
- Bitcoin blockchain released in January 2009 by Satoshi Nakamoto
- US\$13 per coin in 2013 (when we bought) - now US\$4,200+ per coin
- The network is currently processing over 230,000+ daily transactions
- Contributes to over US\$5+ billion of daily global crypto-transactions
- The network's market capitalization is currently over **US\$69+ billion**
- 21 million finite supply, with 16 million coins discovered so far
- Supply is decreasingly dispersed every 10 minutes
- Final coins released on May the 7th, 2140
- **But most important of all is the technology...**

# THE BITCOIN BLOCKCHAIN HAS NO NEW TECHNOLOGY

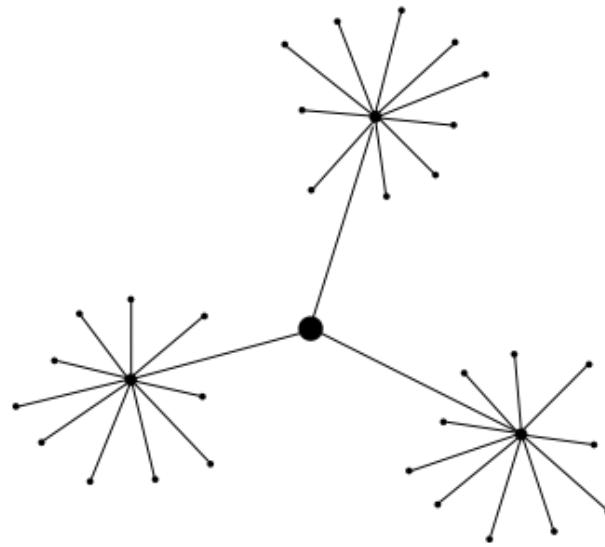


- HASH - Theorized in the 1800s - Coined by IBM in the 1950s
- ECDSA - Digital Signatures using Elliptic Curve Cryptography
- P2P - Peer to peer protocol popularized by Napster in 1999

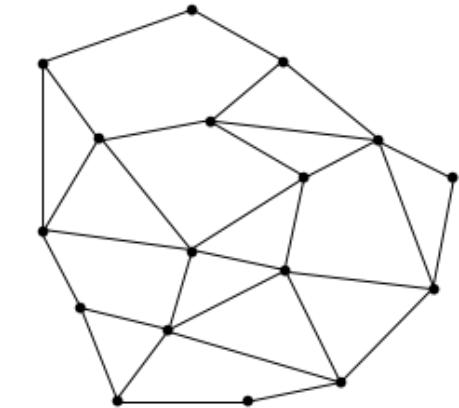
# AN EVOLUTION OF TECHNICAL NETWORK TOPOLOGIES



CENTRALIZATION  
DATABASE

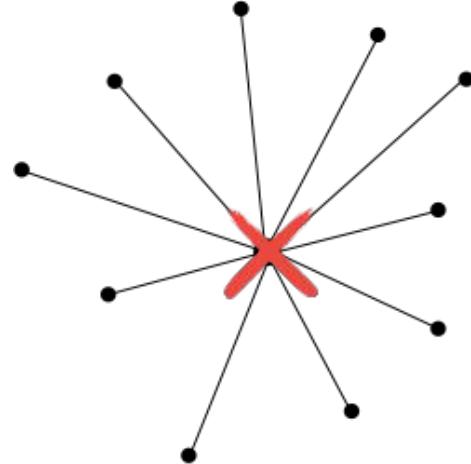


DECENTRALIZATION  
CLOUD

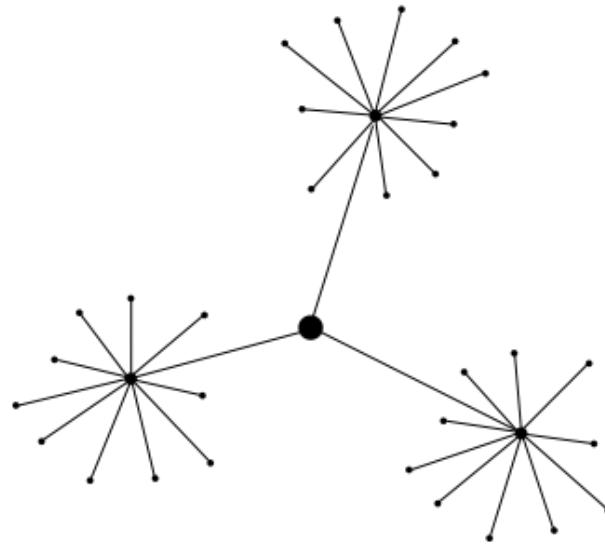


DISTRIBUTION  
BLOCKCHAINS

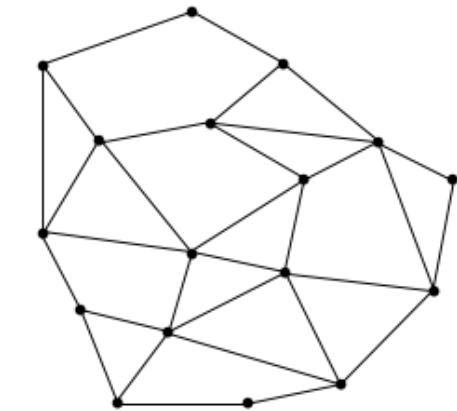
# AN EVOLUTION OF TECHNICAL NETWORK TOPOLOGIES



CENTRALIZATION  
DATABASE

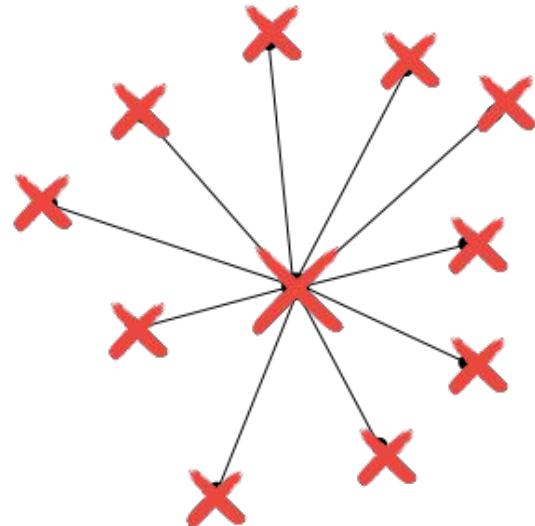


DECENTRALIZATION  
CLOUD

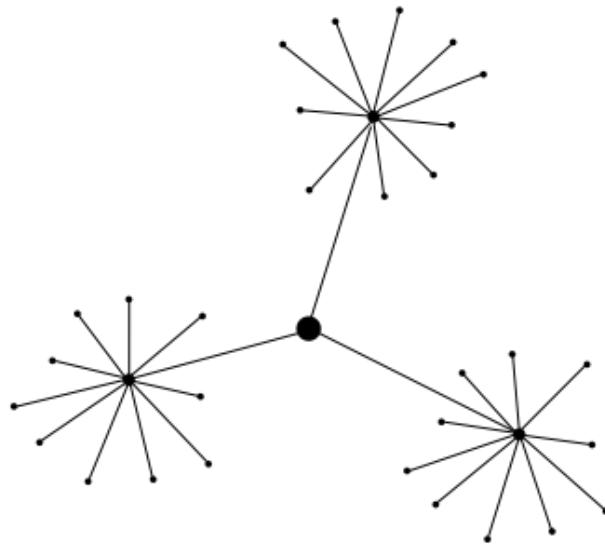


DISTRIBUTION  
BLOCKCHAINS

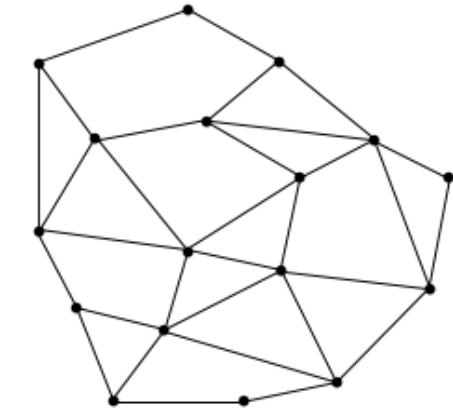
# AN EVOLUTION OF TECHNICAL NETWORK TOPOLOGIES



CENTRALIZATION  
DATABASE

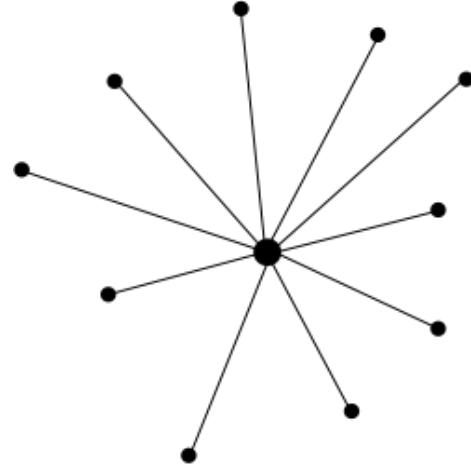


DECENTRALIZATION  
CLOUD

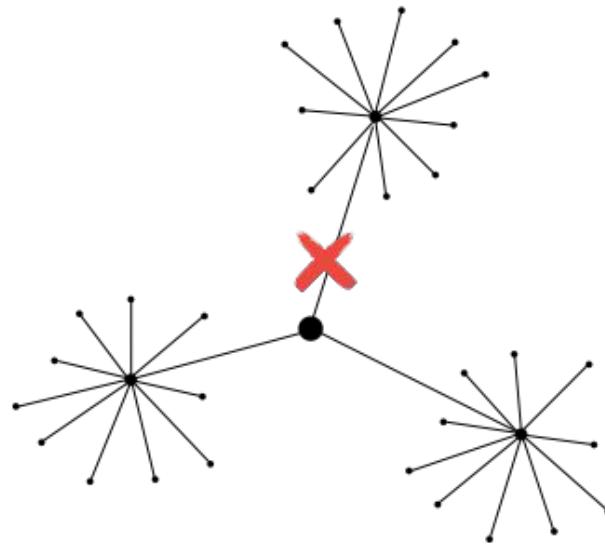


DISTRIBUTION  
BLOCKCHAINS

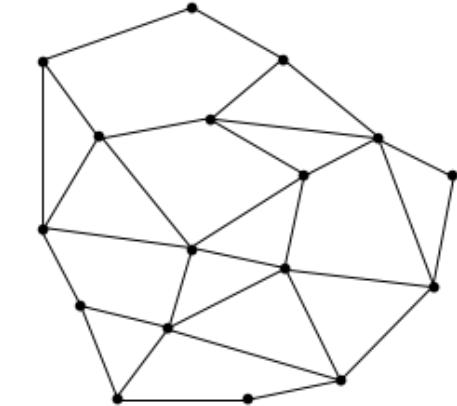
# AN EVOLUTION OF TECHNICAL NETWORK TOPOLOGIES



CENTRALIZATION  
DATABASE

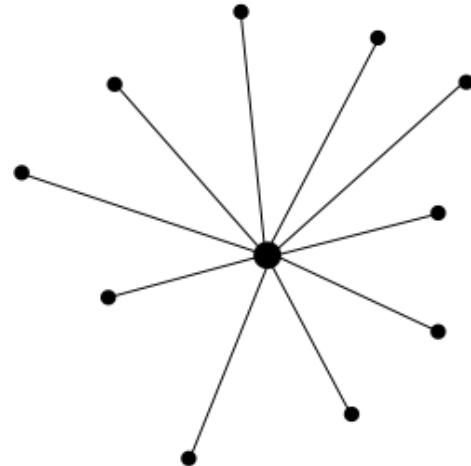


DECENTRALIZATION  
CLOUD

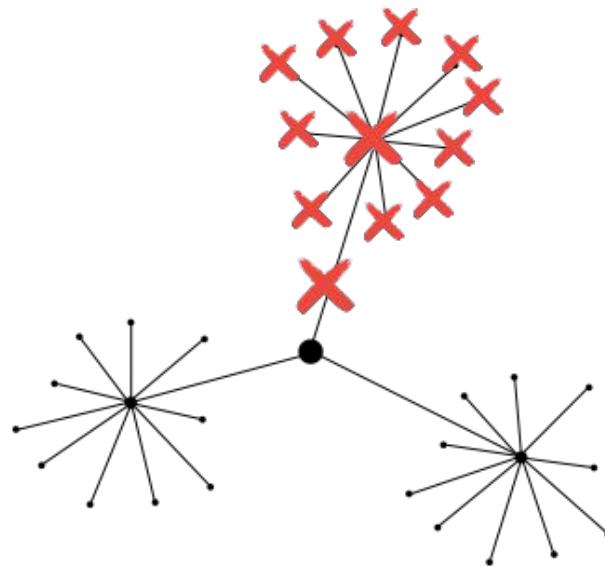


DISTRIBUTION  
BLOCKCHAINS

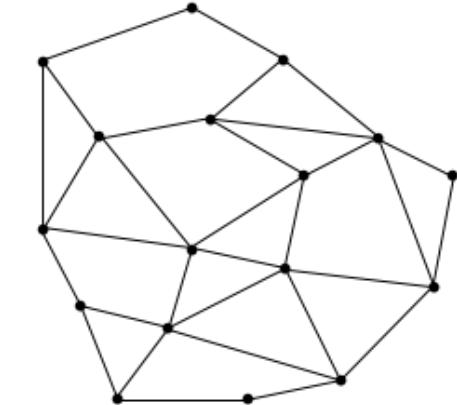
# AN EVOLUTION OF TECHNICAL NETWORK TOPOLOGIES



CENTRALIZATION  
DATABASE

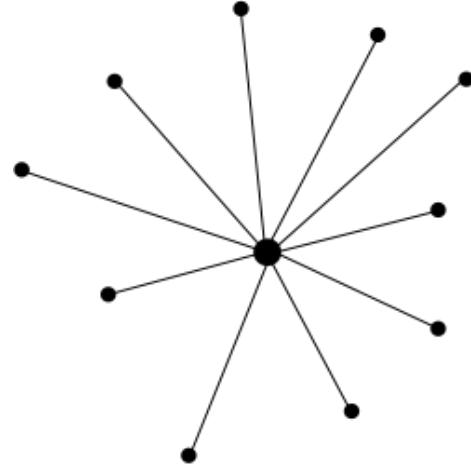


DECENTRALIZATION  
CLOUD

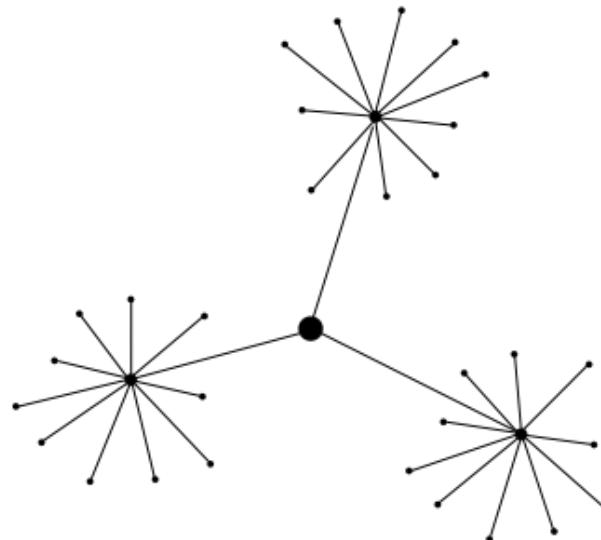


DISTRIBUTION  
BLOCKCHAINS

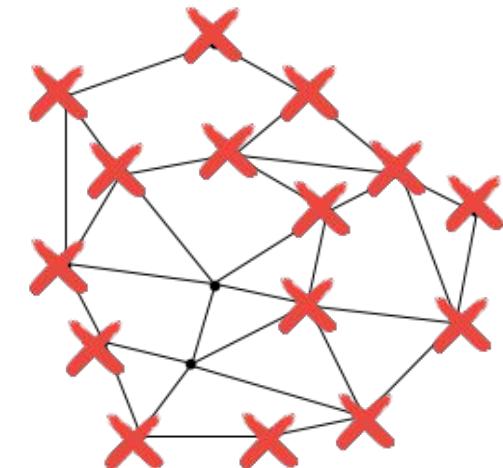
# AN EVOLUTION OF TECHNICAL NETWORK TOPOLOGIES



CENTRALIZATION  
DATABASE

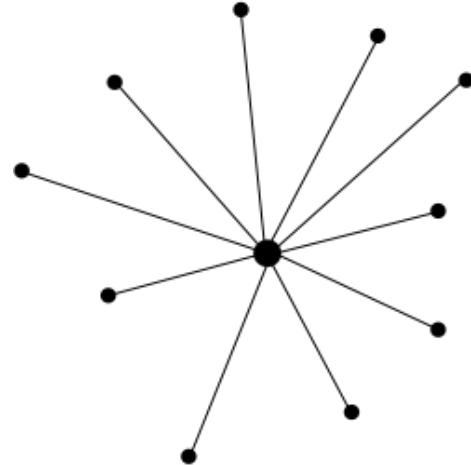


DECENTRALIZATION  
CLOUD

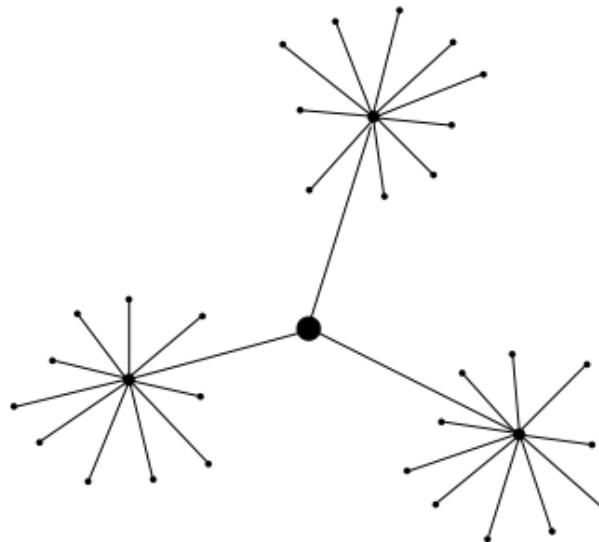


DISTRIBUTION  
BLOCKCHAINS

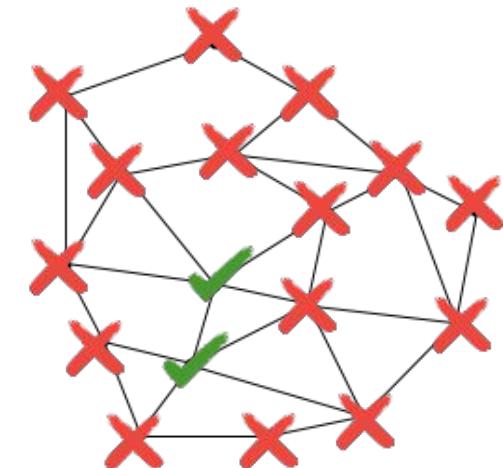
# AN EVOLUTION OF TECHNICAL NETWORK TOPOLOGIES



CENTRALIZATION  
DATABASE

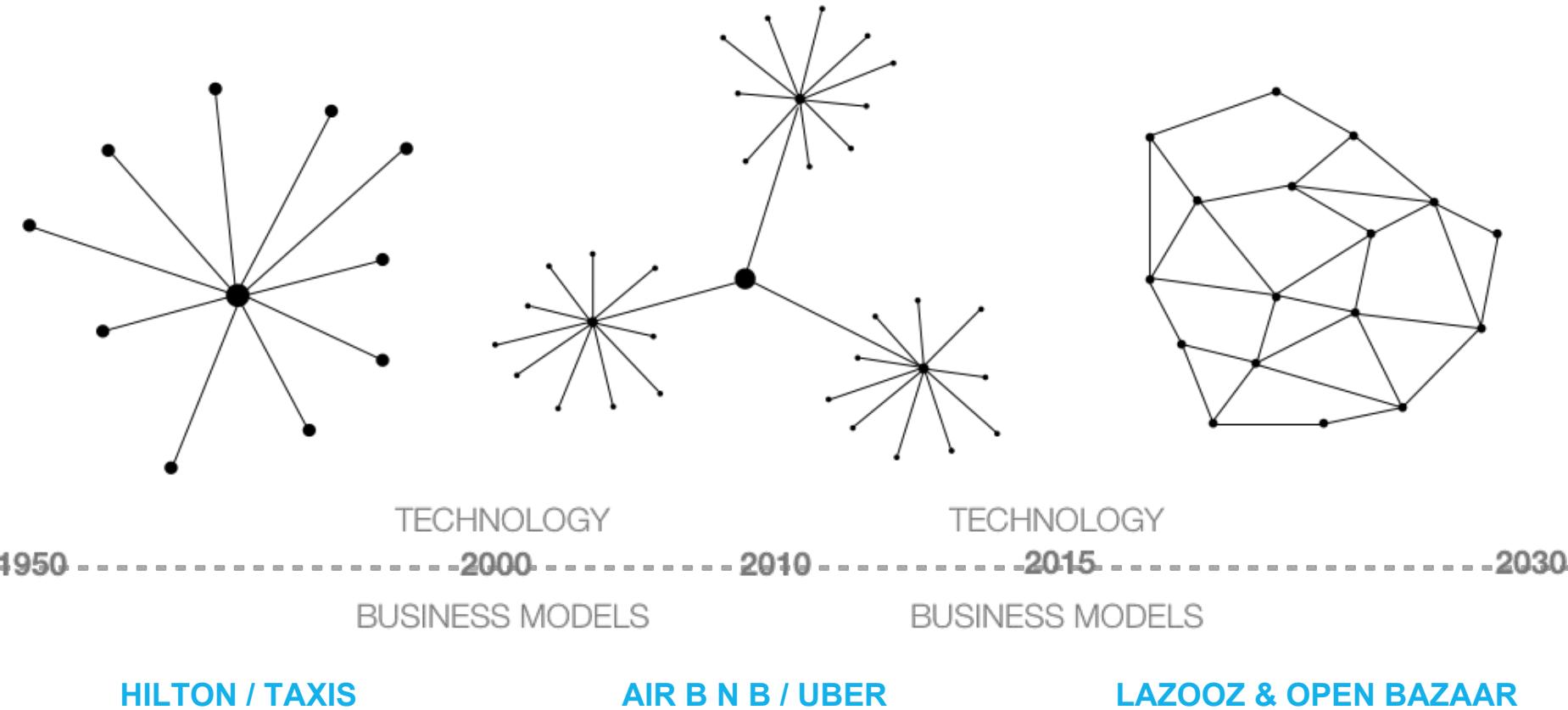


DECENTRALIZATION  
CLOUD



DISTRIBUTION  
BLOCKCHAINS

# OR IS IT THE EVOLUTION OF EVERYTHING ...?



# BLOCKCHAINS ARE MERELY A NETWORK OF NODES

- Each member of the network runs their own node
- With bitcoin, all nodes are equal and no permission is required
- The networks becomes more secure as more nodes join
- All transactions across the entire network are tracked by each node
- On the blockchain - no one knows you're a fridge

# ON THE BLOCKCHAINS - ACCOUNTS ARE KEYS



# WHAT DO THESE KEYS ACTUALLY LOOK LIKE ...?



ONE PUBLIC KEY



MULTIPLY PRIVATE KEYS

- Example of a Bitcoin public address (derived from the public key):  
`1GzBZ7eK6wzNjp1Wt6AxHo73kJL2tzoErq`
- Example of a Bitcoin private key (used to transfer funds from address):  
`L1winVkoRmxMdHKbwssx33Z9ZEuXeJ1eP9CVYvnNn4TdYA32GsWY`
- Example of a Bitcoin extended private key (used by HD protocol):  
`xprv9s21ZrQH143K2Ywhg9bhZ5nd31t3EbXsg8v28gkKjSm9PA3PiZ89dWW6YKxWZa2pgTuErQ65K46KGVfu1xCRBCK3Ppd465QGtH7TmxAEiLv`

SALT = CRYPTO | UN = BOOTCAMP | PW = MCQ4

**MONEY CAN NOW BE EMBEDDED INTO ANYTHING**



THIS SLIDE ONCE CONTAINED 100 DOGECOINS

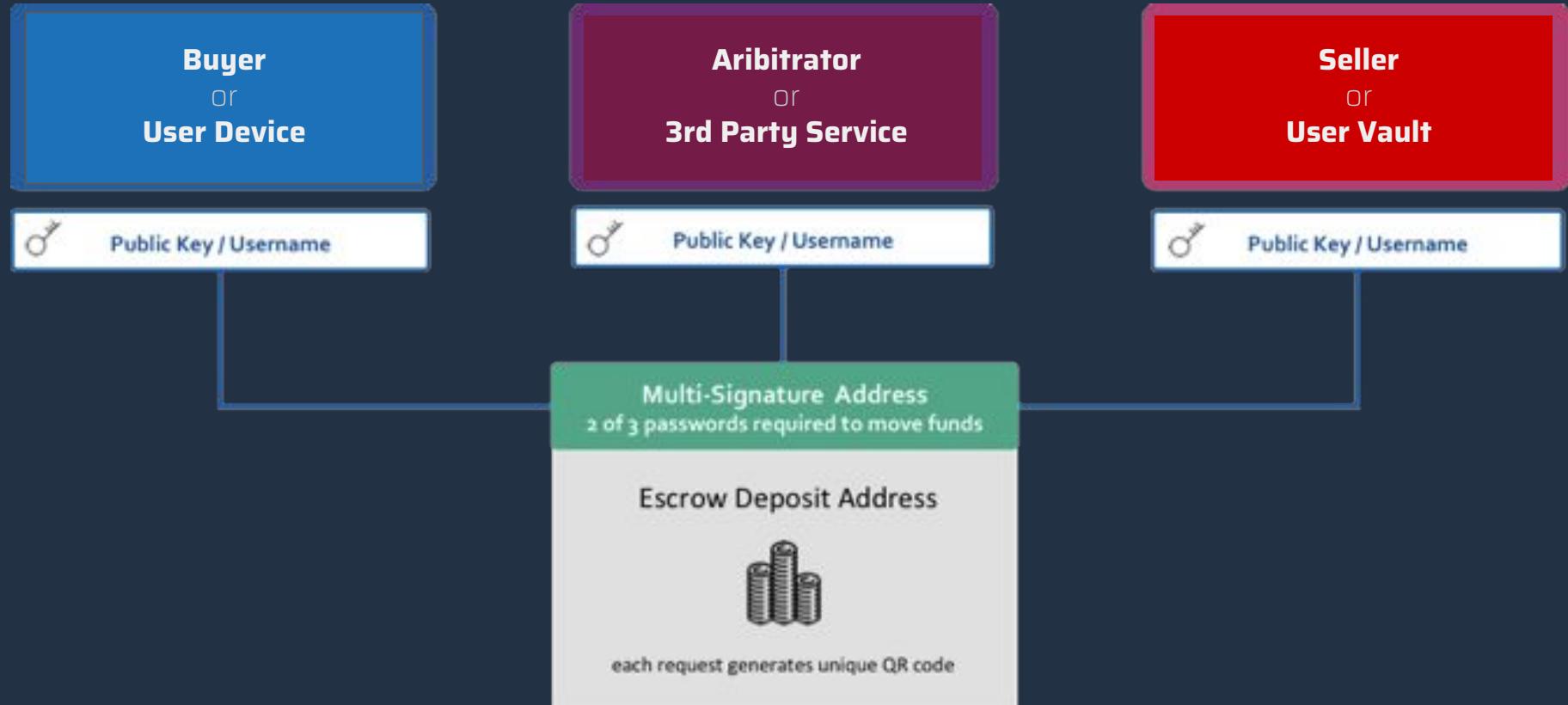
# EACH PUBLIC ADDRESS REQUIRES A PRIVATE KEY TO SPEND



SOME ADDRESSES REQUIRE MULTIPLE KEYS



# USEFUL FOR RECOVERY AND ESCROW SERVICES

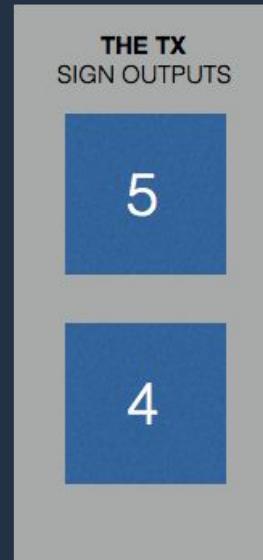
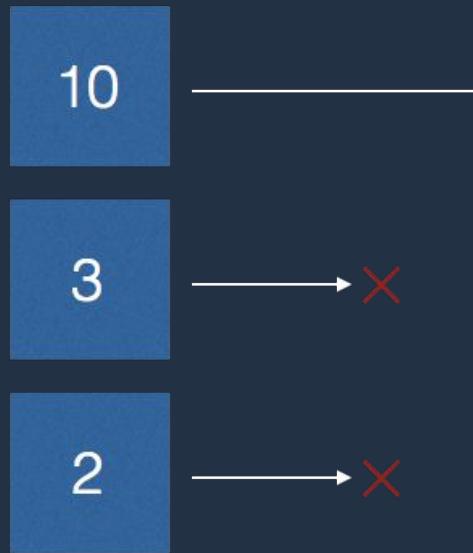


# SO WHAT'S INSIDE A BITCOIN TRANSACTION ...?

- 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)
- However, they can only contain one OP\_Return (38 bytes of arbitrary data)

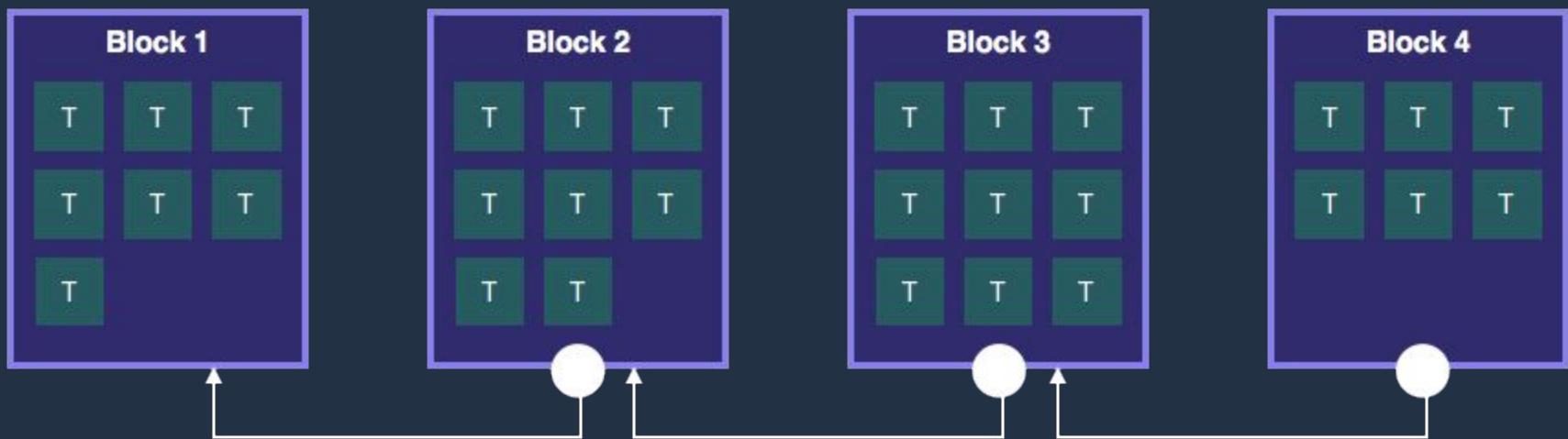
# HOW DOES A BITCOIN TRANSACTION ACTUALLY WORK ...?

ALICE'S UNSPENT INPUTS

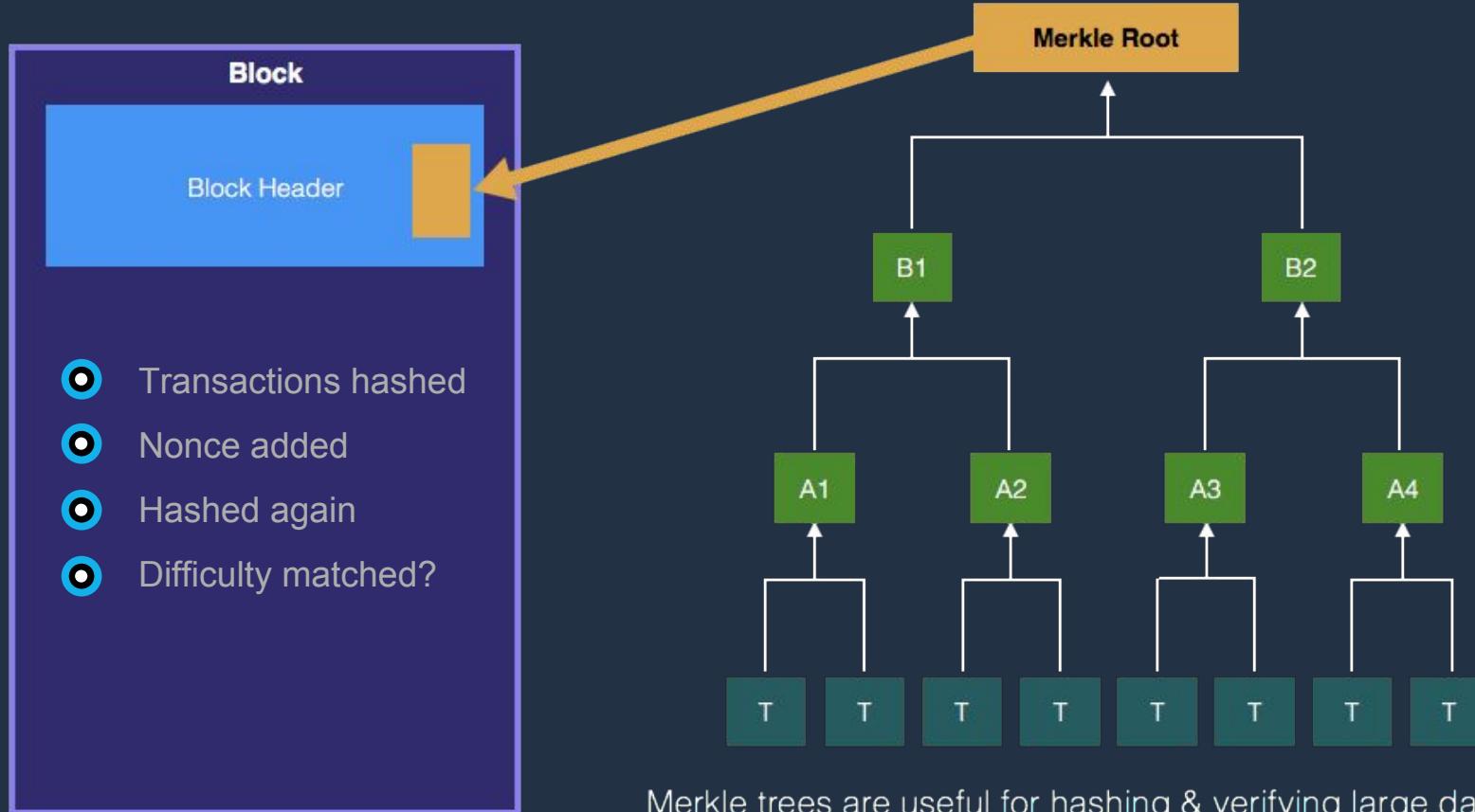


# SO WHERE DO THE BLOCKS COME FROM ...?

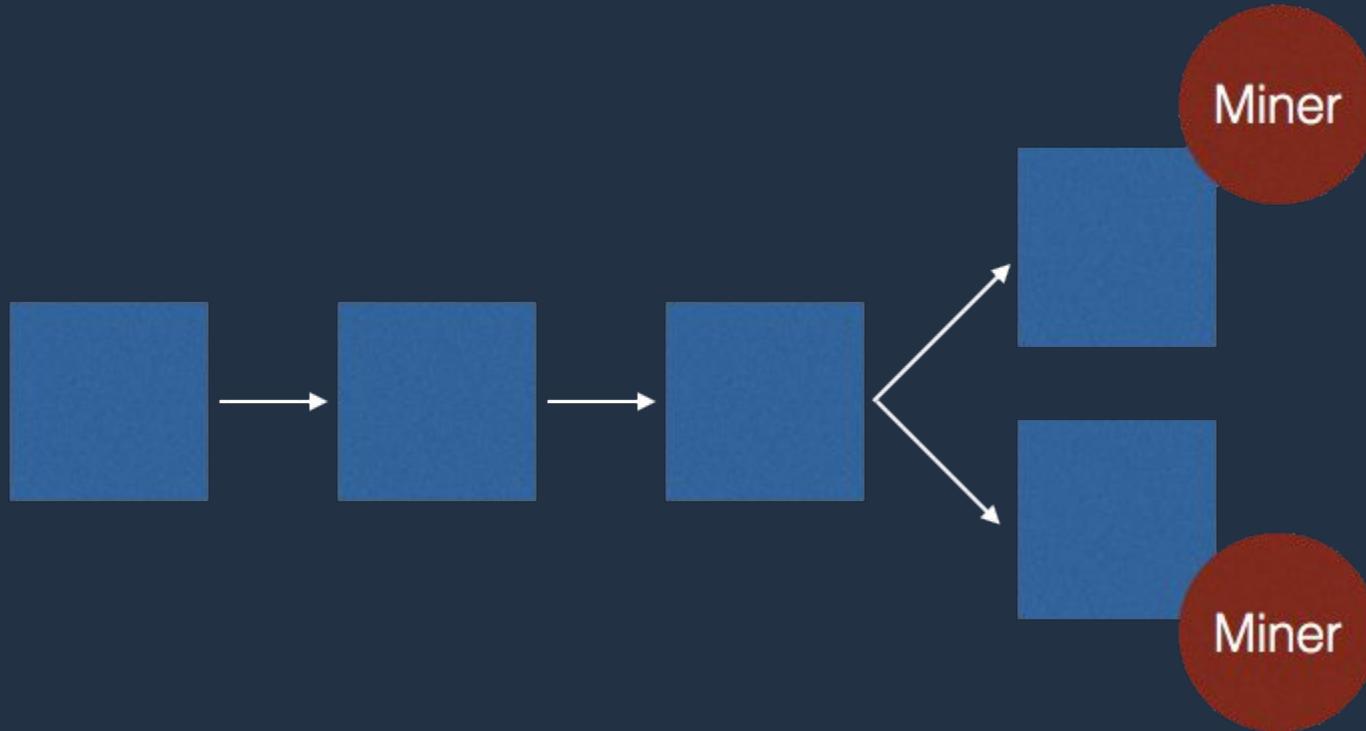
- Transactions are batched into blocks every ten minutes (with Bitcoin)
- The block is added to the chain with a link to the previous block
- With the block added to the chain, its transactions are then **confirmed**



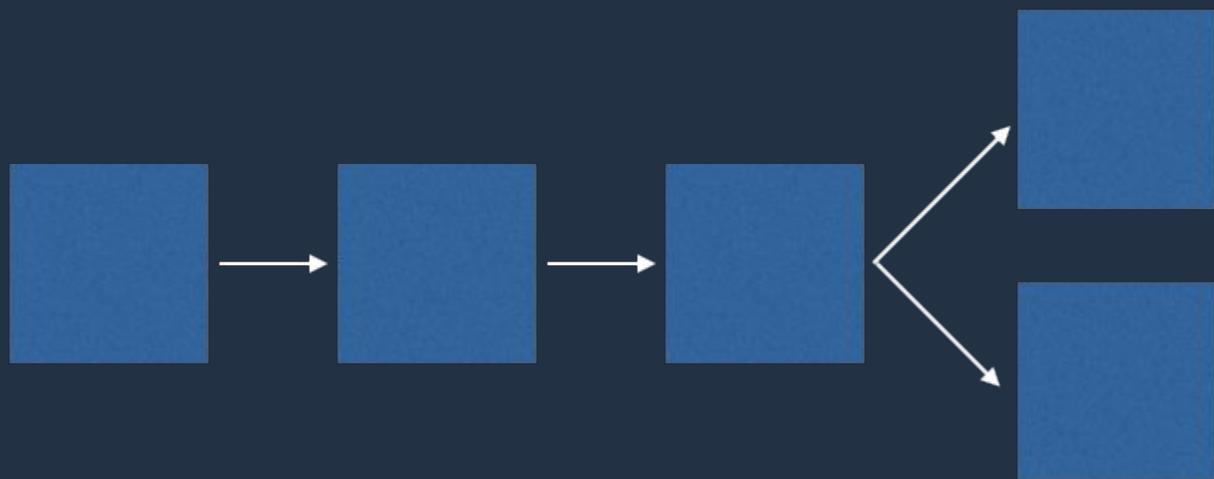
# WHAT IS ACTUALLY LINKING THE CHAINS ...?



# ACCOUNTING FOR IMPERFECTIONS

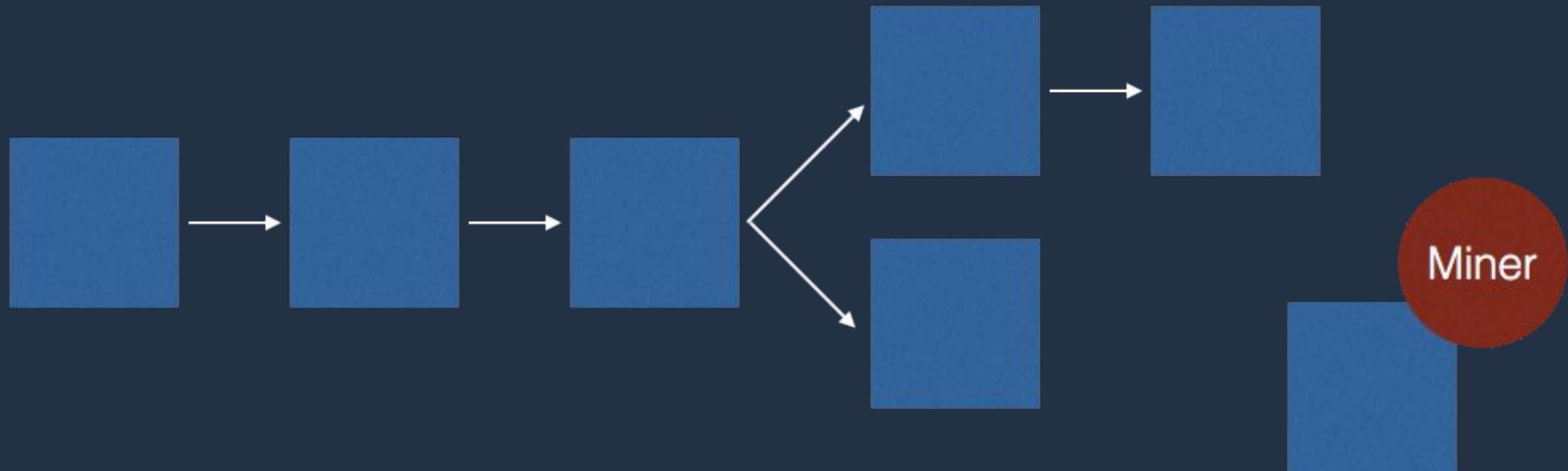


# PROBLEMS RESOLVE THEMSELVES - EVENTUALLY



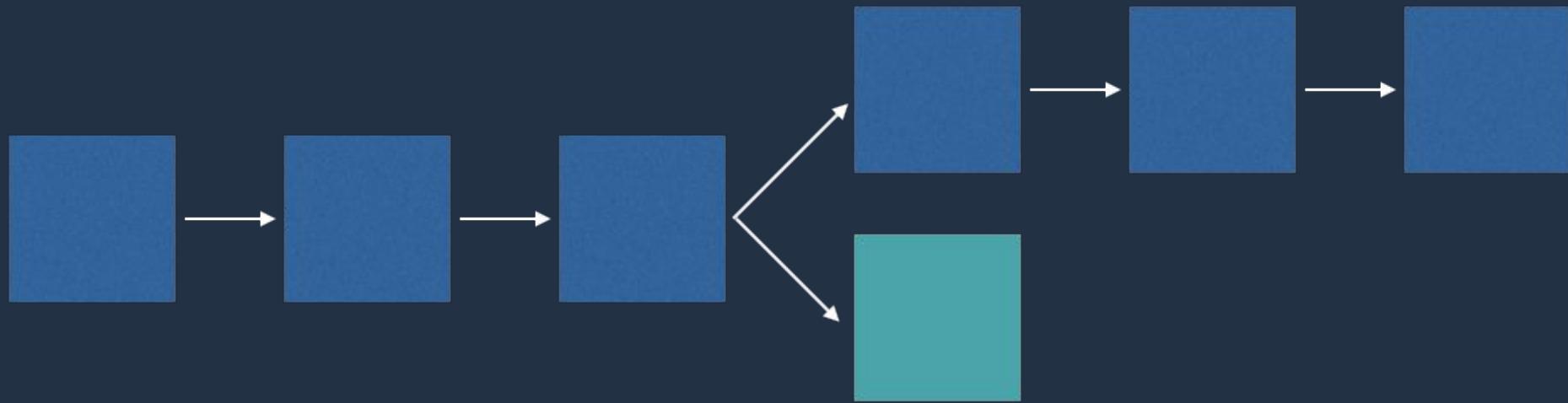
Randomly picks one  
chain if both forks are  
the same length

# THE LONGEST CHAIN ALWAYS WINS



If one fork is longer than the other,  
pick the longest fork

# UN-CONFIRMING ONCE CONFIRMED TRANSACTIONS

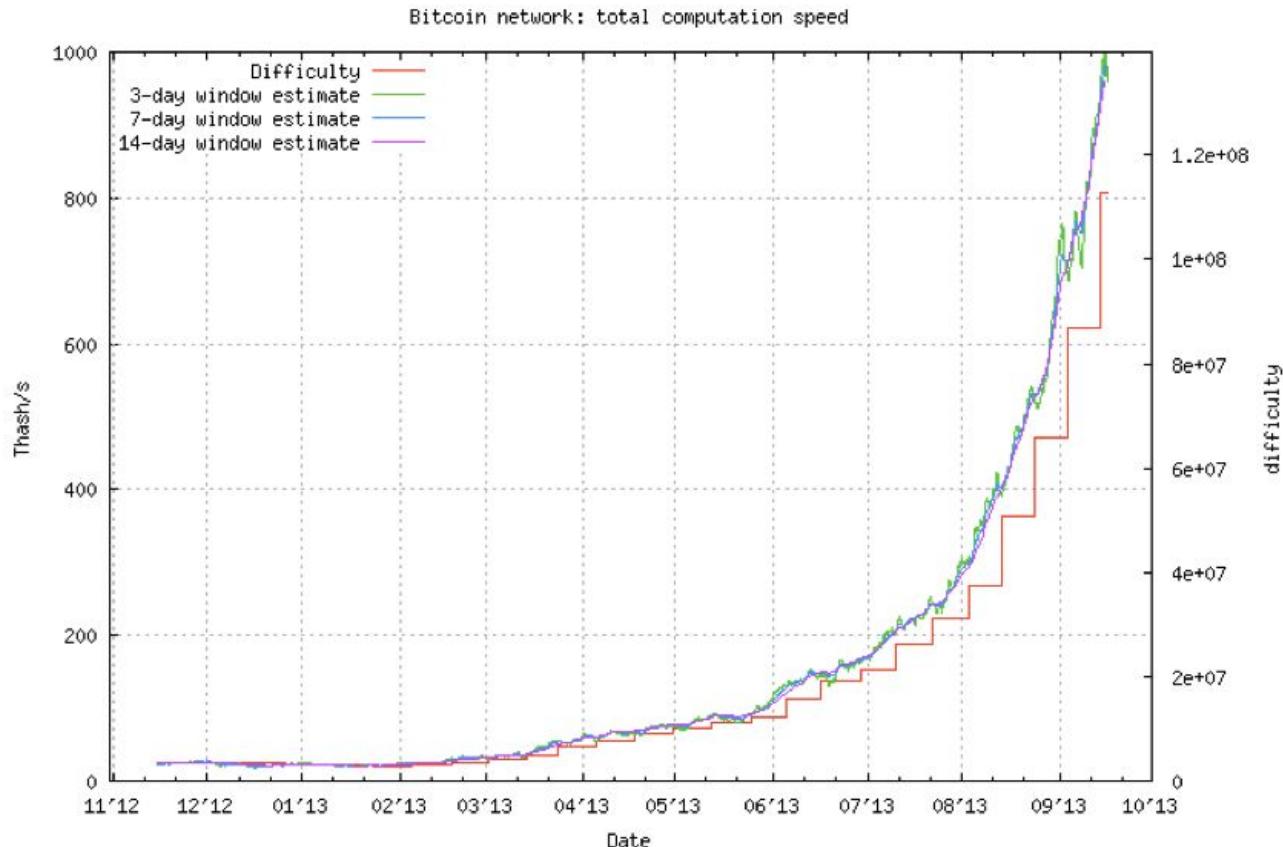


This block is now orphaned!  
After a while, all transactions  
within are returned to the  
memory pool

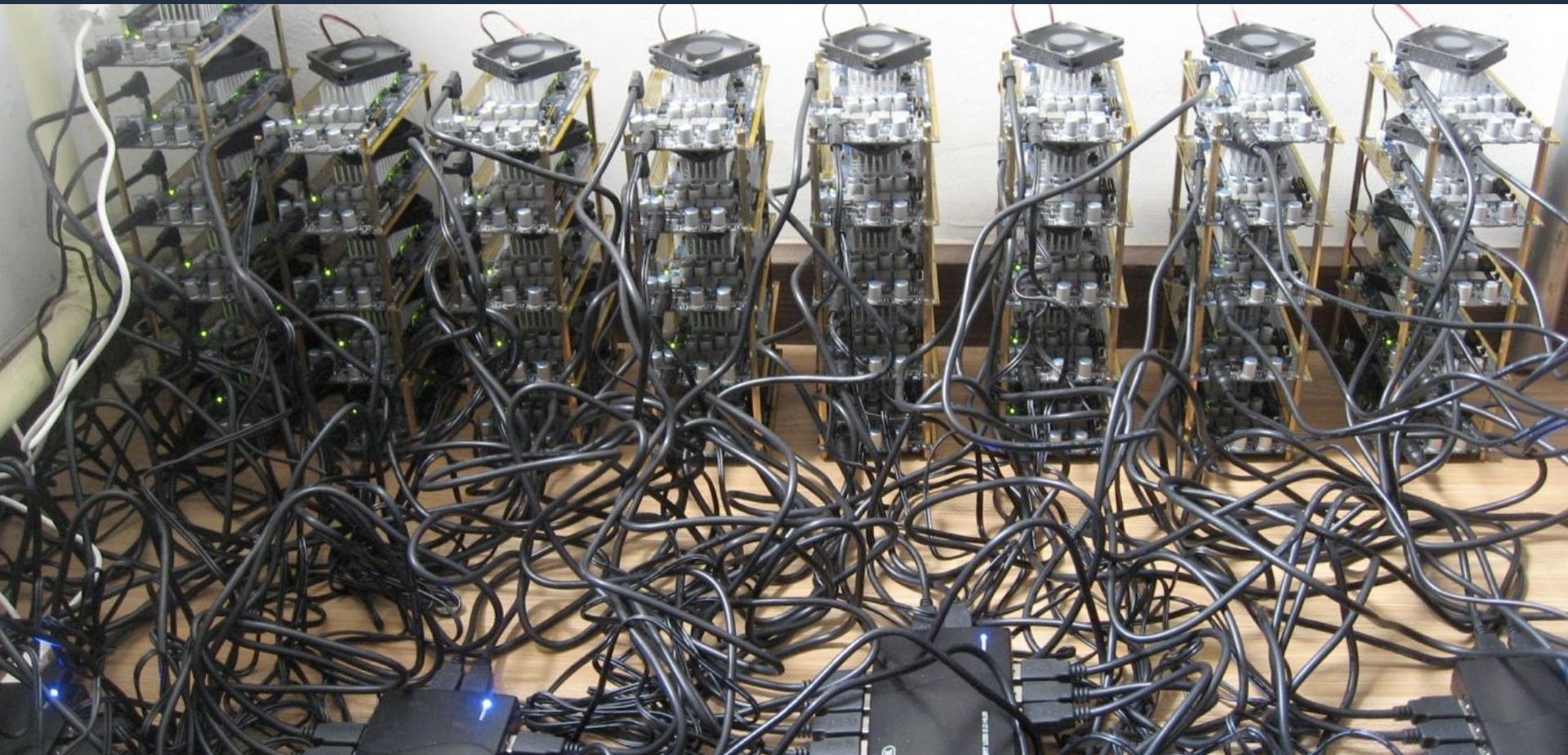
# MINING FOR NUMBERS - NOT GOLD

- 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

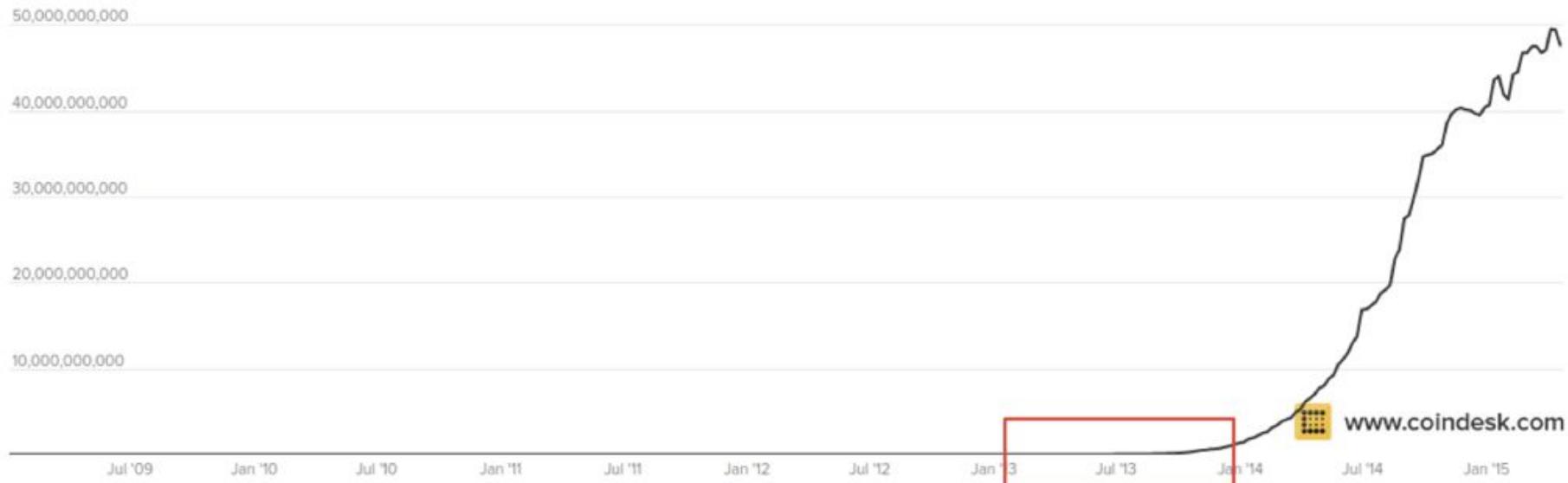
# A PERMISSIONLESS NETWORK NEEDS TO SELF REGULATE



# WHAT WAS ONCE JUST A HOBBY



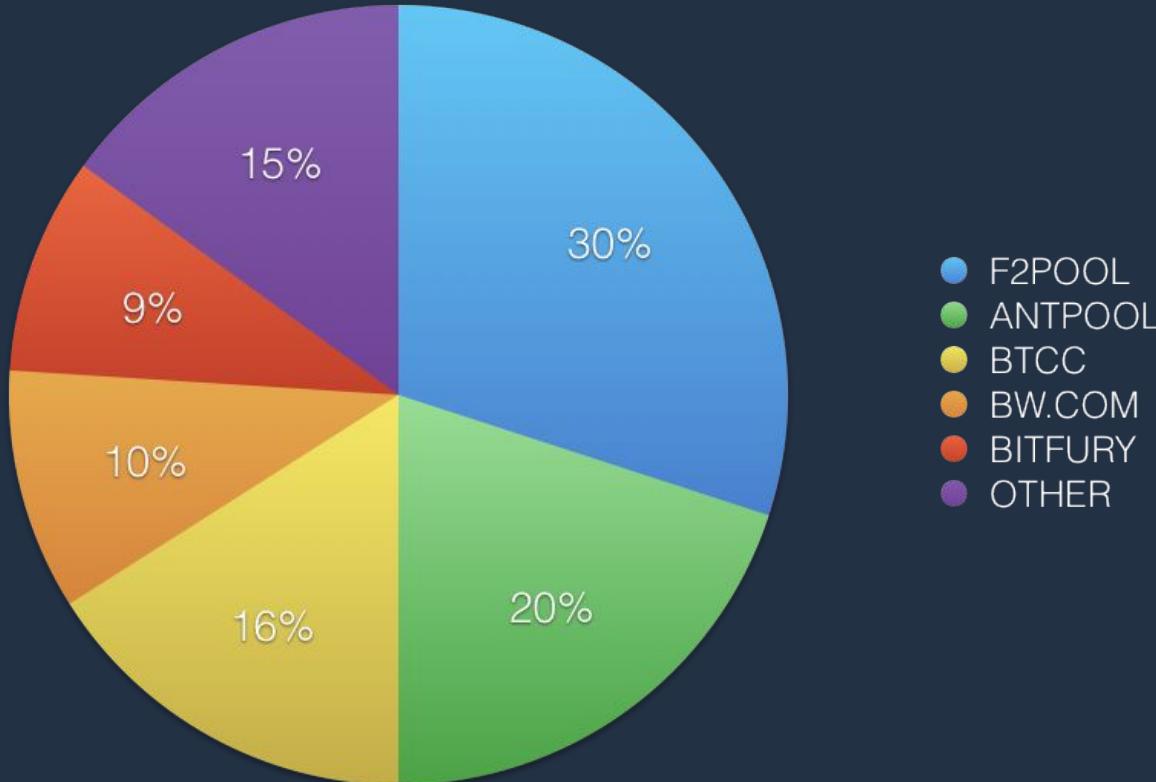
# HAS BEEN GROWING EXPONENTIALLY EVER SINCE



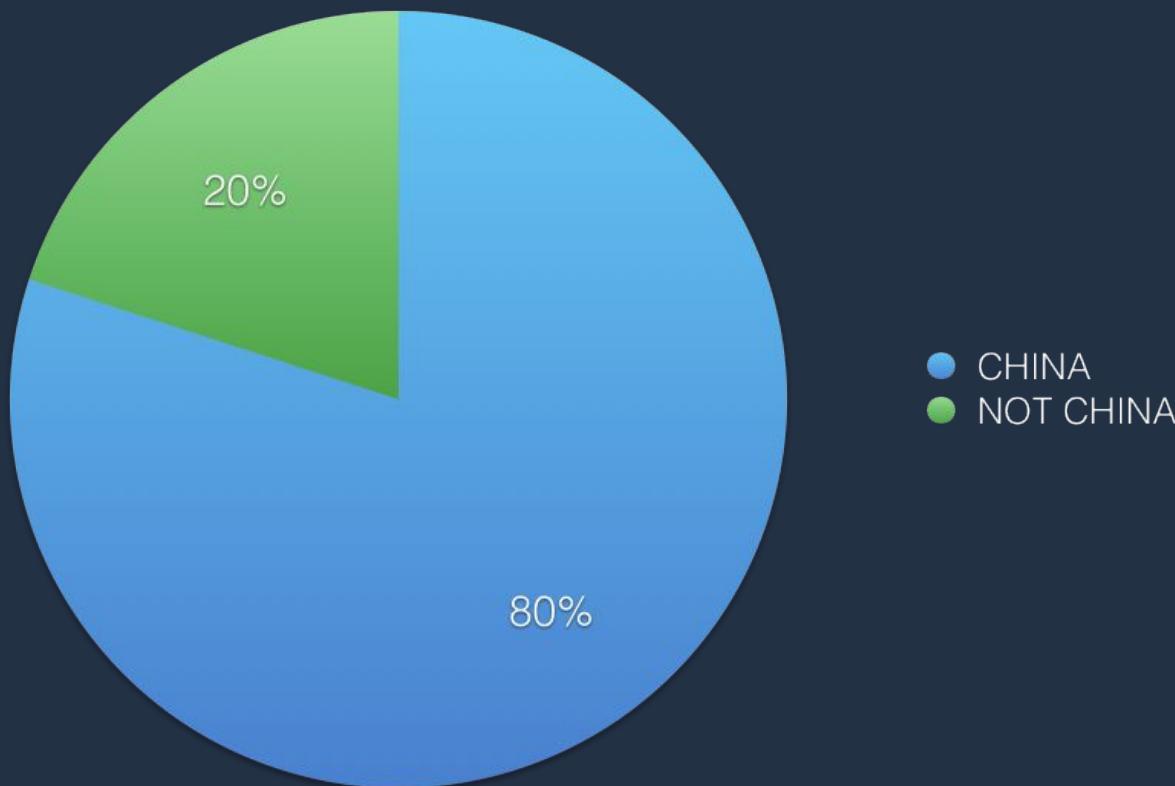
AND IS NOW A BILLION DOLLAR BUSINESS



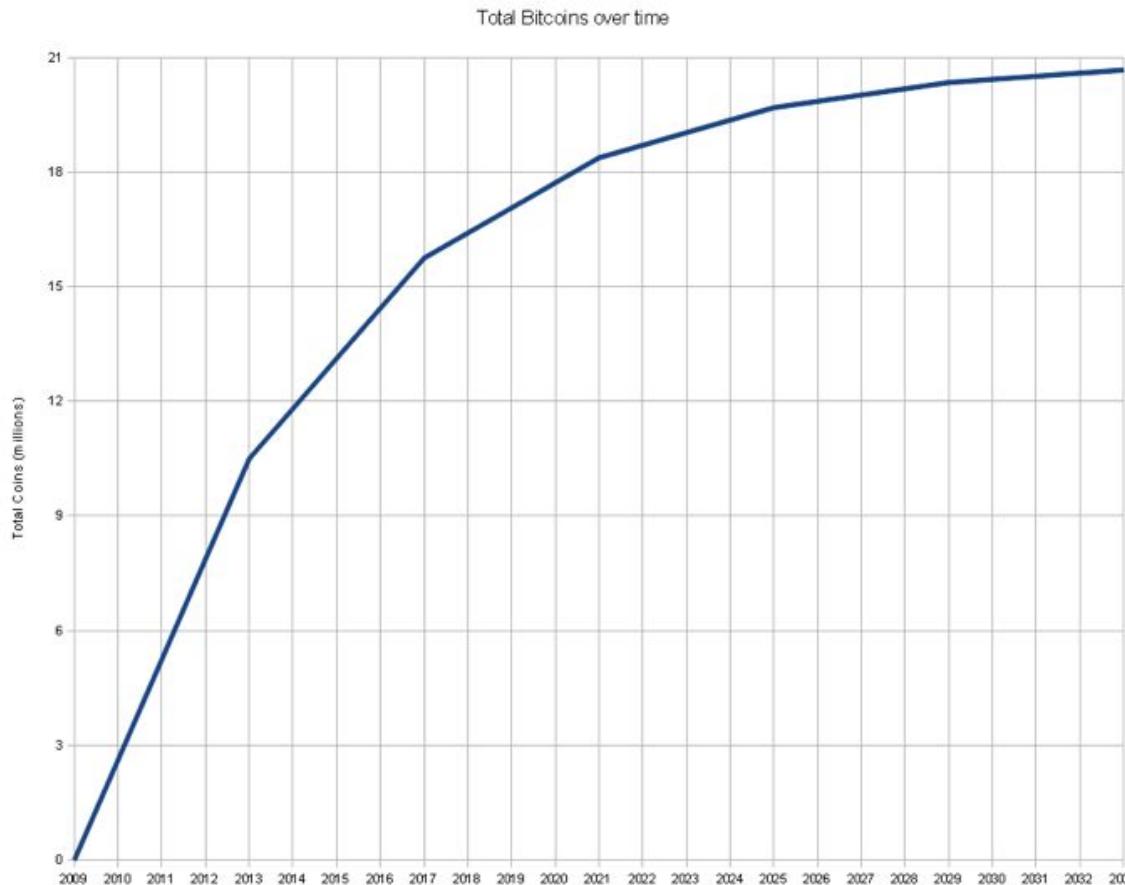
# THE NOT SO DISTRIBUTED ECONOMICS OF MINING



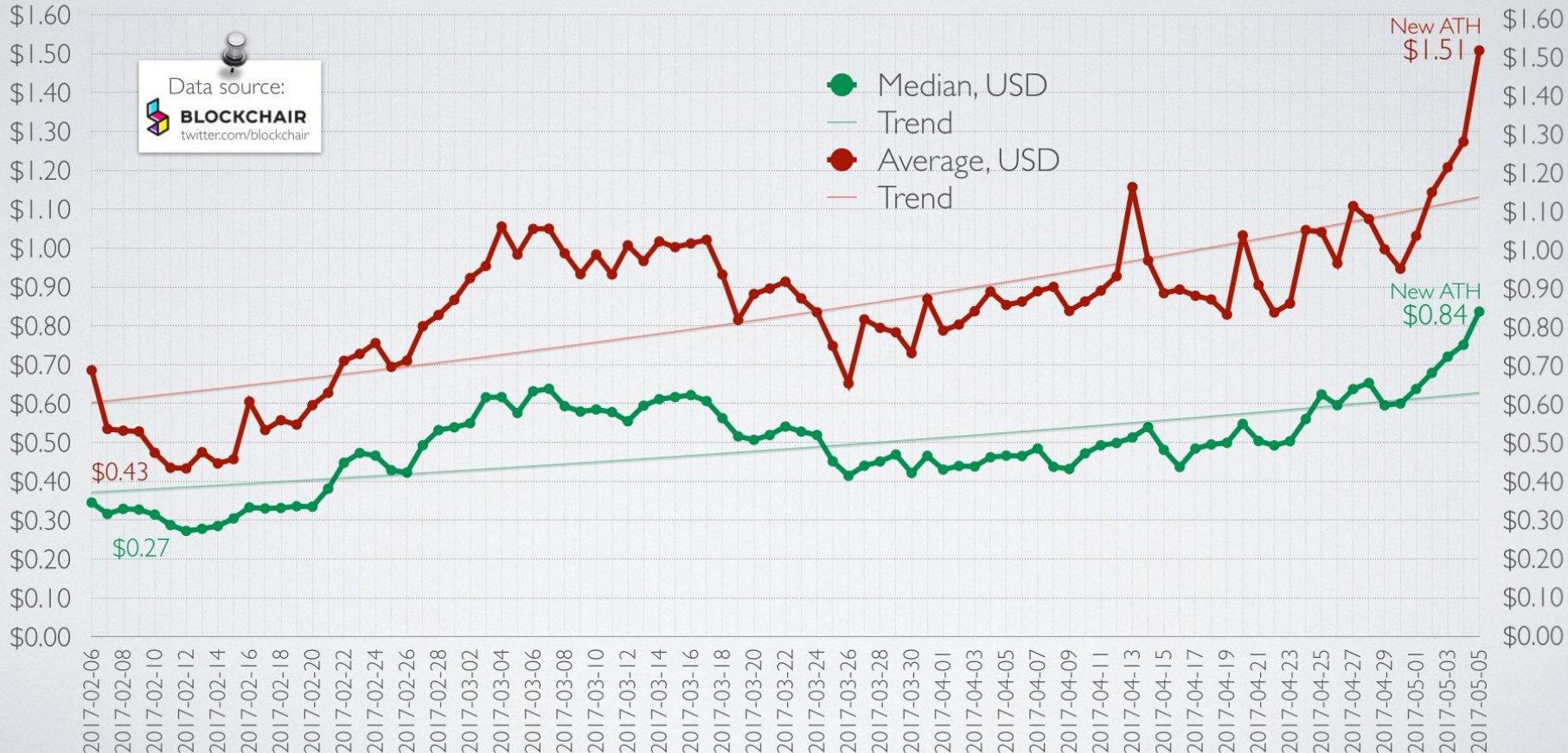
# AS OPPOSED TO THE GEOGRAPHICAL DISTRIBUTION



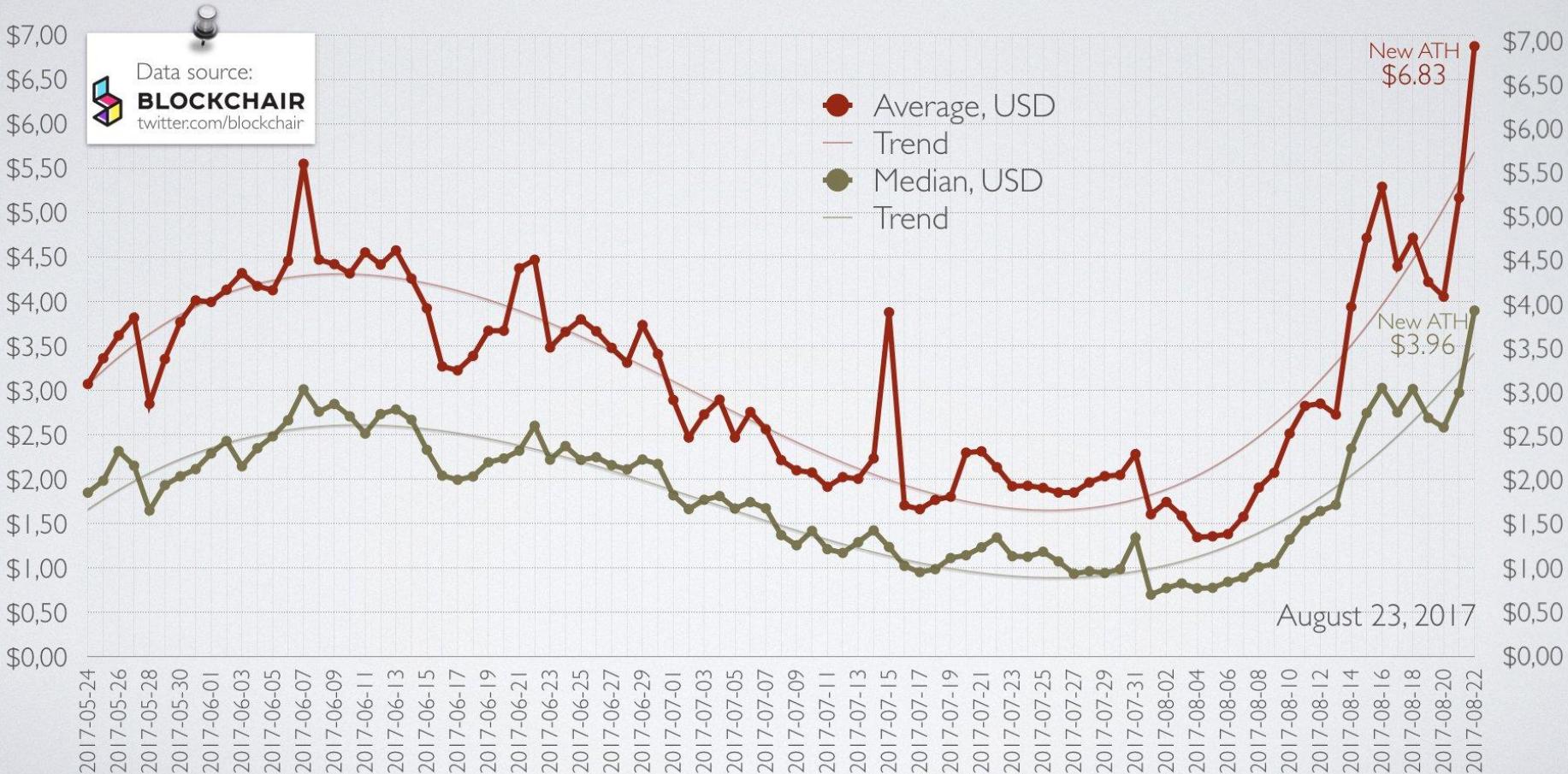
# LONG TERM FUNCTION OF MINERS - IS NOT TO MINE



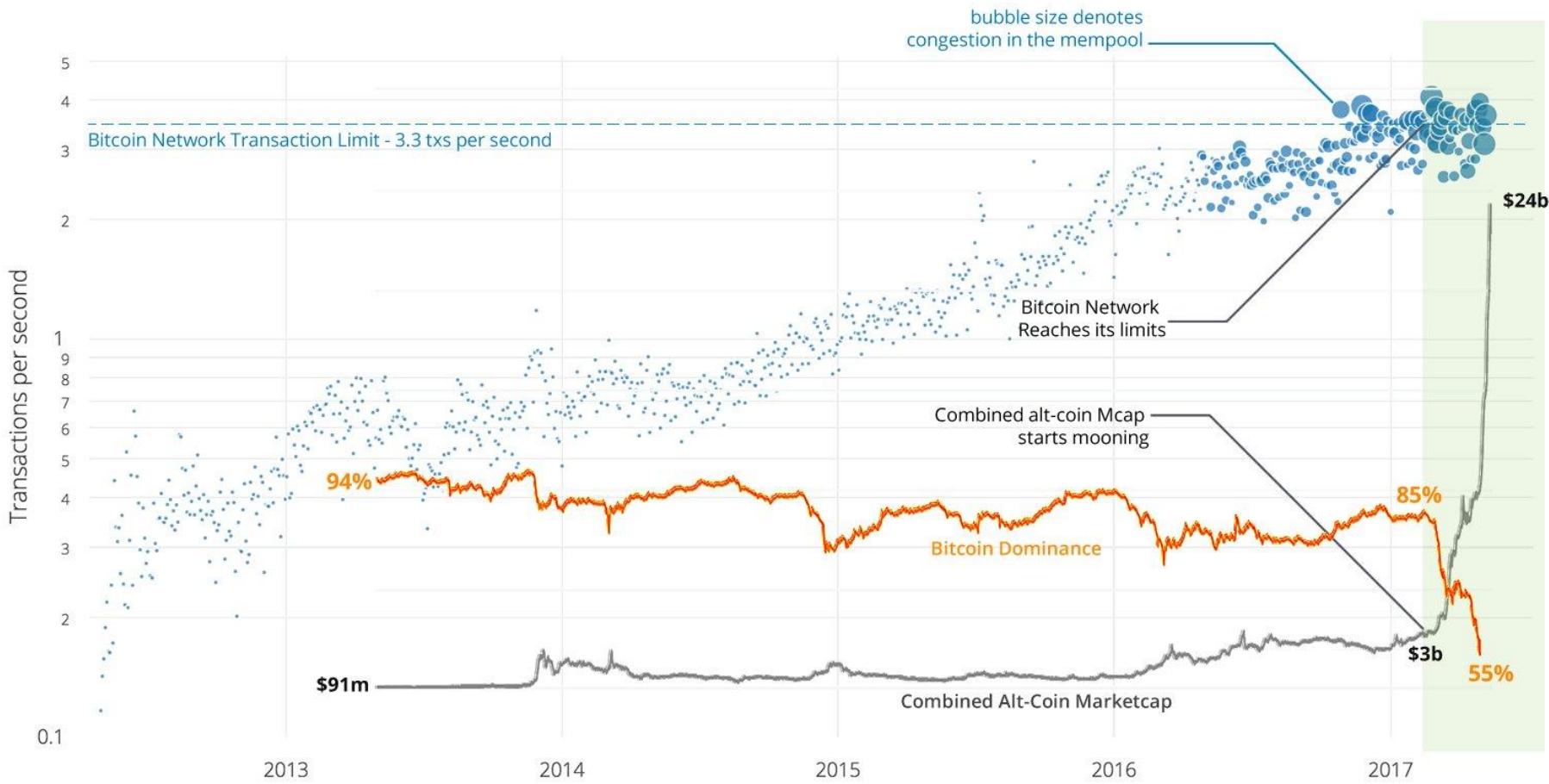
# WITHOUT A DEFINED FEE - CLEARING IS A FREE MARKET



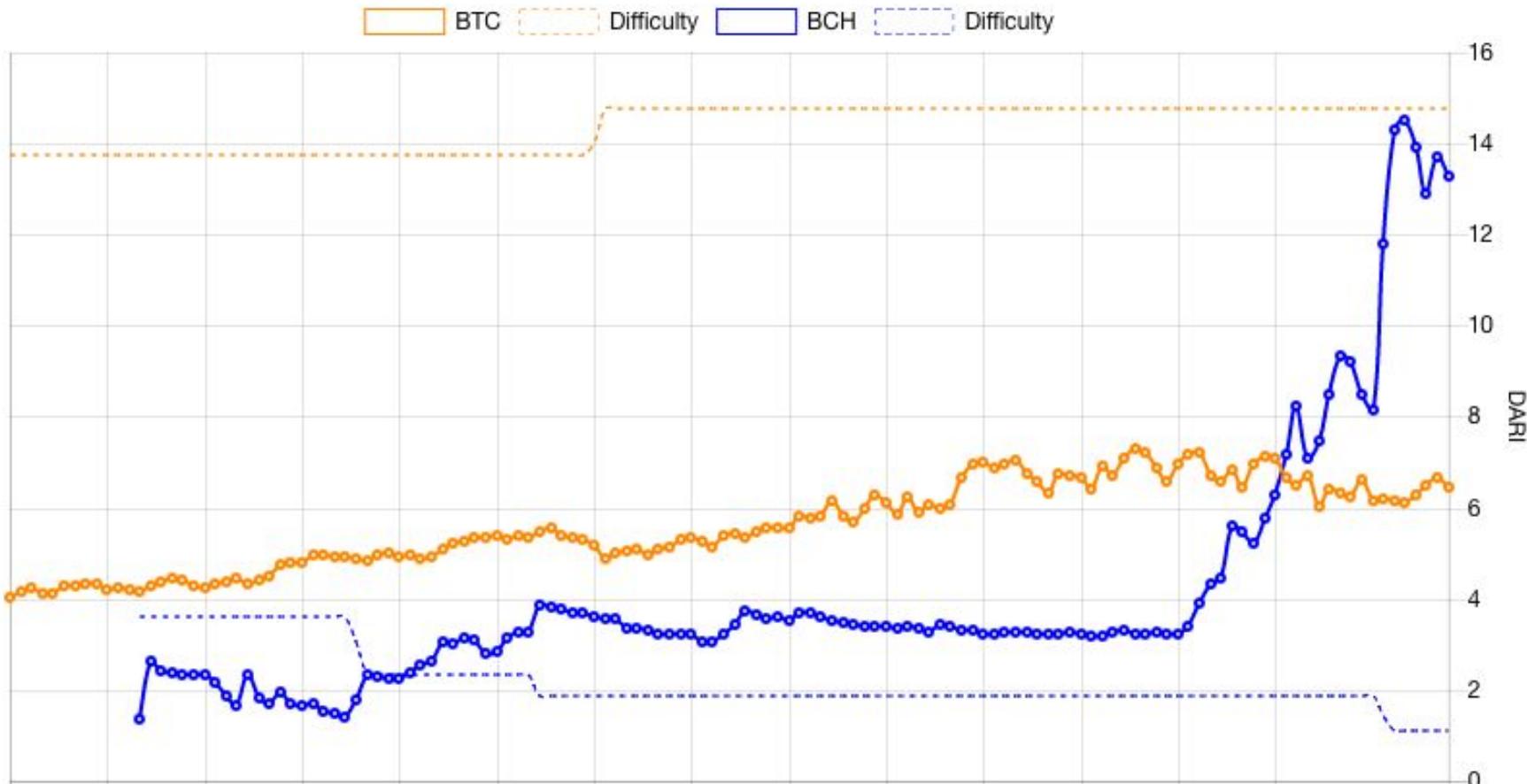
# WITHOUT INCREASING BLOCK SIZE - IT CONTINUES RISING



# THIS CAUSED AN EXODUS



# IN MORE WAYS THAN ONE



## SECTION SUMMARY

# WHAT MAKES THE BITCOIN BLOCKCHAIN SPECIAL?

- No one is in control
- No new technology
- Uses lots of energy
- Is extremely valuable
- **Nothing has changed**

**BITCOIN ISN'T EVERYTHING**

**BILLIONS INVESTED IN BLOCKCHAINS**

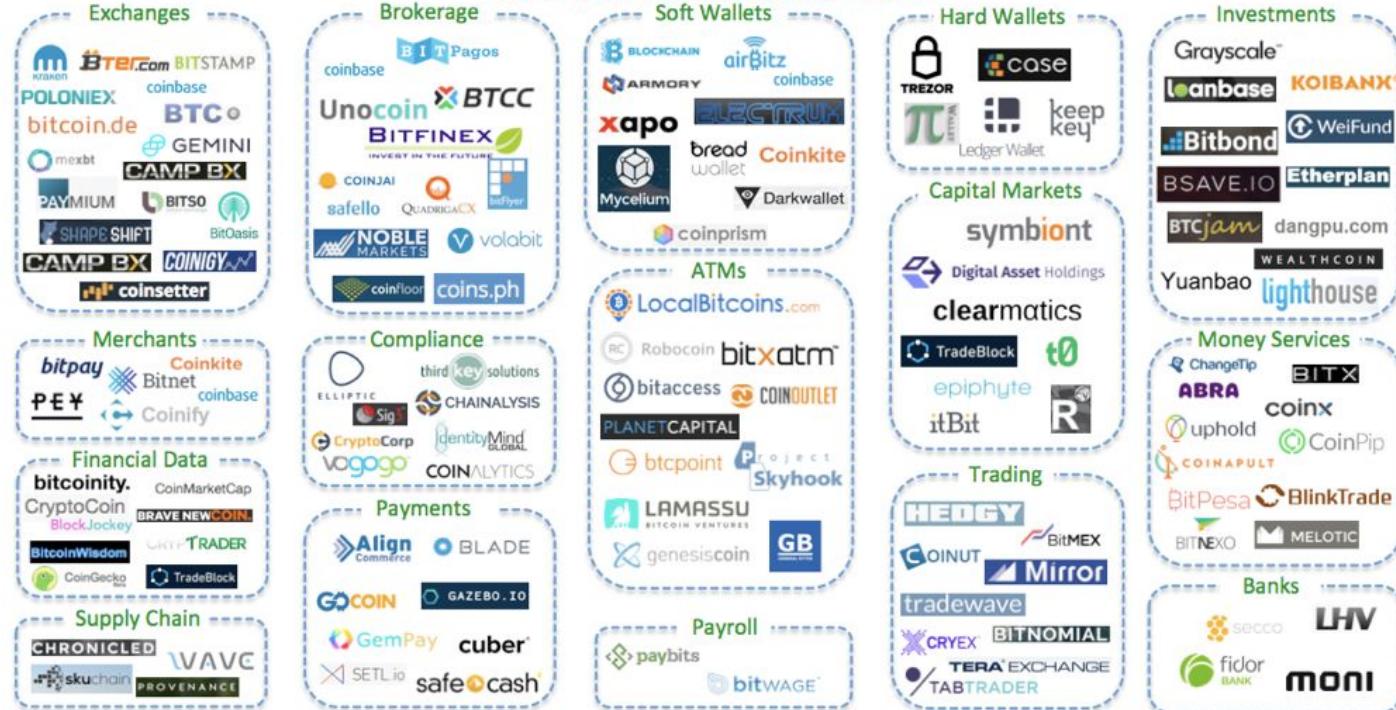
# BANKS ARE MOVING FASTER THAN NORMAL

In 2016, over 100 banks and leading financial institutions started blockchain projects, with more than US\$1 billion dollars being invested into the ecosystem - in just one year!



# BLOCKTECH in FINANCIAL SERVICES Landscape

## APPLICATIONS & SOLUTIONS



## MIDDLEWARE & SERVICES



## INFRASTRUCTURE & BASE PROTOCOLS



# 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-  
boarder payments and loyalty



1st Bank in ASEAN to join an  
Asian Blockchain Consortium



Patented a blockchain  
based wire transfer system



# SPECIAL MENTION GOES OUT TO JP MORGAN

Quorum™ is an **enterprise-focused** version of [Ethereum](#).

Quorum is ideal for any application requiring **high speed** and **high throughput** processing of **private transactions** within a **permissioned** group of known participants. Quorum addresses specific challenges to **blockchain technology adoption within the financial industry, and beyond**.



Privacy &  
Transparency



Performance  
& Throughput



Permission  
& Governance

---

Quorum supports both transaction-level privacy and network-wide transparency, customizable to business requirements

[more info >](#)

# BIG EXPECTATIONS NOW SET

- Accenture claim investment banks can save US\$12 billion a year
- McKinsey believes financial services will save US\$110 billion in 3 years
- White & Case say banks can reduce infrastructure by \$20 billion a year
- Bank of England says DLT could add 3% to a country's economic output
- 80% of top banks to launch DLT projects by 2017 - World Economic Forum
- IBM reports that 15% of big banks will be using blockchains by 2017
- IBM also reported that 65% of top banks will have blockchain trials by 2020

# CONFIRMED BY A RECENT B.I. REPORT

Institution Name	R3 Member	Hyperledger	Proof of Concept	Investment	Accelerator	Patents
Banco Santander			✓	✓	✓	
Bank of America	✓		✓			✓
Barclays	✓		✓		✓	
BBVA	✓		✓	✓	✓	
BNY Mellon	✓		✓			
Citi	✓		✓	✓		
Commerzbank	✓		✓			
Credit Suisse	✓		✓			
Deutsche Bank	✓		✓			
Goldman Sachs			✓	✓		✓
HSBC	✓		✓			
JPMorgan	✓	✓	✓	✓		
Morgan Stanley	✓		✓			
RBS	✓		✓			
UBS	✓		✓		✓	
Wells Fargo	✓	✓	✓			

# HOW CAN BANKS KEEP UP ...?

- Banks traditionally play three fundamental roles:
  - **STORE DEPOSITS** (can now be done with any e-Wallet)
  - **MAKE PAYMENTS** (can now be done with crypto-currency)
  - **PROVIDE CREDIT** (can now be done by P2P operators)
  
- Perhaps more importantly, banks are also the custodians of trust:
  - **TRUSTEE SERVICES** (trust can now be provided by blockchains)
  - **ESCROW PAYMENTS** (can now be programmed with multi-sig addresses)
  - **LETTERS OF GUARANTEE** (can now be issued with smart contracts)

# 20% OF CENTRAL BANKS USING BLOCKCHAINS BY 2019

Cambridge Centre for Alternative Finance reports ( in 2017 ) :

- 13% of central banks experimenting with Bitcoin
- 76% of central banks experimenting with Ethereum technology
- 80% of central banks researching centrally issued digital currency
- 36% of central banks researching regulatory compliance
- 18% of central banks researching identity management

# R3 - BANKING BLOCKCHAIN CONSORTIUM

- Founded by ex-banking CEOs with their CTO as ex-CIO of IBM
- Over 100 financial institutions joined R3 (with large annual fees)
- Members are then able to engage R3 consultants for pilot projects
- Originally utilizing privately forked Ethereum & Eris solutions
- 15 members trial distributed ledgers for trade finance in 2015
- 10 banks trial blockchain (KYC) identity registry in 2016
- Now heavily promoting Corda (in-house permissioned ledger)
- Opened a lab in Singapore and started working with MAS
- Recently raised US\$107M from 40 of its 80 institutional members

# NOT THE ONLY BLOCKCHAIN CONSORTIUM

- ▼
  - 📍 Accounting Consortium
  - 📍 B3i
  - 📍 BlockRx Project
  - 📍 Blockchain Study Group
  - 📍 CULedger
  - 📍 ChinaLedger Alliance
  - 📍 Digital Asset Holdings
  - 📍 Dutch Logistics Group
  - 📍 FCA Sandbox Project
  - 📍 Financial Blockchain Shenzhen Consortium
  - 📍 Fundchain
  - 📍 Global Blockchain Council
  - 📍 Hashed Health
  - 📍 Hyperledger
  - 📍 Hyperledger Healthcare Working Group
  - 📍 ISITC Blockchain Working Group
  - 📍 ISO/TC 307
  - 📍 Kinakuta
  - 📍 Post-Trade Distributed Ledger Group
  - 📍 Project Jasper
  - 📍 Other / No data



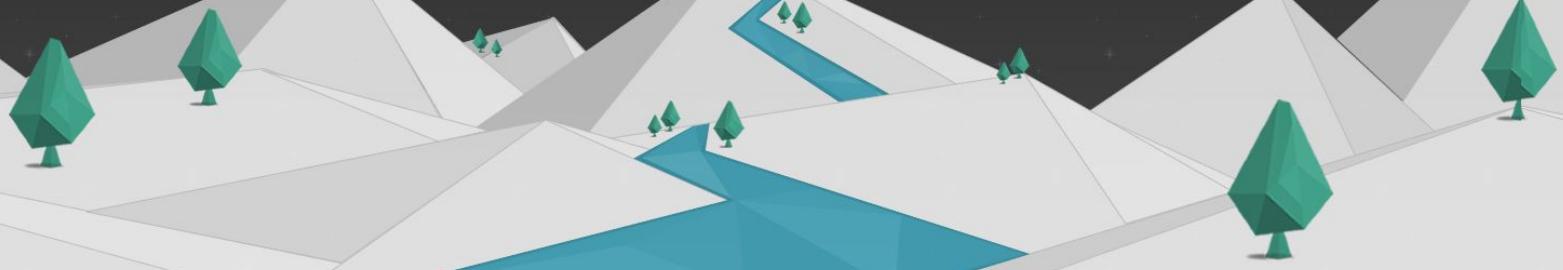
# BCE.ASIA - ASEAN'S FIRST PUBLIC BLOCKCHAIN CONSORTIUM

**cutting through the techno-babble & reporting research to regulators**

from distributed governance to digital trustees with self-sovereign identities at the heart of smart contracts bound by law

REGULATORY REPORTS

MEMBERSHIP REQUEST



## featured ambassadors



# PRIMARY MISSION - MAKING SENSE OF 1,000+ BLOCKCHAINS

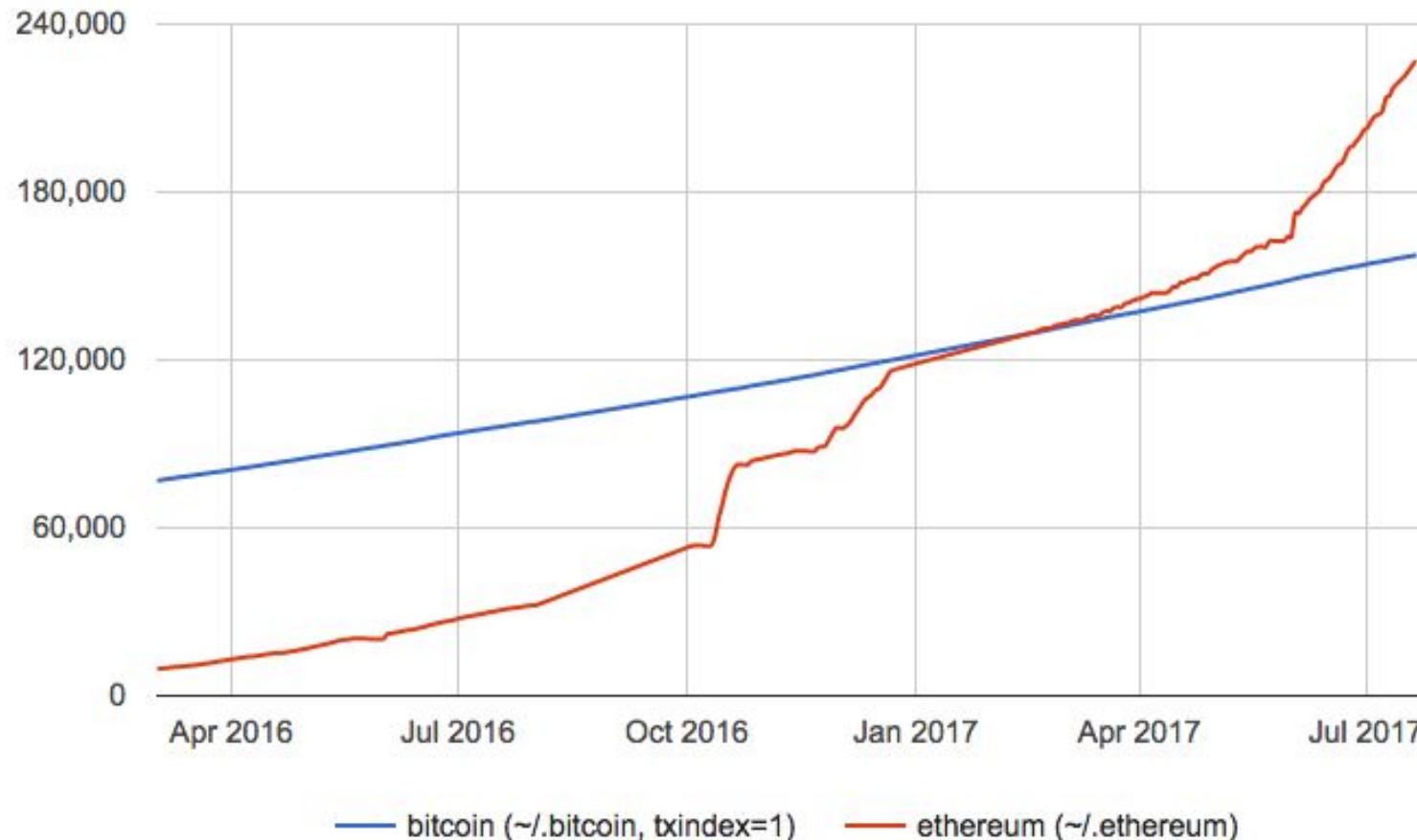


- Coins forked each other with minor tweaks
- Basic breakout alt-coin successes included Litecoin and Dogecoin
- Dash (previously known as DarkCoin) worth noting due to governance

# COMPARING OUR 4 + (1 X 2) FAVOURITE PUBLIC BLOCKCHAINS

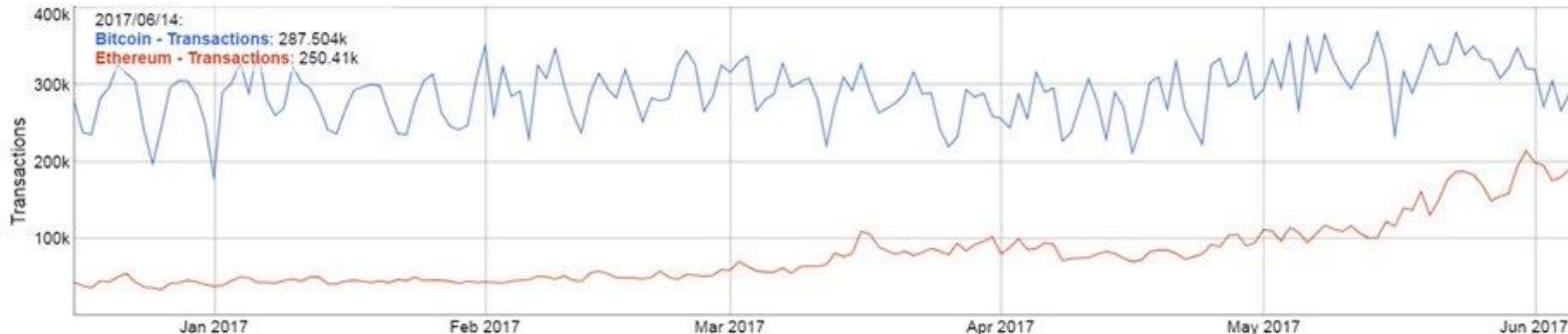
Data from CoinGecko on June 6th	Bitcoin	Litecoin	Dogecoin	Dash	Ethereum	ETC
Coin Limit	21 Million	84 Million	UNLIMITED	22 Million	Unknown	200+ Million
Current Supply	16 Million	51 Million	100 Billion	7 Million	91 Million	91 Million
Mining Algorithm	SHA-256	Scrypt	Scrypt	X11	Ethash	Ethash
Hash-Rate	644 PH/s	7.2 TH/s	6 TH/s	3.6 TH/s	30 TH/s	Unknown
Average Block Time	10 Minutes	2.5 Minutes	1 Minute	2.5 Minutes	10 Seconds	10 Seconds
Launched	03 / JAN / 09	07 / OCT / 11	08 / DEC / 13	19 / JAN / 14	30 / JUL / 15	25 / OCT / 16
US\$ Price per Coin	US\$2,800+	US\$30	US\$0.0038	US\$149	US\$260	US\$17
<b>Current Market Cap</b>	<b>US\$47+ B</b>	<b>US\$1.5+ B</b>	<b>US\$420+ M</b>	<b>US\$1+ B</b>	<b>US\$24+ B</b>	<b>US\$1.6+ B</b>
Size of Raw Blockchain	135 GB	8 GB	21 GB	3 GB	180 GB	120 GB
Hardware Cost of 51% Attack	US\$1.6+ B	US\$240+ M	US\$200+ M	US\$450+ M	Unknown	Unknown

# DOING “ANYTHING” TAKES UP A LOT OF SPACE

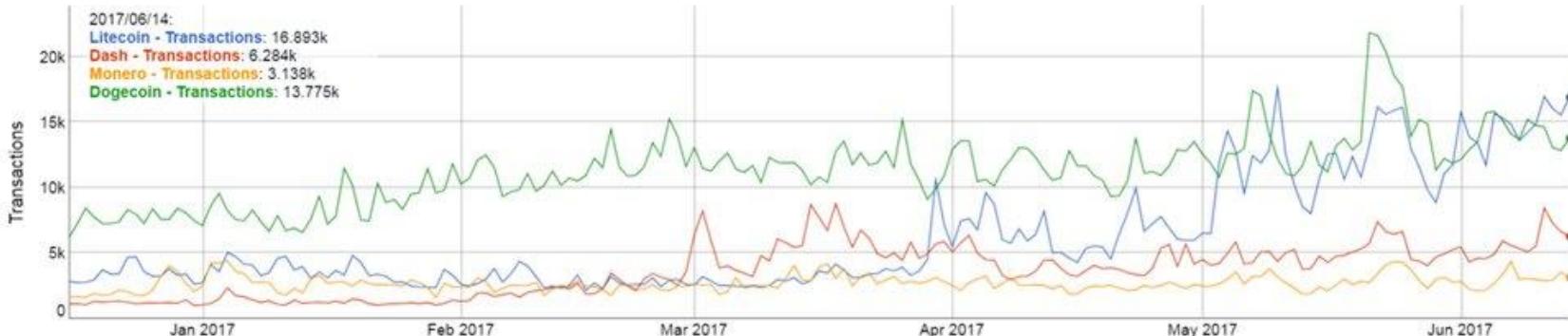


# ONLY ETHEREUM COMPETES ON TRANSACTIONS

Number of Unique Transactions per Day in 2017



1. BTC  
2. ETH

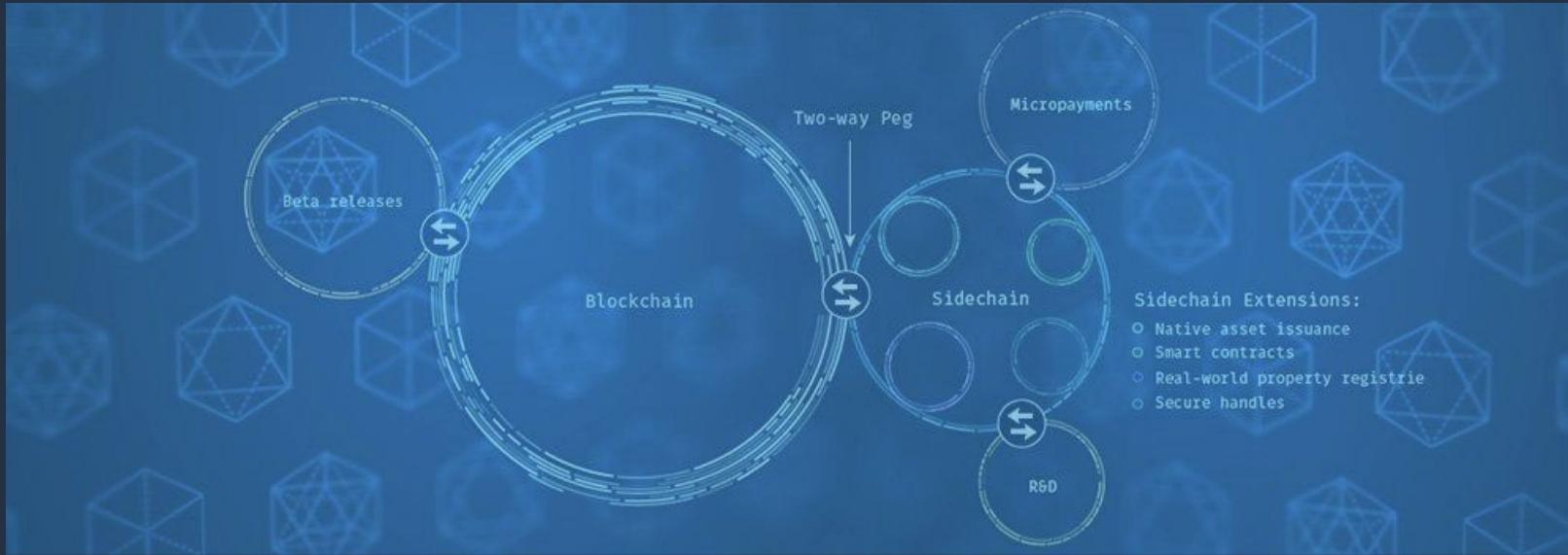


3. LTC  
4. DOGE  
5. DASH  
6. XMR

# THE RISE OF TRULY ANONYMOUS CHAINS / TECHNOLOGY

	zCoin	Dash	Monero	zCash
TOTAL SUPPLY	21.4 million	18.9 million	18.3 million + tail emission	21 million
BLOCK TIME	10 minutes	2.5 minutes	2 minutes	2.5 minutes
BITCOIN CORE	0.8 (0.13 soon)	0.10.0 <sup>1</sup>	No (Cryptonote)	0.11.2 <sup>2</sup>
PROOF OF WORK	Lyra2z transition to MTP	X11 <sup>3</sup>	Cryptonight	Equihash <sup>4</sup>
PRIVACY TECHNOLOGY	Zerocoin	CoinJoin variant	Ring signatures	Zerocash
ANONYMITY SET PER TX	Thousands <sup>5</sup>	3 with each mix	4 by default	All mint TX
REQUIRES TRUST OF MIXER	No	Yes	No	No
HIDES TX AMOUNT	No	No	Yes with RingCT	Yes with shielded tx
TX SIZE	~0.3kb for normal tx 25kb per Zerocoin tx	~0.3kb	12-25kb per tx	<200 bytes for normal tx 1+kb for private tx
PRUNABLE BLOCKCHAIN <sup>6</sup>	Yes	Yes w/ core upgrade	No	Yes
COMPUTATION TIME FOR PRIVATE TX	Seconds	<1 second	<1 second	Minutes
INCENTIVIZED NODES	Znodes	Masternodes	No	No
TRUSTED SETUP	Yes <sup>7</sup>	No	No	Yes <sup>8</sup>
AUDITABLE SUPPLY	Yes	Yes	No	No
OPTIONAL PRIVACY	Yes	Yes	No	Yes
DEVELOPMENT FUNDING	10% of total supply	10% of block reward	Pro-bono	10% of total supply

# EXPANDING THE SCOPE OF EXISTING BLOCKCHAINS

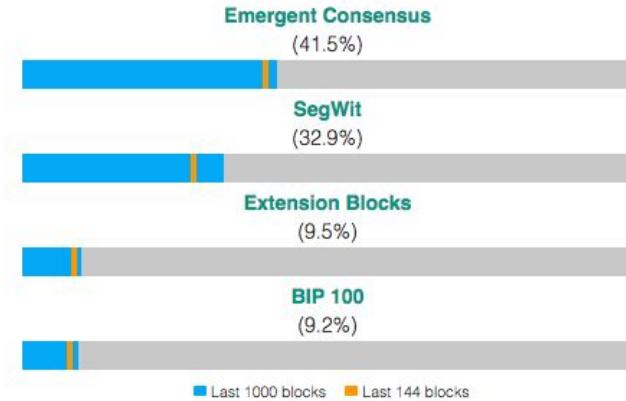


- Funded by LinkedIn founder, sidechains work towards two-way pegging
- Funded by IC3 Consortium, Bitcoin-NG introduces multiple block types
- Funded by Google, Ripple are now working on interledger protocols

# TWO YEARS LATER - PRIVATE BETA ALMOST READY



Mining Pool Support by Proposal



- Blockstream highly influential within the Bitcoin Core developers
- Also at the heart of the block size debate for past two years
- Resisting larger blocks in favour of segregated witness

# SIDETRACKED BY MAKING BITCOIN TRULY UNIVERSAL ...?



# IN THE MEANTIME, WE DEVELOPED OUR BASE PROTOCOLS

## CORTEX

**EVERSTORE**

DISTRIBUTED  
STRUCTURED DATA

 blockauth

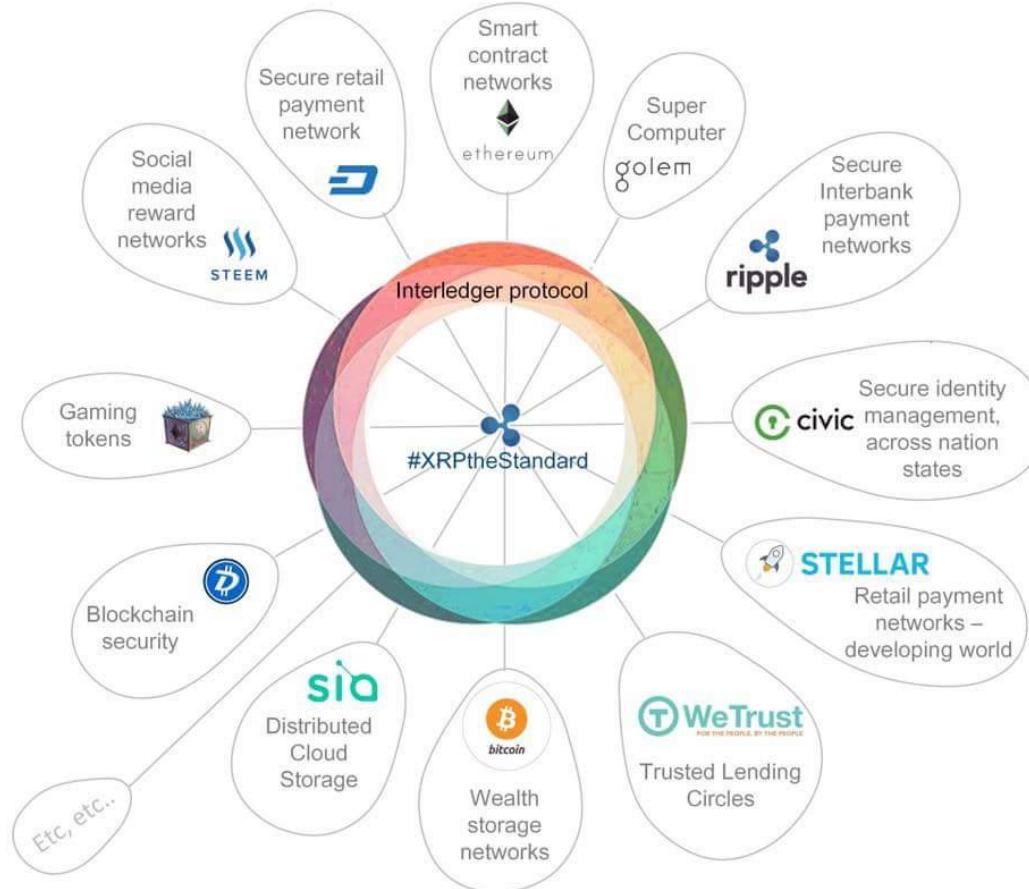
DECENTRALIZED ID &  
AUTHENTICATION

 dnkey

KEY LOGISTICS &  
BROADCASTING

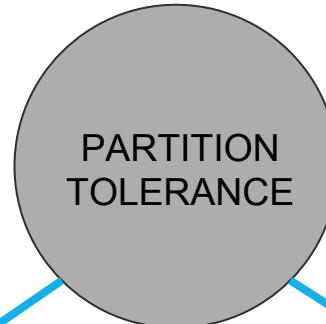
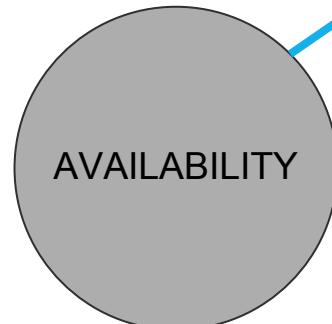
NEUROWARE'S AGNOSTIC PROTOCOLS - DESIGNED TO WORK WITH ANY BLOCKCHAIN

# RIPPLE ALSO WORKING ON AND WITH OTHER PROTOCOLS

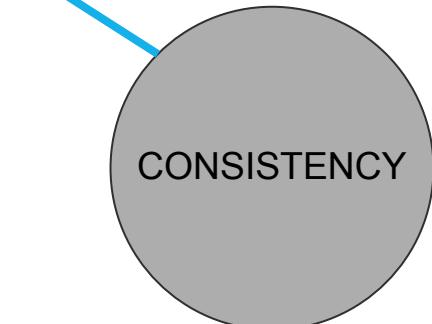


# HOPING THAT HISTORY DOES NOT REPEAT ITSELF

 mongoDB  
 corda  

EVERY NEW  
TECHNOLOGY IS A  
TRADE OFF



 ORACLE®

# PRE-MINED & PERMISSIONED NETWORKS ARE DANGEROUS

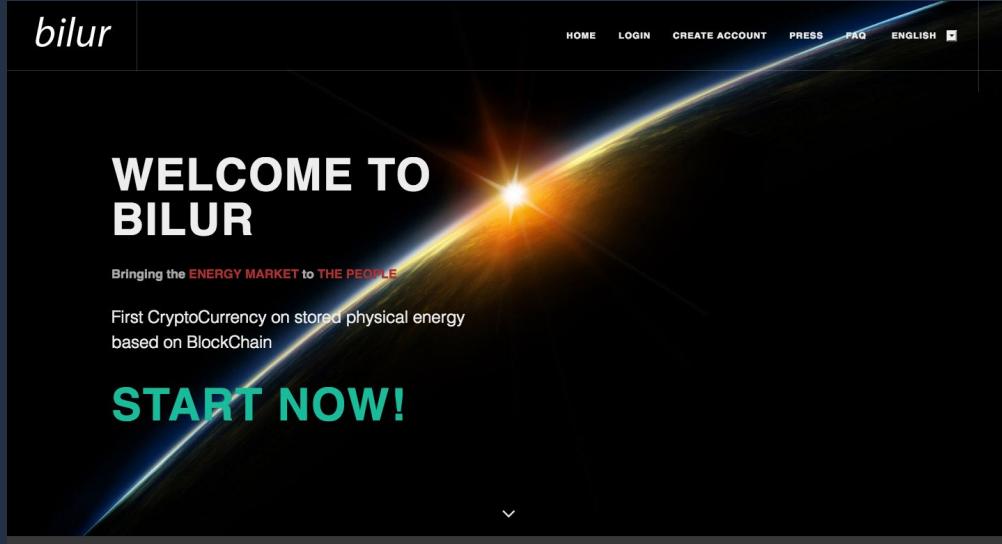


**STELLAR**



- **Ripple & Stellar** - Massive Founder Dispute / Drama
- Founders of premined crypto-currencies distribute wealth
- The process of adding blocks then becomes permission based
- Offering open ledgers that “represent” value is taking a step backward

# ALMOST AS DANGEROUS AS ASSET BACKED TOKENS



- Crude oil backed crypto
- Gold backed crypto
- Brick backed crypto
- Ledgers for transferring; diamonds, land & trainers

# UNLESS THAT ASSET LIVES ON THE BLOCKCHAIN ...?



steemit  
beta



Sign Up

Login

Submit a Story



new hot trending promoted

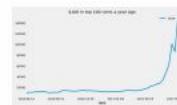
## Welcome to the Blockchain!

Your voice is worth something

SIGN UP

LEARN MORE

Get free STEEM POWER when you sign up today.



### Analyzing the crypto market with Python

I am currently on a trip through Europe, and I have met some interesting individuals whom have recently rea...

1,259.05 ▼ | 602 | 89 | 3 hours ago by furion 69 in python

my Jaxx wallet and moved to:  
Dx39fd73c23aa39ac5152980e81  
24bd9t2f6f45298  
ETC stolen and moved to:  
0xec7f65e0c5694b18c8374361

### PSA Freewallet and Jaxx Getting Robbed – Over 10 Million USD Stolen

There was a bug found in Jaxx.io wallet lately - anyone with 10 second access to your network can get all ...

2,054.66 ▼ | 1,213 | 243 | 23 hours ago by kingscrown 72 in bitcoin



### BeyondBitcoin Bounties -- Whaleshares "Meta-Token" Logo Contest! (Round 2/3) [1000's of Steem in Prizes!]

WhaleShares Logo Contest: Round #2 Begins! Art from Winners of the WhaleShares Contest 1/3...

### Tags and Topics

steemit

life

photography

introduceyourself

art

bitcoin

kr

steem

# AS CONTENT OR REPUTATION

# INDORSE

Decentralised Professional Network

DOWNLOAD WHITEPAPER v0.4.0

GET EARLY ACCESS, UPDATES AND IMPORTANT INFORMATION ON THE PLATFORM

Your Email

SUBSCRIBE

Decentralised Professional Network

# ONE CHAIN TO RULE THEM ALL ...?



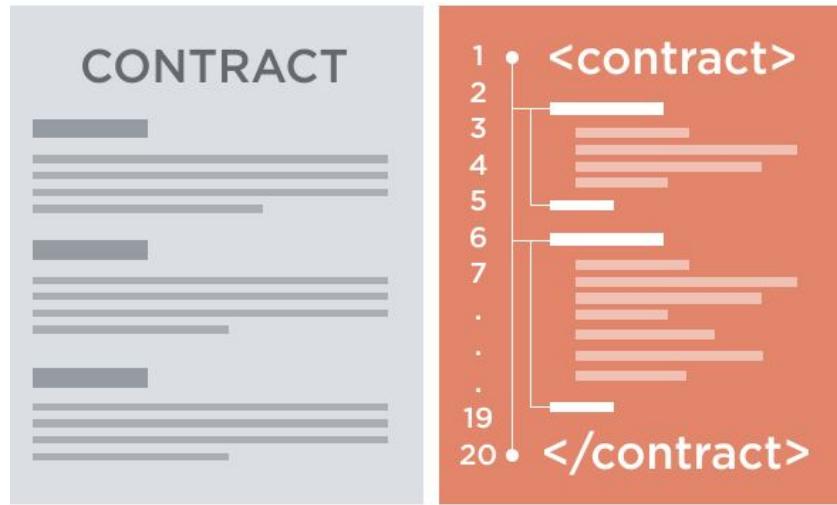
**THE WORLD'S SUPER COMPUTER...?**

- Raised US\$15 Million in **token-sales** when launching their Ether currency
- Aiming to be the first turing complete blockchain, they have almost achieved it
- Heavily supported by Microsoft and also used by IBM for their IoT platform
- Unlike BTC, we know who built it - currently uses PoW, plans to switch to PoS
- However, the more moving parts a system has - the more likely it is to break

# HAVING A KNOWN LEADER HAS IT'S CONSEQUENCES



# ETHEREUM DID HOWEVER POPULARIZE SMART CONTRACTS



- 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

# IN TRUTH - SMART CONTRACTS ARE EVERYWHERE

```
{
  "block_hash": "00000000009f30c59abf2f8556c0949c79b54764f4cbb223ca43527394d3ee2",
  "block_height": 847281,
  "block_index": 24,
  "hash": "235a88e9853c1c116ef47f795f13ce200c2elbf37667e99973e1c829f95b95f7",
  "addresses": [
    "mpNENnsFcL85hpXwfPrYpKZqAkbbFpxLF",
    "mq7tNFrb13E3fsuUbsTsA7keoeYL6gYzv2"
  ],
  "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": "4294967295",
      "sequence": 4294967295,
      "addresses": [
        "mpNENnsFcL85hpXwfPrYpKZqAkbbFpxLF"
      ],
      "script_type": "pay-to-pubkey-hash"
    },
    {
      "prev_hash": "42662b2544a7f59alabd004a8e15c714f108f553f1dd3f0617982eb5b8ac468c",
      "script": "483045022100f7ab281bcb60550098f62a097b6dbe79a9f35261aae9dc01aec54a08e8212b02201261b2d0f44545a551fe54f1777597e747523f0a66b7fc74521828c67f23887012103530d0cbdfcd448b8d96ac9c1cbdc88a2f60e05a7f16e7ab321185afb0523e9fc",
      "sequence": 4294967295,
      "addresses": [
        "mpNENnsFcL85hpXwfPrYpKZqAkbbFpxLF"
      ],
      "script_type": "pay-to-pubkey-hash"
    }
  ],
  "outputs": [
    {
      "value": 86124000,
      "script": "764914695469844938fd58e5cf59987f4cc063d4d657a788ac",
      "addresses": [
        "mq7tNFrb13E3fsuUbsTsA7keoeYL6gYzv2"
      ],
      "script": "764914695469844938fd58e5cf59987f4cc063d4d657a788ac"
    }
  ]
}
```

# THEY ARE NEITHER SMART NOR CONTRACTS

- 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>

- There are even a few hidden puzzles on the blockchain...

OP\_HASH256

6fe28c0ab6f1b372c1a6a246ae63f74f931e8365e15a089c68d6190000000000

OP\_EQUAL

# ETHEREUM MADE IT REALLY EASY

```
contract MyToken {  
  
    string public standard = 'Token 0.1';  
    string public name;  
    string public symbol;  
    uint8 public decimals;  
    uint256 public totalSupply;  
  
    function MyToken( ... )  
    function transfer( ... )  
    function approveAndCall( ... )  
    function transferFrom( ... )  
  
}
```

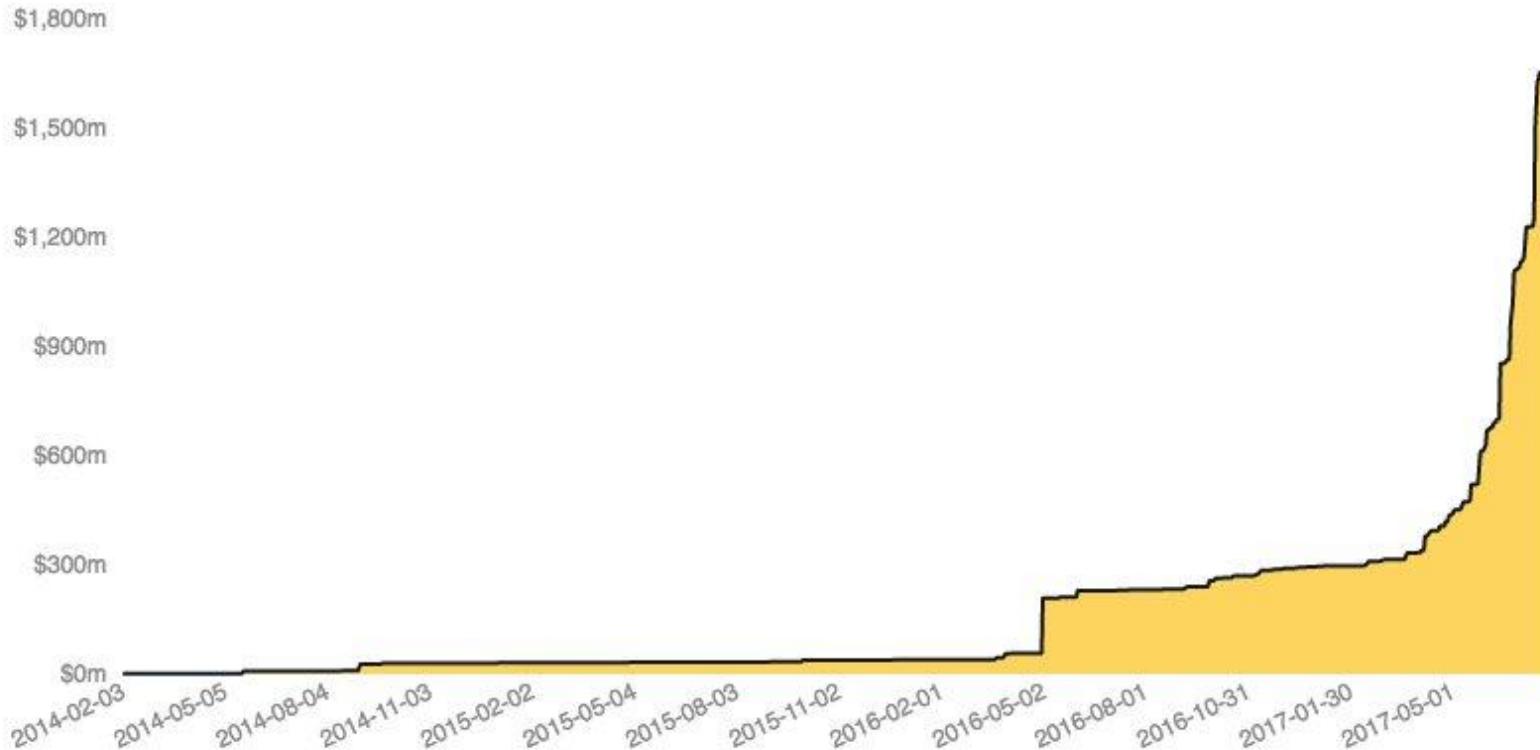
# EASY TO DO COMPLICATED THINGS - SUCH AS GOVERNANCE

- 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...

# AS WELL AS REALLY STUPID THINGS

All-Time Cumulative ICO Funding



# TOKENS CREATED ON ETHEREUM TRADING IN THE BILLIONS

#	Name	Platform	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Golem	Ethereum	\$369,051,857	\$0.447405	824,872,000	\$23,620,300	33.01%	
2	Augur	Ethereum	\$332,608,100	\$30.24	11,000,000	\$26,894,400	40.16%	
3	Gnosis	Ethereum	\$262,692,489	\$237.82	1,104,590	\$3,228,750	11.98%	
4	MaidSafeCoin	Omni	\$192,340,206	\$0.425012	452,552,412	\$2,746,470	12.94%	
5	DigixDAO	Ethereum	\$181,536,400	\$90.77	2,000,000	\$1,952,920	5.25%	
6	Ardor	Nxt	\$162,615,140	\$0.162778	998,999,495	\$3,555,530	9.56%	
7	Round	Ethereum	\$126,268,350	\$0.148551	850,000,000	\$320,571	10.27%	
8	Ionomi	Ethereum	\$122,684,790	\$1.41	87,000,000	\$2,883,910	21.92%	
9	SingularDTV	Ethereum	\$110,911,200	\$0.184852	600,000,000	\$287,238	11.73%	
10	Aragon	Ethereum	\$82,178,411	\$2.45	33,605,167	\$3,316,810	58.30%	

STARTING HERE - WORLD'S LARGEST CROWDFUND / HACK

# THE DAO IS AUTONOMOUS. |

1071.36 M

DAO TOKENS CREATED

10.73 M

TOTAL ETH

116.81 M

USD EQUIVALENT

1.10

CURRENT RATE  
ETH / 100 DAO TOKENS

15 hours

NEXT PRICE PHASE

11 days

LEFT  
ENDS 28 MAY 09:00 GMT



US\$150M WOULD HAVE BEEN US\$4B WITHOUT THE FORK

# THE DAO IS AUTONOMOUS. |

1071.36 M

DAO TOKENS CREATED

10.73 M

TOTAL ETH

116.81 M

USD EQUIVALENT

1.10

CURRENT RATE  
ETH / 100 DAO TOKENS

15 hours

NEXT PRICE PHASE

11 days

LEFT  
ENDS 28 MAY 09:00 GMT



INSTEAD WORTH US\$200+ MILLION ON THE FORK

# THE DAO IS AUTONOMOUS. |

1071.36 M

DAO TOKENS CREATED

10.73 M

TOTAL ETH

116.81 M

USD EQUIVALENT

1.10

CURRENT RATE  
ETH / 100 DAO TOKENS

15 hours

NEXT PRICE PHASE

11 days

LEFT  
ENDS 28 MAY 09:00 GMT



# QTUM - 1st REGIONAL SUCCESS - US\$15M IN 5 DAYS

## CROWDSALE RESULTS

QTUM SOLD

51,000,000 QTUM

TIME SPENT

117 HOURS



11,156.766

BTC



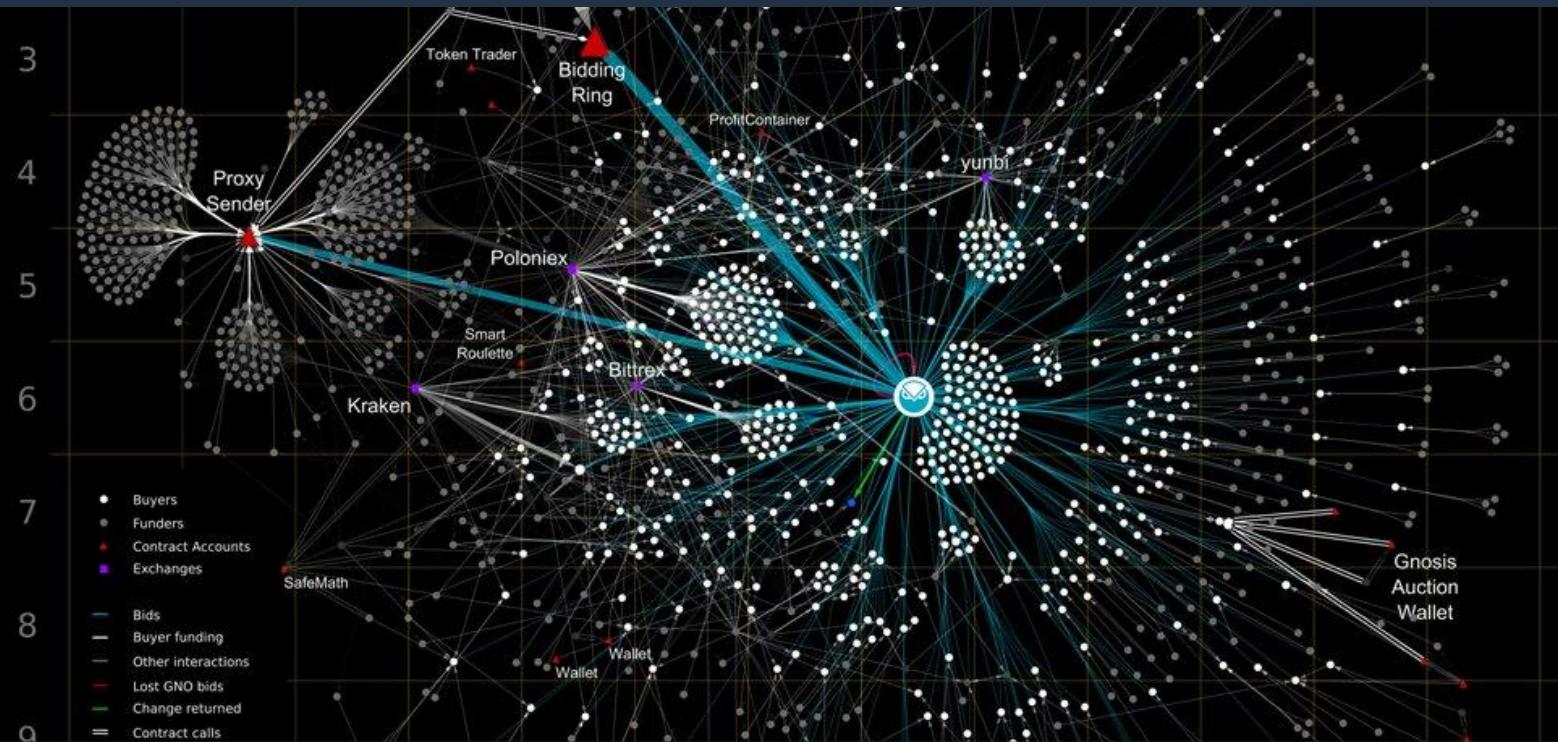
77,081.031

ETH

100.00 %

NOW WITH SELF GOVERNANCE PROTOCOL  
(similar to dash - with votable parameters for block size and gas prices)

# GNOSIS - US\$12M IN JUST UNDER 10 MINUTES



NOW HAS A MARKET CAP OF US\$200+ MILLION  
(pre-product - let alone pre revenue)

# BAT RAISED US\$35M IN UNDER 30 SECONDS



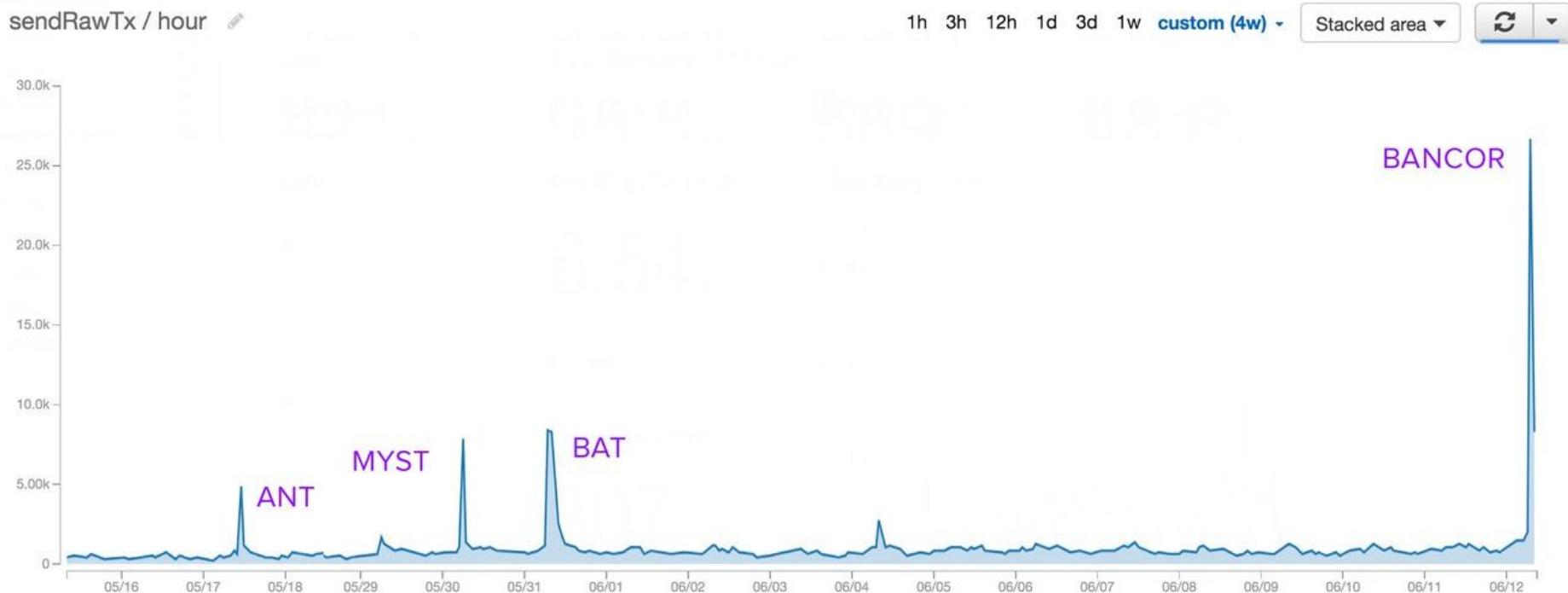
## basicattentiontoken

INTRODUCING BLOCKCHAIN-BASED  
DIGITAL ADVERTISING

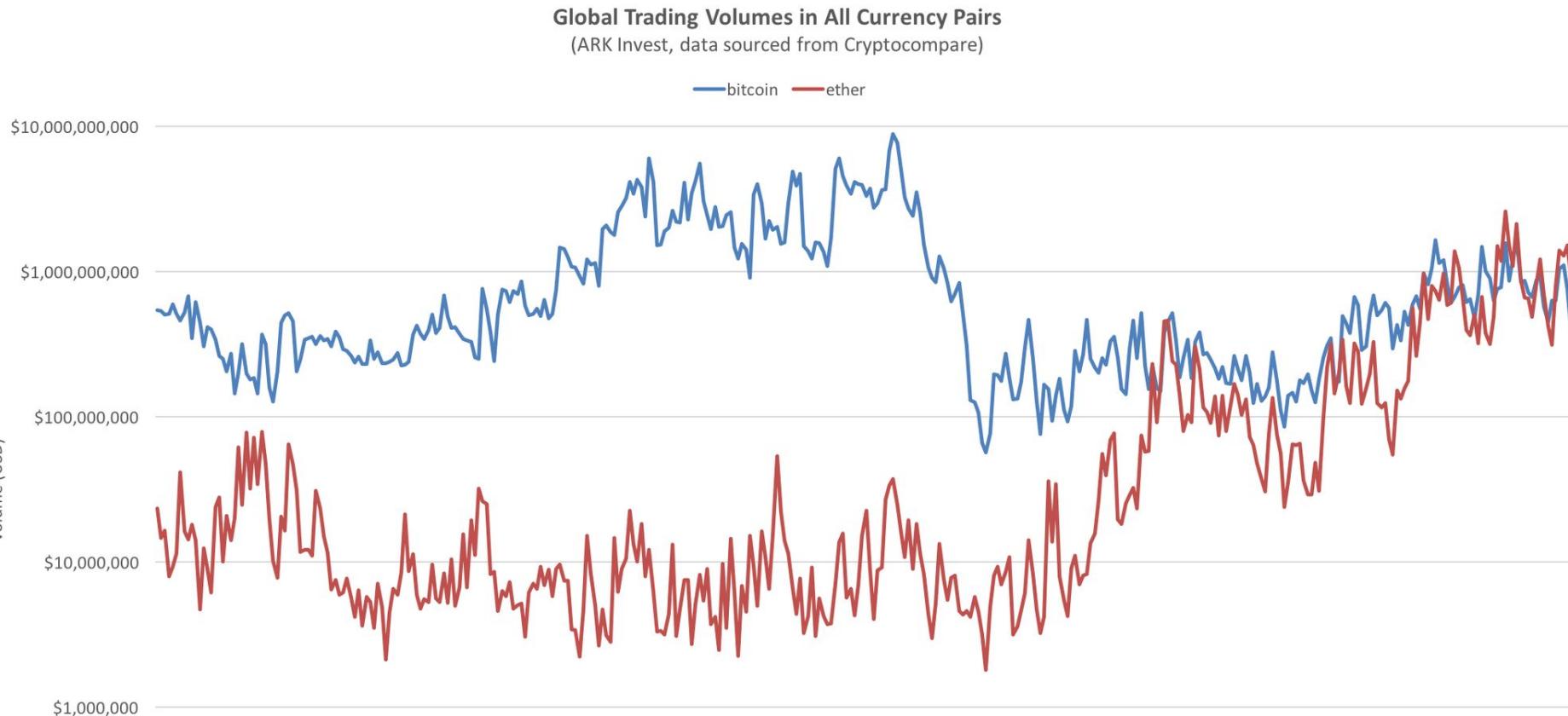
The BAT Sale is now closed. Thank you to all who participated!

SO MUCH INTEREST IT TEMPORARILY BROKE ETHEREUM  
(network was flooded for hours with some TXs spending US\$2K+ for fees)

# BANCOR - US\$3.5M PER LINE OF CODE ( 40 LINES )



# SO IS IT BTC BLOCK SIZE OR ETH ICOs CAUSING THE RISE ...?



# ECOBITS - MALAYSIA'S FIRST ICO - US\$4.5M IN 30 DAYS

## EcoBit Market Capitalisation



**0.02**  
USD  
Market Price

**0.031**  
USD  
High Price

**0.030**  
USD  
Low Price

**169,155,555.54**  
USD  
EcoBit Market Capitalisation

# LIKE MANY - IT USED MISLEADING MARKETING METHODS

English | Bahasa

[Sign Up](#) | [Sign In](#)



News

Sections

## EcoBit not working with UNDP



Melati A. Jalil, Yasmin Ramian

Updated 4 days ago · Published on 5 Jul 2017 7:13PM · 0 comments



### EDITOR'S PICK

one hour ago

Dalam dunia Umno,  
1MDB tetap bukan isu  
By Noel Achariam, Melati A. Jalil, Diyana Ibrahim



about 2 hours ago

DAP bukan Umno,  
tindakan RoS boleh  
beri kesan sebaliknya  
By The Malaysian Insight



10 hours ago

5 legal strikes in chief  
justice's extension, Bar  
Council says  
By The Malaysian Insight



11 hours ago

Centre for peace to be  
built in Putrajaya  
By The Malaysian Insight



### VOICES

one day ago

Who is responsible for your  
health?  
By Lim Chee Han



# SO WHY ARE SO MANY PEOPLE INVESTING ...?

	NAME	▼ CHANGE (%)	ICO DATE	ICO PRICE ⚡	CURR. PRICE
	NXT Buy Instantly	+391046%	09/28/13	\$ 0.000	\$ 0.066
	IOTA	+104825%	11/25/15	\$ 0.000	\$ 0.456
	Ethereum Buy Instantly	+95847%	07/22/14	\$ 0.311	\$ 298.799
	Neo	+90669%	10/01/15	\$ 0.032	\$ 28.864
	Spectrecoin	+48228%	11/20/16	\$ 0.001	\$ 0.392
	Stratis Buy Instantly	+46663%	06/20/16	\$ 0.007	\$ 3.401
	Ark	+24101%	11/07/16	\$ 0.010	\$ 2.409
	Lisk Buy Instantly	+6062%	02/22/16	\$ 0.076	\$ 4.712
	Storj Buy Instantly	+4934%	07/18/14	\$ 0.009	\$ 0.454

# COINLIST - 1st ICO PLATFORM FOR ACCREDITED INVESTORS



## A New Legal Framework

We're working with top legal experts to create the Simple Agreement for Future Tokens (SAFT), a robust legal framework and standard for token sales in the United States. Inspired by the YC SAFE, token creators and investors using the SAFT avoid wasting time creating and reviewing one-off legal agreements. You can focus on what matters: building valuable technology. The SAFT will be completely open-source and available for all to use.

[About The SAFT](#)

# FILECOIN - 1st TO RAISE - US\$180M IN UNDER 60 MINUTES



## Filecoin

Filecoin is a decentralized storage network, powered by a blockchain and a native token



\$4.94 USD/FIL • \$

**\$197,944,845**

TOTAL RAISED ⓘ

**\$4.94 USD/FIL**

Current minimum price, calculated using:  
max(\$1, \$197,944,845/\$40,000,000)

**INVEST IN FILECOIN ➔**

24

7

46

5

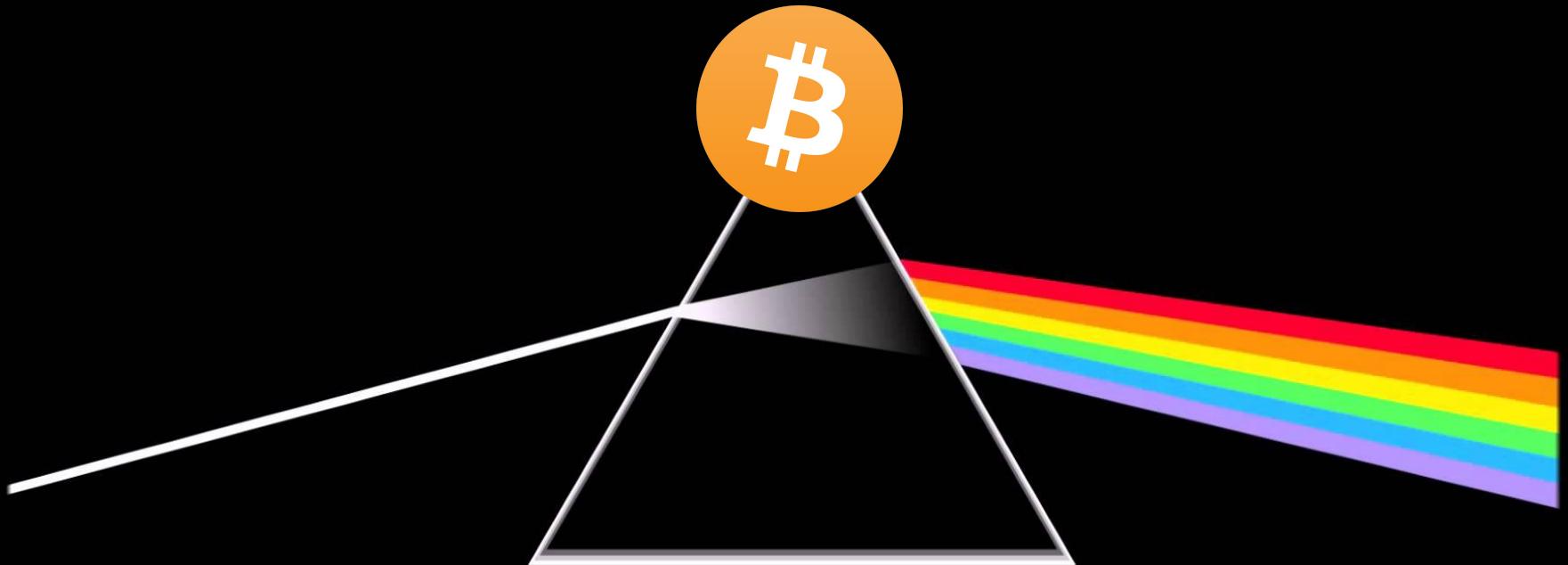
DAYS

HOURS

mins

SECS

# THE DARK SIDE OF CRYPTO



ICO SCAMS = PENNY STOCKS & RAILWAY BONDS | PONZIS FOREVER | DRUGS = CASH REMAINS KING

LARGEST JOINT EFFORT SO FAR INVOLVING 5 COUNTRIES



# OneCoin



JOIN THE  
FINANCIAL  
REVOLUTION

# RANSOMWARE NOT DESIGNED FOR BITCOIN

 Wana Decrypt0r 2.0

**Ooops, your files have been encrypted!**

**English**



**What Happened to My Computer?**

Your important files are encrypted.  
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Payment will be raised on**  
5/15/2017 18:47:17

**Time Left**  
  
02: 23: 59: 28

**Your files will be lost on**  
5/19/2017 18:47:17

**Time Left**  
  
06: 23: 59: 28

**Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.  
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.  
You only have 3 days to submit the payment. After that the price will be doubled.  
Also, if you don't pay in 7 days, you won't be able to recover your files forever.  
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window.  
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

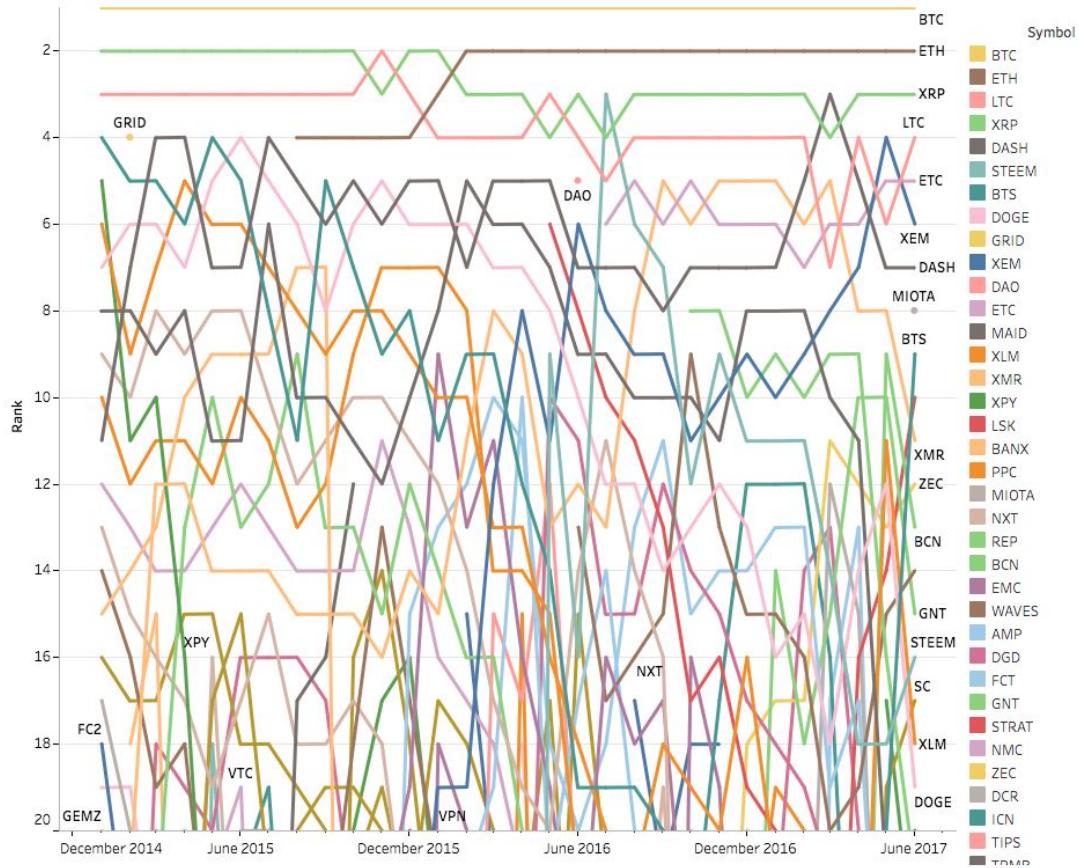
 **Send \$300 worth of bitcoin to this address:**

**115p7UMMngoj1pMvkpHjcRdfJNxj6LrLn**

**Contact Us**

**Check Payment**      **Decrypt**

# MAKING SENSE OF THE ROLLERCOASTER RIDE



# THE OTHER SIDE OF THE COIN - SECURITY METHODS



## SECTION SUMMARY

### BEYOND BITCOIN - WHAT ELSE IS IMPORTANT?

- Thousands of alternatives
- Very few bring anything new
- Ethereum has given birth to ICOs
- What's most important is interoperability

BLOCKCHAINS  
**IN ASIA**

# SINGAPORE - LEADING THE WAY

DBS - First bank (globally) to launch a public blockchain competition

DBS & Standard Chartered - first banks (regionally) to use blockchains

OCBC first bank (regionally) to settle intrabank cross border payments

MAS - First regulator (regionally) to issue digital currency on blockchains

QTUM - 1st new blockchain in region to receive over US\$1 million



# SINGAPORE - MAKING INTERNATIONAL HEADLINES



Otonomos  
@Otonomos

Follow

@Otonomos is serving clients from 26 countries as of July! Can't wait to see how many more by the end of the year!



Incorporate online in Singapore, HK, UK, Cayman Islands via blockchains  
(in discussions with Delaware)



# SINGAPORE - MAKING THEIR OWN HISTORY



Ethereum Core Team and Founder  
(Vitalik) relocated to Singapore



# CHINA - MOST INFLUENTIAL NATION

Over 60% of Bitcoins mined in China

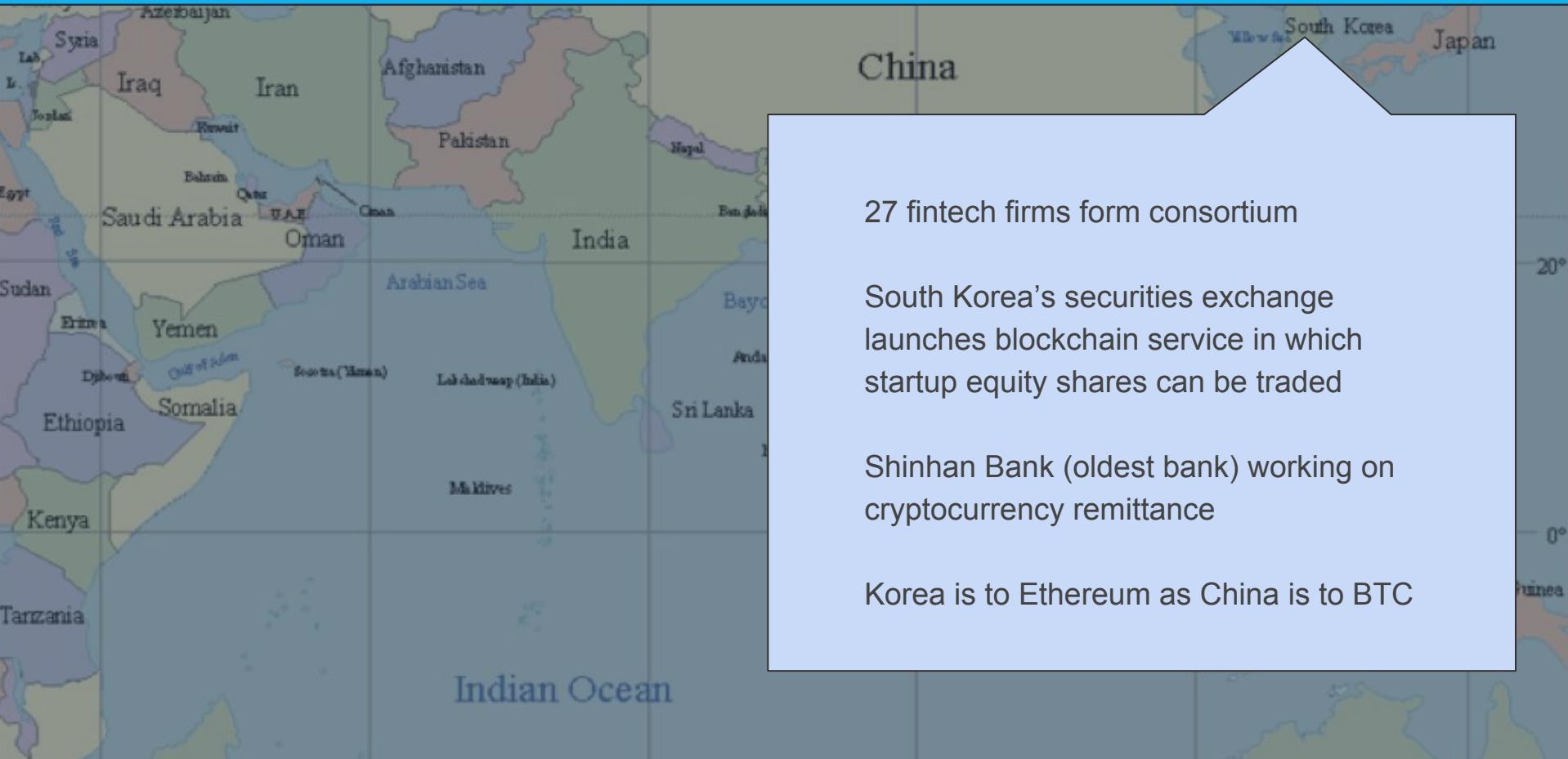
10 banks hiring 30 blockchain  
developers at a 50% salary premium

Postal Savings Bank of China sent  
100 asset TXs on its own Blockchain

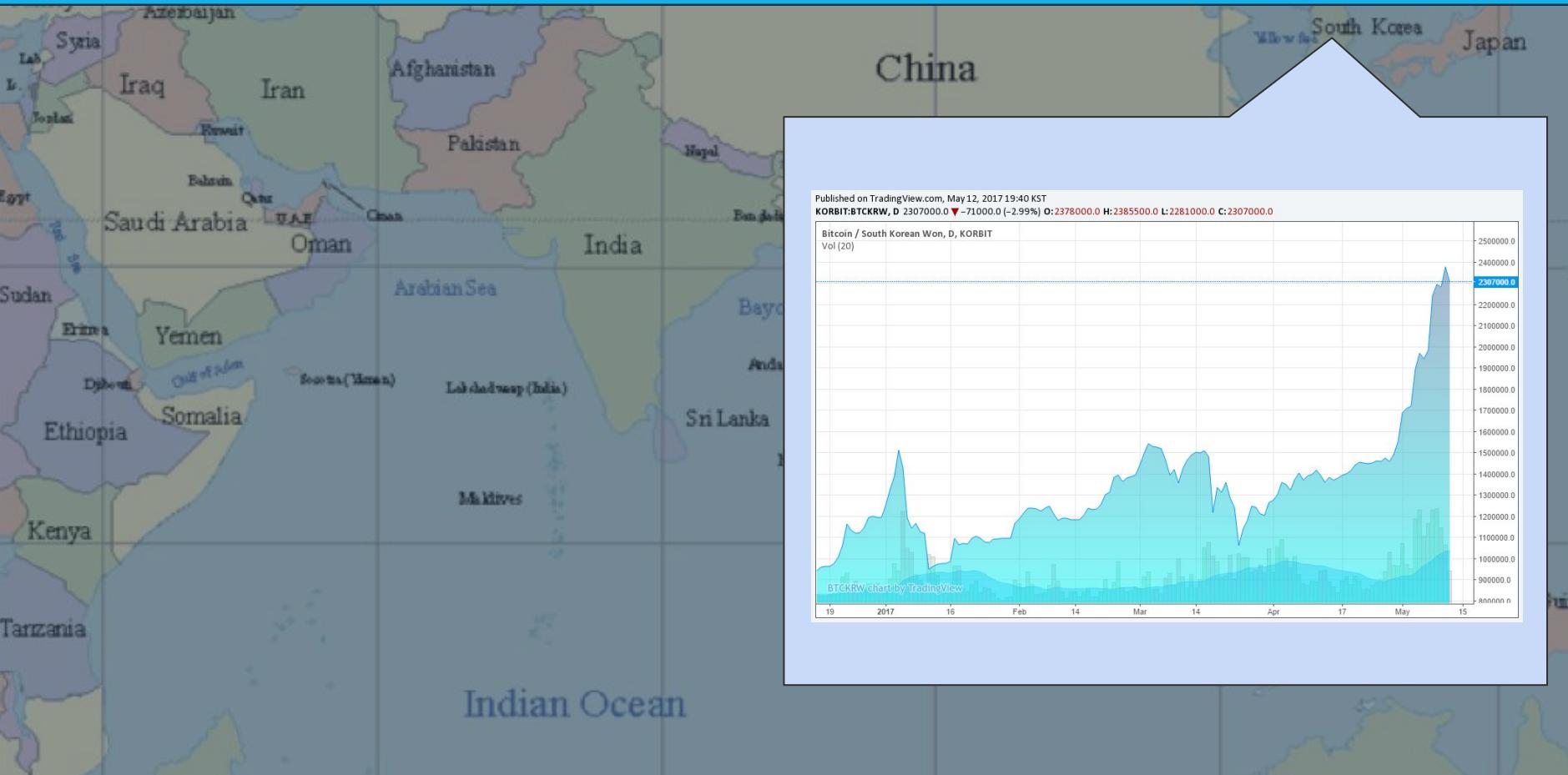
US\$1.44 billion fund for blockchains

**Recently banned ICOs**

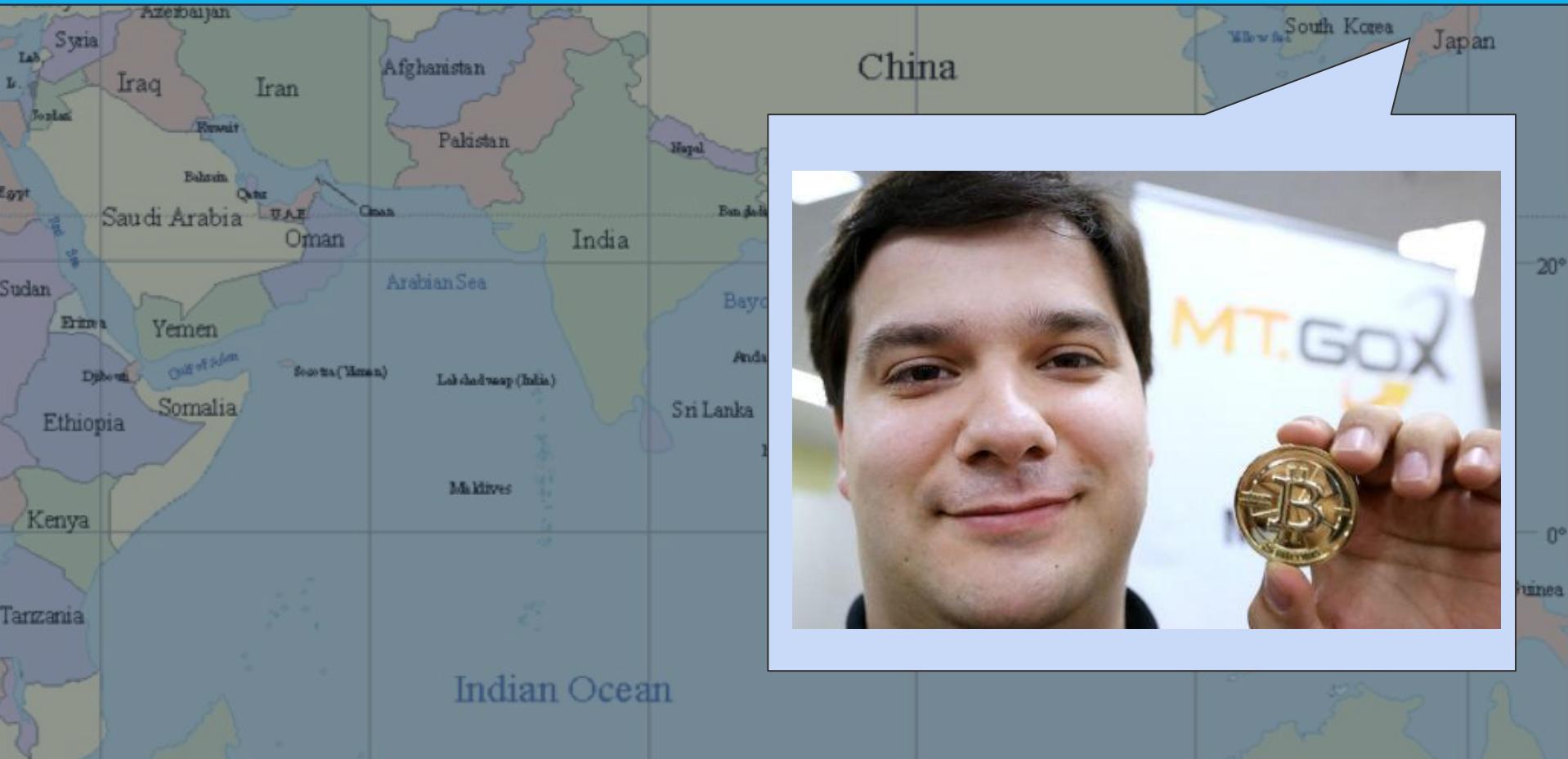
# KOREA - SLOW TO START BUT QUICK TO ACTION



# KOREA - PAYING OVER 20% MORE THAN MOST



# JAPAN - FIRST TO GET GOXXED - LOSING US\$450M++



# TRUSTEES (US\$90M) NOW WORTH US\$600M

Bankrupt Mt. Gox's bitcoins could pay off its debt



△ T L △ S | Data: CoinDesk, Mt Gox trustee. Claims accepted by trustee as of 15 March 2017

# AS A RESULT - JAPAN AMONGST FIRST TO REGULATE

China

42 banks form ripple consortium, now over 100 members partnering

Stock exchange partners with IBM

Mizuho Financial Group and others use DLT for interbank payments

Merchants to reach 250K in 2017

# JAPAN - NOW ACCEPTED BY LARGEST RETAILER



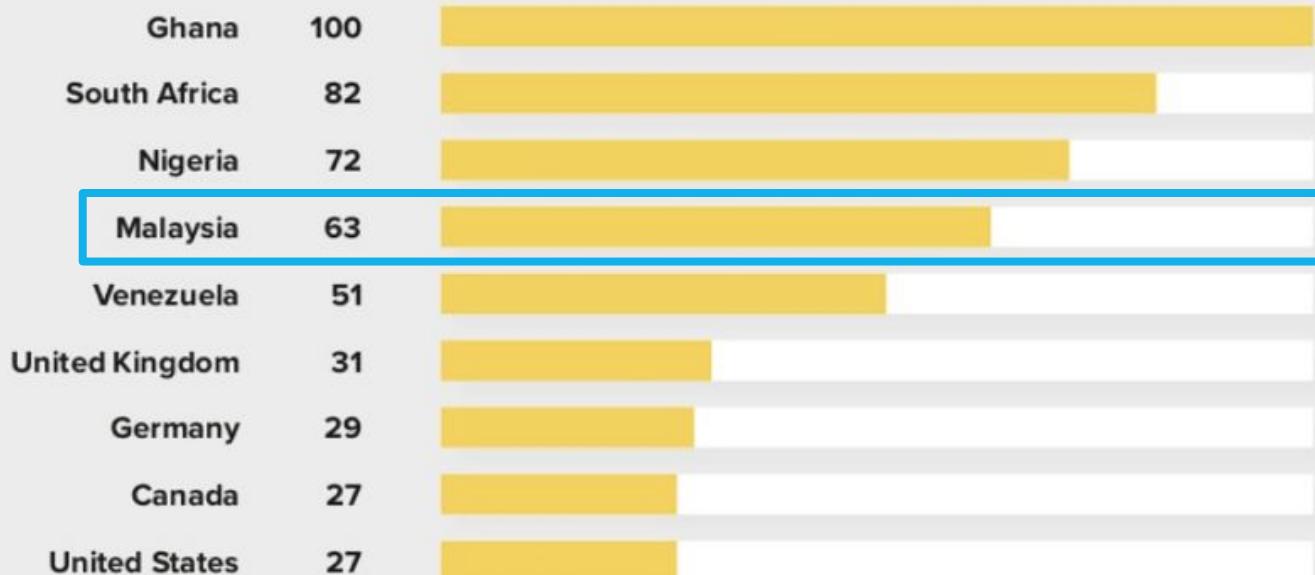
BLOCKCHAINS  
**IN MALAYSIA**

# BLOCKCHAINS BOLEH - INTERESTING MALAYSIAN FACTS

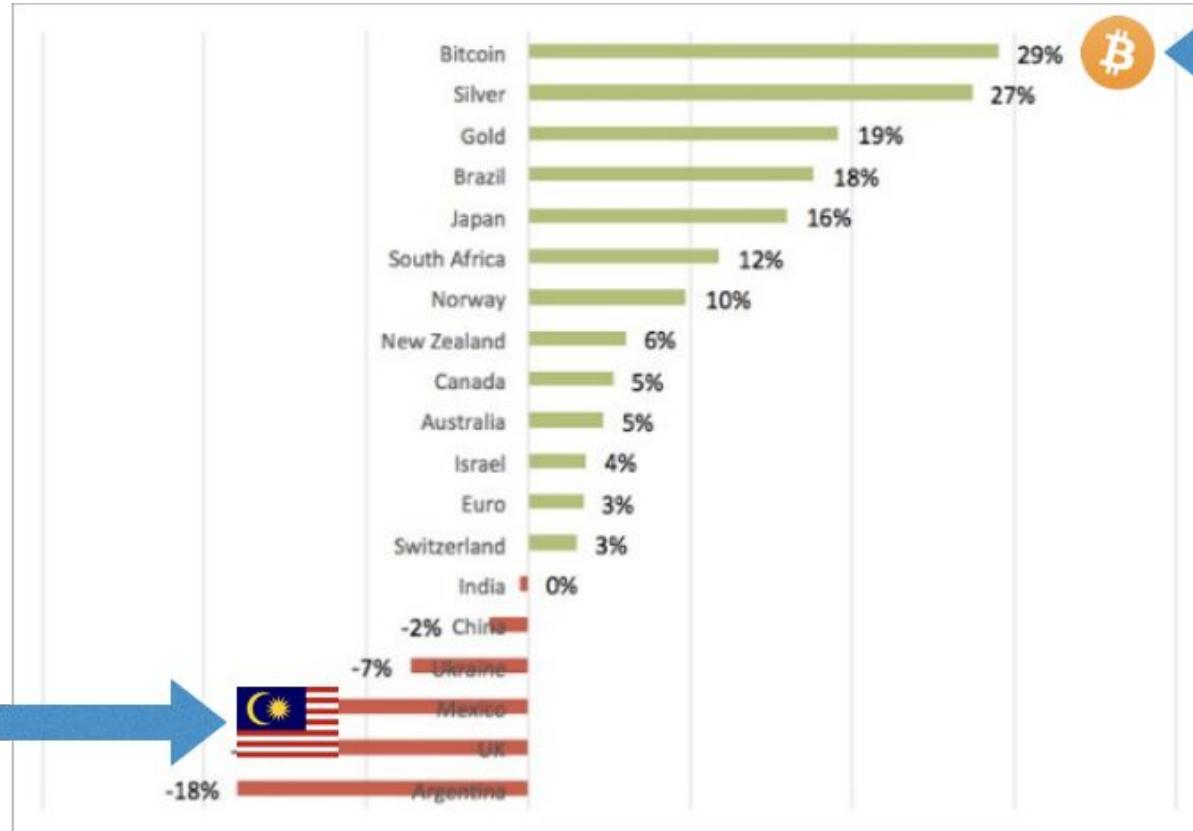
- In 2012 - Malaysia was LEADING the Bitcoin mining race in Asia
- Malaysia was LEADING manufacturer of ASIIC (used by miners)
- First petrol station in Asia accepting Bitcoin was in Malaysia
- First co-working space in Asia accepting Bitcoin was in Malaysia
- First global VPN service accepting Bitcoin was also in Malaysia

# WHERE DO WE ( MALAYSIA ) STAND ...?

Bitcoin Q2 & Q3 2016



# THE OTHER SIDE OF THE STORY



# OUR 1st CLIENT WAS ONE OF SIX LICENSED ECF OPERATORS

ataplus

Dogecoin (Testnet) Blockchain / ATA-Plus V0.0.1 / Datastores / Investments

Credits: 254.00000000 FLUSH LOGOUT

COMMITS

DATSTORES

- ISSUERS
- COMPANIES
- INVESTORS
- INVESTMENTS**
- SECTORS
- ADD NEW

SCHEMA

DOCUMENTATION

6 Months Sitewide Total Investments

RM Invested (Millions)

Month	Investment (Millions)
January	0.40
March	0.35

sort by  search investments

f2583c4bbc1d7f70fe776ef8de24e3e9131884de2be5ed3365fe72e53fa2177

Key	Value
Index: Investment ID [ auto ]	bf28617205e695439c0dd2285a76d7c1

**ADD NEW RECORD**

74c87dfa57a94dc86666209cd87a01b5

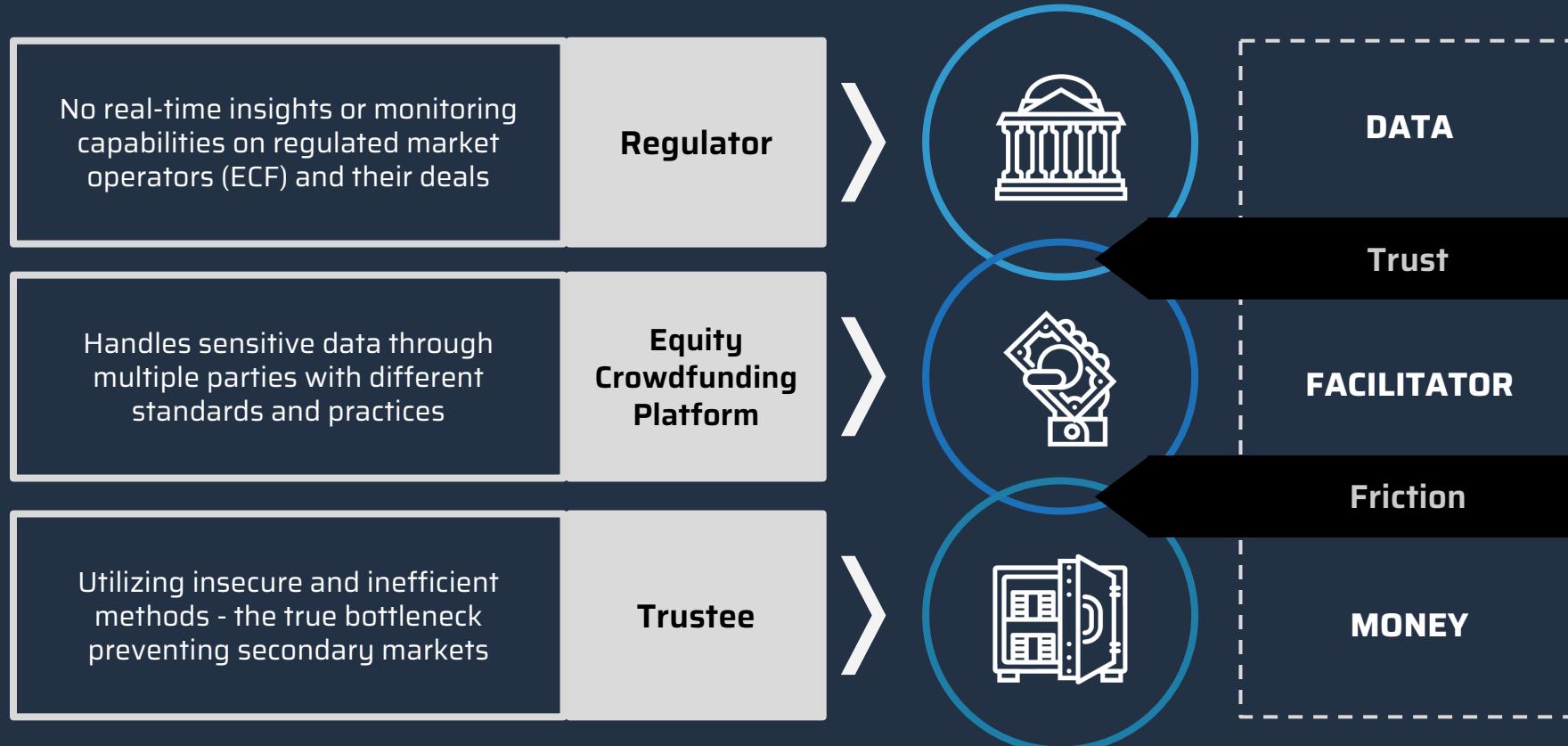
Date of Investment

“For ECF to flourish, there must be a deep depository of trust and transparency that is frictionless & inclusive. Neuoware’s tech enables us to provide all that and more!”

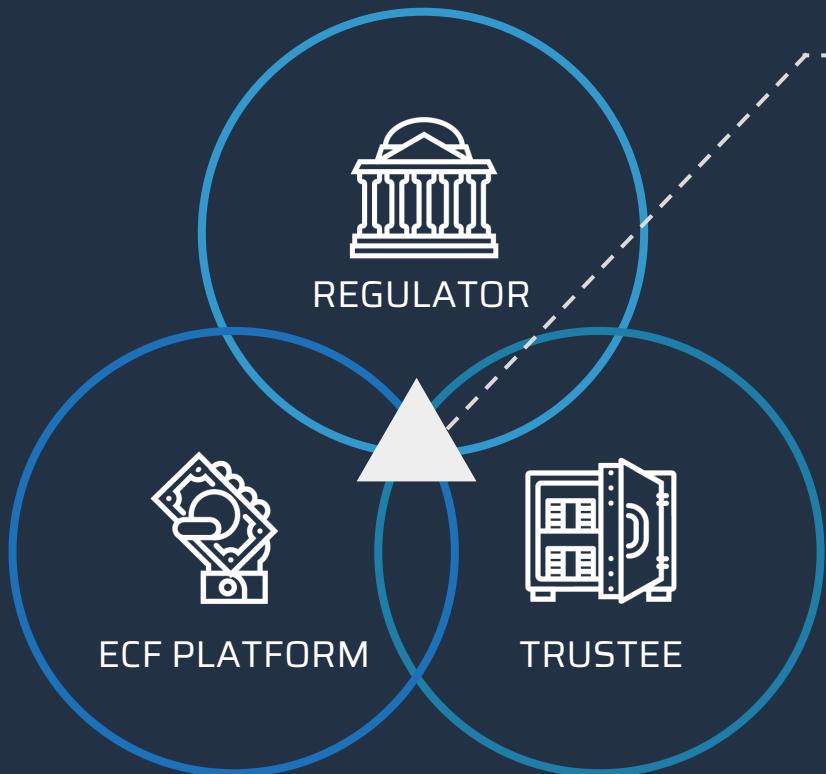
  
Kyri - Co-Founder & Director of Licensed ECF Platform

powered by neuoware

# PRESENTING A CASE STUDY FOR BLOCKCHAIN FINTECH



# BLOCKCHAINS SOLVES INDIVIDUAL & GROUP PROBLEMS



## Automated Secondary Markets

1

Real-time analytics and automated reporting with an inescapable audit trail of everything

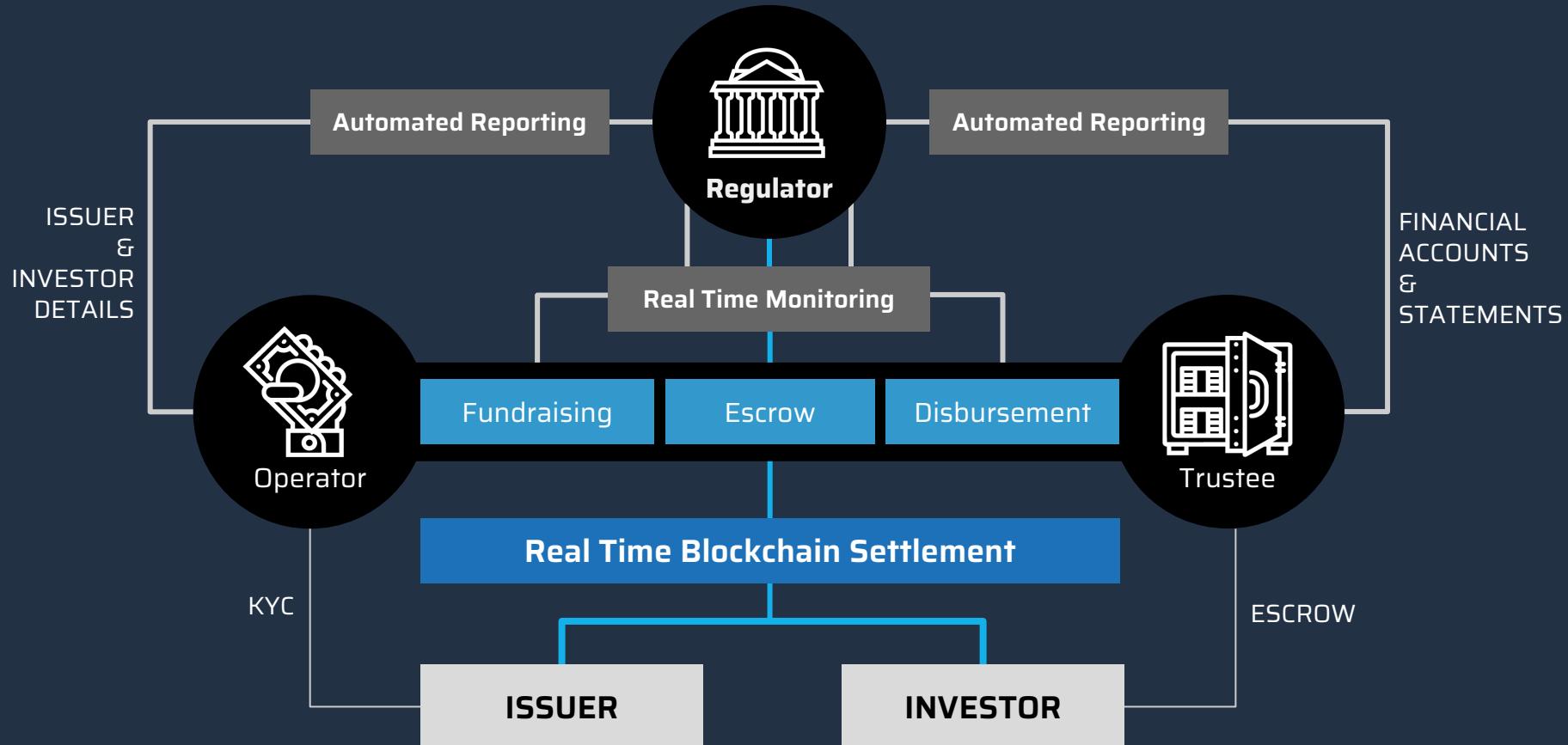
2

Single distributed tamper-proof database securely sharing data with all parties

3

Smart-contract enabled transactions reduce friction, costs and delays in settlement

# SECONDARY MARKETS EMPOWERED BY BLOCKCHAINS



# OUR OTHER CLIENTS & PARTNERS ARE MOSTLY MALAYSIAN



BANK NEGARA MALAYSIA  
CENTRAL BANK OF MALAYSIA



Suruhanjaya Sekuriti  
Securities Commission  
Malaysia



MINISTRY OF FINANCE MALAYSIA

500startups  
coinsilium

FINNOVASIA

TEDx BFM<sup>89.9</sup>  
The Business Station

Asia 8th Annual Premier Banking Technology Event

BankTechAsia '16  
Where banking meets technology...

CyberSecurity  
MALAYSIA



DBS

axiata

ataplus



sains®

THE MALAYSIAN  
INSURANCE INSTITUTE



Maybank

# COINGECKO - PROFITABLE MALAYSIAN BUSINESS

CoinGecko Beta Follow @coingecko Follow 853 Like Chart Commodities Data Buzz ... Sign In Sign Up English

Search Coins

฿ - BTC - All Hashing Algorithms -		Total	MktCap	Liquidity	Developer	Community	Public Interest	Last 7 Days		
Rank	Coin	%	฿	฿	%	฿	%	฿		
1	Bitcoin	96 + 0.5	฿16,248,112 + 2.543%	118139.30	98 + 0.5	11974 + 779 + 1364 + 393 + 2066 + 913	94 + 501 + 2.23 + 132	213664 + 561 + 169012	87 + 9,380,000 + 10539	
2	Ethereum	85 + 0.4	฿4,181,995 + 1.984%	76444.15	93 + 0.4	3379 + 1179 + 463 + 1984 + 1705	72 + 751 + 85 + 29.9 + 65	32579 + 164 + 2.28 + 61075	56 + 302,000 + 24497	
3	Litecoin	75 + 2	฿315,383 + 0.809%	52212.93	85 + 0.2	1199 + 966 + 249 + 148 + 144	62 + 66 + 27 + 24.5 + 13	22437 + 59 + 1.17 + 23327	42 + 409,000 + 174781	
4	Ripple	74 + 3	฿753,065 + 37.271%	70260.68	87 + 0.3	1269 + 397 + 251 + 247 + 199	49 + 20 + 1 + 12.9 + 36	2234 + 20 + 494 + 23406	54 + 122,000 + 63256	
5	Dash	71 + 0.5	฿473,649 + 0.424%	18547.81	82 + 0.5	410 + 228 + 1003 + 119 + 39 + 206 + 159 + 23	53 + 31 + 1 + 14.8	4220 + 31 + 10764 + 19935	47 + 255,000 + 46914	
6	Monero	70 + 0.2	฿265,592 + 1.465%	4601.59	85 + 0.2	514 + 307 + 143 + 100 + 558 + 387 + 155	54 + 52 + 0.9 + 26.0 + 155	9793 + 52 + 3022 + 11548	44 + 318,000 + 96178	

f 560  
t 13  
in 3  
tw 1  
em 1  
crown 1

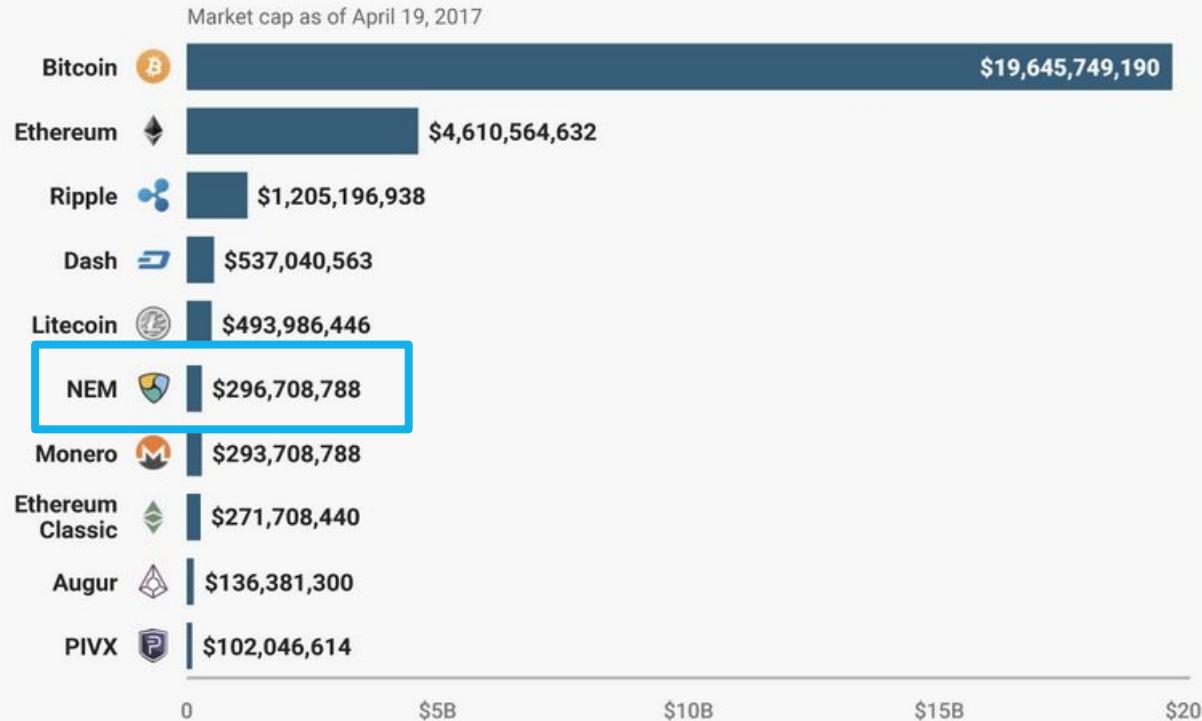
# COINGECKO - A VERY DIFFERENT PERSPECTIVE ON NEM

฿ - BTC - All Hashing Algorithms -		Total	MktCap	Liquidity	Developer	Community	Public Interest	Last 7 Days				
Rank	Coin	%	฿	=	%	★	</>	%	○	%	●	□
16	 LBRY Credits 	53 + 0.6	฿1,477 + 3.310%	139.65	77	208 252 34 11 107 5 69 278	41	1157 ▲ 2 8842 ¥ 0.02 3394	35	48,800 ↳ 1 378400 ฿ 0.00003348		
17	 Storjcoin X 	52 + 0.6	฿7,572 + 1.319%	19.06	81	137 180 31 25 443 5 421 29	41	1200 ▲ 4 2608 ¥ 0.06 10386	35	37,900 ↳ 1 201256 ฿ 0.00015004		
18	 BitShares 	52 + 0.8	฿10,626 + 1.088%	65.70	71	133 186 75 30 199 5 98	41	1133 ▲ 3 7979 ¥ 0.02 5833	36	75,100 ↳ 1 529201 ฿ 0.00000412		
19	 NEM 	52 + 0.3	฿49,606 + 2.678%	115.28	62	40 36 30 16 316 5 218	33	171 ▲ 2 2371 ¥ 0 3093	38	318,000 ↳ 1 263853 ฿ 0.00000551		
20	 Lumens 	51 + 1	฿16,603 + 1.524%	78.61	60	271 149 64 14 112 50 0	40	789 ▲ 3 4970 ¥ 0.06 8358	41	379,000 ↳ 1 316512 ฿ 0.00000240		
21	 Namecoin 	51 + 0.8	฿3,526 + 2.633%	29.90	74	132 133 33 28 91 5 34 292	41	2571 ▲ 2 1442 ¥ 0 3318	42	100,000 ↳ 1 1632993 ฿ 0.00023929		
22	 Vertcoin 	50 + 0.1	฿1,528 + 11.306%	27.91	63	81 49 31 16 40 5 36 0	46	4070 ▲ 3 2612 ¥ 0.06 25801	43	75,600 ↳ 1 1299032 ฿ 0.00004637		

# MARKET CAPITALIZATION NOT EVERYTHING

57

## 10 CRYPTOCURRENCIES HAVE A MARKET CAP OVER \$100M



# 11 DLTs NOW HAVE US\$1B+ MARKET CAPITALIZATIONS



USD ▾

Connect With Us



#	Name	Market Cap ▾	Price	24hour VWAP	Available Supply	24 Hour Volume	%24hr	Trade
1	Bitcoin BTC	\$79,916,901,602	\$4805.10000000	\$4790.1838	16,614,775	\$2,049,440,000	4.93%	Buy / Sell
2	Ethereum ETH	\$28,345,793,482	\$288.17387033	\$295.2986	95,037,194	\$538,813,000	-2.16%	Buy / Sell
3	Ripple XRP	\$9,663,005,412	\$0.23932035	\$0.2545	38,600,451,446	\$552,001,000	-6.78%	Buy / Sell
4	Bitcoin Cash BCH	\$5,544,270,358	\$330.73000000	\$317.7455	16,679,313	\$413,545,000	-0.98%	Buy / Sell
5	Litecoin LTC	\$2,675,045,037	\$50.16490499	\$49.7366	53,310,157	\$147,556,000	-3.38%	Buy / Sell
6	Dash DASH	\$2,173,946,826	\$287.75439901	\$289.2927	7,612,525	\$46,803,000	-4.05%	Buy / Sell
7	NEM XEM	\$1,950,848,999	\$0.20934140	\$0.2167	8,999,999,999	\$6,482,390	9.31%	Buy / Sell
8	NEO NEO	\$1,456,955,000	\$28.16906080	\$28.5921	50,000,000	\$82,776,200	-6.17%	
9	Monero XMR	\$1,319,896,407	\$86.83800000	\$86.8955	15,198,178	\$43,496,900	-2.08%	Buy / Sell
10	IOTA IOT	\$1,287,253,285	\$0.46311900	\$0.4567	2,779,530,283	\$16,939,500	-5.36%	
11	Ethereum Classic ETC	\$1,101,502,233	\$11.33800000	\$11.3416	96,321,365	\$42,054,200	-4.34%	Buy / Sell

ONLY 6 MONTHS AGO

Everything Else

Bitcoin



# 3 MONTHS AGO



Other billion dollar markets:  
Ethereum X 2, Ripple,  
NEM, Litecoin & Dash

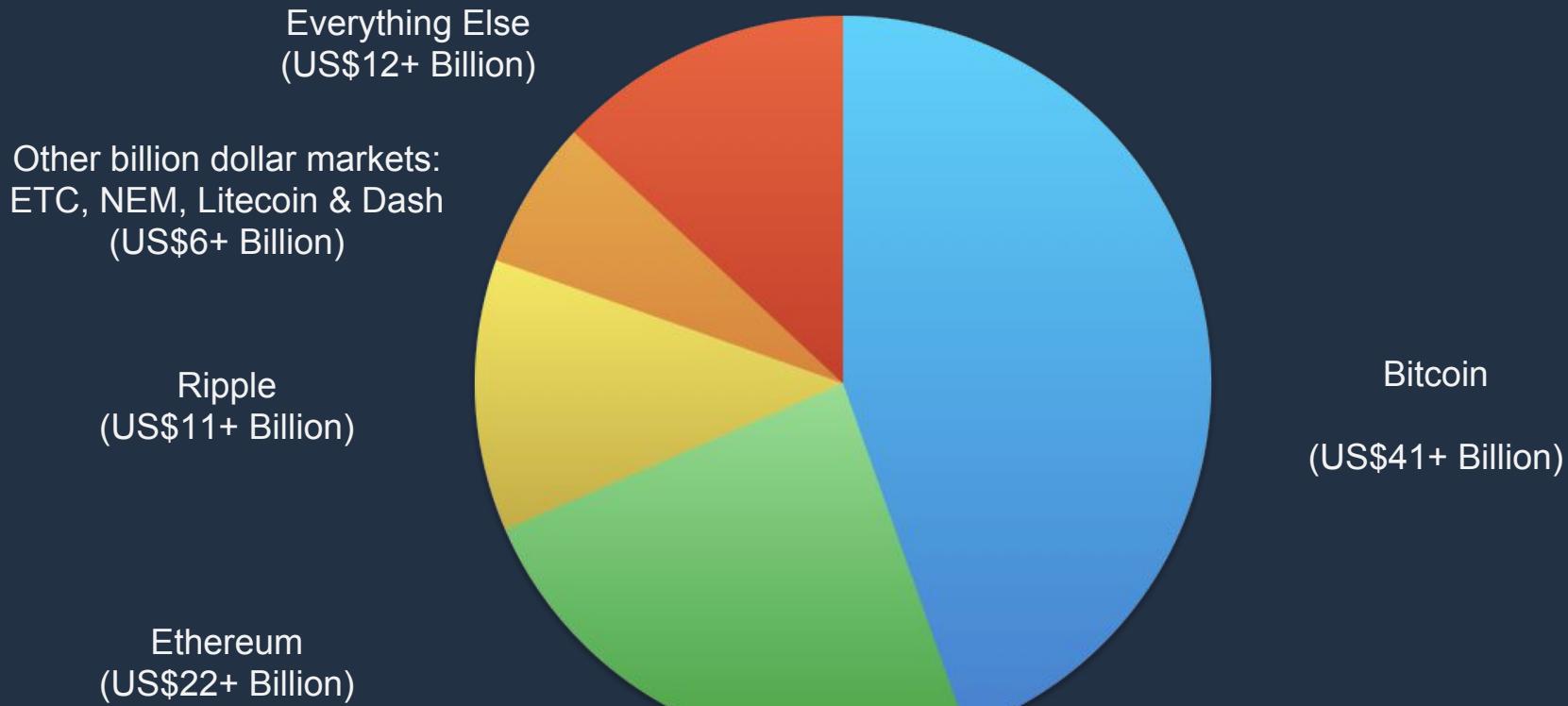
(US\$38+ Billion)

Everything Else  
(US\$7+ Billion)

Bitcoin

(US\$38+ Billion)

# A MONTH AGO



# ETHERSCAN - MALAYSIAN BASED - FUNDED BY DCG

 Etherscan  
The Ethereum Block Explorer

LOGIN  GO LANGUAGE

HOME BLOCKCHAIN ACCOUNT TOKEN CHART MISC

**TOTAL SUPPLY OF 88,464,230.97 ETHER  
\$10.56 @ 0.01085 BTC/ETH**

**LAST BLOCK**  
3104622 (14.40s Avg)

Hash Rate  
7,766.31 GH/s

**TRANSACTIONS**  
16160931

Network Difficulty  
111.68 TH

**14 day Ethereum Transaction History**



**Blocks**

View All

Block 3104622  
Mined By Ethpool\_2  
> 15 secs ago  
3 txns IN 12 secs  
Block Reward 5.00015 Ether

Block 3104621  
Mined By Ethermine  
> 27 secs ago  
5 txns IN 13 secs  
Block Reward 5.00409 Ether

Block 3104620  
Mined By 0x96338149e0f6c26...  
> 40 secs ago  
4 txns IN 4 secs  
Block Reward 5.00187 Ether

Block 3104619  
Mined By DwarfPool1  
> 44 secs ago  
0 txns IN 20 secs  
Block Reward 5 Ether

**Transactions**

View All

TX# 0X8C82912A90EB24422A0DD89...  
From 0xea674fdde714fd9... To 0xdc17d353b01285...  
> 15 secs ago  
Amount 1.0045803417014828 Ether

TX# 0X30803DA432AD0EC50B674EB...  
From 0xf34a762291e2578... To 0xfc82a5fe25a5cd...  
> 15 secs ago  
Amount 0.09972424738776952 Ether

TX# 0XF3AE03CD8978780C11C59...  
From 0x267179261a34b... To 0x44e9bfdb5eb0651...  
> 15 secs ago  
Amount 1.506161 Ether

TX# 0X69429B51113744361D7EF7D...  
From 0xea674fdde714fd9... To 0xb2db84a2574811...  
> 27 secs ago  
Amount 1.0055965023717969 Ether

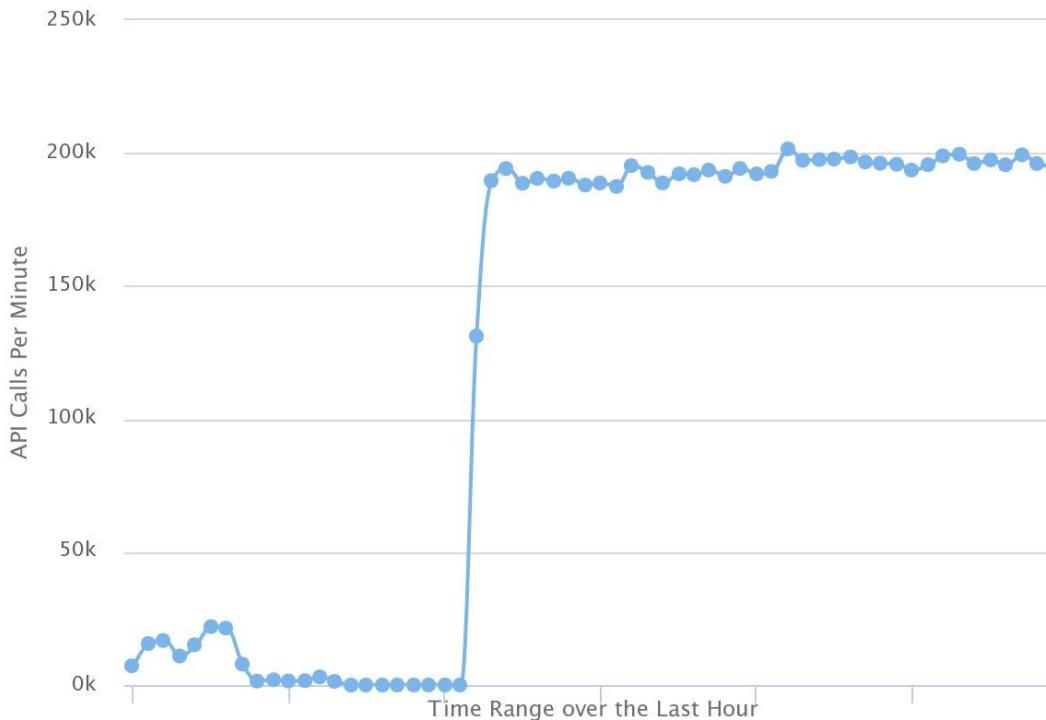
# API ACCESS GROWING - ESPECIALLY WITH EACH NEW ICO

## ETHERSCAN API STATISTICS (Last Hour)

Api-Key:

Total Requests: 7,439,127

Click and drag in the plot area to zoom in

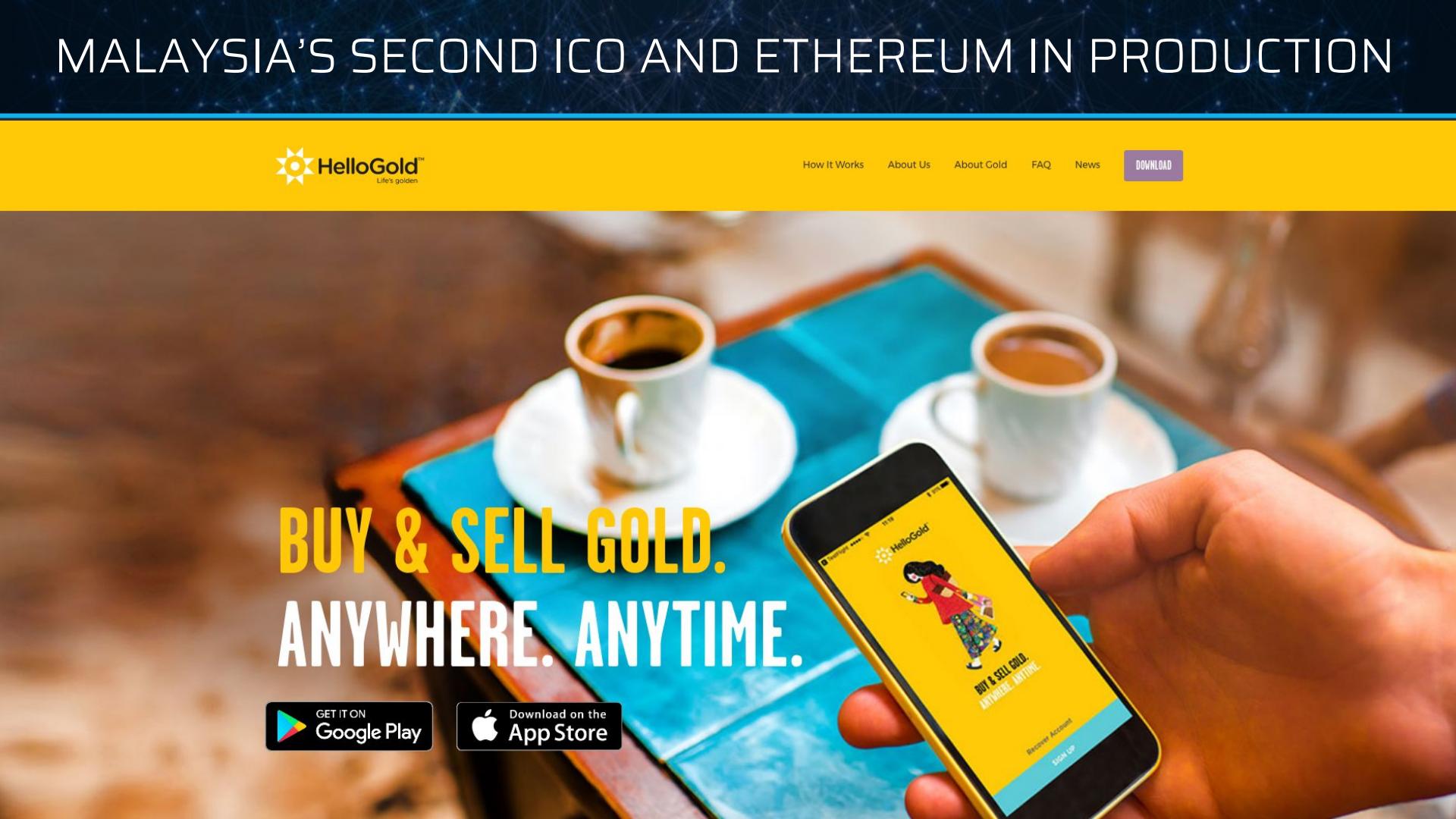


# MALAYSIA'S SECOND ICO AND ETHEREUM IN PRODUCTION



How It Works   About Us   About Gold   FAQ   News

DOWNLOAD



**BUY & SELL GOLD.  
ANYWHERE. ANYTIME.**



# MONEY MATCH - USING RIPPLE IN PRODUCTION

## Why you're making the right choice



### FASTER

Send your money in seconds, with just a few simple clicks.



### CHEAPER

Save up to 90% vs your bank, thanks to our low fees and real rates.



### CONVENIENT

Exchange money when you want, where you want. All within your finger tips.



### TRANSPARENT FEE

No unexpected fees, no unfair charges, no surprise exchange rates.

## Accreditations & Partners



FTEG

Financial Technology  
Enabler Group

BANK NEGARA MALAYSIA  
*Central Bank of Malaysia*

MoneyMatch is an Approved Participant in Bank Negara Malaysia's Fintech Regulatory Sandbox.



C27  
*Digital Marketing & Product Design*

C27 focuses on effective performance marketing and seamless UX design for all MoneyMatch products.



MSC MALAYSIA  
*MSC Tier 1 status*

MSC status is a recognition awarded by the Government of Malaysia for ICT businesses.

T S LIEW, NURZILA & CO  
*Advocates & Solicitors*

TS LIEW, NURZILA & CO  
*Legal Counsel*

T S Liew, Nurzila & Co provides top to corporate legal work, and business advisory services.

# OTHER USE CASES WE HAVE EXPLORED IN MALAYSIA

## BANKING

From AML & KYC cost reductions to reward schemes & reaching the unbanked or general key-signing

## HEALTHCARE

Complete and immutable family histories of every related diagnosis and condition available from 1 key

## ACCOUNTING

Creation of programmable processes & automated auditing trails increase transparency & efficiency

## LEGAL

Cryptographically secure document notarization, copyright protection, and dispute settlement

## GOVERNANCE

Increase the accountability of public officials and offer total transparency in voting & elections

## LOGISTICS

Tracking of shipping cycles and provenance systems that autonomously verify actions

## GAMING

Share digital assets between an entire network of games, or use the blockchains to create immutable persistent open-worlds

## ASSETS

Track possession of your property in the digital economy by creating, managing, storing, or sharing multiple asset classes

## INSURANCE

Integrated insurance and medical services can be intelligently designed to quickly and contractually settle claims with cryptographically

## SECTION SUMMARY

# WHAT'S HAPPENING IN ASIA?

- Malaysia was at one time leading the way in Asia
- Singapore & China are now leading their own ways
- Malaysia has LOTS of blockchain knowledge & talent
- FinTech is no longer the only active use-case

TIME TO GET HANDS ON WITH  
**WALLETS**

# THIS IS KNOWN AS A PAPER WALLET



# ACCOUNTS CREATED BY ANYONE, ANYTIME, ANYWHERE

## INPUT CONTROL

<b>Input Type</b>	Private Keys
-------------------	--------------

<b>Private Key 1</b>	Private key to use?
----------------------	---------------------

[ANOTHER KEY](#)

<b>Blockchain</b>	Dogecoin
-------------------	----------

<b>Fee</b>	Leave blank for default
------------	-------------------------

<b>Optional Data</b>	Data added to chain
----------------------	---------------------

<b>Change</b>	Auto Return
---------------	-------------

<b>Address 1</b>	Send to this address
------------------	----------------------

<b>Amount 1</b>	How much to send?
-----------------	-------------------

[ANOTHER ADDRESS](#)

[RESET](#)

[BUILD](#)

Generate new cryptographic keys or re-create  
deterministic ones below:

[GENERATE KEY-PAIR](#)

[SETUP MULTI-SIG](#)

[SPEND MULTI-SIG](#)

[DERIVE CHILD KEYS](#)

Additional Tools:

[POST DATA](#)

[FETCH DATA](#)

[SEARCH ▾](#)

Enter address or TXID here

# CONTENTS CAN BE VERIFIED BY USING BLOCK EXPLORERS



Networks ▾

Blockchain API

Wallet API

Blog

Such Search...



## Address Details (D)

DGtEipQbxhKNUkg5g1PTQ4x88J14L3tHQe

Little Shibe

Address DGtEipQbxhKNUkg5g1PTQ4x88J14L3tHQe

Coin Dogecoin (DOGE, Ð)

Balance 100.00000000

Pending Nothing

Received 100.00000000

Transactions 1

Shortlink <https://chain.so/a/hoq9jru>

Other Info [Raw Data](#)



Send Dogecoin

Transaction ID: e57cb8c069b287c4fd837930036b68d78bbe55e83346e57980ea799b6322caa2

May 9, 2017 at 19:59

Confirmed

# GENERATING KEYS RANDOMLY WITH THE QT (180GB )

 bitcoin [Introduction](#) [Resources](#) [Innovation](#) [Participate](#) [FAQ](#) [English](#)

## Choose your Bitcoin wallet

Find your wallet and start making payments with merchants and users.

 Mobile  Desktop  Hardware  Web

---

 Bitcoin Core  Bitcoin Knots  Bither  GreenBits  Coin.Space  Simple Bitcoin

 MultiBit HD  Armory  Electrum  mSIGNA  Bitcoin Wallet  breadwallet

 **Take time to educate yourself**

Bitcoin is different from what you know and use every day. Before you start using Bitcoin for any serious transaction, be sure to read [what you need to know](#) and take appropriate steps to [secure your wallet](#). Always remember that it is your responsibility to choose your wallet carefully and adopt good practices in order to protect your money.

[Network Status](#) [Legal](#) [Privacy Policy](#) [Press](#) [About bitcoin.org](#) [Blog](#)

© Bitcoin Project 2009-2017 Released under the MIT license

# DOGECOIN ( 25GB ) - GOOD FOR TESTING

**CHOOSE YOUR WALLET.**



**MultiDoge**  
The Dogecoin Light Wallet.



**Dogecoin Core.**  
The Dogecoin "Full" Wallet.  
Community maintained User Manual.

Learn how to set up your wallet with the [Getting Started Guide](#).

---

What are the differences between the two?

You have to sync with the blockchain to use Dogecoin. MultiDoge is a "light" wallet. It syncs with the blockchain by "skimming" through the blockchain, providing fast sync times. Dogecoin Core, on the other hand, is a "full" wallet. It syncs by downloading it, providing a solid-working Dogecoin wallet.

---

Advantages and Disadvantages?

# THIS IS AN ADVANCED BRAIN WALLET ( ALL CHAINS 0GB )



**Setup Wizard**  
(Here to help you get started)

[INSTALL GUIDE](#) [DOCS](#)

## SALT GENERATION

Before we create any addresses we first need to establish a device salt. Each piece of information you enter is hashed and re-hashed before ever leaving the browser. We never see any of your details from the resulting hashes. At the end of the process a device salt is generated that we can use to more securely create new accounts.

Once entering these details you cannot change them later or recover them without recreating this process with the exact same data.

STEP 1: SALT GENERATION    STEP 2: CREATE ACCOUNT    HELP

**Generating Your Device Salt**  
This is a one time installation process. Please read the instructions carefully..

**RESET** **IMPORT**

Required Salt Components		Optional Security & Settings	
Your Name	Using your actual name is easier to remember	App URL	http://localhost/neuroware/blockstrap/framework/manual.htm
Your Username	Pick a simple yet memorable username	Salt Component	-- Select Additional Salt Components --
Your Password	This cannot be changed later	API Service	Blockstrap
Repeat	Confirm your password again	Profile Photo	<input type="button" value="CHOOSE FILE"/>
Password		Add Photo to Salt?	<input type="button" value="SET"/> <input type="button" value="NO"/>
Date of Birth	Day <input type="button" value="▼"/> Month <input type="button" value="▼"/> Year <input type="button" value="▼"/>	Create custom question for salt?	<input type="button" value="SET"/> <input type="button" value="NO"/>
City of Birth	It is easier to remember your real city of birth		

**NEXT STEP**

# WHERE TO BUY COINS ...?

coinbase

Products ▾

Help

1 BTC = \$1,671.18

Sign In

Sign Up

## BUY AND SELL DIGITAL CURRENCY

Coinbase is the world's most popular way to buy and sell bitcoin, ethereum, and litecoin.

Enter your email address

Get Started

New to bitcoin? | What is ethereum?

NOW SURPASSED 10 MILLION USERS

## Coinbase Users



# LOTS OF ATMs IN EUROPE



Getting Bitcoin  
can't be easier.

[SEE PRODUCTS](#)[Order](#)

# CLOSER TO HOME - ONLY TRUSTED EXCHANGE IN MALAYSIA

LUNO

BTC/MYR 7,930    Help    Blog    Sign In    Sign Up

Luno makes it safe and easy to buy, store and learn about Bitcoin in Malaysia

Sign up on our Website    Download on the App Store    GET IT ON Google Play

Global Bitcoin community  
20 million +

Available in  
Malaysia

Buy bitcoin with

The wallet is easy to navigate and  
really functional.

★★★★★

# WITH BITCOIN YOU CAN SHAPESHIFT TO ANY CRYPTO

 ShapeShift

About API + Tools Resources Support COIN CAP English

**The Safest, Fastest Asset Exchange on Earth**

Trade any leading blockchain asset for any other.  
Protection by Design. No Account Needed.

BTC	XRP	ETH	LTC	DASH	XMR	MAID	DOGE	WAVES	BTS
\$1,676.6100	\$0.2101	\$85.3395	\$26.6958	\$87.6530	\$27.6971	\$0.3206	\$0.0011	\$1.0838	\$0.0369
-6.07%	11.4%	0.8%	-11.67%	-3.79%	-7.28%	-3.2%	-5.5%	-10.58%	-2.46%

Choose Which Assets to Trade

Deposit      Receive

 Bitcoin       Dogecoin

Quick      Precise

Continue

# WHO OWNS WHAT ...? WHERE ARE THE KEYS ...?

- Paper Vs Brain
- Hardware Vs Software
- Hard Drive Vs Web-Service
- Pseudo-Random Vs Deterministic
  
- Exchanges are **NOT** wallets ...  
(1 exchange hacked every 3 months)

# TREZOR - MOST POPULAR BITCOIN HARDWARE WALLET



Shop TREZOR Wallet Docs Blog Contact Follow us ▾

## Bitcoin wallet.

The original & most secure hardware wallet.



Buy for \$99

Supported platforms:



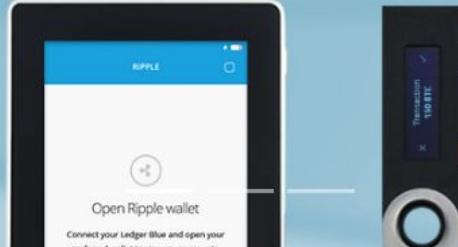
New TREZOR owner? [Start now](#) ▶

# LEDGER IS ANOTHER HARDWARE ALTERNATIVE

NOW AVAILABLE

## Ledger Wallet Ripple

For Ledger Nano S & Blue



[CLICK HERE FOR HELP & CONTACT](#)

# JAXX - RECENTLY HACKED - STILL A GOOD CHOICE ...?

# Jaxx

YOUR BLOCKCHAIN INTERFACE

[Support](#)[View Source Code](#)[Install Now](#)

**Android**  
Mobile  
Tablet



**iOS**  
Mobile  
Tablet



**OS X**  
Desktop



**Chrome**  
Extension



**Firefox**  
Extension



**Windows**  
Desktop



**Linux**  
Desktop



**Hardware**  
Coming soon

# EXODUS - GOOD ALTERNATIVE WITH BUILT IN SHAPESHIFT

The screenshot displays the Exodus mobile application's interface, specifically the "Exchange" feature. The top navigation bar shows the title "EXODUS - GOOD ALTERNATIVE WITH BUILT IN SHAPESHIFT".

**Left Sidebar:**

- EXODUS** logo and balance: \$39.54 USD.
- Portfolio** icon.
- Wallet** icon.
- Exchange** icon (selected).
- Backup** icon.
- Settings** icon.

**Exchange Section:**

**EXCHANGE** section:

- Bitcoin (BTC) selected.
- Available: 0.00753959 BTC.
- Input field: 0.007 (BTC).
- Output field: 4.65 (USD).

**RECEIVE** section:

- Ethereum (ETH) selected.
- Available: 0.99696144 ETH.
- Input field: 0.38022516477 (ETH).
- Output field: 4.52 (USD).

**Bottom Summary:**

YOU ARE EXCHANGING  
0.007 BTC  
\$4.65

YOU WILL RECEIVE  
0.38022516477 ETH  
\$4.52

**Buttons:**

- A large orange "EXCHANGE" button at the bottom center.
- A small "X" icon in the top right corner of the main window.

TIME TO GET HANDS ON WITH  
**CRYPTOGRAPHY**

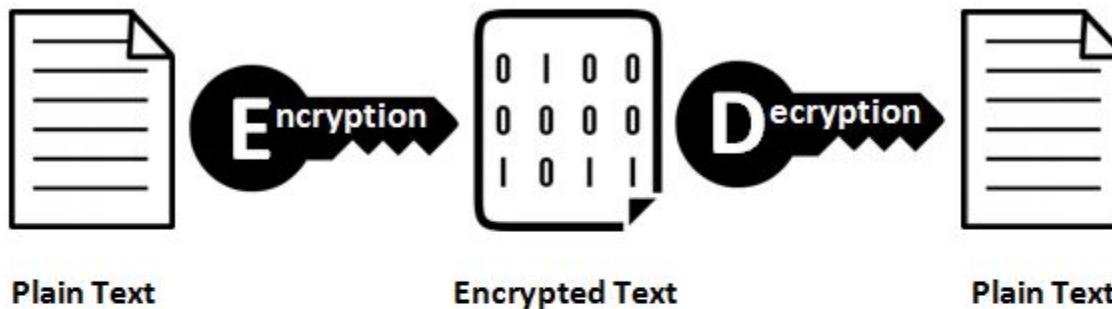
# REMEMBER - BITCOIN HAS NO NEW TECHNOLOGY



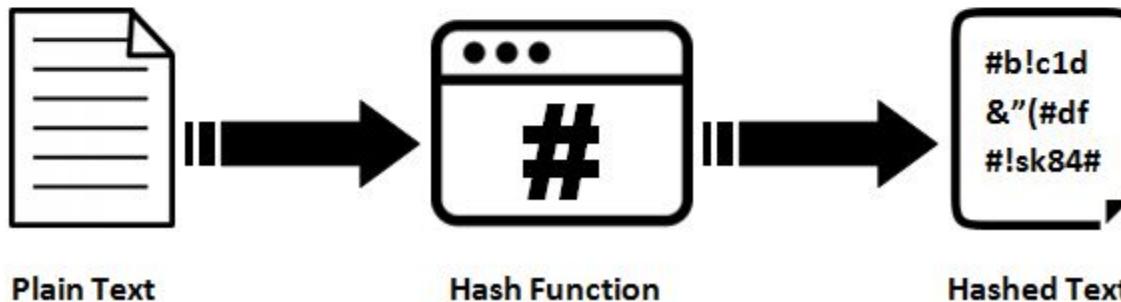
- HASH - Theorized in the 1800s - Coined by IBM in the 1950s
- ECDSA - Digital Signatures using Elliptic Curve Cryptography
- P2P - Peer to peer protocol popularized by Napster in 1999

# TERMINOLOGY - HASHING Vs ENCRYPTION

Encryption & Decryption



Hashing Algorithm



# EXPLORING CRYPTOGRAPHY WITH THE BCE TOOLBOX

blockchain embassy asia

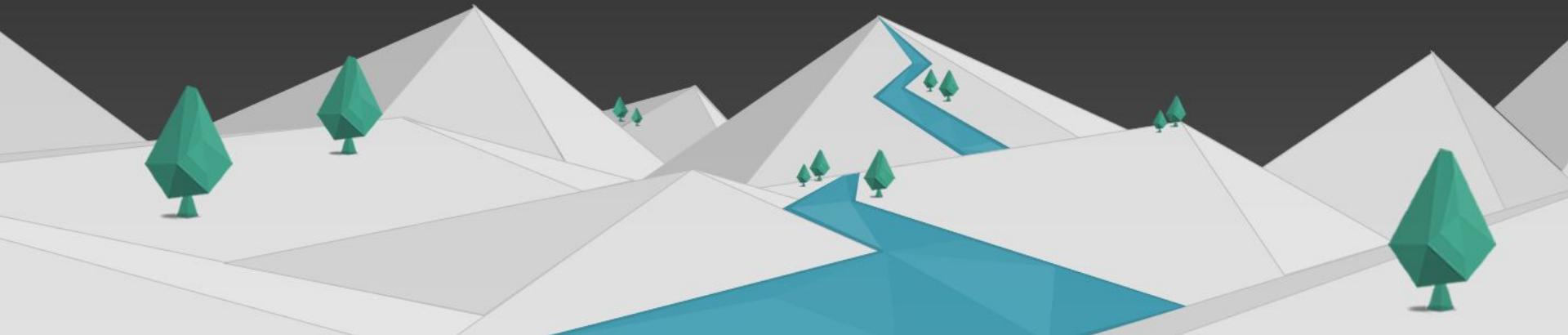
ABOUT US | **TOOLBOX** | CONTACT US | NEWS

## welcome to the embassy crypto asset toolbox

build and send transactions without storing keys - should not be used for anything other than educational purposes

DOWNLOAD

LEARN MORE



# DETERMINISTIC KEYS DO NOT NEED TO BE STORED

blockchain embassy asia

Private Key 1 Private key to us

GENERATE KEY-PAIR

POST DATA

Generate Key Pairs

ABOUT US | TOOLBOX | CONTACT US | NEWS

Send to this address

How much to send?

ANOTHER ADDRESS

DERIVE CHILD KEYS

or TXID here

Combining the fields above will result in the following key-pairs and public address:

```
var hash = bitcoin.crypto.sha256(salt + seed + pw + chain).toString("hex")
var keys = $.fn.blockstrap.blockchains.keys(hash, chain, 1, false, true);
```

HD Public	dgub8kXBZ7ymNWj	HD Private	dgpv51eADS3spNJI		
Public		027a17a97a0ded57	Private		QRsVW5oo53fJbwY
Public Address		check	DRSxsjC8l4z9Y6LDQvA3mGhAuSGTeZNG7T		

# MULTI-SIGNATURE KEYS ARE WHERE IT GETS INTERESTING

blockchain embassy asia

ABOUT US | TOOLBOX | CONTACT US | NEWS

Private Key 1 Private key to use

GENERATE KEY-PAIR

POST DATA

Send to this address

How much to send?

ANOTHER ADDRESS

DERIVE CHILD KEYS

The three keys are combined via the following function:

```
var ms_keys = $.fn.blockstrap.multisig.generate(false, chain, keys, 2);
```

Multi-Sig Address 9xHD5hnDj5a6PtBvDBcnUsuDLRqEgYTQvo

Redeem Script 522102595379e4ae19dc034b13053b91cc0803b

### Create Multisignature Account

Generate a multi-signature account by filling-out the details below:

Blockchain	Dogecoin
Contract Type	2 of 3
1st HD Extended Key	r93ZcqgqcaMZKKcCgCicFG6bSGYejd4QD9vh
2nd HD Extended Key	GGazVJYTUj3EprikD8Tb269VDQZVbnopLxoH
3rd HD Extended Key	THBYPJ7sL5xpEVujzABQqmqZ1LafsWHdTx49

The three keys are combined via the following function:

```
var ms_keys = $.fn.blockstrap.multisig.generate(false, chain, keys, 2);
```

TIME TO GET HANDS ON WITH  
**DATA**

# SCHEMA CAN BE ACHIEVED WITH CHILD KEYS

blockchain embassy asia

Private Key 1 Private key to use

GENERATE KEY-PAIR

POST DATA

ABOUT US | TOOLBOX | CONTACT US | NEWS

Send to this address

How much to send?

ANOTHER ADDRESS

DERIVE CHILD KEYS

or TXID here

**Derive Child Keys**

Derive child keys from any extended key using the form below:

Blockchain	Dogecoin		
Extended Key	dgpv51eADS3spNjhA8LNQwKsHGwuRJbCyG1		
Key Depth	0	Key Index	0
Child Path	1, 2017, 99999999, 0		
Key Depth	4	Key Index	0
Derived HD Public Key	dgub8tcZjURztsHtR5ABhs6BTHZr3ZSmnXRFu7		
Derived HD Private Key	dgpv59jYPnW7LidZ8DW2fdUDLS2Fb158xQPYc		
Derived Private (WIF) Key	QUjRUShYepkbvxqXJPnucZX3CkpDRhERQihd		
Derived Address	DBpKzChit4Kit16G9SL5hmrQN9F59sWHZML		

# DATA CAN BE ENCODED AND ENCRYPTED IN TRANSACTIONS

The screenshot shows a web application interface for managing blockchain data. At the top, there's a navigation bar with links to 'ABOUT US', 'TOOLBOX' (which is underlined), 'CONTACT US', and 'NEWS'. Below the navigation, a dark overlay covers most of the page, except for a central modal window titled 'Post Data'. This modal contains several input fields:

- Blockchain:** A dropdown menu set to 'Dogecoin'.
- HD Private Key:** A text field with placeholder text 'Expecting an extended private key'.
- Data:** A text field with placeholder text 'Added to blockchain'.
- Child Path:** A text field with placeholder text 'Optional oomma separated list'.
- Encryption:** A dropdown menu set to 'None'.
- Encryption Salt:** A text field with placeholder text 'Add an optional custom secret'.

At the bottom of the modal are two buttons: 'RESET' and 'POST' (in a teal-colored button). In the background, through the dark overlay, you can see other parts of the website, including a 'GENERATE KEY-PAIR' button, a 'POST DATA' button, and a 'DERIVE CHILD KEYS' button.

our mission to educate a diverse selection of organizations in the legal and technical implications of blockchains has brought industries together

Neuroware | BloqCert

**v0.1**

# ISSUER SCHEMA

- Public Issuer Key [ 0 ]

dgub8o2PnEtYA9bELuMkkiuNppWBbVowjuTnV5FTNvW51fLKP3GNVRzY  
RDGkQZT8E6RTY5hP6SSeLmZWyvnXBcnDEdwakiWzPpjz1Druf4FRqpw

- Name [ 0, 1 ]

- URL [ 0, 2 ]

- Email [ 0, 3 ]

- e9e3d62918a41c5cd69496078013115a1447634f0788edd4e728ca2dda2457b1
- e21d0a6f2dc3f8214c8f99b63878ee96e918735e7c3e93d9a94b02d828902785
- a0d5a11fa6f93888c4e8ae3db9bf7d8801f3a0d235a7002ddb0e893a4d1f4607

# COURSE SCHEMA

- Public Course Key [ 1 ]

dgub8o2PnEtYA9bEPppPC8Fyzm6pA5LEH4UzA63QvsSuQ8obq8i7FtZcj1  
iFGZWY9gnYhkqP248D84paE4irgNNfQdbRKwTUwcfluKSGsj5qQ4a

- Course 1 - Name [ 1, 1, 1 ]

- Course 1 - URL [ 1, 1, 2 ]

- Course 1 - Description [ 1, 1, 3 ]

- be8b2a5773f07743d07834f59868b78c47687b4c937f674d4eff2b5f579e780a
- 420cfdf1c1bc3088cd95c38eed84d79912725c45bbc3dcde706576c3583da3c8
- 616f7851520e6322fd96f112b793480ae8b71b2e88e61c061e1102afbe30c860

# TEACHER SCHEMA

- Public Teacher Key [ 2 ]

dgub8o2PnEtYA9bERx2nsr18YRYCo5EzV2LQsCSrJEoDo3beiwuFoCSZ8j  
vyG8xcSnWbYgcrrErjKNENRLsV1j5RakcAaGPZL7u4Ev296Eha1Dt

- Teacher 1 - Name [ 2, 1, 1 ]

- Teacher 1 - URL [ 2, 1, 2 ]

- Teacher 1 - Email [ 2, 1, 3 ]

- d3497b1695c23264df311053fd318df0008f64bd2464eb250e849b6318bb7ddf
- 32650252128ba57c03ba6fde1d98372bebf9bc85ab12b25ccb79779040bbe30f
- 537ecfc04eed493426e4efe11b6624e58fcd1fd6cd8326a2784588ea7b4b4029

# STUDENT SCHEMA (ID = 123)

- Public Student Key [ 3 ]

dgub8o2PnEtYA9bEWD57mDzwzGveHGDGiQje9AaYd5KVQDNv9MmjDvS5s  
QRWXWg6F9vMbabsGijLaCMT1UsEk4NNRdo8aAgvA1y9jva8xfFwALXE

- Student 1 - Name [ 3, 1, 1 ]

- Student 1 - URL [ 3, 1, 2 ]

- Student 1 - Email [ 3, 1, 3 ]

- 58f297fbc6fc91d31a6adc5c2166521e113cd5bf9a067dc0ba915a60e4ff4697
- c8710e386477d6bc56b7c9036098b92517435a05f59bb02ca780101fd51511d1
- 4a59ae470431217015cda9c832d1333e521b7f1006718114e30e6ea9cdeee11e



email the team anytime - [founders@neuroware.io](mailto:founders@neuroware.io)