Demystifying Blockchains

(understanding the technology behind the myths)

presented by

neuroware

DISCLAIMER - I BOUGHT BITCOINS WHEN THEY WERE US$10

Mark Smalley - CEO (Neuroware.io)

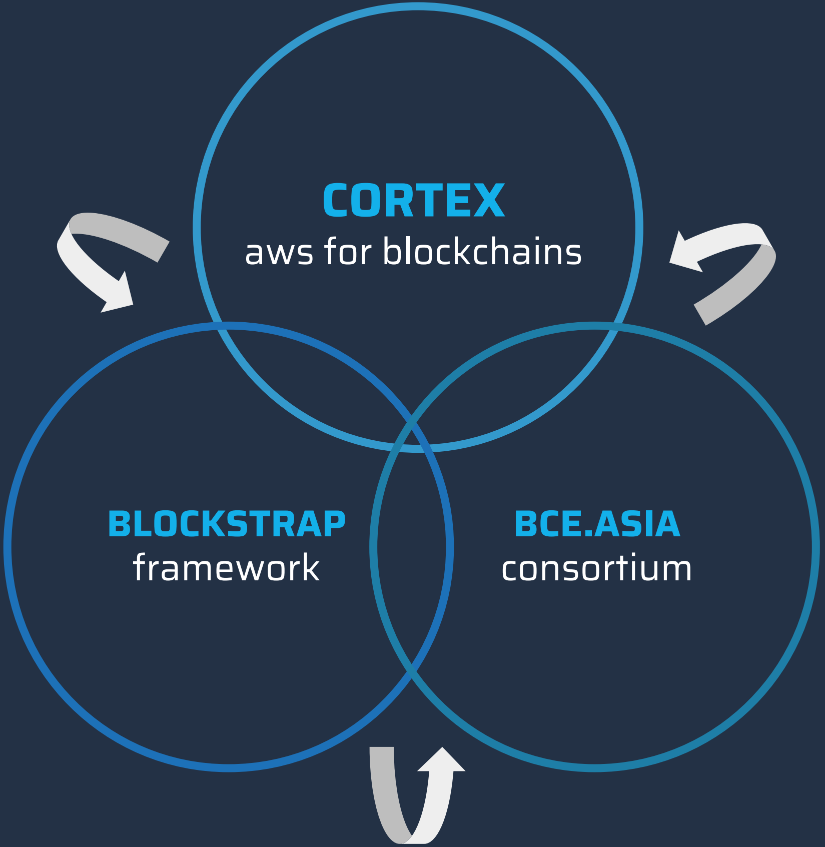
Living in Malaysia for the past 20 Years

Building FinTech Applications for 15 Years

Building Blockchain Apps for 5 Years

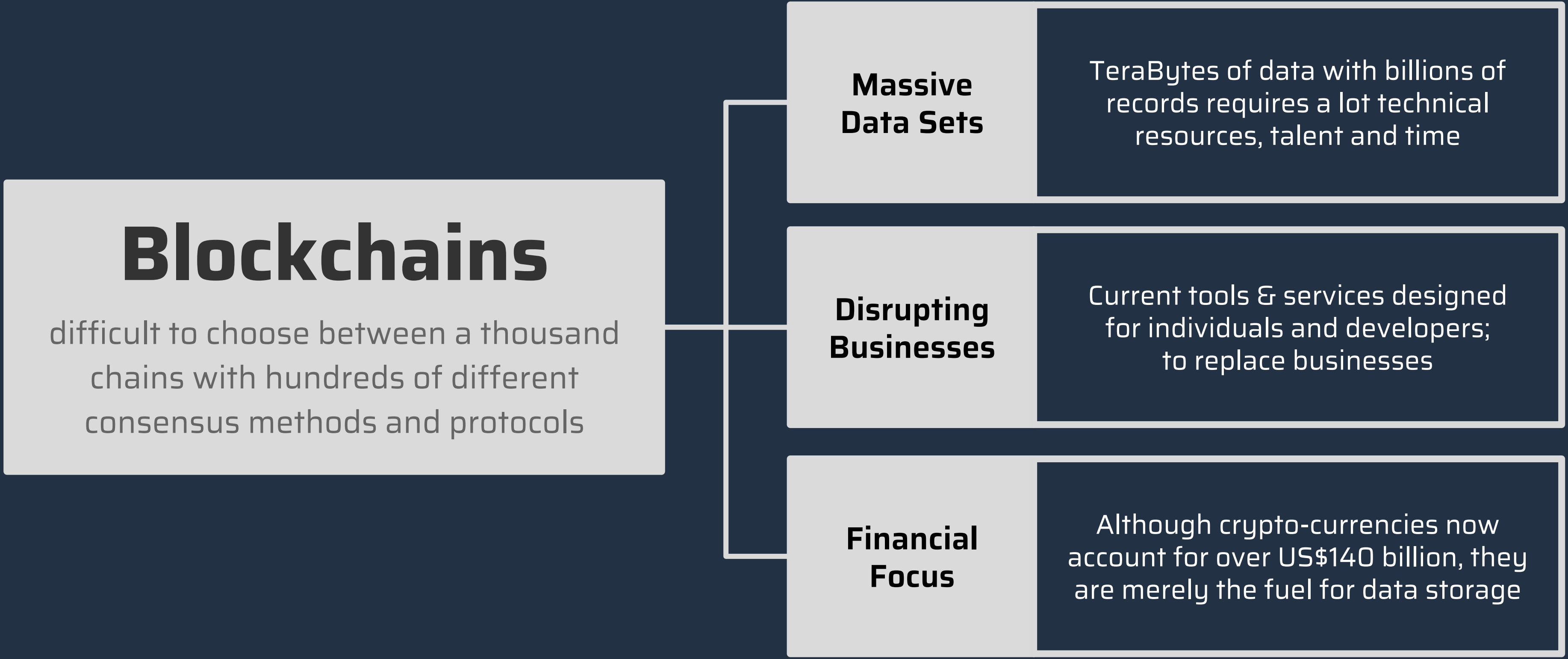
Despite a Family of Financial Advisors,
I’ve only ever made one investment …

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

ENOUGH ABOUT ME

WHAT ARE BLOCKCHAINS …?

THE BEST IDEAS ARE RARELY NEW ONES

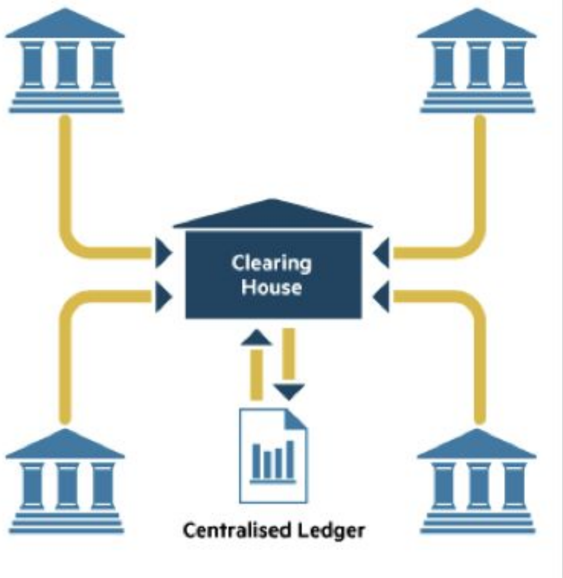
SHOPPING WAS ALMOST AS CHALLENGING AS BANKING

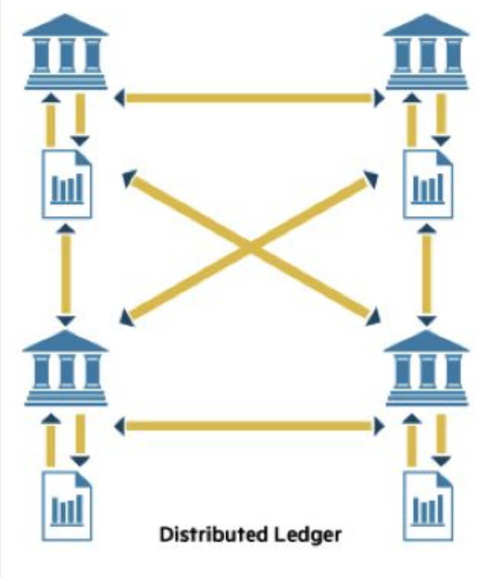
SO THEY INVENTED THE WORLD'S FIRST PUBLIC LEDGER

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

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)

BLOCKCHAINS

(underlying tech / shared public ledger)

VS

ETHEREUM

(open network for building anything)

PRIVATE NETWORKS

(very similar to traditional database)

VS

PUBLIC BLOCKCHAINS

(enables permissionless innovation)

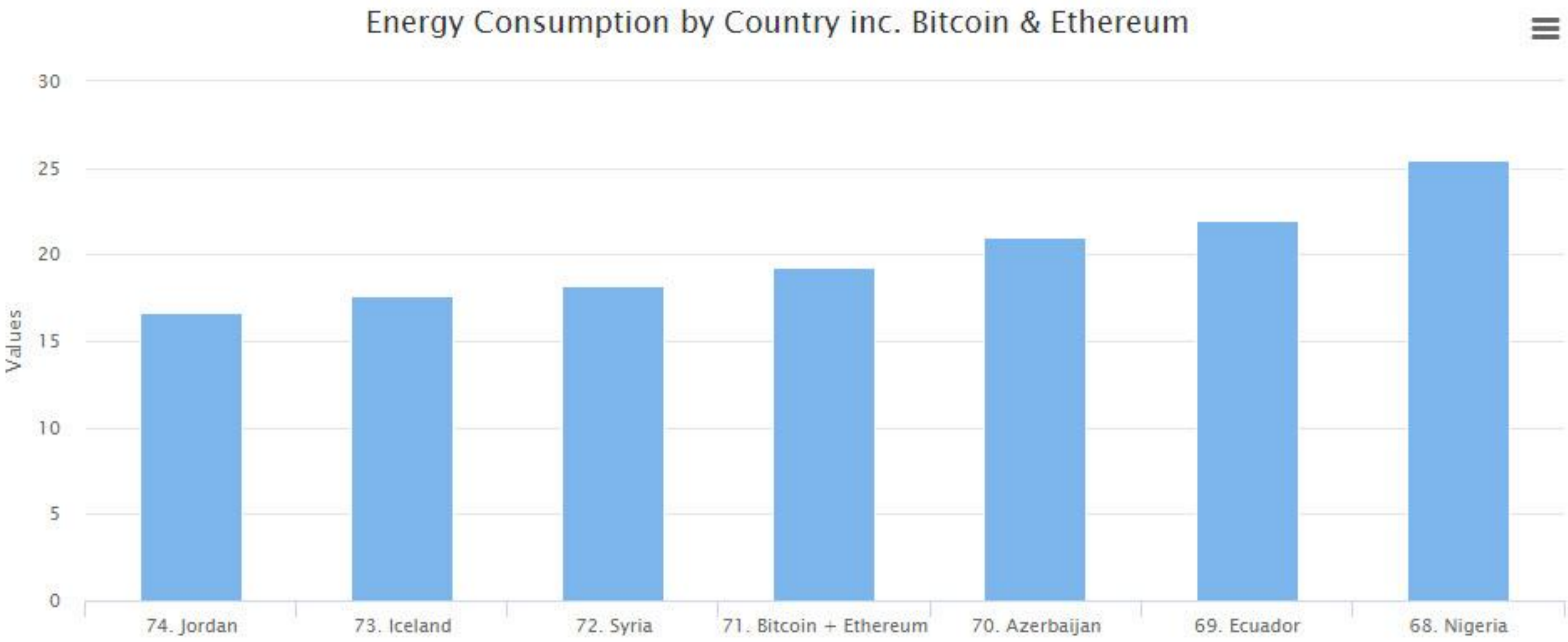
PERMISSIONED LEDGERS

(puts new central controllers into authority)

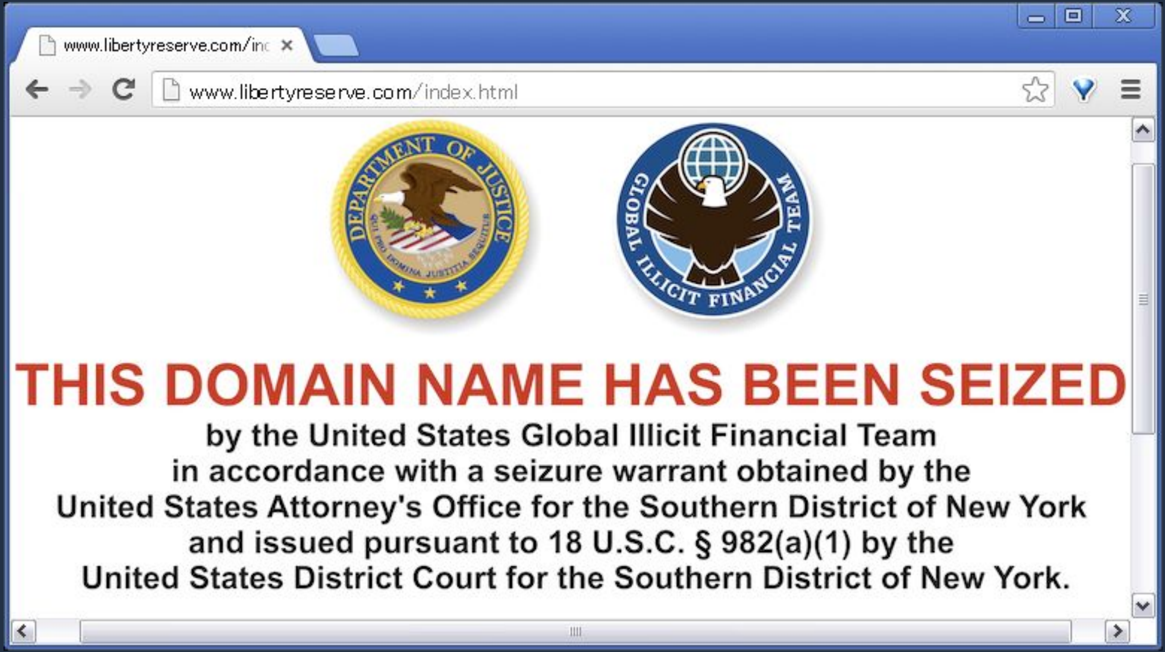
VS

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

MORE ENERGY THAN ICELAND, SYRIA, AND JORDAN



BUT WHY ...?



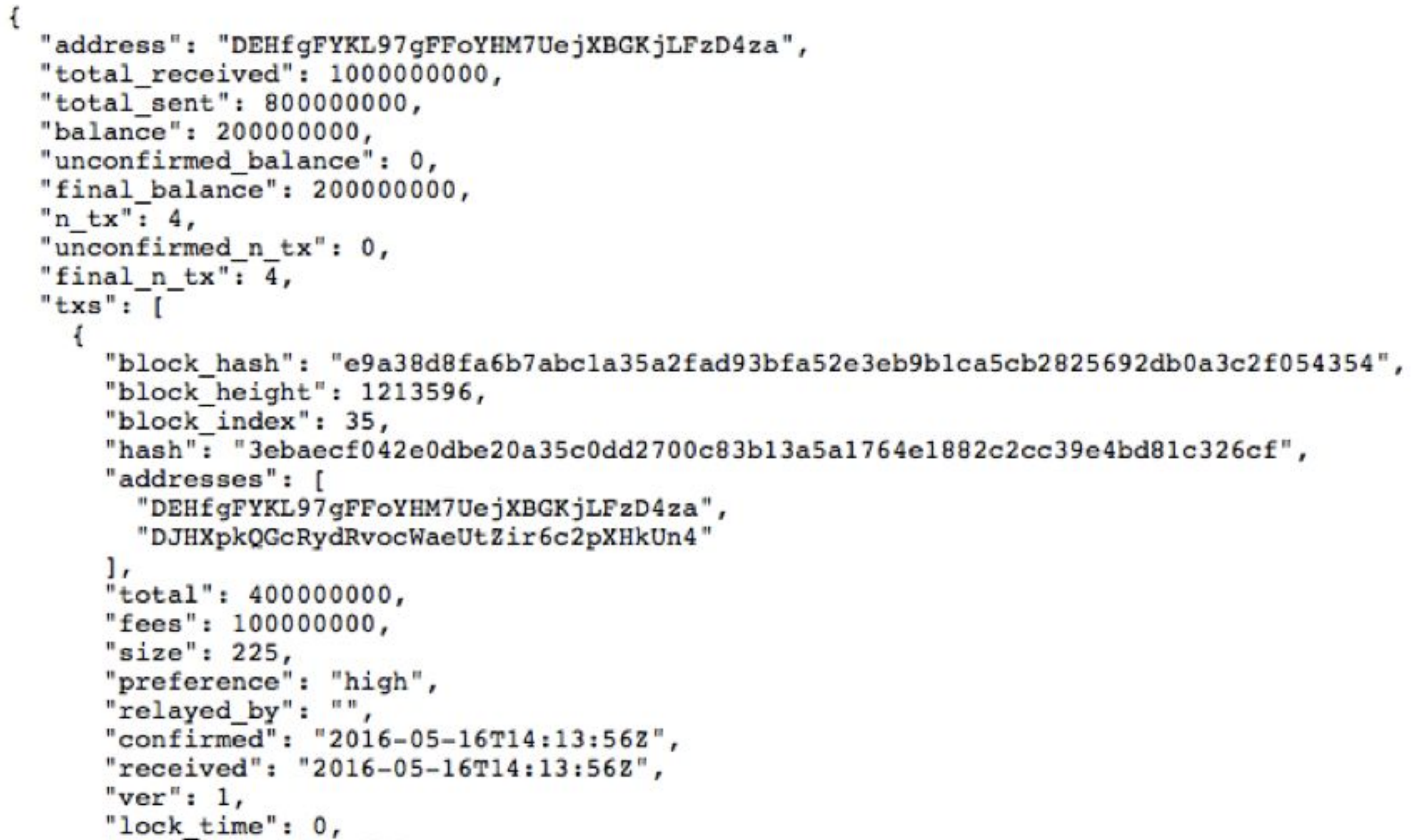
www.libertyreserve.com/inc
www.libertyreserve.com/index.html
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
GLOBAL ILLICIT FINANCIAL TEAM

THIS DOMAIN NAME HAS BEEN SEIZED

by the United States Global Illicit Financial Team
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 982(a)(1) by the
United States District Court for the Southern District of New York.

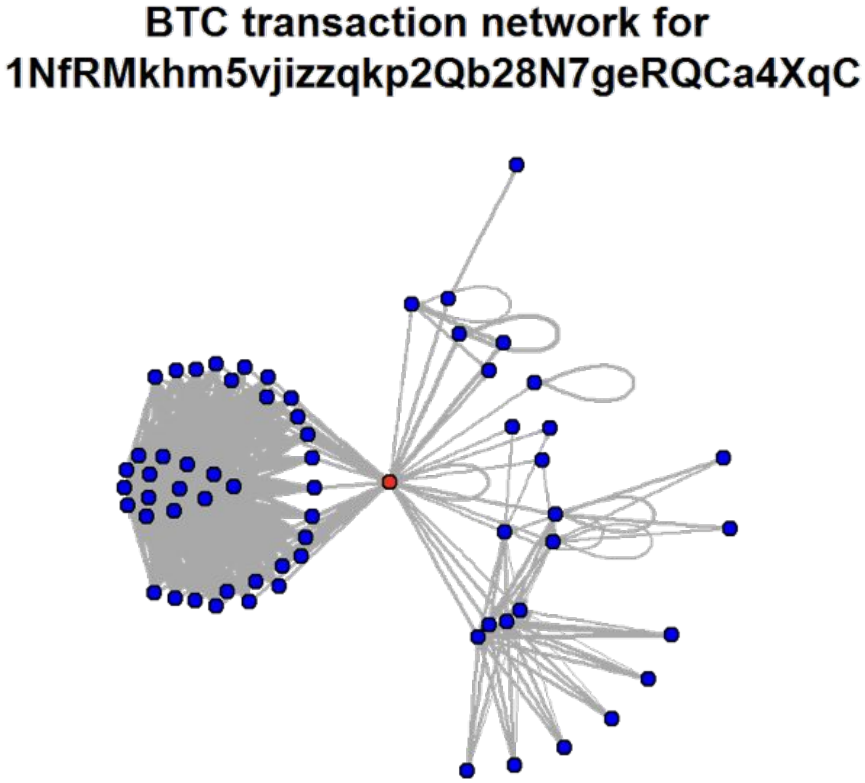
- FLOOZ - Shut down by FED in 2001
- LIBERTY RESERVE - Shut down by FED in 2013

TRUST IS SOLVED VIA TRANSPARENCY - LIKE ON YAP



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

EVERYONE HAS A COPY OF EVERYTHING - PSEUDO ANONYMOUS



BTC transaction network for
1NfRMkhm5vjizzqkp2Qb28N7geRQCa4XqC

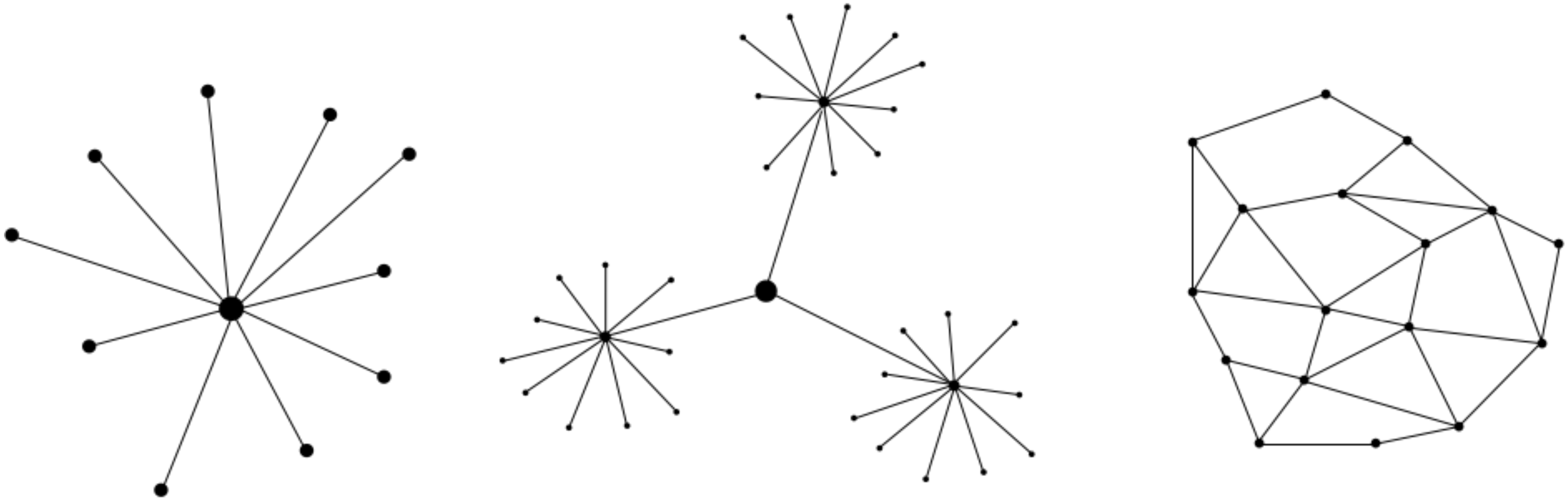
EXPLORING THE TECHNOLOGY

HOW AND WHY DO BLOCKCHAINS WORK …?

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 NETWORKS & BUSINESS MODELS



TECHNOLOGY TECHNOLOGY

1950 - - - - 2000 - - - - 2010 - - - - 2015 - - - - 2030

BUSINESS MODELS BUSINESS MODELS

HILTON / TAXIS

AIR B N B / UBER

LAZOOZ & OPEN BAZAAR

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

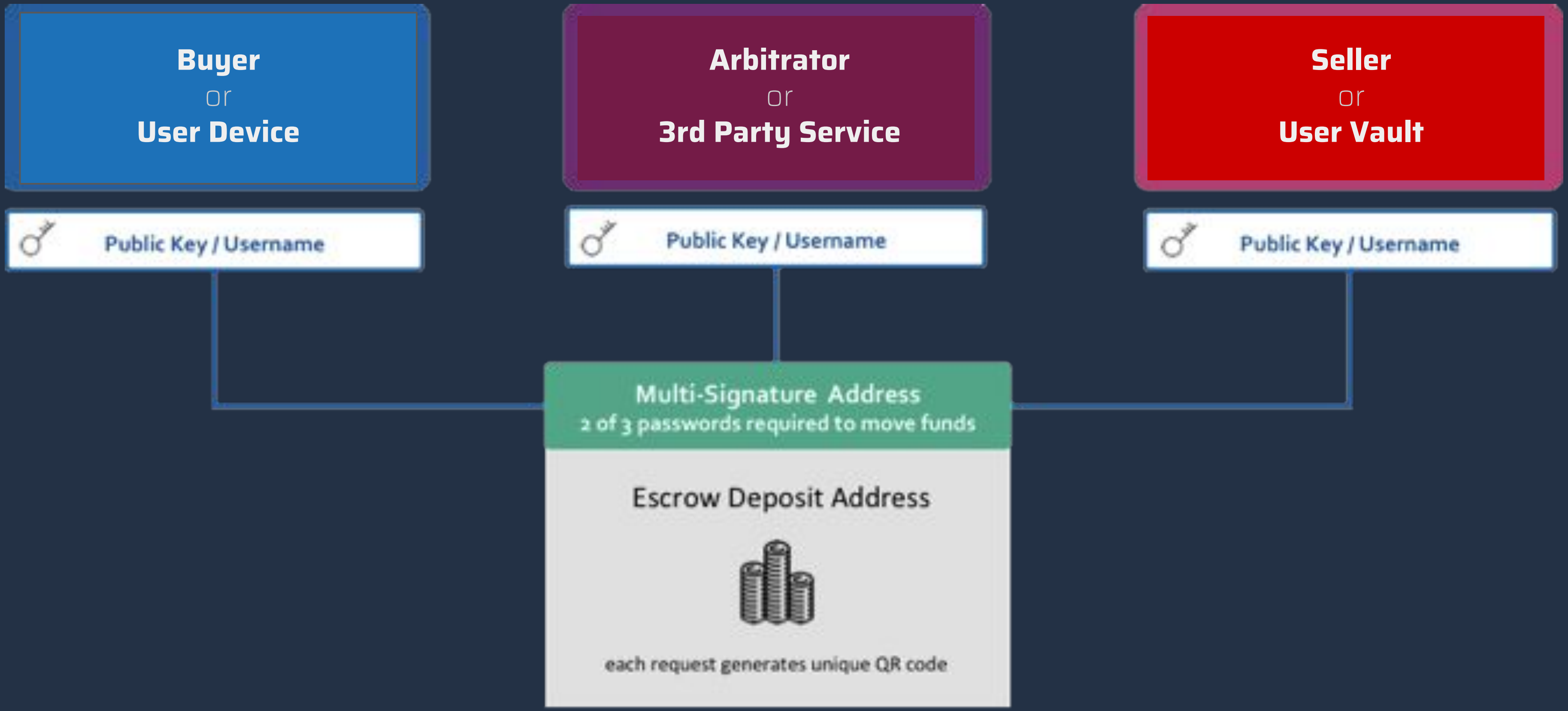
- Example of a Bitcoin public address (derived from the public key): 1GzBZ7eK6wzNjp1Wt6AxHo73kJL2tzoErq
- Example of a Bitcoin private key (used to transfer funds from address): L1winVkoRmxMdHKbwssx33Z9ZEuXeJ1eP9CVYvnNn4TdYA32GsWY
- Example of a Bitcoin extended private key (used by HD protocol): xprv9s21ZrQH143K2Ywhg9bhZ5nd31t3EbXsg8v28gkKjSm9PA3PiZ89dWW6YKxWZa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

EACH PUBLIC ADDRESS REQUIRES A PRIVATE KEY TO SPEND

ALLOWING US TO EMBED MONEY - 2018 DOGECOIN

SOME ADDRESSES REQUIRE MULTIPLE KEYS

USEFUL FOR RECOVERY AND ESCROW SERVICES



Buyer
or
User Device

Public Key / Username

Arbitrator
or
3rd Party Service

Public Key / Username

Seller
or
User Vault

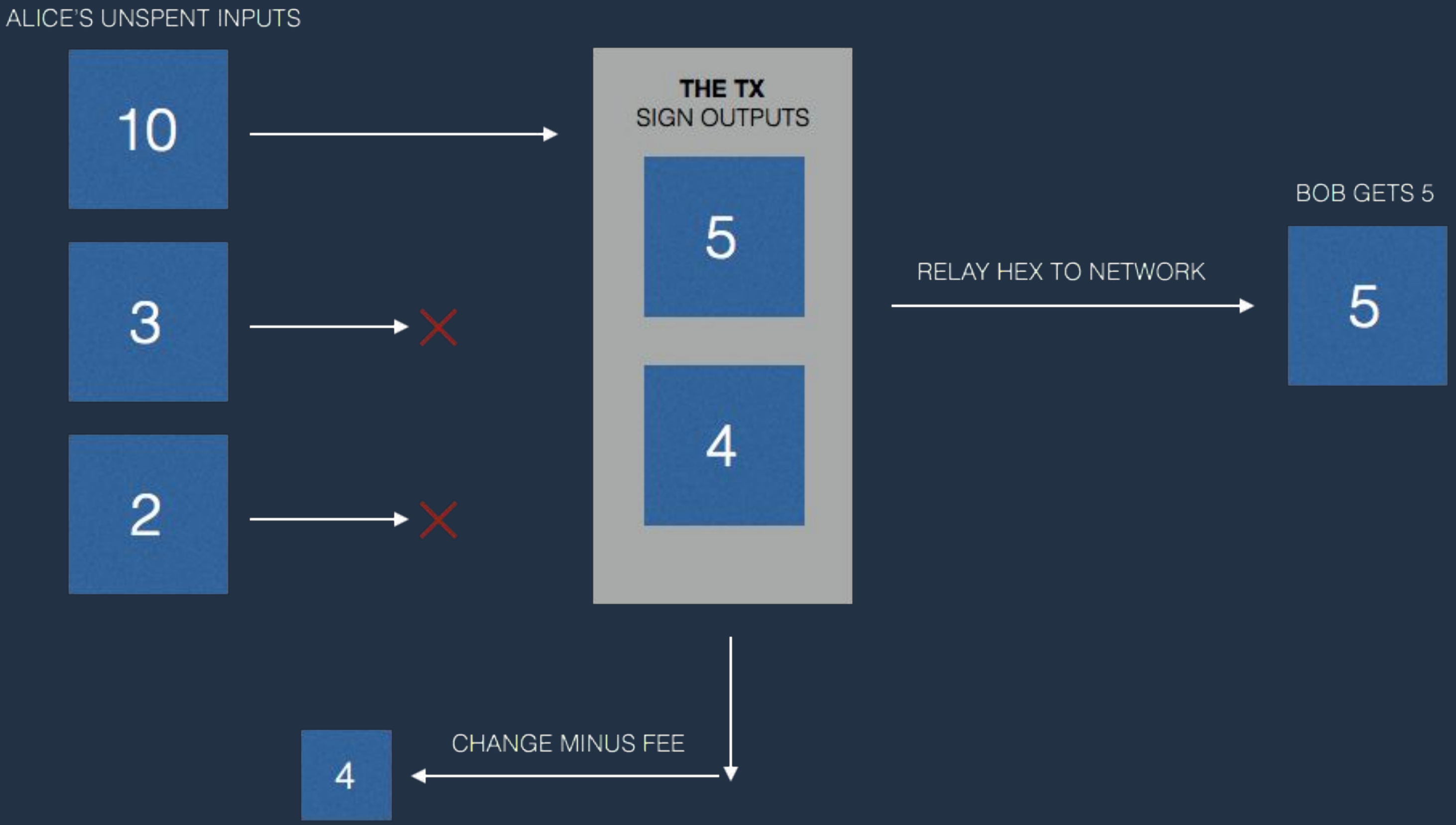
Public Key / Username

Multi-Signature Address
2 of 3 passwords required to move funds

Escrow Deposit Address

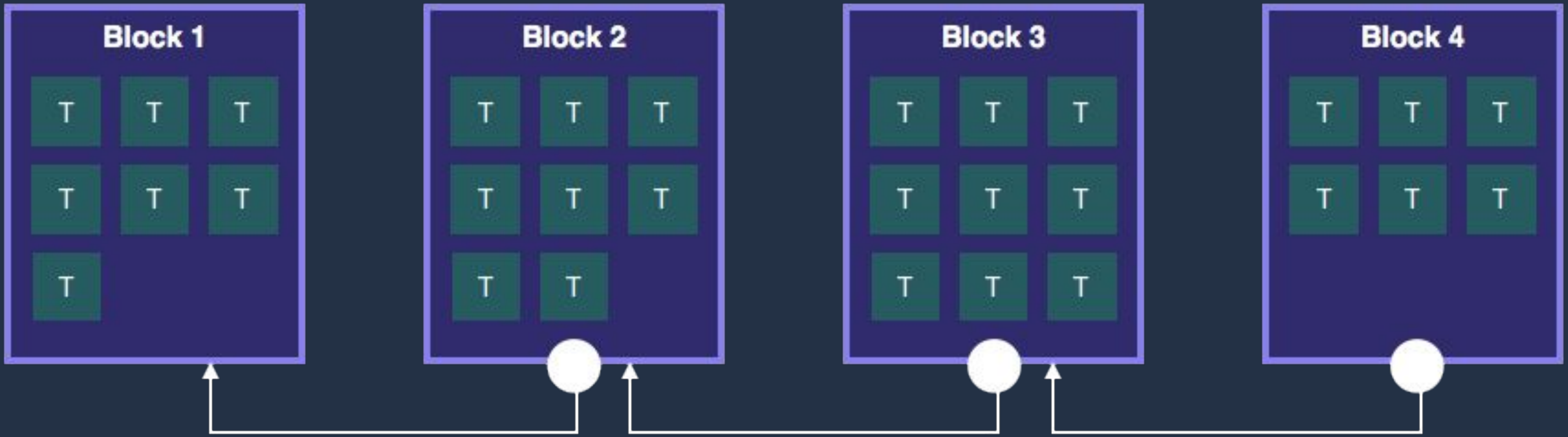
each request generates unique QR code

HOW DOES A BITCOIN TRANSACTION ACTUALLY WORK ...?



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**



WHY DO WE HAVE TO WAIT FOR BLOCKS …?

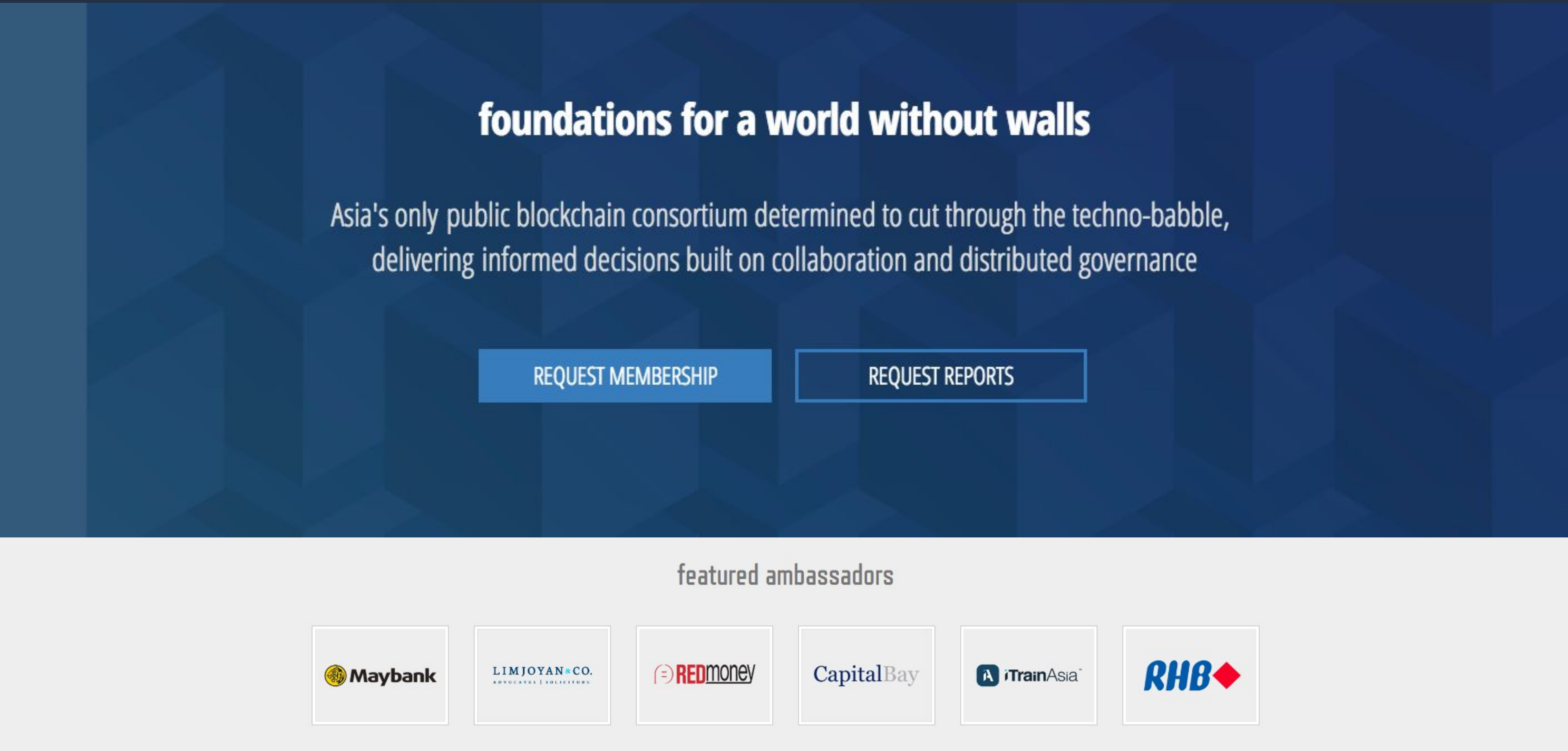
- To reach consensus as to which node has the right to add the next block to the chain, miners compete in a race to solve cryptographic equations
- Miners gather and in-turn verify unconfirmed transactions into blocks
- They then add a nonce (one use number) to the block and hash it
- If the hash has 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

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

CoinGecko Data - June 6th, 2017	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
Current Market Cap	**US$47+ B**	**US$1.5+ B**	**US$420+ M**	**US$1+ B**	**US$24+ B**	**US$1.6+ 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

LET’S NOT FORGET - THERE ARE NO COINS

BCE.ASIA - ASEAN'S FIRST PUBLIC BLOCKCHAIN CONSORTIUM



foundations for a world without walls

Asia's only public blockchain consortium determined to cut through the techno-babble, delivering informed decisions built on collaboration and distributed governance neuroware

email the team anytime - founders@neuroware.io