

Demystifying Blockchains

(understanding the technology behind the myths)

presented by



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



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

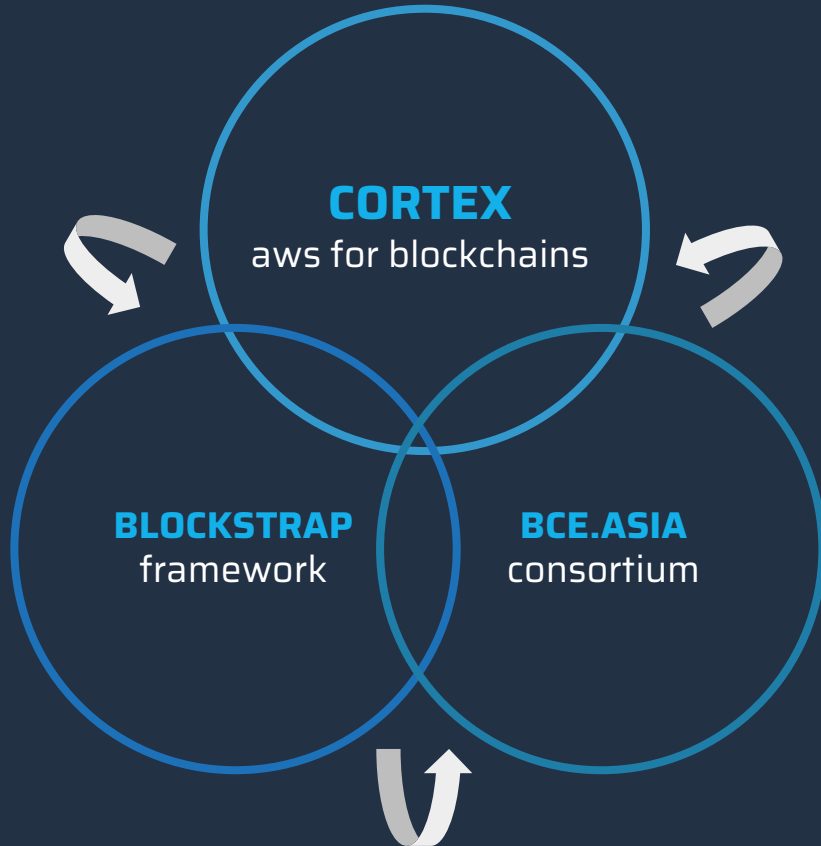
Living in Malaysia for the past 20 Years

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

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

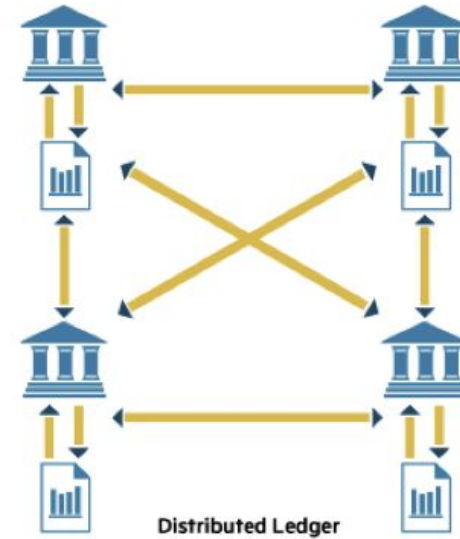
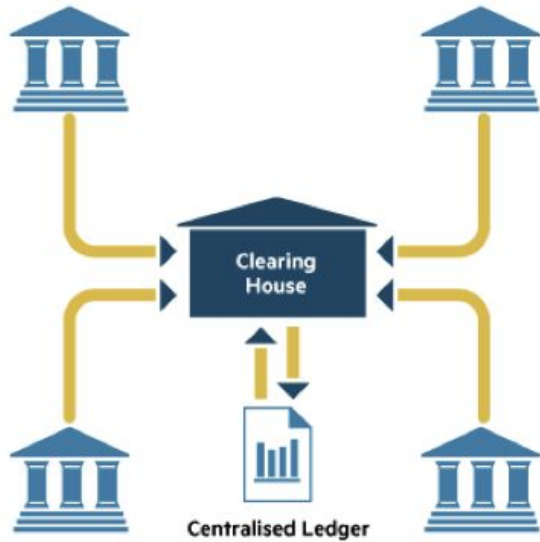


THEY USED GROUP CONSENSUS - SAME AS BITCOIN



- 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

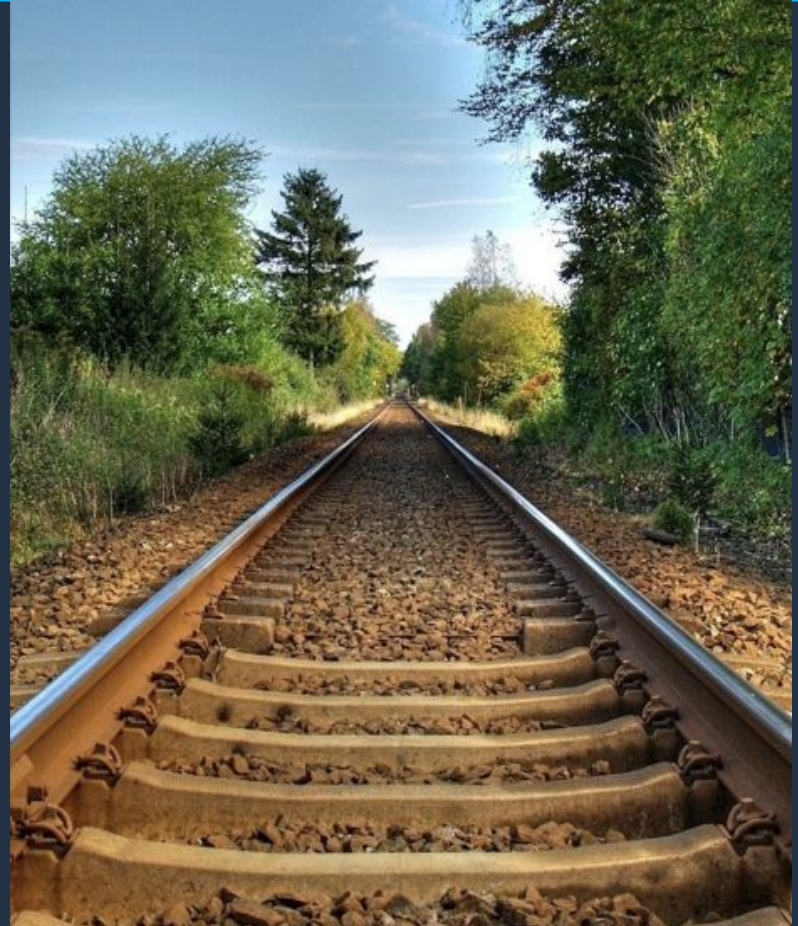
(the first application / popular digital asset)

BLOCKCHAINS

(underlying tech / shared public ledger)



VS



ETHEREUM

(open network for building anything)



VS

PRIVATE NETWORKS

(very similar to traditional database)



PUBLIC BLOCKCHAINS

(enables permissionless innovation)



VS

PERMISSIONED LEDGERS

(puts new central controllers into authority)



EXPLORING THE TECHNOLOGY

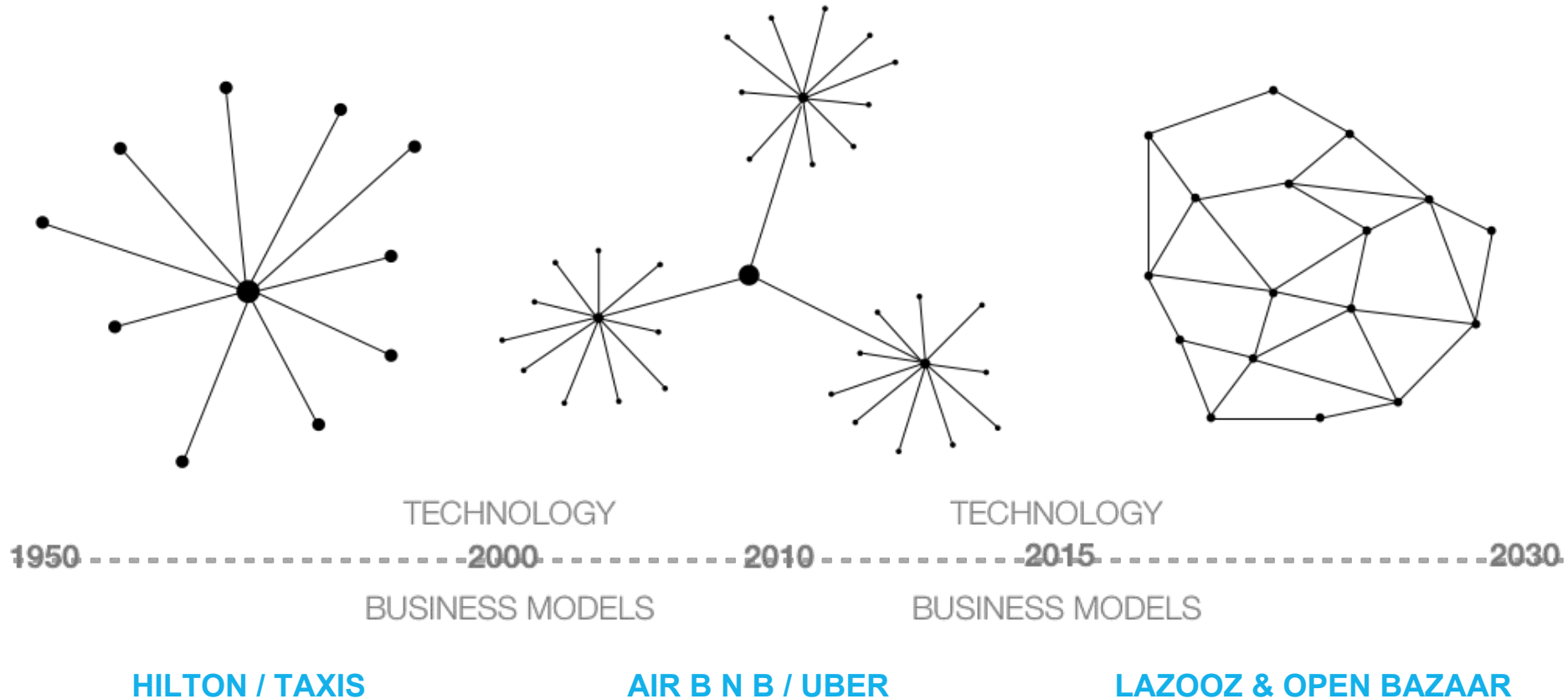
HOW AND WHY DO BLOCKCHAINS WORK ...?

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



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

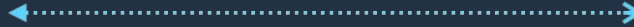
ON THE BLOCKCHAINS - ACCOUNTS ARE KEYS



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



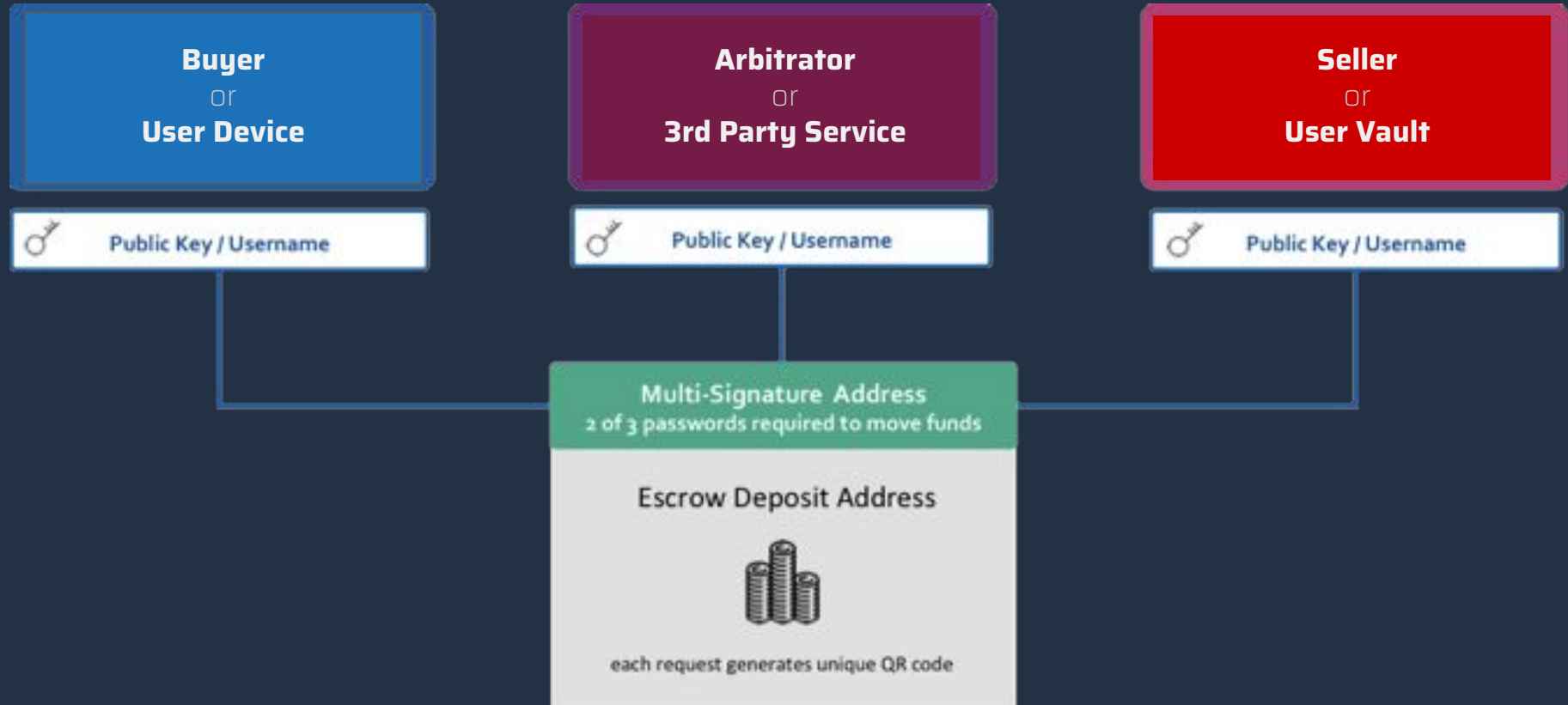
ALLOWING US TO EMBED MONEY - 2017 DOGECOIN



SOME ADDRESSES REQUIRE MULTIPLE KEYS



USEFUL FOR RECOVERY AND ESCROW SERVICES



HOW DOES A BITCOIN TRANSACTION ACTUALLY WORK ...?

ALICE'S UNSPENT INPUTS

10

3

2

THE TX
SIGN OUTPUTS

5

4

RELAY HEX TO NETWORK

BOB GETS 5

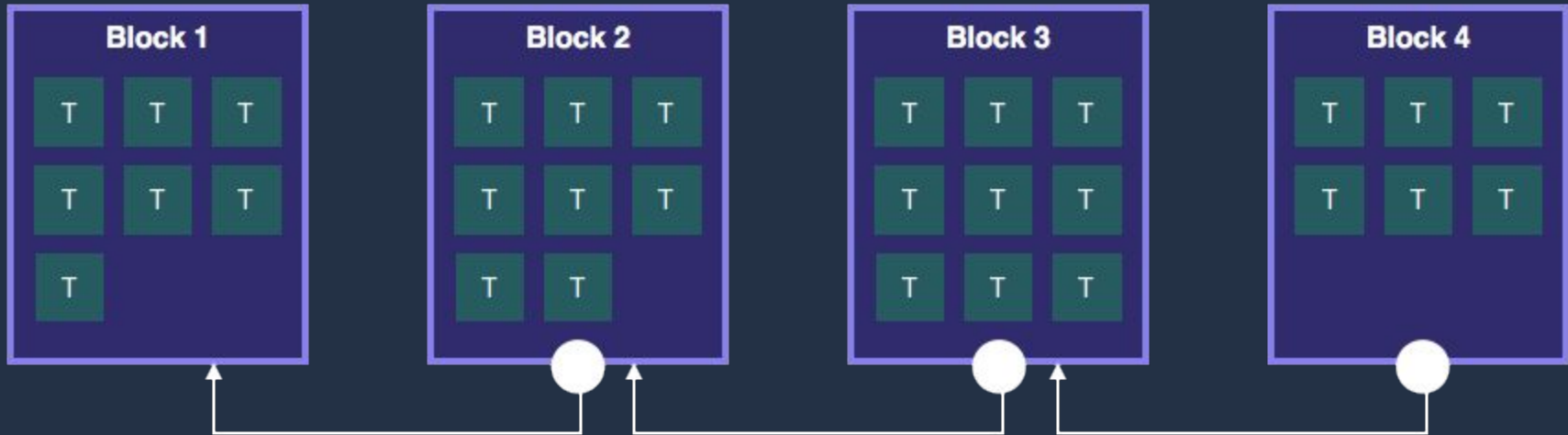
5

CHANGE MINUS FEE

4

SO WHERE DO THE BLOCKS COME FROM ...?

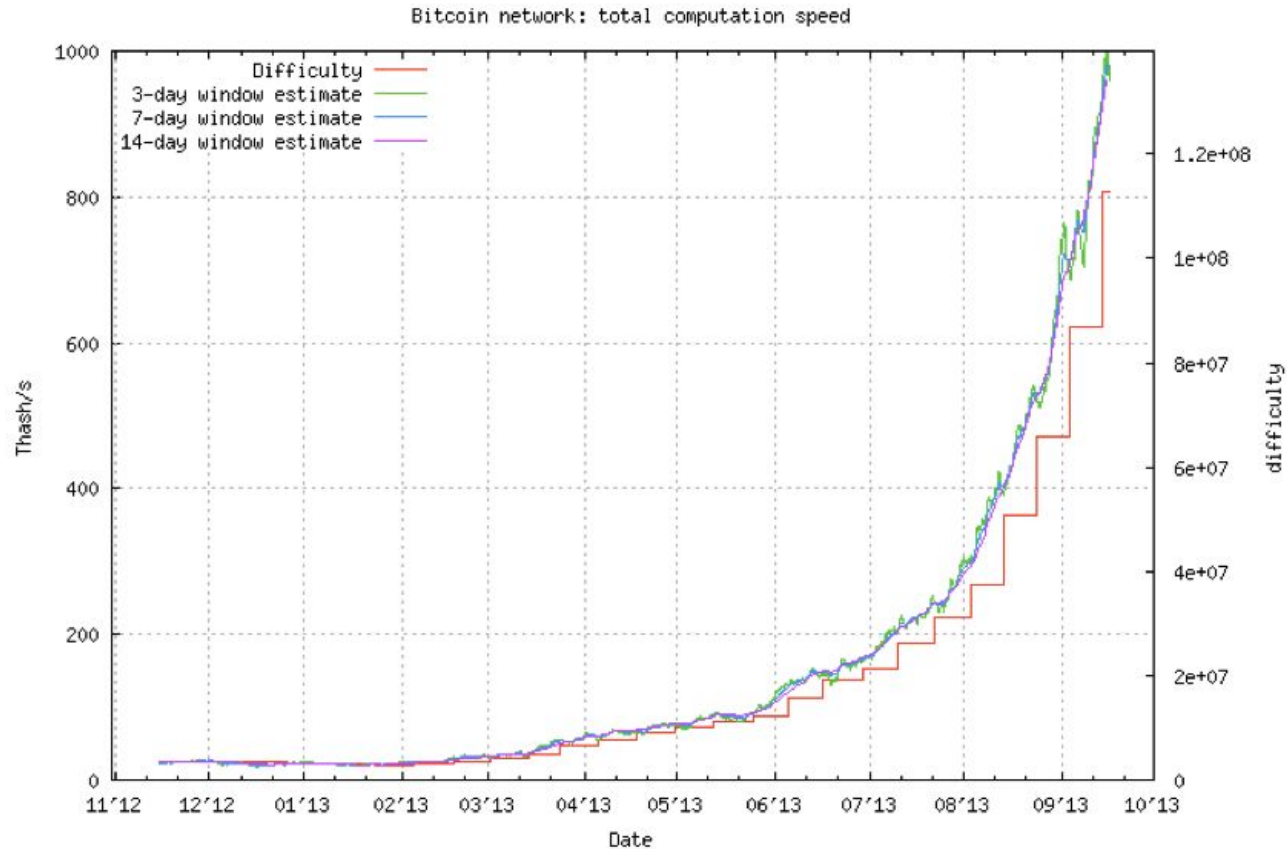
- Transactions are batched into blocks every ten minutes (with Bitcoin)
- The block is added to the chain with a link to the previous block
- With the block added to the chain, its transactions are then **confirmed**



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

A PERMISSIONLESS NETWORK NEEDS TO SELF REGULATE



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
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

ACTIVE USE-CASE 01

BLOCKCHAIN BASED ENERGY MARKETS

BENEFITS OF A BLOCKCHAIN BASED ENERGY NETWORK

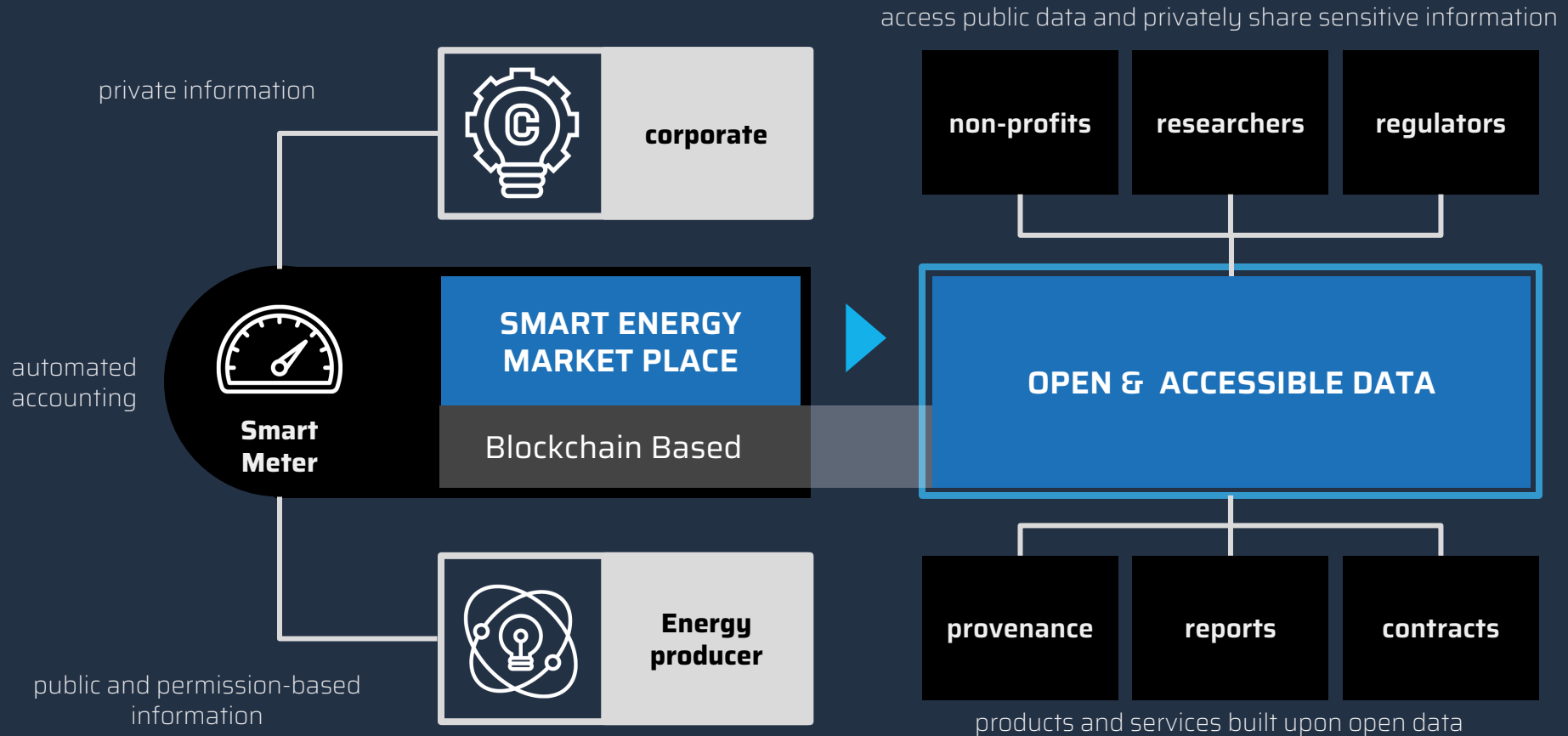
Improving the quality of life for everyone whilst saving costs:

- **SMART METERS** - moving beyond insecure connected cloud devices
- **SMART GRIDS** - store, trade and track energy distribution and transactions
- **SMART CITIES** - introduce new automated services and business models

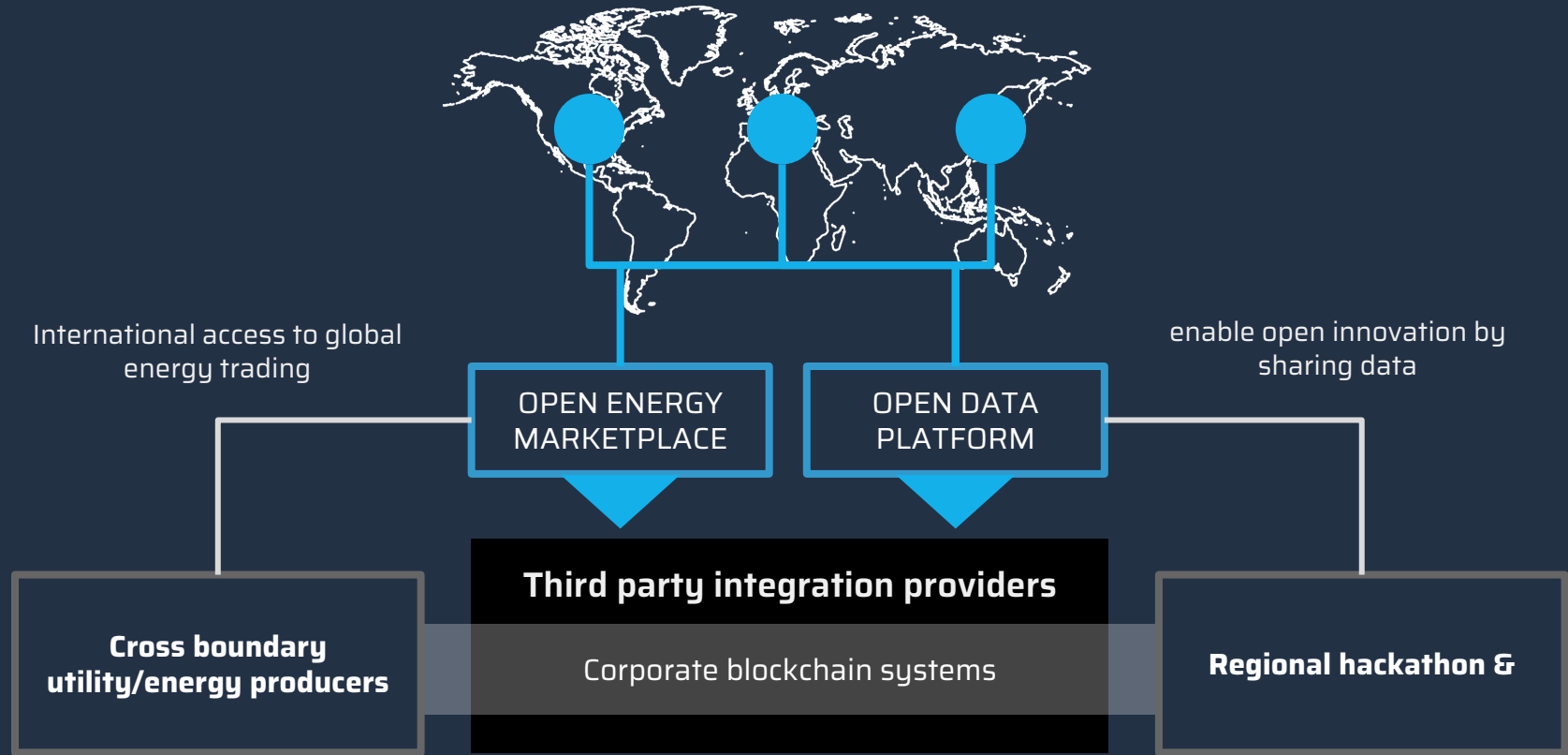
Improving businesses whilst introducing new revenue streams:

- **SMARTER RELATIONSHIPS** - securely share data between trusted parties
- **SMARTER COMPLIANCE** - automate regulation with coded contracts
- **SMARTER DECISIONS** - network analytics with tamper proof audit trails

SECURELY EMPOWERING OPEN INNOVATION



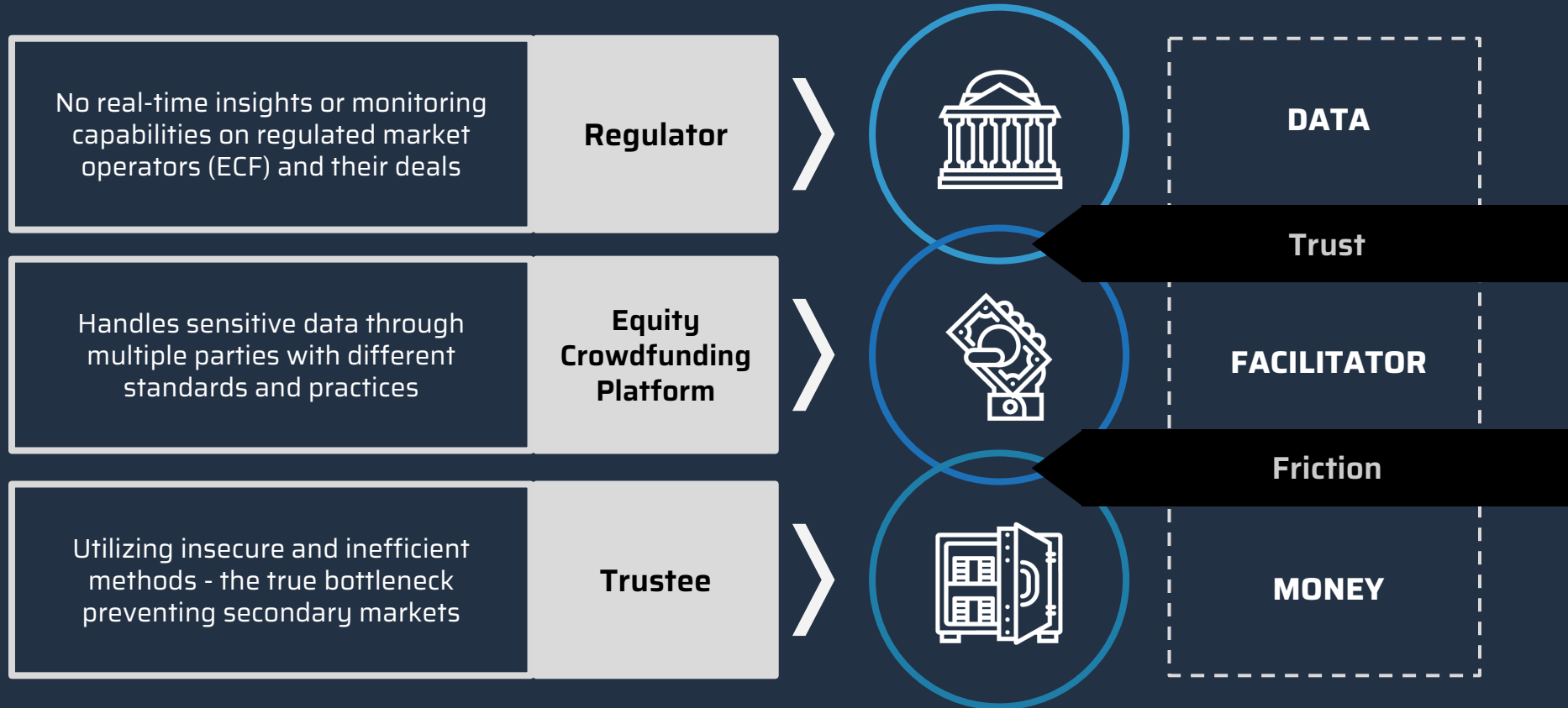
FOUNDATIONS FOR A GLOBAL ENERGY MARKETPLACE



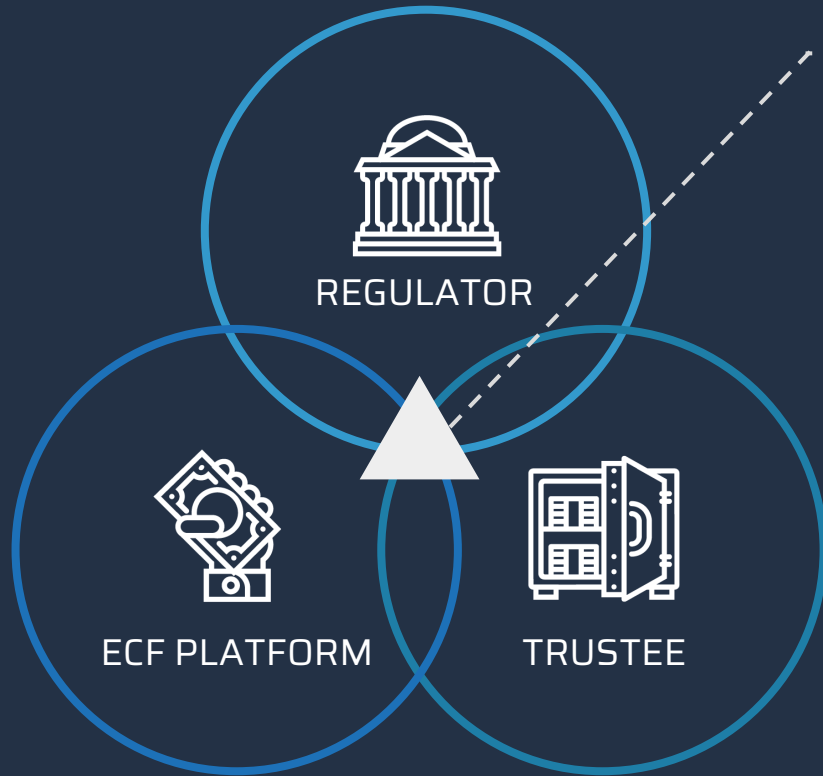
ACTIVE USE-CASE 02

BLOCKCHAIN BASED SECONDARY MARKETS

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

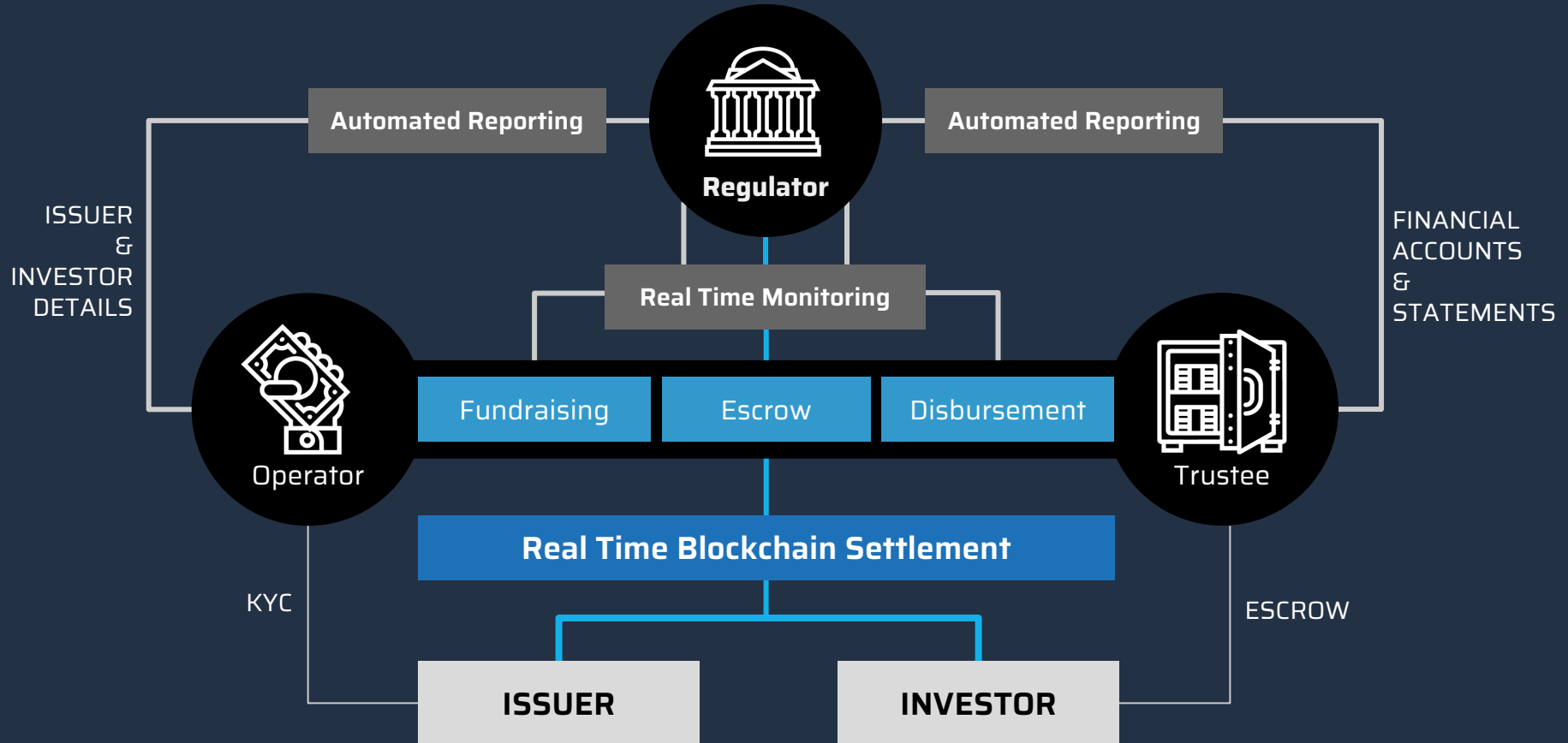
2

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



FINAL THOUGHTS

HOW DO BANKS FIT IN ...?

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)

BCE.ASIA - EDUCATING ORGANIZATIONS & REGULATORS

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





neuroware

email the team anytime - founders@neuroware.io