unlimited

unleash your own chain reaction | unchain your future

knowledgehut

Hotel Inn Bangkok Silom, 23 May 2018

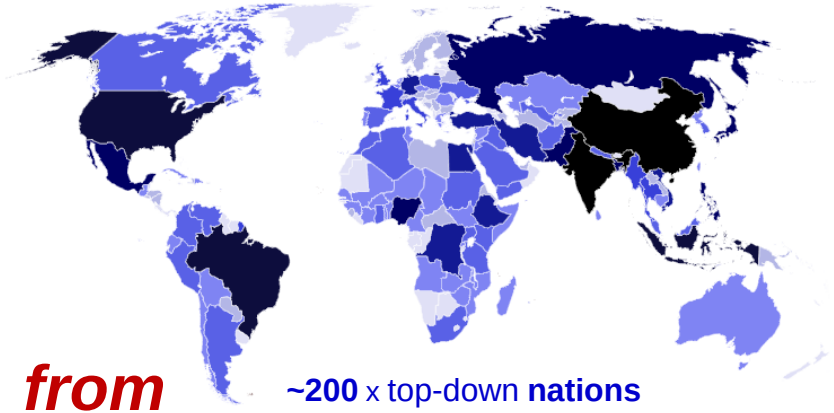
Giovanni Di Noto

our core motto

changing the way we work

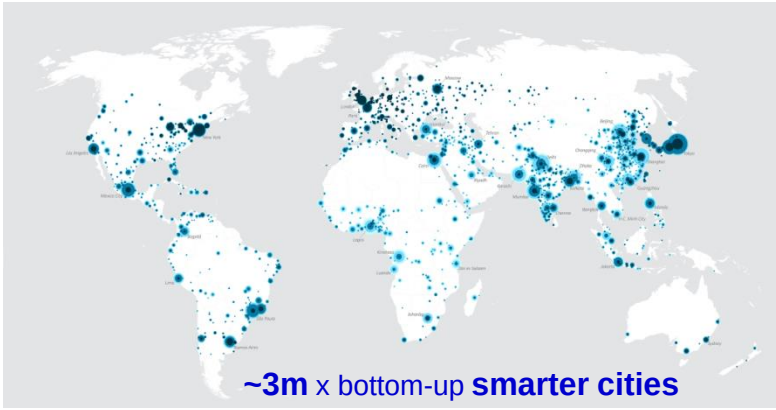
cloudyBoss believes in ***glocalisation*** and increasing market ***complexity*** *with world dynamics shifting*

from **few dominant *fiat* currencies**



from **~200** x top-down **nations**

to **distributed stable and sustainable value systems**



to **~3m** x bottom-up **smarter cities**

from **0.5b brands + 4.7b workers**

to 8b humans interacting via clusters/ecosystems with b's of smarter **glocal SME's**

SKYE technology in context

skye

Blockchain Clustering

Keystone

Unique Data Model

ANIMA

Artificial Intelligence with a Soul

COBRA

cloudyBoss Omni-currency Banking Rotation Account

- ***SKYE*** *enterprise blockchain cluster ecosystems*
- ***NEXT+*** *cloud enterprise management engine*
- ***OT*** *automation & dematerialization program*
- ***360*** *solutions for industries & smarter cities*
- ***startospheric*** *acceleration programs*

CLOUDY BOSS
Safer Smarter Enterprising

Skye
Blockchain Clusters

ANIMA
Artificial Intelligence with a Soul
Keystone
your enterprise DNA

background

SME's
governments
public institutions
start-ups and incubators
large and medium enterprises

backed by IBM

Agenda

1. the journey so far
2. core concepts & mechanics
3. SKYE live demonstrations
4. from use cases to case studies
5. a quantum leap into the future
6. wrap-up

BBC explains cryptocurrencies in 2 minutes

the mother of all bubble charts, or the mother chart of all bubbles

stock markets
~$70t

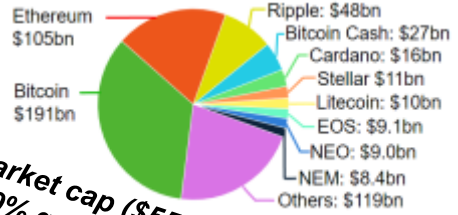
all money
~$90t

hard cash
(notes, coins)
~$35t

USD
$4t

$.5t

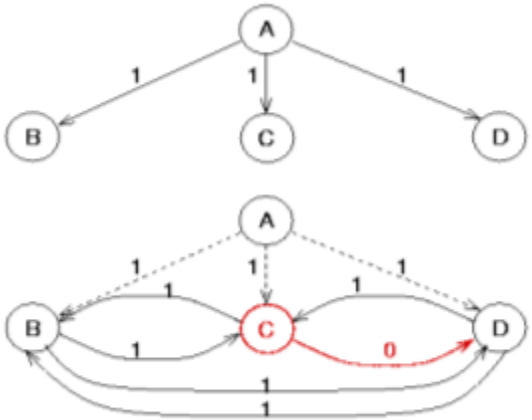
all-cryptos market cap ($555b) as of Feb 2018
3 folds (200% growth) PY value ($180b)

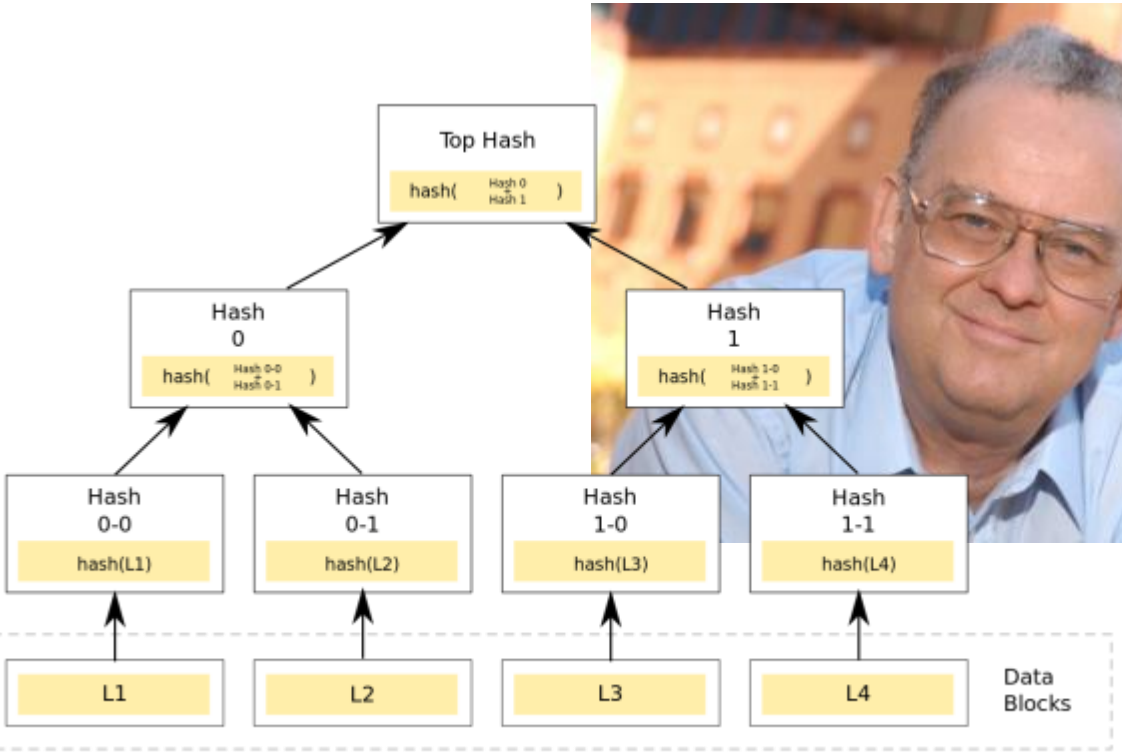


blockchain the journey so far

…origins

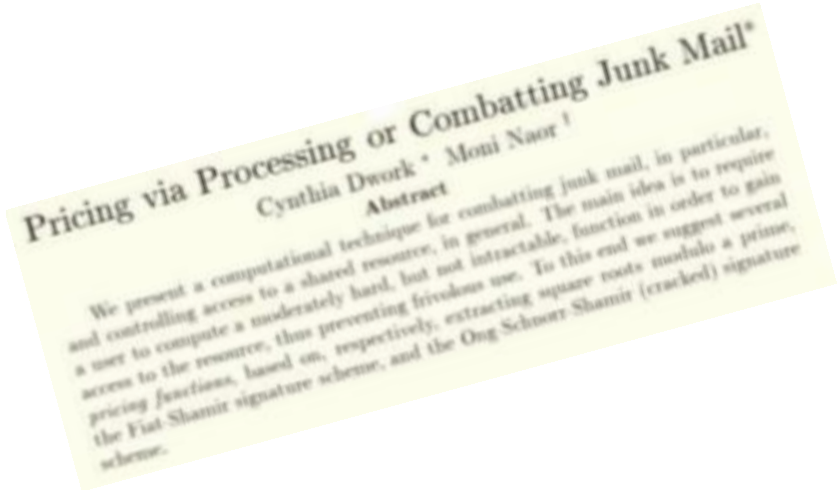
When	Who	What
1979	Ralph Merkle (below)	"***Hash trees***" US patent no 4309569
1982	Lamport, Shostak, Pease	"*The Byzantine Generals Problem*" paper, basis for **consensus** protocols





the 90's

when	who	what
1979	Ralph Merkle	"***Hash trees***" US patent no 4309569
1982	Lamport, Shostak, Pease	"The Byzantine Generals Problem" paper, basis for consensus protocols
1991/92	Stornetta, Haber, Bayer	"Chain of blocks" then "Merkle trees" paper applying hash trees to data validation
1993	Cynthia Dwork, Moni Naor	"***computing cost*** *as a solution to spam*", basis for "***Proof of Work***" concept in mining
1999	Jakobsson, Juels	Further formalisation of the PoW concept
	Castro, Liskov	PBFT (Practical Byzantine Fault Tolerance) algorithm



Pricing via Processing or Combatting Junk Mail*

Cynthia Dwork † Moni Naor ‡

Abstract

We present a computational technique for combatting junk mail, in particular, and controlling access to a shared resource, in general. The main idea is to require a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use. To this end we suggest several pricing functions, based on, respectively, extracting square roots modulo a prime, the Fiat-Shamir signature scheme, and the Ong-Schnorr-Shamir (cracked) signature scheme.

the 00's

when	who	what
1979	Ralph Merkle	"***Hash trees***" US patent no 4309569
1982	Lamport, Shostak, Pease	"The Byzantine Generals Problem" paper, basis for consensus protocols
1991/92	Stornetta, Haber, Bayer	"Chain of blocks" then "Merkle trees" paper applying hash trees to data validation
1993	Cynthia Dwork, Moni Naor	"***computing cost*** *as a solution to spam*", basis for "***Proof of Work***" concept in mining
1999	Jakobsson, Juels	Further formalisation of the PoW concept
	Castro, Liskov	PBFT (Practical Byzantine Fault Tolerance) algorithm
Jul 2008	Giovanni Di Noto	"*the money-poly conundrum: basis for a* ***decentralised digital currency framework***" Griffiths University (Brisbane Australia) | ENV100 paper submission
Sep 2008	Lehman Brothers	Investment bank Lehman Brothers collapse (**GFC** starts)
Oct 2008	Satoshi Nakamoto	*"Bitcoin"* white paper solving the ***double-spending*** conundrum. metzdowd.com
Jan 2009		bitcoin.org, version 0.1 of the bitcoin software and mining of **1st bitcoin block**

the 10's

when	who	what
Jul 2015	Vitalik Buterin and team	ethereum **world computer** and **scripted** (solidity language) **smart contracts**
Dec 2015	Linux Foundation team	Open source Hyperledger project for **enterprise blockchain** starts
Jul 2017	Linux Foundation team	**Hyperledger Fabric** SDK 1.0 announced
	cloudyBoss team	**SKYE** (enterprise **blockchain clusters** + unscripted **skye-contracts**) released

	bitcoin	ethereum
concept	cryptocurrency	world computer
coin release method	early mining	through ICO
block time	~10 minutes	~12/15 seconds
protocol	SHA-256	ETHASH
hardware property	ASIC	ASIC-resistant

HYPERLEDGER
FABRIC SDK Go

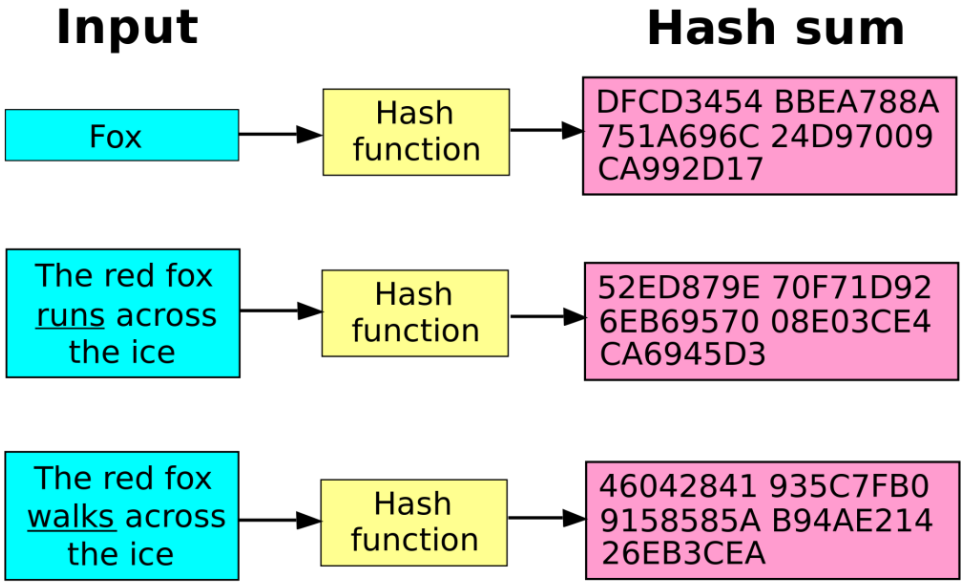
CLOUDY BOSS
Safer Smarter Enterprising

skye
Enterprise Block Chain Clusters in minutes

blockchain core concepts & mechanics

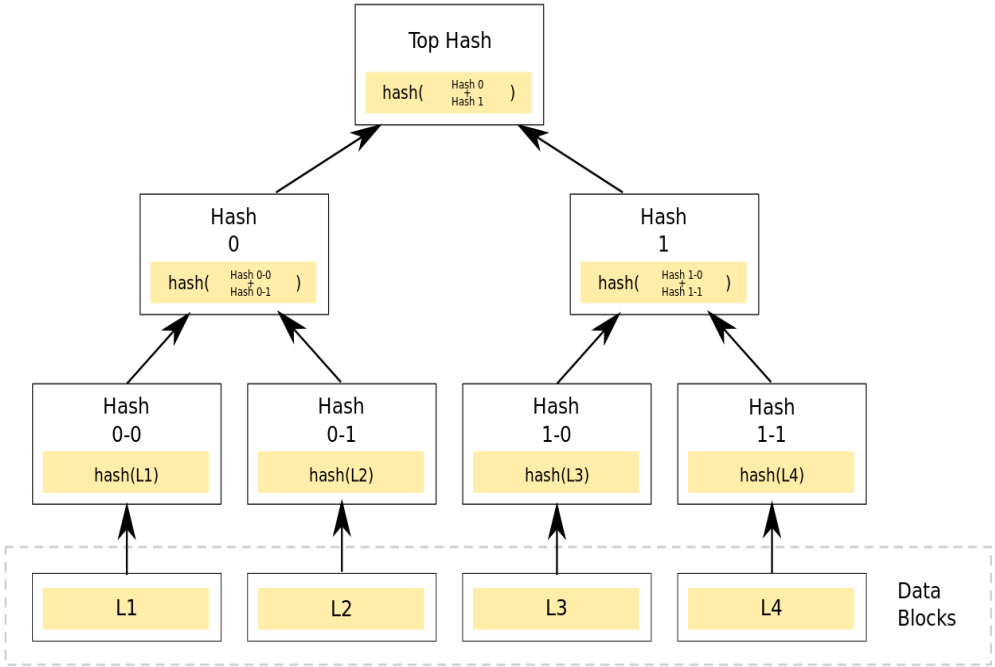
hashing

- **non-trivially translates a value to another**
- **uniquely translates (~nil collisions)**
- **irreversible 1-way function**



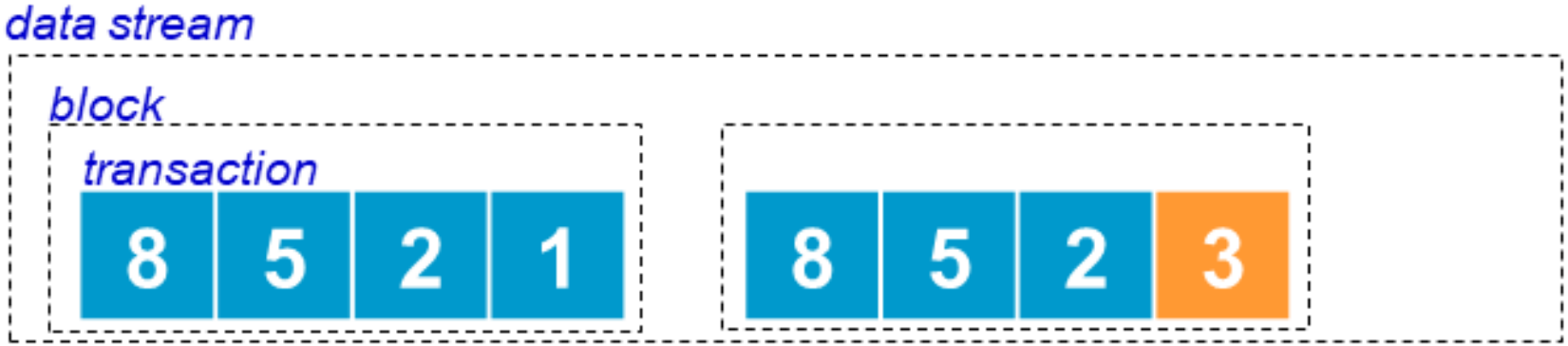
hash tree

Keyword	Description
Merkle Tree	a binary tree where the parent root hash is a function of child hashes derived from data leaves
Transaction	a value, balance, change of state or other data, corresponding to a leaf in a hash tree
Block	a group of transactions (leaves) ultimately pointing to the same top (or root) hash



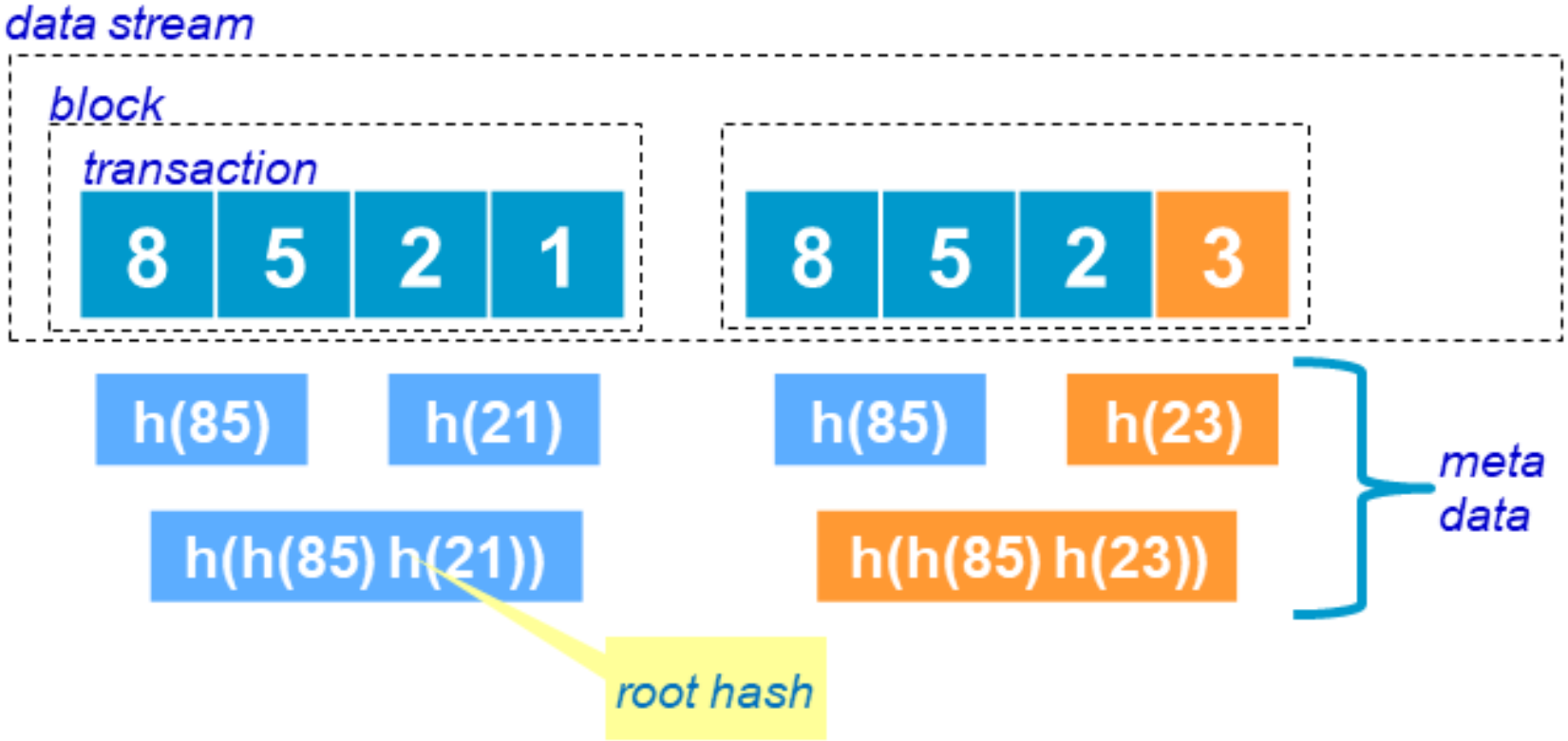
hash tree arithmetic 1/3

comparing data (without any Merkle tree arithmetic)



hash tree arithmetic 2/3

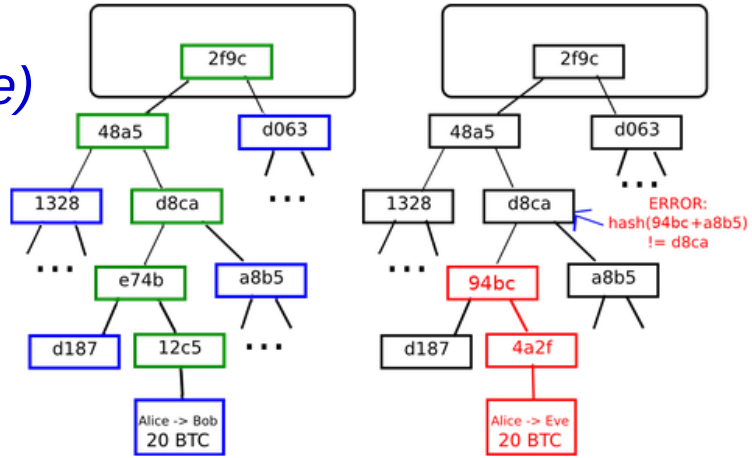
efficiently verifies the integrity of leaves (data) with hashes

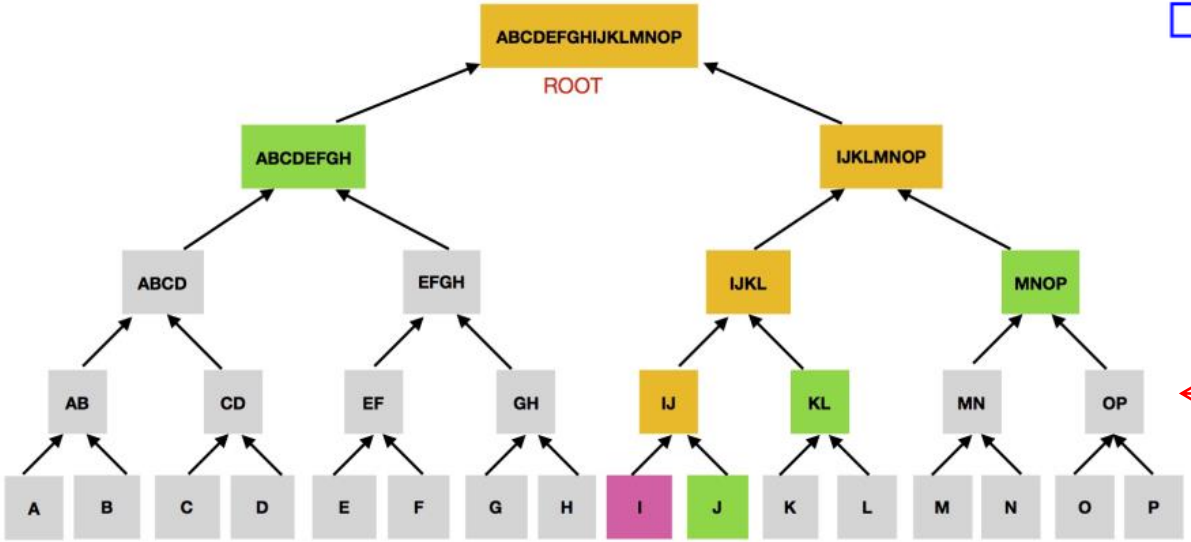


hash tree arithmetic 3/3

identifying validation errors more quickly via hashes

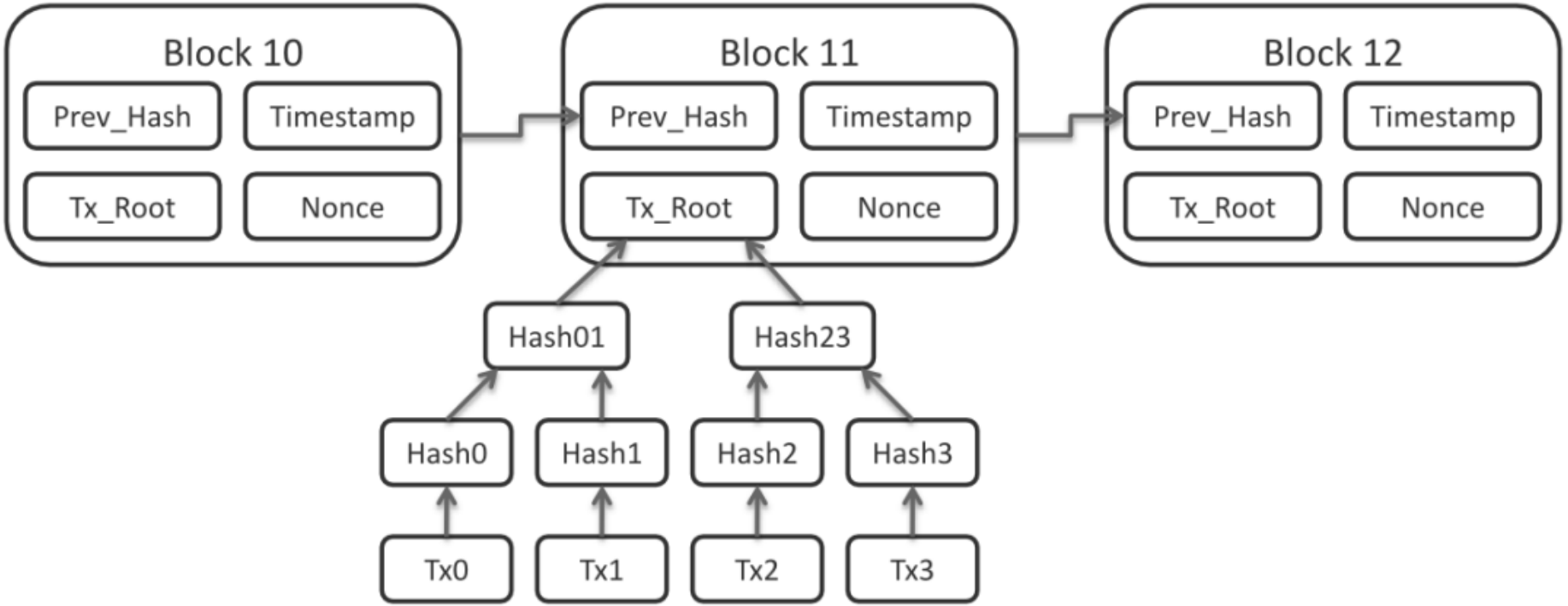
- *Transactions are **interdependent** (unalterable)*
- *They are validated via their **Merkle paths***
- *A Merkle path requires **$\log_2(N)$** hashes*





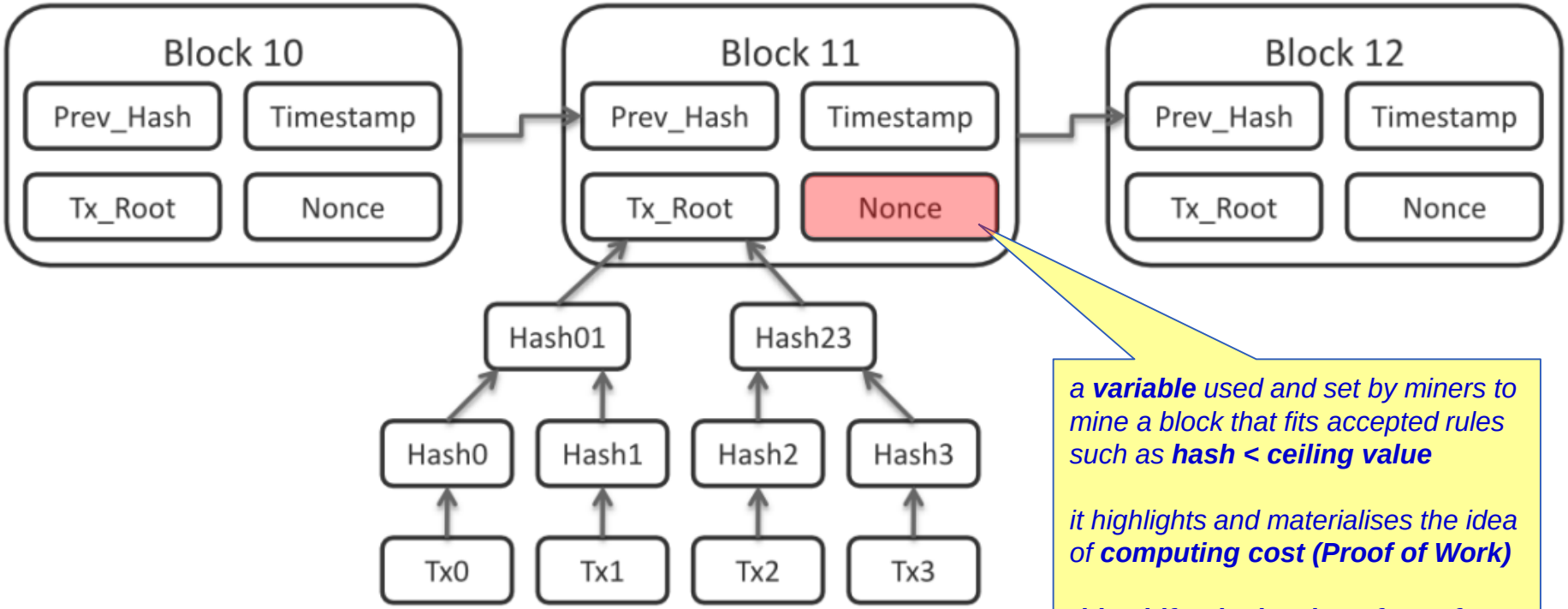
N (number of transactions)	$\log_2(N)$
4	2
16	4
1500	11

block-chain = ever-growing Merkle tree



$$B_{n+1} = f(B_n)$$

what's the nonce for?



*a **variable** used and set by miners to mine a block that fits accepted rules such as **hash < ceiling value***

*it highlights and materialises the idea of **computing cost (Proof of Work)***

this shifts the burden of proof on one side of the ecosystem (miner)

why bitcoin is ASIC* centric?

GPU

Graphics Processing Unit

FPGA

Field-Programmable Gate Array

ASIC

App Specific Integrated Circuit

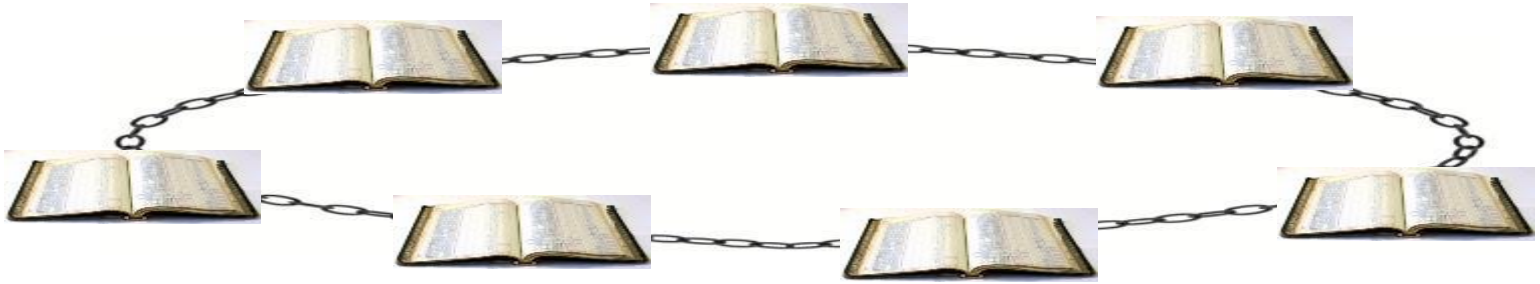
Alternative ASIC-resistant Proofs

- **PoS** | Proof of Stake
  example: ethereum ecosystem uses PoS
  how much cryptos do you hold?
  for how long?

- **PoI** | Proof of Importance
  example: NEM ecosystem uses PoI
  how much cryptos do you hold?
  how many transactions?

nem

ecosystems



Keyword	Description
Immutability	The property of an auditable transaction which irrefutable details (similarly to a **posted** transaction in a conventional accounting ledger) are no longer altered
Distributed ledger DLT, hyper ledger	shared immutable ledger kept up-to-date over discrete nodes (organisations and/or computers) which are all part of a same cluster, ring or ecosystem of nodes
Node	A single instance of a distributed ledger such as a server in a multi-node ecosystem
Ecosystem, cluster, ring	A group of at least 3 nodes each carrying an instance of a same distributed ledger
Byzantine fault tolerance	a consensus protocol for ecosystems to run when nodes crash or act maliciously
Consensus	an agreement on the state of the ledger reached via PBFT, PoW, PoS, PoI…
Propagation	The act of propagating a transaction across all nodes of an ecosystem
Genesis transaction	The first transaction in a distributed ledger

multi-chain ecosystems

Keyword	*Description*
Mining	process by which bitcoin rewards nodes for solving math puzzles to create new coins
Trust-less	a decentralised modus operandi devoted of censorship typical of ***open blockchains***
Cryptocurrency	digital currency relying on mining and open blockchains to avoid double-spending
Bitcoin, Ether, Litecoin	cryptocurrencies, each with their own blockchain protocol and other rules
Multichain	meta-system of various ecosystems with distinct blockchain protocols

open *vs* private blockchain ecosystems

Keyword	*Description*
Enterprise blockchain SKYE, hyper-ledger, ebc, private blockchain	a set of blockchain DLT use cases <u>other than</u> cryptocurrencies. Mining, ICO, PoW or trustlessness are generally alien to private blockchains. Vice-versa, permissions (to control participating nodes), speed and consensus are required for data integrity.
MSP	Member Service Provider. An admin node in a private blockchain
Permission	Control mechanism to allow node participation into a private ecosystem and/or grant access to data

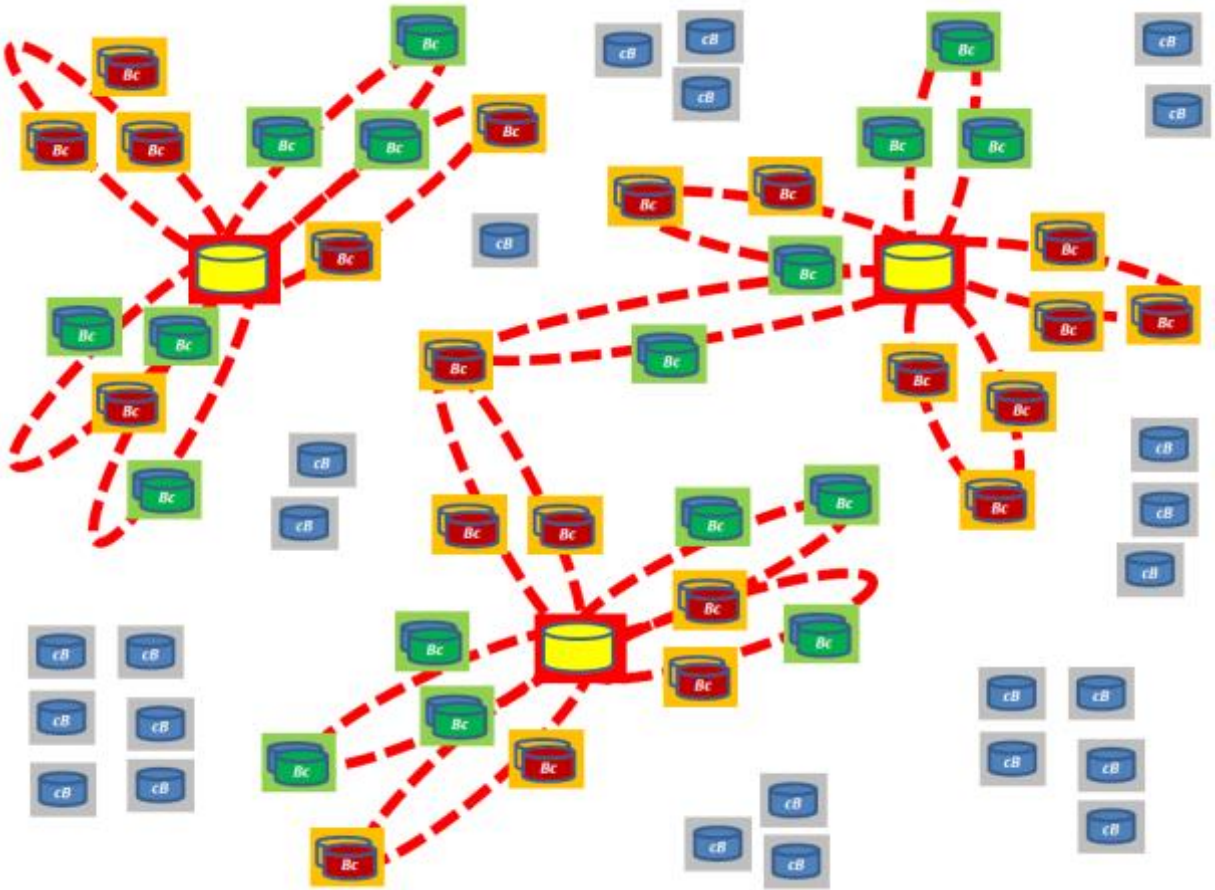
Enterprise DLT
SKYE live demo

some context

legend

- genesis node (ring MSP)
- ring of nodes (cluster)
- baseline ring node
- permitted ring node
- independent node

cloudyBoss environment



SKYE rings

- *1 node belongs to 0 or more rings*
- *1 ring has min 3 or more nodes*
- *1 ring has 1 or more modules*

node data

- *Any node (ring or not) data can be encrypted*
- *Authorised users see encrypted data*
- *Ring data is immutable (chained)*
- *Permitted ring data is encrypted*
- *Permitted nodes see ring data*

creating a SKYE blockchain cluster takes seconds

SKYE ring

RGA

DEMO 1

nd1

1. *organisations **nd1** and **nd2** agree to form **RGA***
2. ***nd1** initialises **RGA***
3. ***nd1** refers **nd2** and asks **nd2** for a reference*
4. ***nd2** refers **nd1***
5. ***aut** confirms/activates once (genesis, BFT) **RGA***

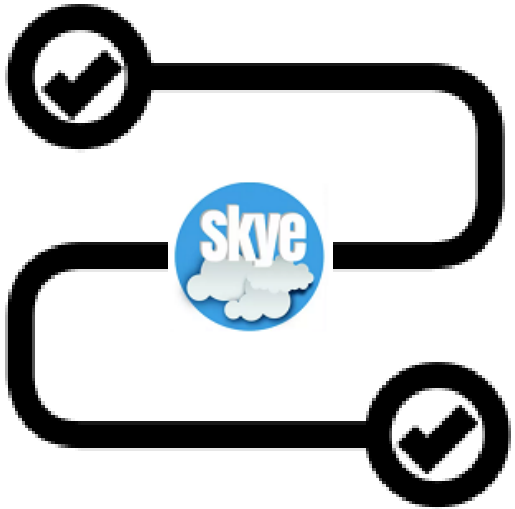
nd2

aut

some context

SKYE minimum workflow levels

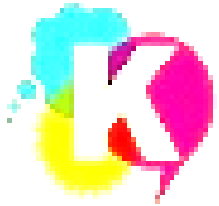
- all cB transactions are subject to workflow
- SKYE workflow floor level triggers propagation
- SKYE workflow floor level depends on each module



posting data to a SKYE blockchain cluster

SKYE ring

RGA



DEMO 2

nd1

1. ***nd1*** *creates a record with a low workflow*
2. *the record exists only in* ***nd1***
3. *the record workflow is set to a cluster floor level*
4. *the record now propagates across all nodes*
5. ***nd2*** *and all other nodes see the new record*

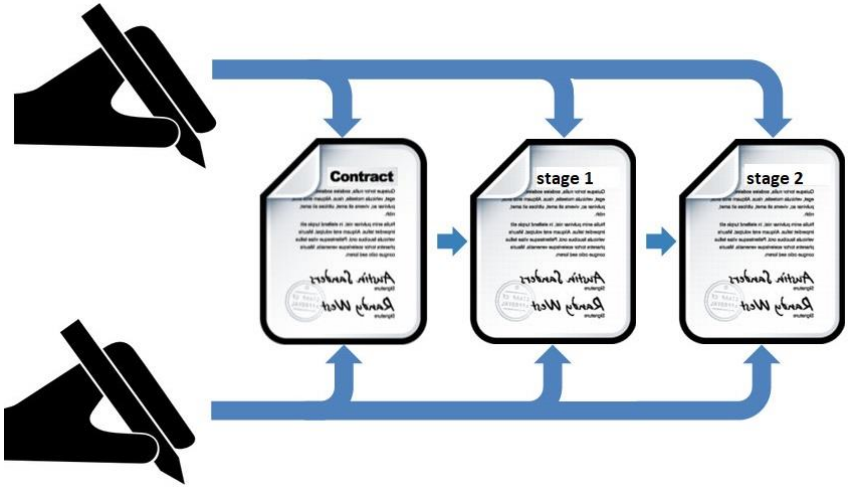
nd2

nd*x…*

some context

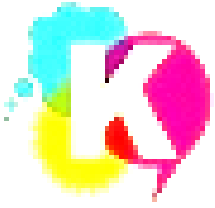
SKYE multi-stage e-contract options

- actions achieved via ***delayed*** document:
  - content published, invoice issued, payment triggered, stock released, etc.



- *floor level* workflows activate action/s on a:
  - "**unanimity**" basis | (100%) all stakeholders, or
  - "**quorum**" basis | *n*% (a few) stakeholder/s, or
  - "**first**" basis | (0%) 1st party to set floor level

SKYE multi-stage e-contracts



nd1

1. ***nd1*** *and* ***nd2*** *agree on the following terms:*
   a) ***nd1*** *will provide services to* ***nd2***
   b) ***nd2*** *shall pay* ***nd1*** *invoice once both* ***nd1+nd2*** *agree that the job is completed*
2. ***nd1*** *creates a [****100% quorum basis****] e-contract and [****delayed****] invoice*
3. ***nd1*** *creates and* ***nd2*** *e-signs the* ***SKYE e-contract***
4. ***nd1*** *sets workflow to "completion" (50% quorum) → nothing happens*
5. ***nd2*** *sets workflow to "completion" (100% quorum) →* ***invoice [posted]***

nd2

SKYE

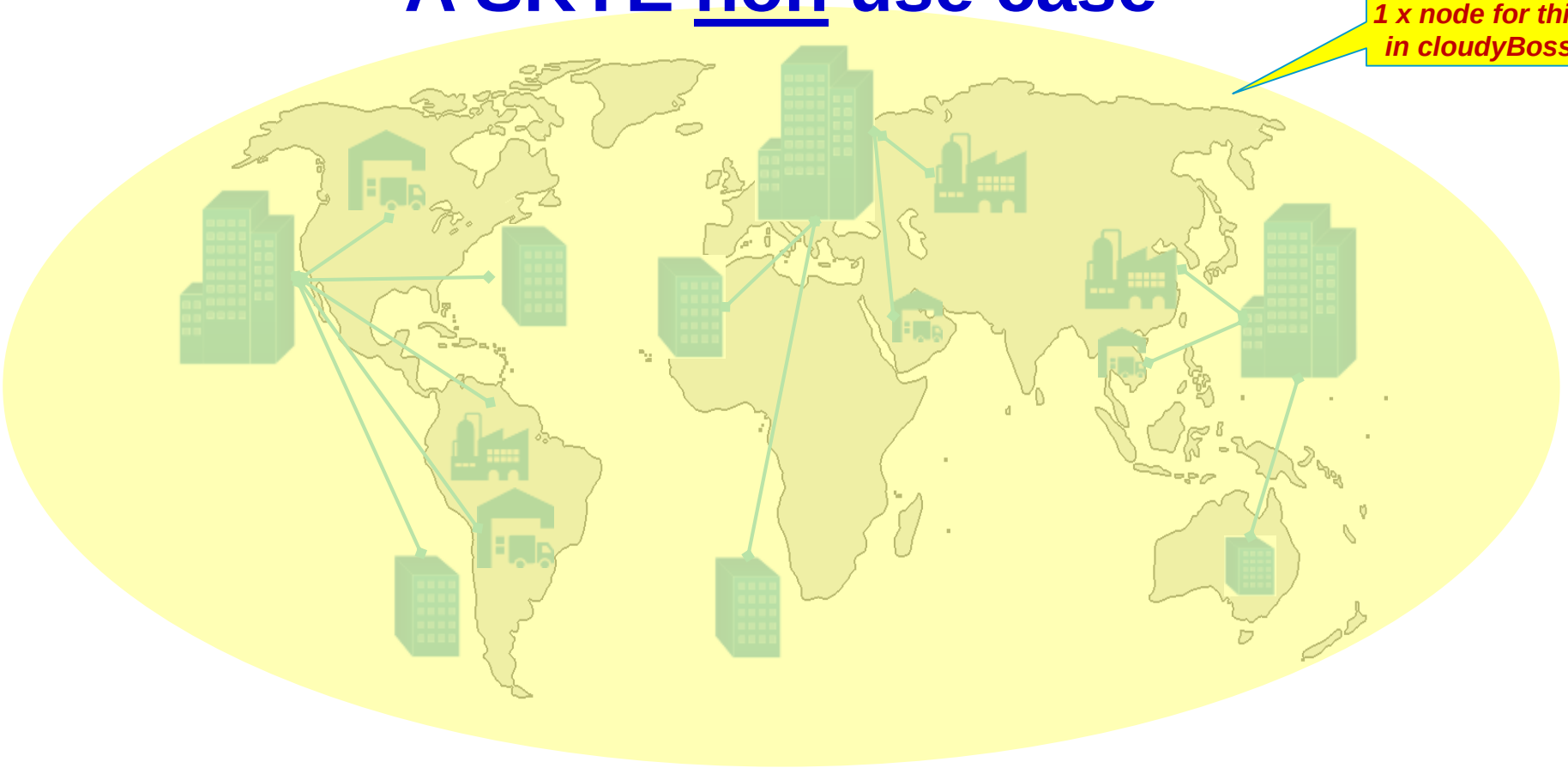
e-contract

from use cases to case studies

a need for **independent** parties to **operate together** under a safe, streamlined **tamper-proof ecosystem**

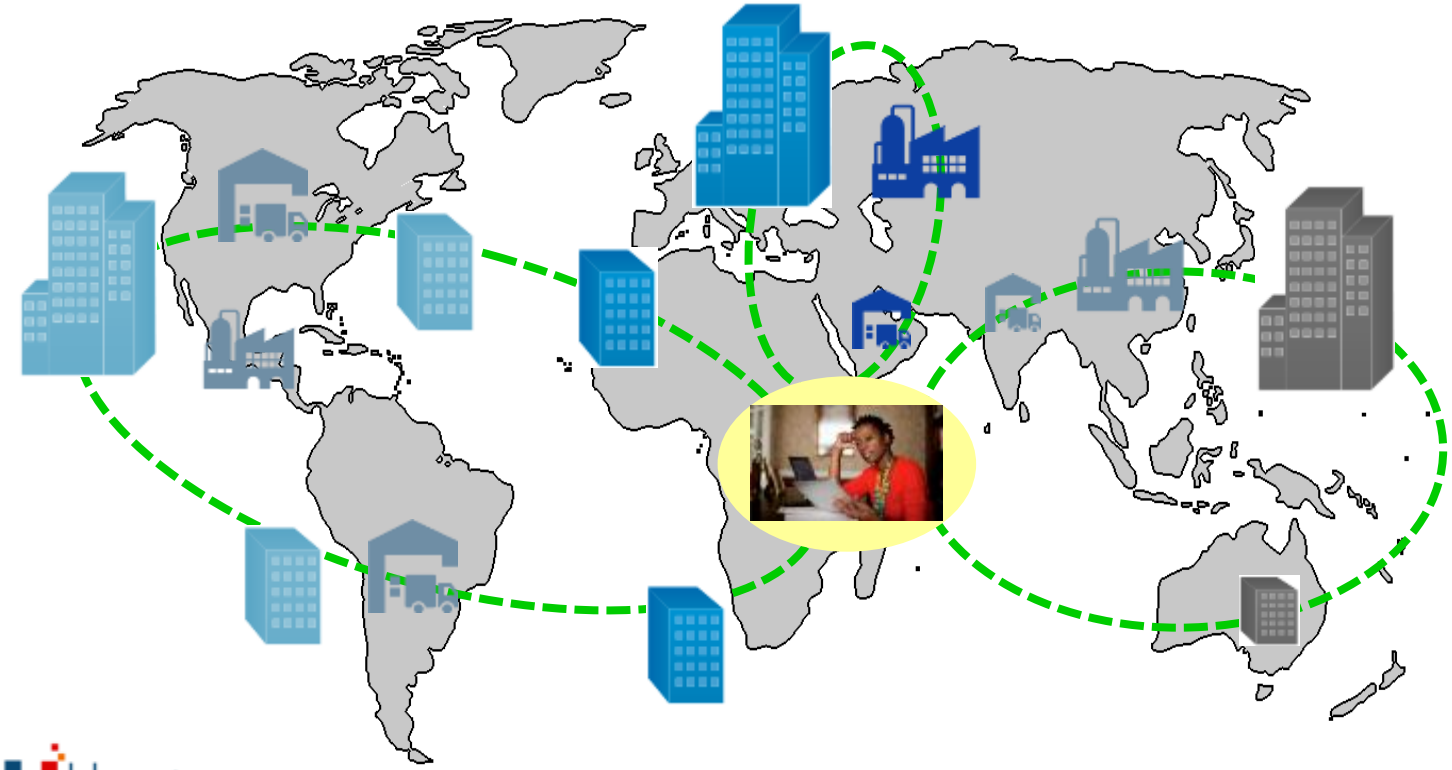
conventional international organisational structure

A SKYE non use case

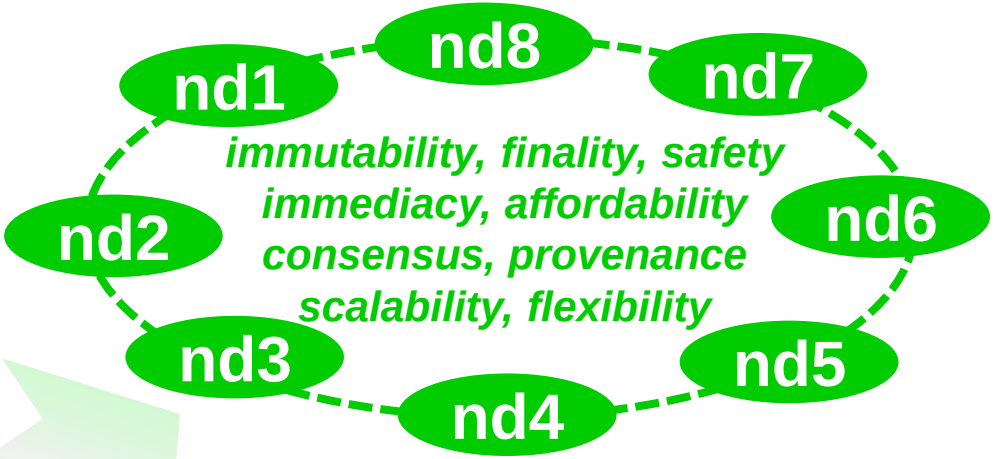


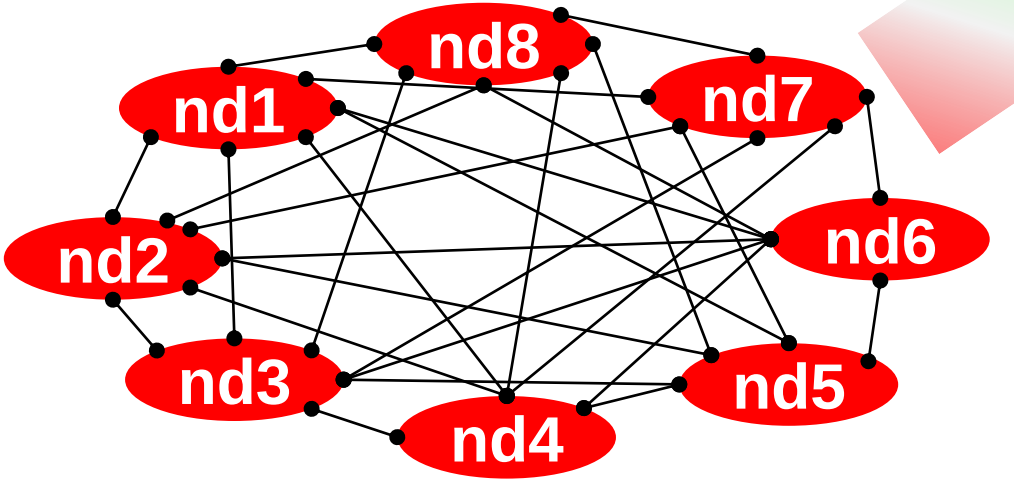
innovative international organisational structures

MaaS (Multinational as a Service)



API business trivialisation





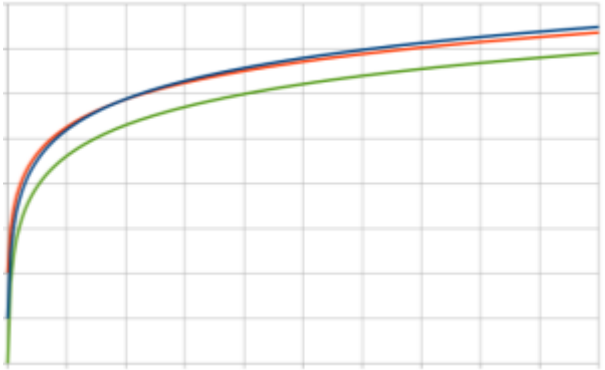
inefficient, expensive, vulnerable, scale poorly, inflexible

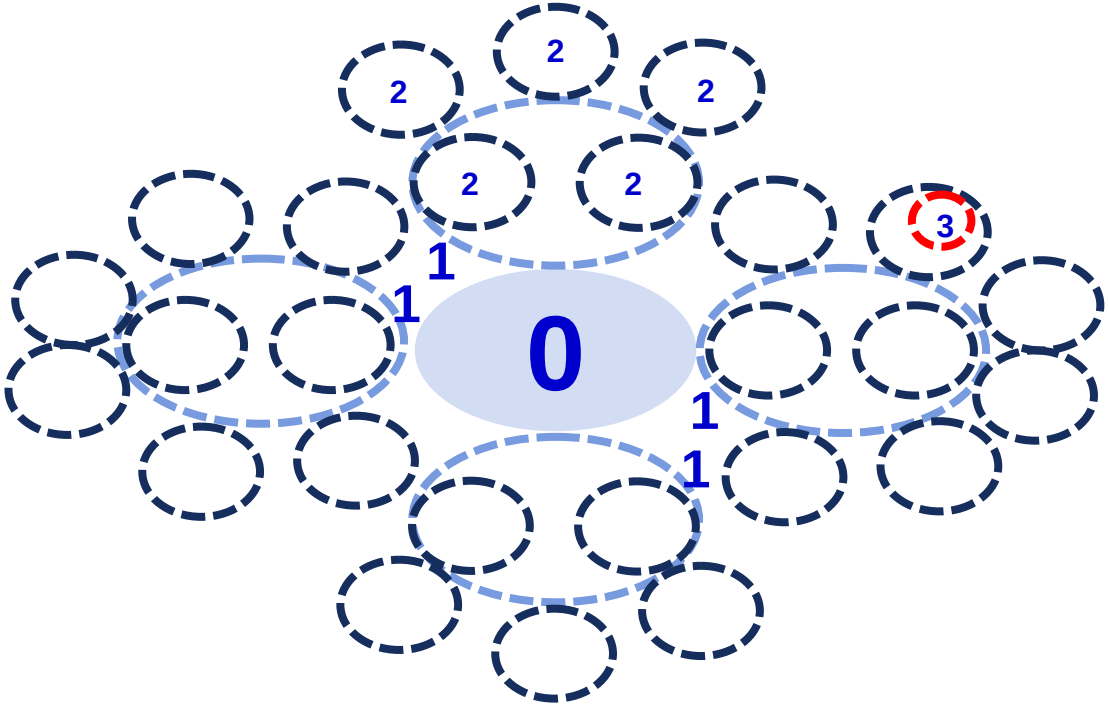
DLT-based **franchising** organisational model
enhanced efficiencies, decreased complexity

If you are a franchisor yet to consider DLT, ***your peers already are !***

from MLM to cBM (cluster business model)

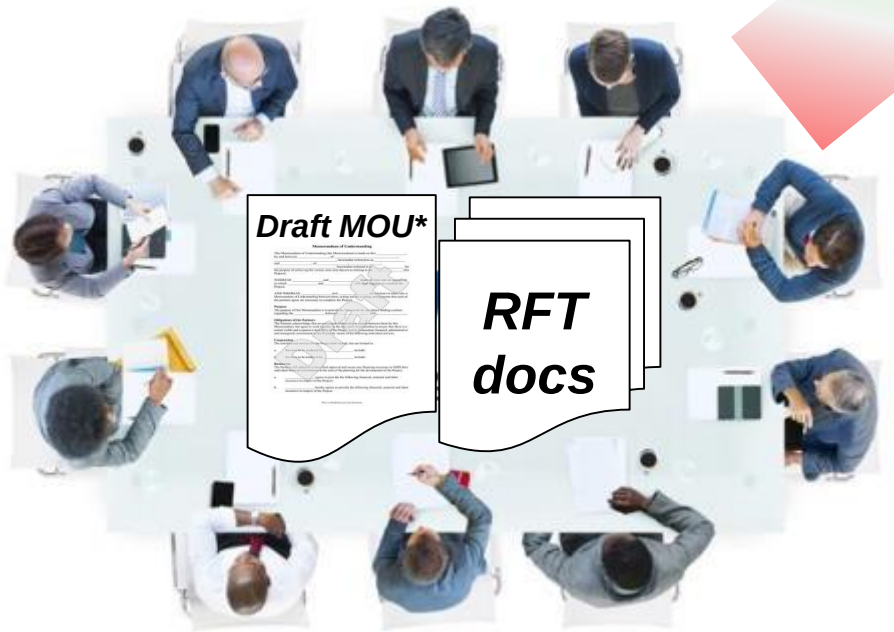
asymptotic margin control
via ring level (or generation) + level factor

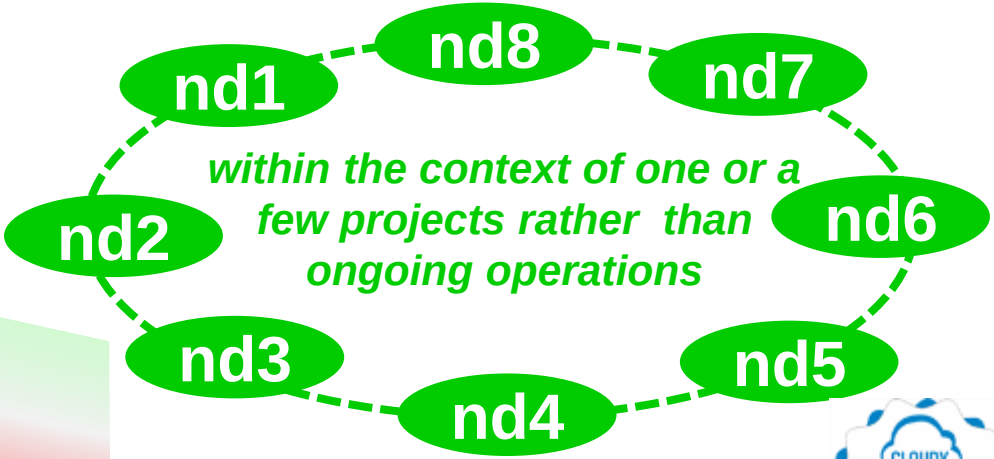




- *more **relevant to hyper-connected world** than old-school geo-segmentation*
- *scale-neutral **distributed fairness** + **infinite returns** at any level*
- ***asymptotic margin control** via ring level factor*

consortium trivialisation





Until now, consortiums formed when 1 supplier alone could not enter a large tender (and related project).

A consortium pools capabilities from different independent parties and distributes risk exposures.

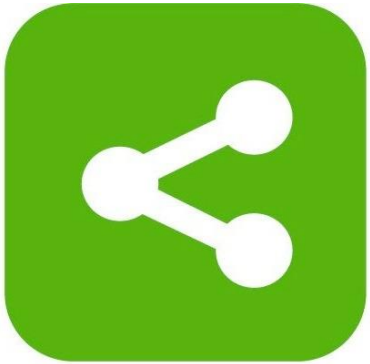
Commercial lawyers tend to get involved in the drafting of complex MOU and other legal documents.*

*smart contracts trivialise consortiums allowing pooling and risk mitigation on **any-value projects anywhere**, especially where the parties do not know each other.*

** MOU = Memorandum of Understanding*

industry-based registries

1. complex **value chains** / provenance / recalls
2. risk analysis / **insurance** / benchmarking
3. product categorisations / **market baskets**
4. self-regulatory data / **factual v fake** data
5. **pooled research** / segmentation
6. **credit records** / fraud detection
7. **governance breaches**
8. **industry standards**



more registry use cases

solving the *fake news* social epidemic

immutable academic records

global patents

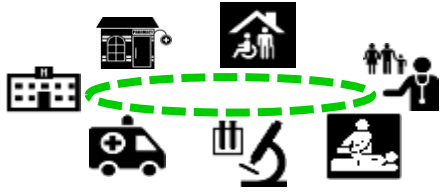
The newest strongest
data integrity standard

e-government | any type of public registries

significant life event registries

elections, electoral registries

land and property registries



electronic medical records

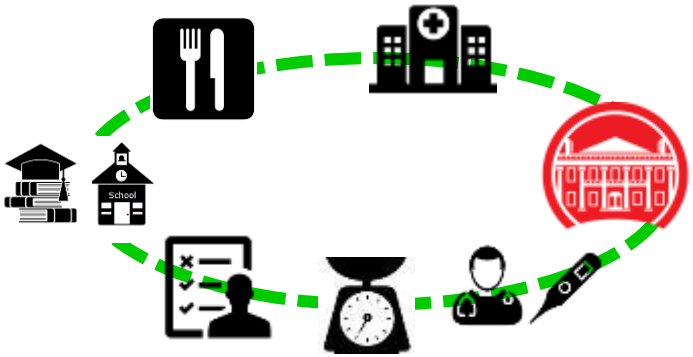
criminal records

BLOCKCHAIN

The newest strongest ***data integrity standard***

constituencies expect any government to adopt ***highest possible standards of governance*** *and provide absolute assurance on the integrity of any type of public records*

e-government | standards, accreditations & certifications



- *dangerous goods*
- *pharmaceuticals*
- ***building trades***
- ***electricals***
- *food products*
- *aerospace*
- *automotive*
- *healthcare*

Queensland Government
Department of Energy

Australian Government
Department of the Environment and Energy

IEEE

TCP/IP is NOT BF* tolerant

*as it sets a new **highest standard** on data integrity, **blockchain** unveils pitfalls with all sub-standard protocols, and **challenges all existing legislations on digital evidences**.*

** BF = Byzantine Fault*

JUXTIT *moneyless SKYE e-contracts*

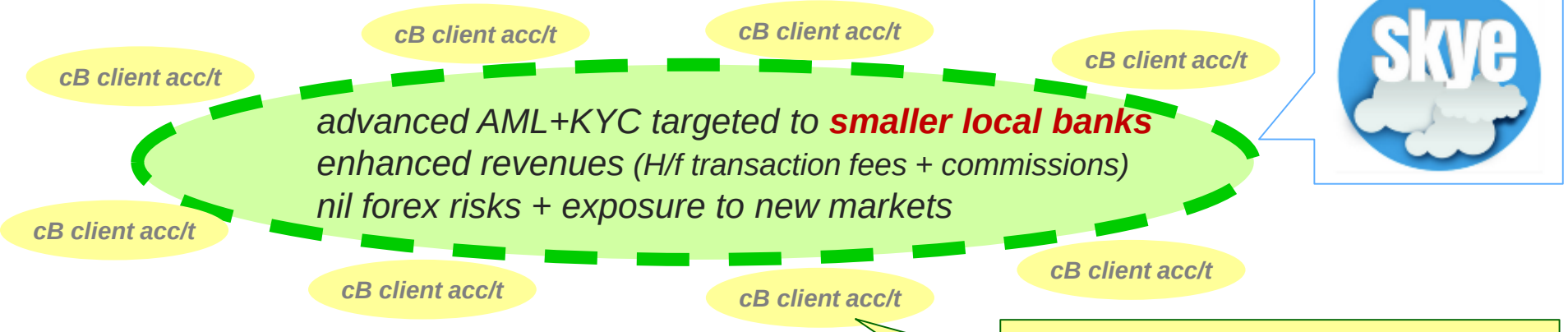
COBRA

cloudyBoss Omni-currency Banking Rotation Account

CLOUDY BOSS

cloudyBoss Pty Ltd - Sydney Australia | www.cloudyBoss.com | info@cloudyBoss.com

- most agile 21st century cloud SME's operate globally
- multicurrency treasury is a core dimension of their business
- ***… but it is very difficult to open a multicurrency banking account***
  - larger international banks have strict prohibitive access criteria and are expensive
  - bitcoin and other cryptocurrencies are niche and/or risk-exposed to regulations
  - smaller local banks are unable to maintain multiple foreign currency positions



- *operate seamlessly internationally*
- *receive passive COBRA incomes*
- *integrated bank account / ledger*
- ***cost-neutral smart cloud ERP***
- *integrated online banking*
- *built-in insurance*

COBRA
cloudyBoss Omni-currency Banking Rotation Account

a quantum leap into the future

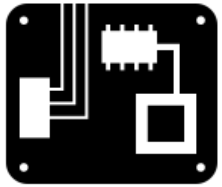
DLT is currently based on **blockchain** technology

blockchain technology relies on **cryptography**

QC (quantum computing) trivialises PK encryption

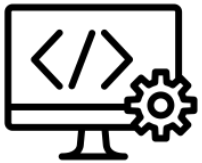
- QC ~instantaneously solves classic hard encryption
- **QC** threatens / **trivialises blockchain** technology
- **…but QC means *unchained* immutability**

3 dimensions to a quantum world



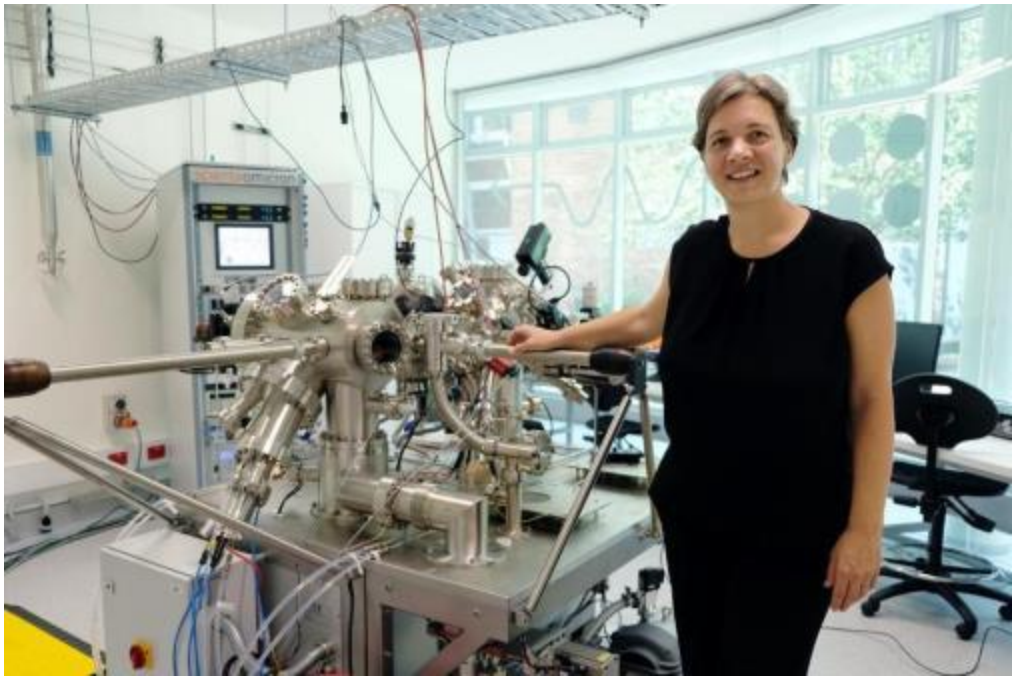
Quantum computing hardware

Quantum communications

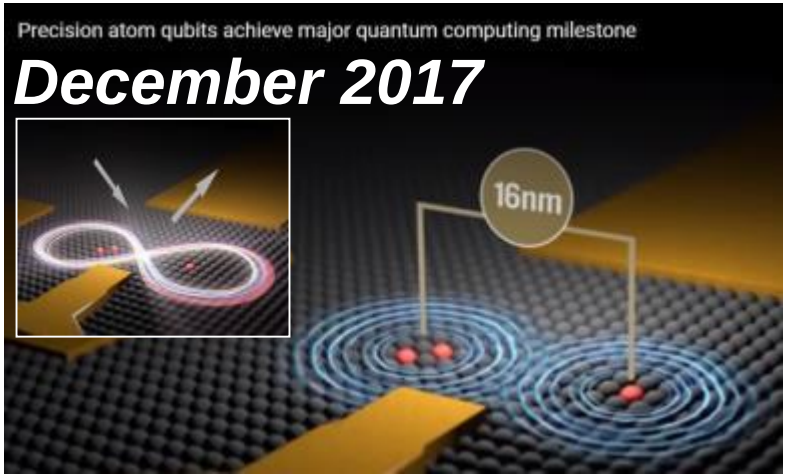


Quantum software

QC (quantum computer) on silicon a reality



2018 Australian of the Year ***Scientia Prof Michelle Simmons***
UNSW (Sydney – Australia) | CQC²T



Scientia Prof Sven Rogge

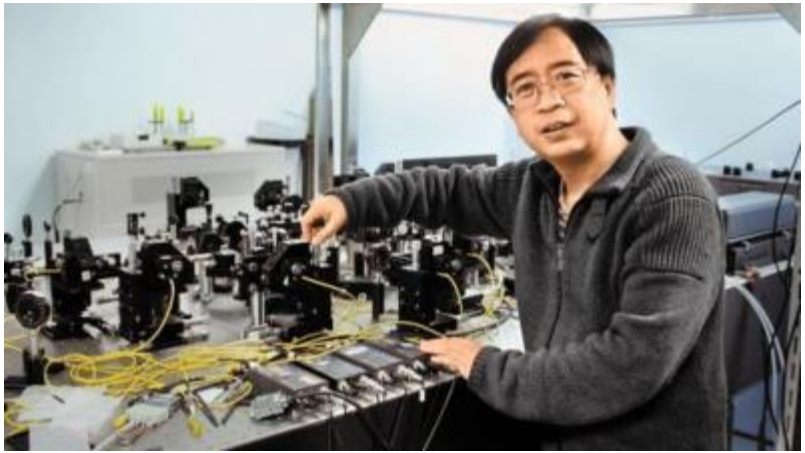
PhD candidate Sam Gorman

Scientia Prof Andrew Dzurak

Pioneering low-noise long-life (30 secs) QC nano-manufacturing

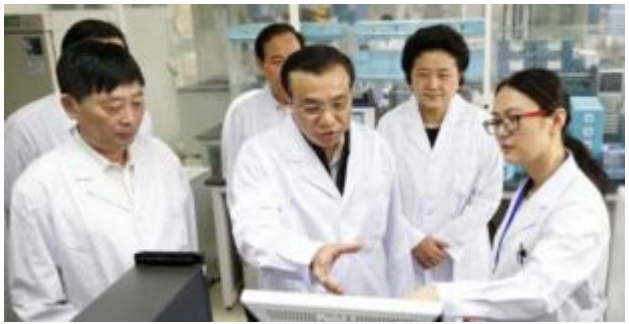
changing the rules in quantum communications

Lead scientist Pan Jianwei



and his research team @ QUESS | China

Quantum Experiments at Space Scale



- *long-distance (1200 km) message transmission*
- *one-time pad **QKD** (Quantum Key Distribution)*
- ***detectable** attempts to intercept / **eavesdrop***
- *basis for a **quantum-secure** commercial net*
- *integrated satellite QC + ground QC nets*

cloudyBoss research team on post-Boolean QC

"If you believe you understand quantum mechanics, then you do NOT understand quantum mechanics" ***Richard Feynman***


Kiran Chandrasekaran


Raghav Bhatnagar

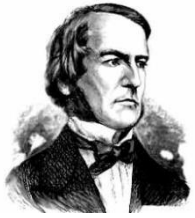

Tanya Shrivastava

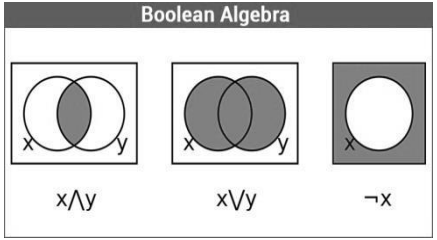

Giovanni Di Noto

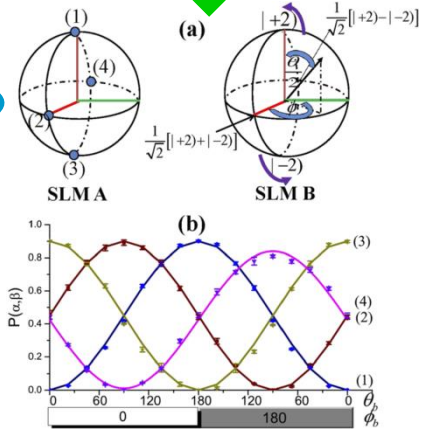

Uta Beyer

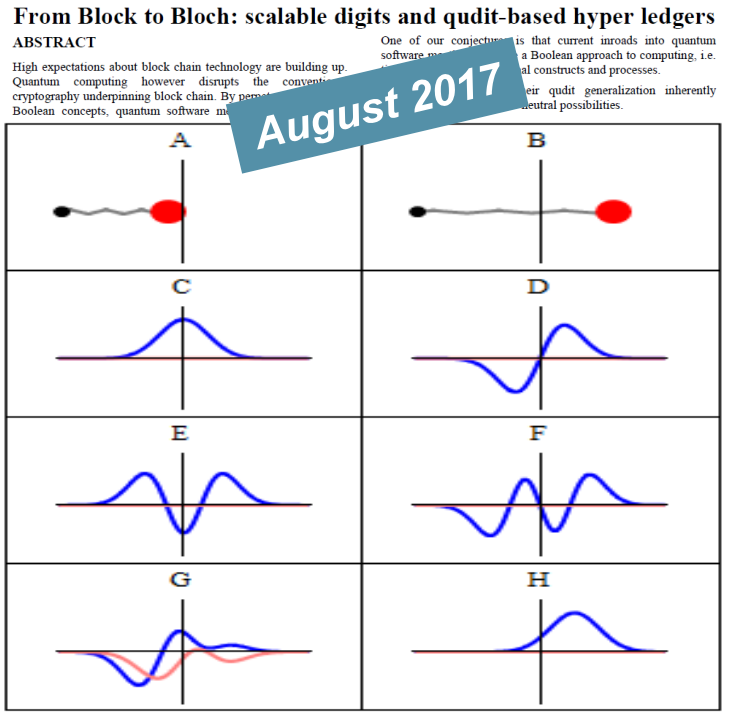
- qu**bit** is an unfortunate name, especially the **bit** part
- a **bit** (binary digit) is either **true** or **false** (0 or 1)
- a **qubit** is described by a **wave function**
- **qu**dits are described via **Bloch spheres**
- **QC** needs **post-Boolean** algebra

too old for that ch...ain
time to retire…


George Boole 1815-1864

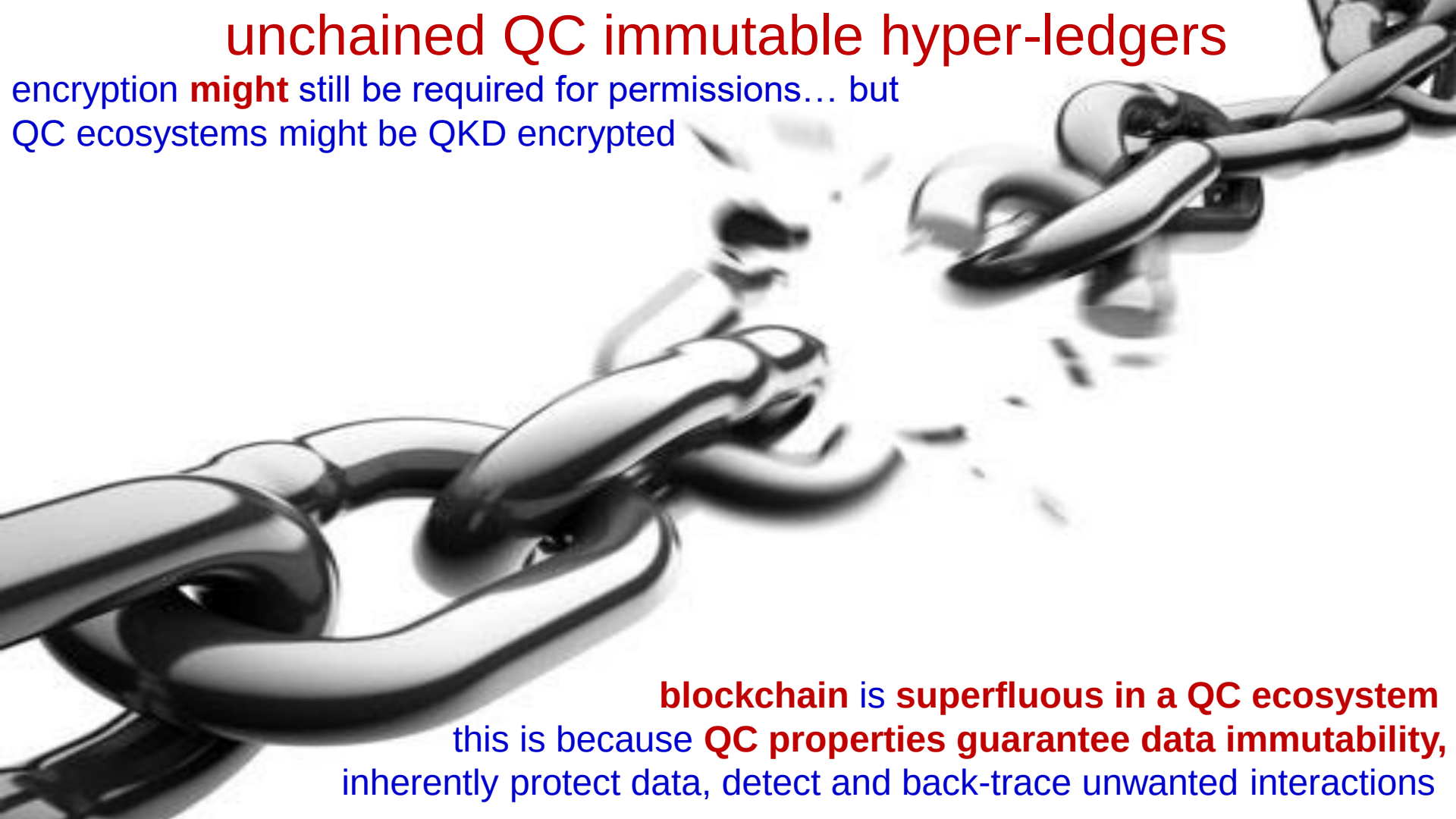






unchained QC immutable hyper-ledgers

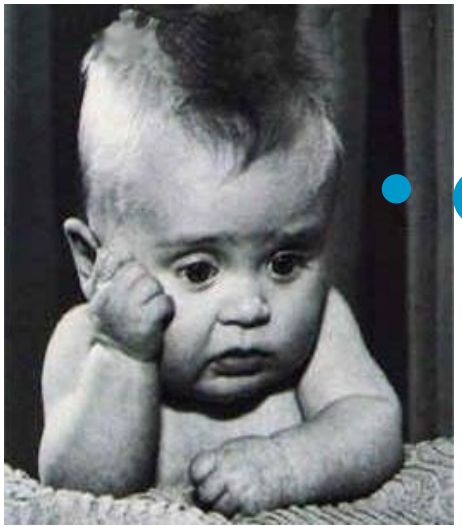
encryption **might** still be required for permissions… but
QC ecosystems might be QKD encrypted



blockchain is **superfluous in a QC ecosystem**
this is because **QC properties guarantee data immutability,**
inherently protect data, detect and back-trace unwanted interactions

wrap up

who	*stage*	*options*
coder / developer	**Beginner**	1. Self-learn 2. Join an open-source group 3. Attend other workshops on the topic of interest **4. Attend my blockchain technology workshops** 5. Apply to an internship with pertinent organisation such as cB
	Advanced	1. Re/assess personal (or company) goals 2. sharpen skills across all DLT areas, or 3. Specialise into one or few DTL areas **4. Assess opportunities to support** 5. Explore quantum cryptography



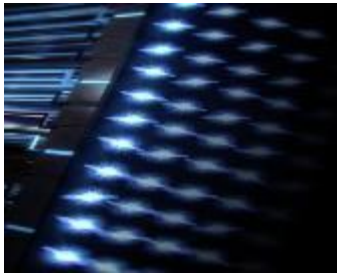
Enterprise DLT
or Cryptocurrency ?
Is that even a question ?

who	*scope*	*options*
project implementer	**all areas**	1. Reconcile project goals against pertinent DLT area 2. Scan market for best solution provider/s 3. Evaluate and activate solution/s
client organisations	**all industries**	1. Nominate enabling party (both geo and functional scopes) 2. Assess business model vs existing or new DLT use cases 3. Engage with potential DLT ecosystem node stakeholders 4. Conduct thorough feasibility research to define scope/s 5. Implement (solely or as a consortium where pertinent)
industry / institutional representation bodies	**all areas**	1. Prepare for, define or strengthen your industry DLT future 2. Facilitate DLT ecosystems for your members 3. Become active DLT ecosystem operators

"If you look at the various strategies available for dealing with a new technology, sticking your head in the sand is not the most plausible strategy."

Ralph Merkle

who	*protocol*	*options*
DLT industry players	**any**	1. Mitigate industry ***reputational risks*** via self-regulation 2. Solve / define the ***multi-chain protocol challenge*** 3. Prepare for post-quantum ***unchained*** DLT future 4. Distributed immutability beyond ledger/business 5. Solve ***single internet vulnerability*** multi-threat



HYPERLEDGER

ripple
Interledger

CLOUDY BOSS

Skye

info@cloudyboss.com