Blockchain Technologies: What, Why and Why not

Beyond Bitcoin

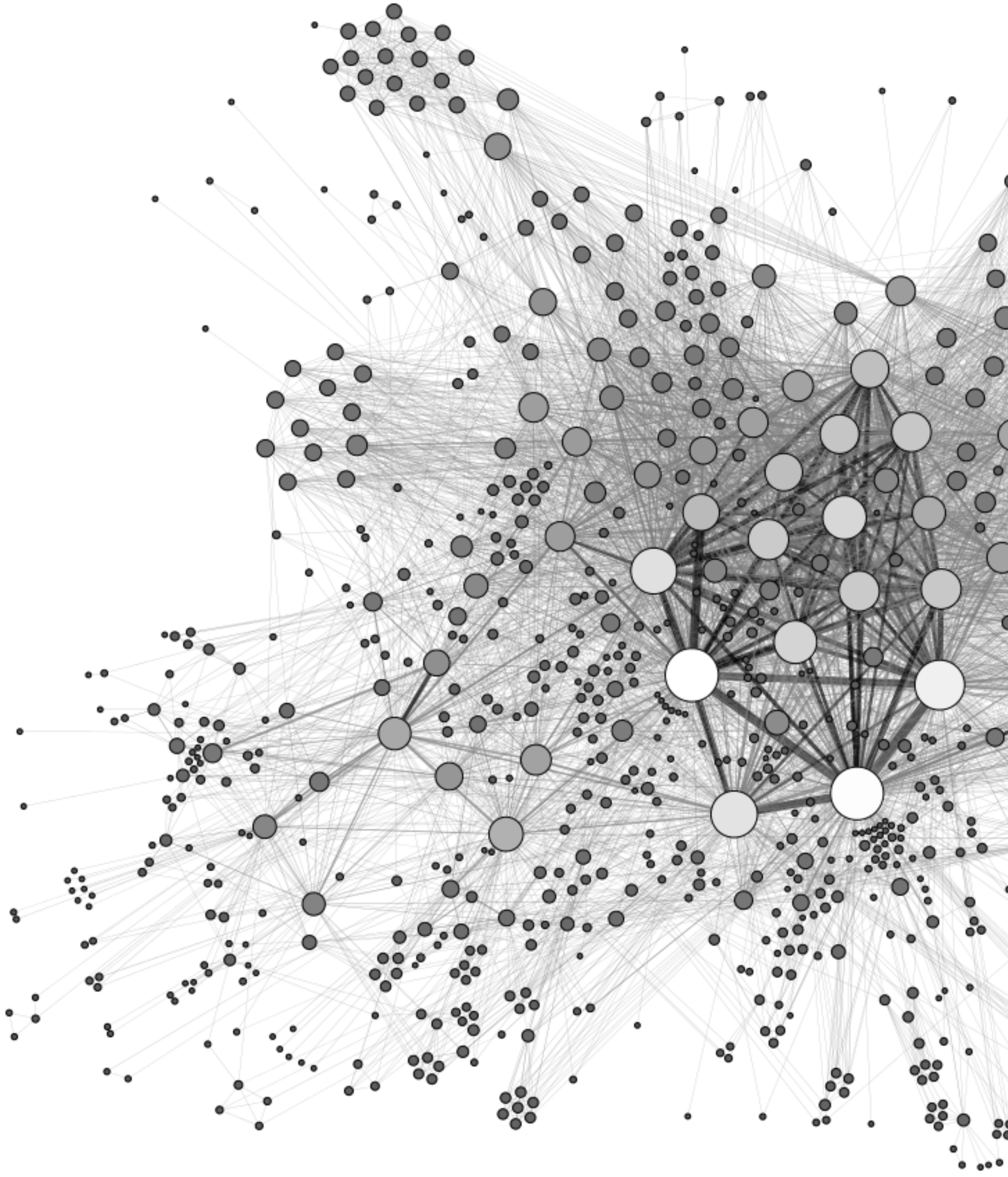
Régis Barondeau, Ph.D.

Professor in Management and Technology
ESG UQAM
barondeau.regis@uqam.ca

in linkedin.com/in/regisbarondeau

www.regisbarondeau.com

March 20, 2019



A brief history of blockchain

INSIDE THIS WEEK: TECHNOLOGY QUARTERLY
The Economist
The king's role in Thailand's chaos
Eurabian cities
After Mumbai
Sperm and intelligence
Our books of the year
DECEMBER 6TH–12TH 2008
www.economist.com
Where have all your savings gone?

INSIDE: A 14-PAGE SPECIAL REPORT ON CARS IN EMERGING MARKETS
The Economist
Can China save the world?
In search of Republican brains
Life without nuclear weapons
The threat of deflation
Sarkozy, the secret socialist
NOVEMBER 15TH–21ST 2008
www.economist.com
Redesigning global finance
WTO
BRETTON WOODS
IMF

2008

“A woman/man becomes creative, whether she/he is an artist or scientist, when she/he finds a new unity in the variety of nature. She/he does so by finding a likeness between things which were not thought alike before.”

Jacob Bronowski

Photo par Grasso Luigi

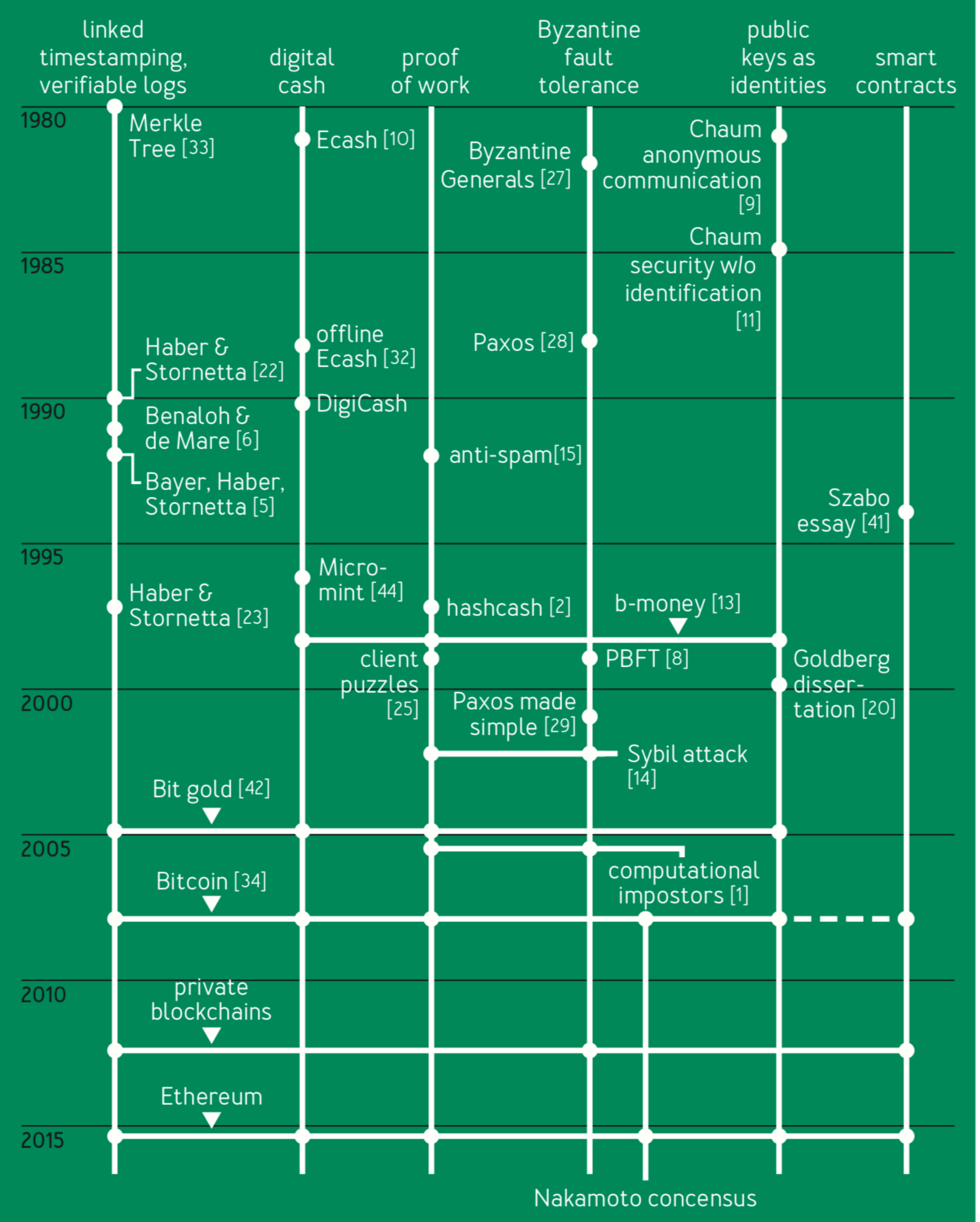
bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

2008

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network […]."



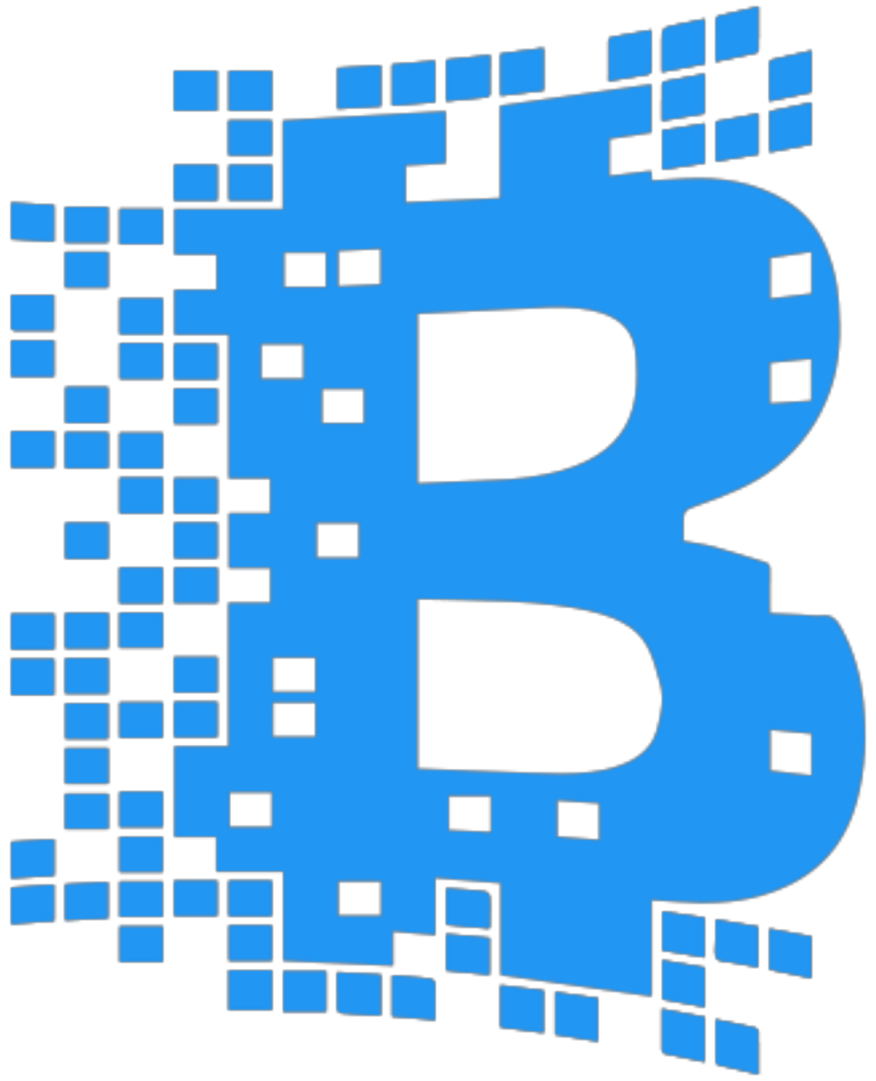
Bitcoin's Academic Pedigree

THE CONCEPT OF CRYPTOCURRENCIES IS BUILT FROM FORGOTTEN IDEAS IN RESEARCH LITERATURE

ARVIND NARAYANAN AND JEREMY CLARK

Bitcoin

- First blockchain
- First digital cash system that works
- First rare digital asset (≠ double-spending)
- Independent from the monetary system
- No more double-entry bookkeeping
- Deintermediation
- Consensus by code => trust
- Distributed ledger => decentralization



Source : https://icons8.com/icon/new-icons/all

What is blockchain?

INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA
The Economist
Our guide to America's best colleges
Myanmar's free-ish election
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
OCTOBER 31ST–NOVEMBER 6TH 2015
Economist.com
The trust machine
How the technology behind bitcoin could change the world
IN BLOCKCHAIN WE TRUST

2015

"**BITCOIN has a bad reputation**. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the "dark net".

This is unfair. The value of a bitcoin has been pretty stable, at around $250, for most of this year. Among regulators and financial institutions, scepticism has given way to enthusiasm (the European Union recently recognised it as a currency). But most unfair of all is that **bitcoin's shady image causes people to overlook the extraordinary potential of the "blockchain", the technology that underpins it.** This innovation carries a significance stretching far beyond cryptocurrency. The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. **Simply put, it is a machine for creating trust.**"

Oct 31st 2015 | From the print edition

“Blockchain is a type of distributed ledger in which value-exchange transactions are sequentially grouped into blocks. Each block is chained to the previous one and immutably recorded across a peer-to-peer network, using cryptographic trust and assurance mechanisms. Transactions can include programmable behavior.”

Source: Gartner Hype Cycle for Blockchain Business, 2018

Take away: Think beyond Bitcoin to embrace the Internet of value.

Blockchain Demo

Anders Brownworth

https://anders.com/blockchain

BITCOIN TRANSACTION REQUEST MESSAGE

“David sends 5 BTC to Sandra”

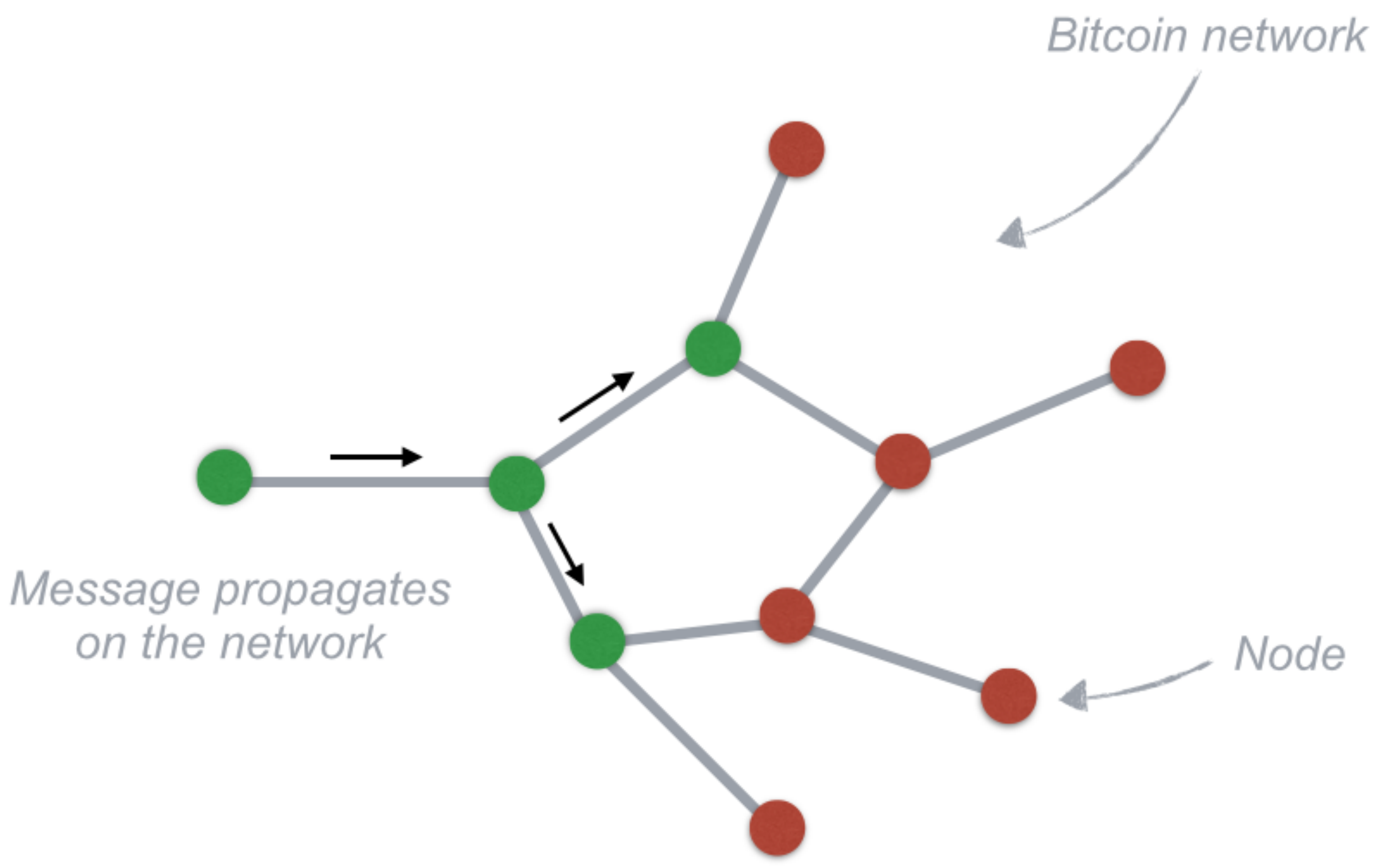
David → Sandra 5 BTC

LEDGER 🔴

Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23

LEDGER 🟢

Account owner	Value
Mary	4
John	56
Sandra	**88**
Lisa	16
David	**182**
Brian	23



Each *node* receives the transaction request message, updates its own copy of the *ledger* and passes on the message to the nearby *nodes.*

Source: https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae

Some blockchain technologies

Consensus Mechanisms

Sidechains/channels

Distributed Ledger

DApps

Metacoin Platforms

Blockchain

Quantum Proof Blockchain

Smart Contracts

Zero Knowledge Proof

Cryptocurrency Wallets

Blockchain PaaS

Blockchain Interoperability

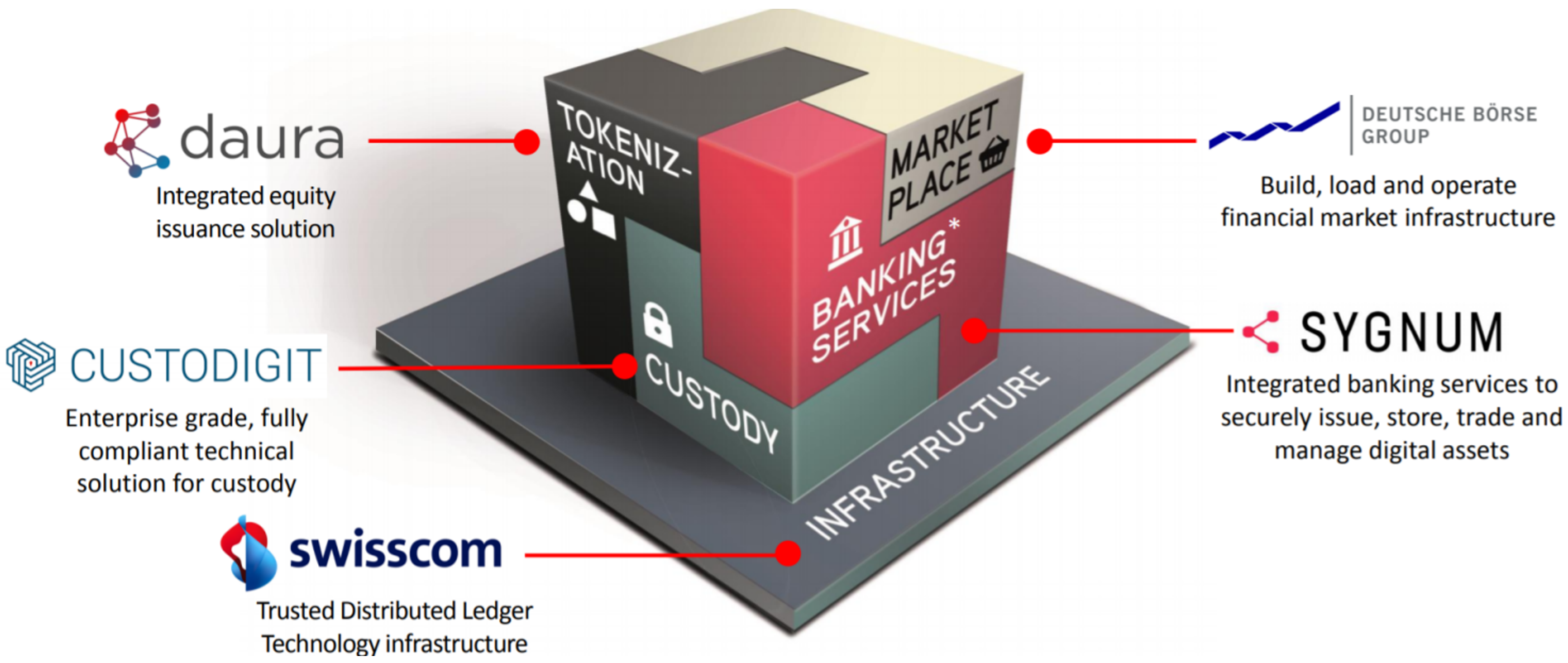
Cryptocurrency Mining

Things as Customers

Technologies	Definitions	Impacts	Solutions
Consensus Mechanisms	Distributed network governance rules and protocoles	Network security by the code	PoW, PoS, PBFT, Proof of Space, etc.
Smart Contracts	Program that verifies and executes business processes	May replace some legal documents	Solidity (Ethereum)
Zero Knowledge Proof	Privacy-preserving messaging protocols. Proves information veracity to both parties	Privacy protection	Zk-Snarks - ZoE (Ethereum)
Blockchain platform as a service	Blockchain software services offered on the cloud	Testing proof of concepts	Bluemix (IBM), Azure (Microsoft), BlockCypher, BlockApps
Things as Customers	Things will have the capacity to buy, sell and request services	New business models	Caterpillar

Why through use cases

Deutsche Börse, Swisscom Team Up to Build Digital Asset ‘Ecosystem’


daura
Integrated equity issuance solution
CUSTODIGIT
Enterprise grade, fully compliant technical solution for custody
swisscom
Trusted Distributed Ledger Technology infrastructure
DEUTSCHE BÖRSE GROUP
Build, load and operate financial market infrastructure
SYGNUM
Integrated banking services to securely issue, store, trade and manage digital assets
TOKENIZ-ATION
MARKET PLACE
BANKING SERVICES*
CUSTODY
INFRASTRUCTURE

“Deutsche Börse Group, Germany-based owner of the Frankfurt Stock Exchange, has partnered with major telecoms and IT provider Swisscom and Switzerland-based fintech firm Sygnum to build what the firms are calling a “trusted digital asset ecosystem.”

Swisscom announced Monday that the proposed ecosystem would provide a number of solutions in the digital assets space, including issuance, custody, liquidity provision and banking services, all using blockchain technology.”

Source: Coindesk, March 11, 2019

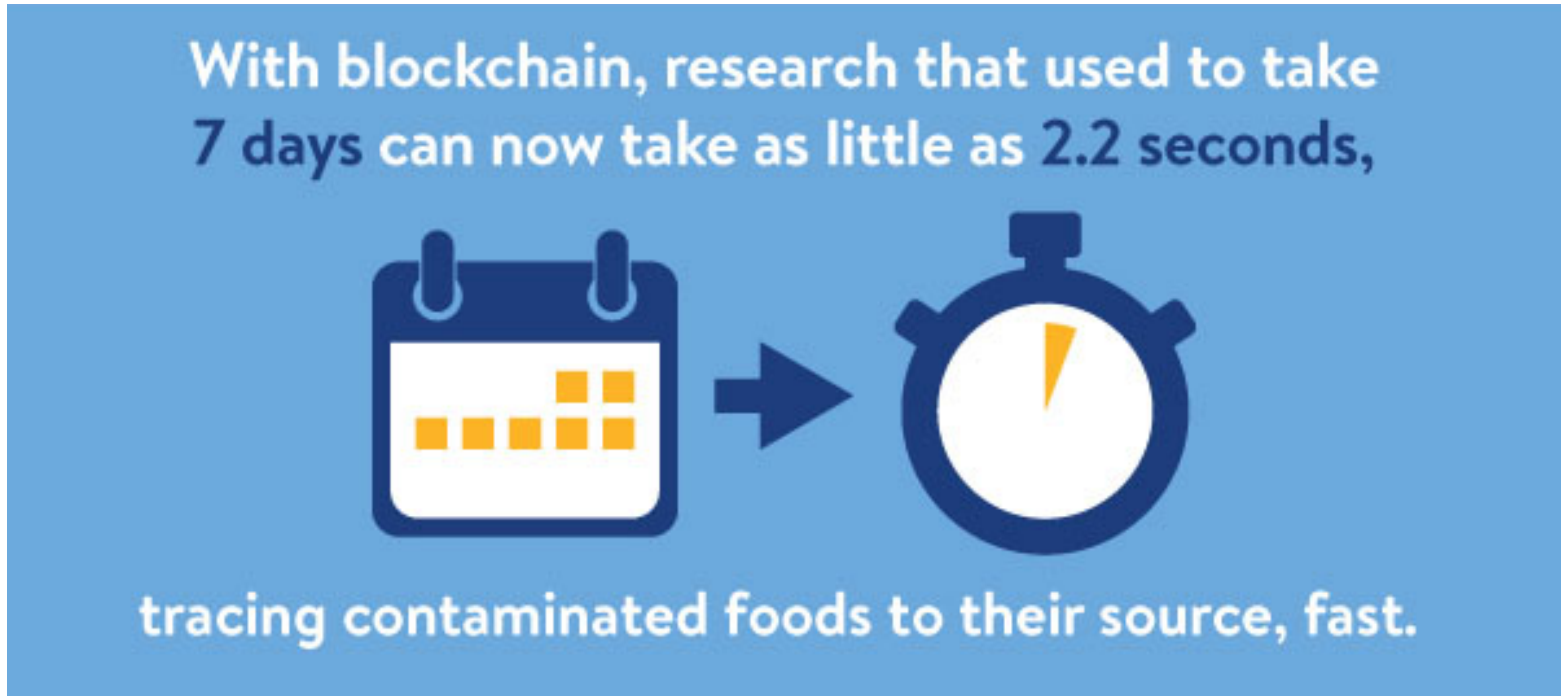
Bee’ah, Hamriyah Free Zone Authority partner to launch Sharjah’s first Blockchain platform

حفل توقيع مذكرة تفاهم بين هيئة المنطقة الحرة بالحمرية وبيئة
Signing Ceremony of MOU between Hamriyah Free Zone Authority and Bee’ah
bee’ah
HAMRIYAH FREE ZONE AUTHORITY

“The HFZA Waste Permit Portal is the first platform in Sharjah that utilises blockchain technology to validate, process and store transactions. As the digital ledger is built on a blockchain network, all transactions are completely secured, essentially eliminating any human error or fraud. The customised portal will not only save customers operating within the free zone time and money when applying for permits, but also reduce the downtime it takes for permits to be issued from several days to only a few hours..”

Source: Emirates News Agency February 17, 2019

In Wake of Romaine E. coli Scare, Walmart Deploys Blockchain to Track Leafy Greens

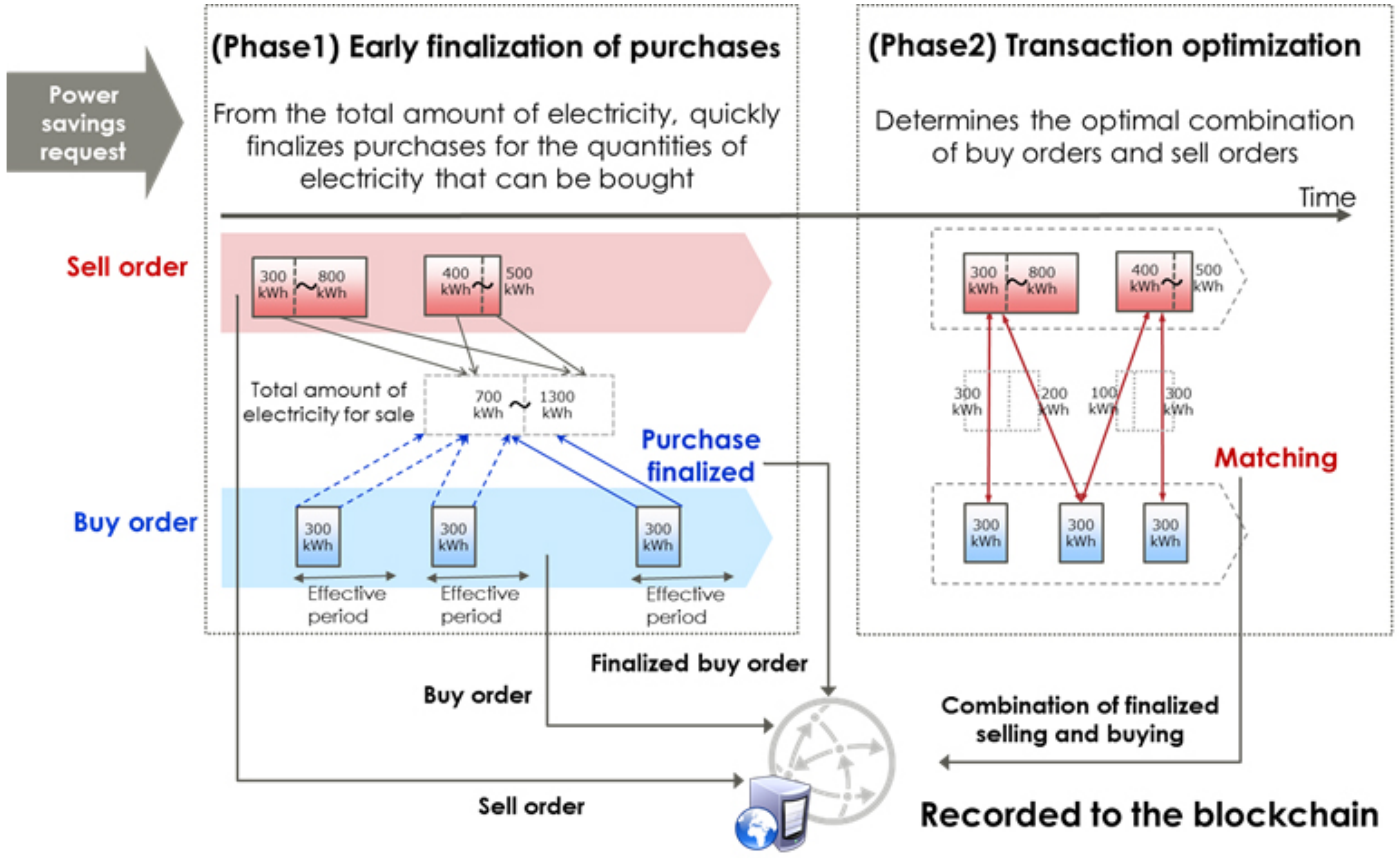

With blockchain, research that used to take 7 days can now take as little as 2.2 seconds,
tracing contaminated foods to their source, fast.

"Enhanced ability to trace a contaminated food back to its source will help government agencies and companies to identify the source of a foodborne disease outbreak, coordinate more effective recalls of foods thought to be contaminated, and learn where past problems began. We think these steps will strengthen future prevention efforts and better protect the public's health from the threat of foodborne illness."

Robert Tauxe, MD, director of CDC's Division of Foodborne, Waterborne, and Environmental Diseases

Source: Walmart September 24, 2019

Fujitsu Develops Blockchain-based Exchange System for Electricity Consumers


Power savings request
(Phase1) Early finalization of purchases
From the total amount of electricity, quickly finalizes purchases for the quantities of electricity that can be bought
(Phase2) Transaction optimization
Determines the optimal combination of buy orders and sell orders
Time
Sell order
300 kWh ~ 800 kWh
400 kWh ~ 500 kWh
Total amount of electricity for sale
700 kWh ~ 1300 kWh
Purchase finalized
Buy order
300 kWh
300 kWh
300 kWh
Effective period
Effective period
Effective period
300 kWh ~ 800 kWh
400 kWh ~ 500 kWh
300 kWh
200 kWh
100 kWh
300 kWh
Matching
300 kWh
300 kWh
300 kWh
Finalized buy order
Buy order
Sell order
Combination of finalized selling and buying
Recorded to the blockchain

"Fujitsu Limited and Fujitsu Laboratories Ltd. today announced that they have applied blockchain technology to develop a system for trading related to energy shortages and surpluses among electricity consumers, including factories and retail stores. […]

Fujitsu has now devised a system in which electricity consumers can efficiently exchange among themselves the electricity surpluses they have produced through their own electricity generation or power savings. The company then applied blockchain, and with the cooperation of ENERES Co., Ltd., the system was used in a simulation using the actual data of electricity consumption. The result was an approximately 40% improvement to the DR success rate."

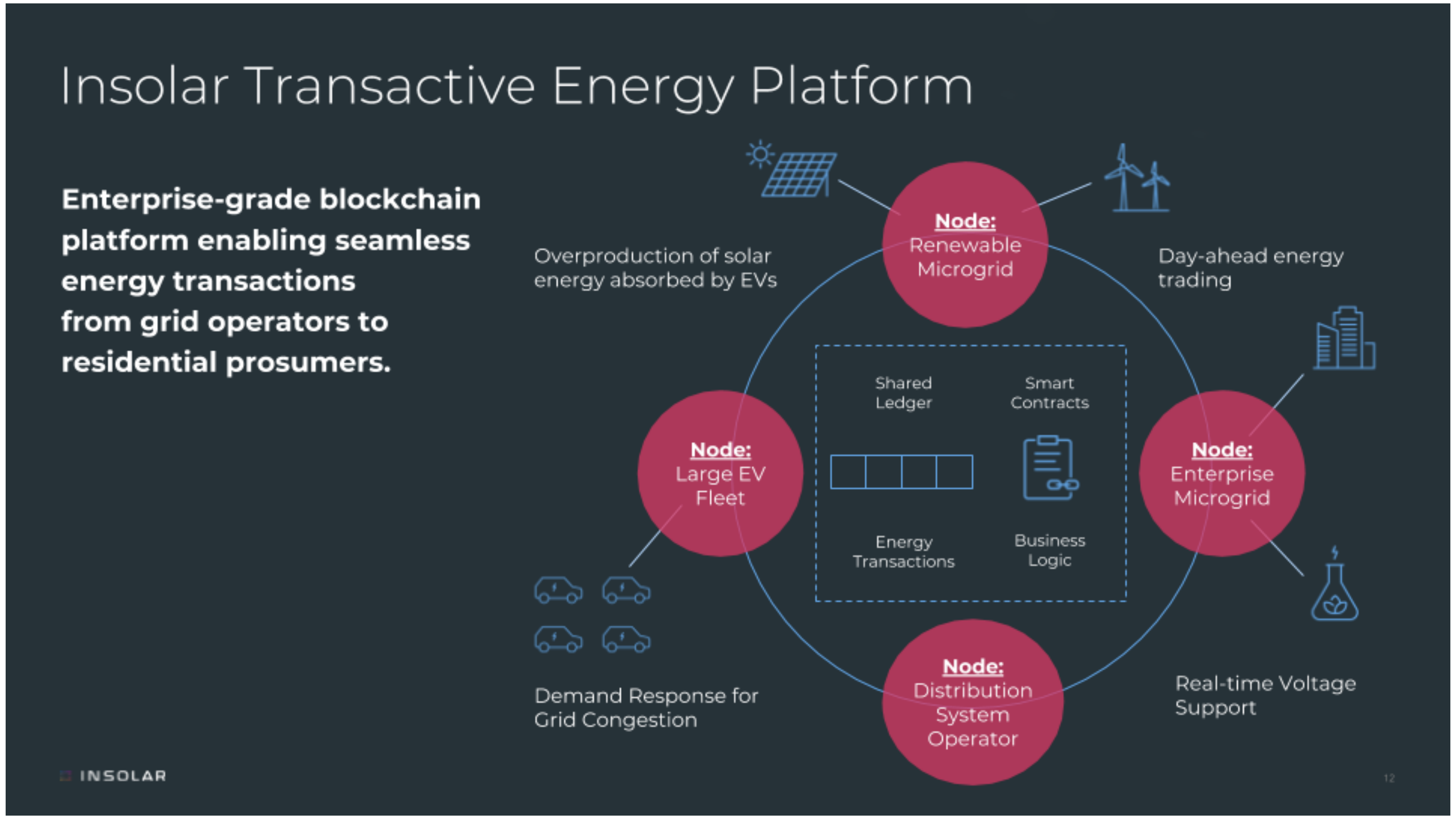
Source: Fujitsu Press Release January 30, 2019

Insolar to test blockchain for transactive energy systems with Toronto company

“Funded in part by a federal grant from Natural Resources Canada (NRCAN), the Insolar blockchain will be integrated into a transactive smart grid prototype, which is designed to improve the uptake of distributed generation of renewables, electric vehicles, energy storage systems, and smart thermostats.

The partnership will demonstrate the concrete benefits of introducing a distributed ledger system to enable a transactive energy platform (TEP) — a revolutionary innovation with huge positive climate and economic impact.”

Source: Insolar March 19, 2019

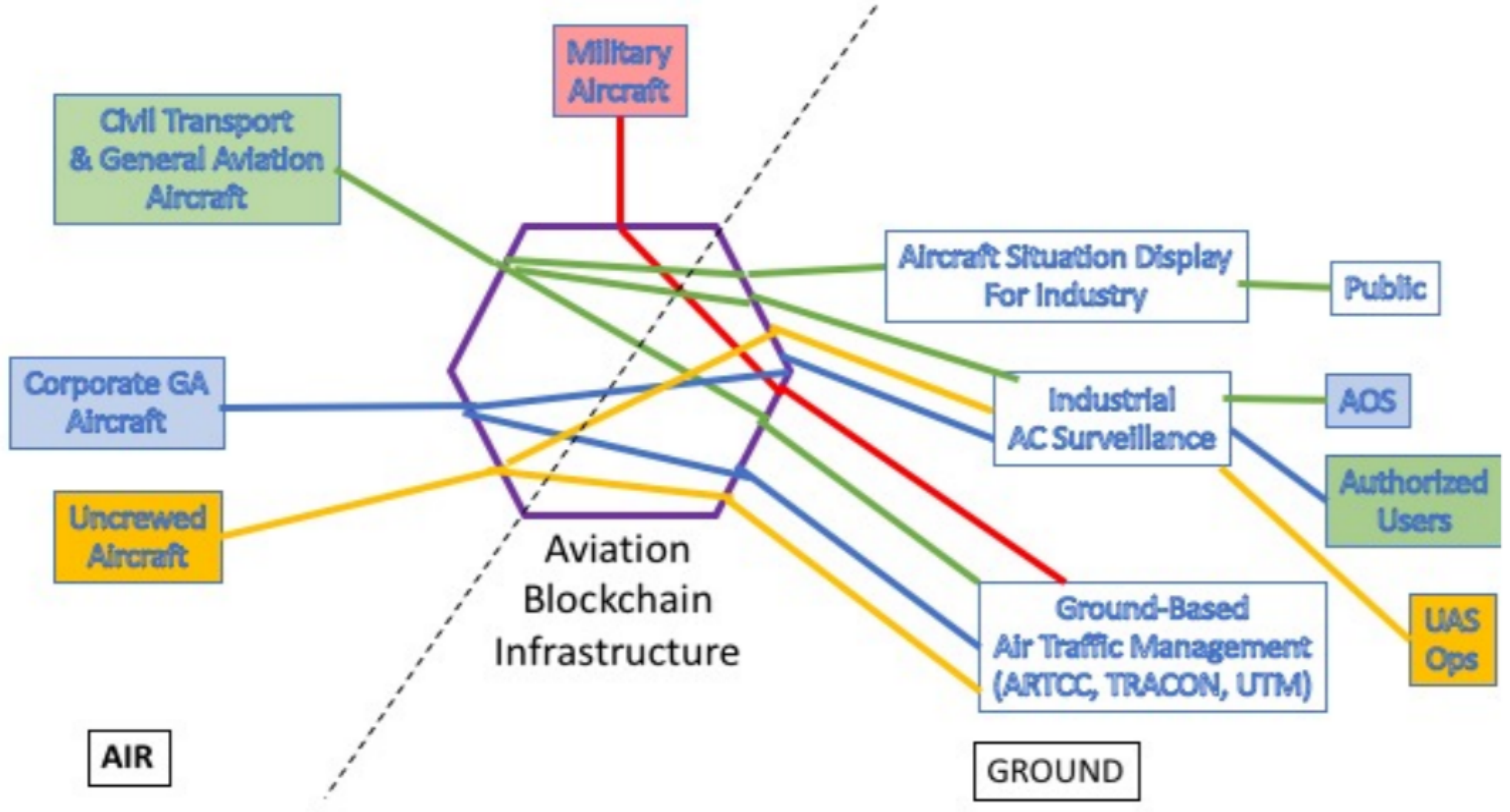


Insolar Transactive Energy Platform

Enterprise-grade blockchain platform enabling seamless energy transactions from grid operators to residential prosumers.

Node: Renewable Microgrid
Overproduction of solar energy absorbed by EVs
Day-ahead energy trading
Shared Ledger
Smart Contracts
Energy Transactions
Business Logic
Node: Large EV Fleet
Node: Enterprise Microgrid
Node: Distribution System Operator
Demand Response for Grid Congestion
Real-time Voltage Support
INSOLAR
12

NASA Eyes Blockchain Tech to Secure Aircraft Flight Data


Military Aircraft
Civil Transport & General Aviation Aircraft
Corporate GA Aircraft
Uncrewed Aircraft
Aviation Blockchain Infrastructure
Aircraft Situation Display For Industry
Public
Industrial AC Surveillance
AOS
Authorized Users
UAS Ops
Ground-Based Air Traffic Management (ARTCC, TRACON, UTM)
AIR
GROUND

Source: Coindesk January 11, 2019

“Starting Jan. 1, 2020, the U.S. has been mandated by the Federal Aviation Administration (FAA) to use a new surveillance system – Automatic Dependent Surveillance Broadcast (ADS-B) – which will publicly broadcast aircrafts’ identity, position and other information.

That has raised security concerns among stakeholders, Reisman said in his paper, explaining that the ADS-B system “does not include provisions for maintaining these same aircraft-privacy options, nor does it address the potential for spoofing, denial of service, and other well-documented risk factors.”

Civil aircraft companies would prefer to keep some data private, he writes, for example, to counter tracking executives as part of corporate espionage operations.”

Porsche introduces blockchain to cars

“The car becomes part of the blockchain, making a direct offline connection possible – that is, without diversion through a server. Taking 1.6 seconds, the process of opening and closing the car via an app is up to six times faster than before. ”

“Moreover, the technology makes it possible to assign temporary access authorisations for the vehicle – in a secure and efficient manner. A protected connection to vehicle data and functionalities can be established using blockchain. At the same time, it protects all communication between participants. Third-party providers can be integrated without the need for additional hardware, simply by using ‘smart contracts’.”

“Porsche is also working on new business models based on blockchain […] With this basis, the future of autonomous driving will see improved functions on offer.”

Source: Porsche Newsroom, February 22, 2018

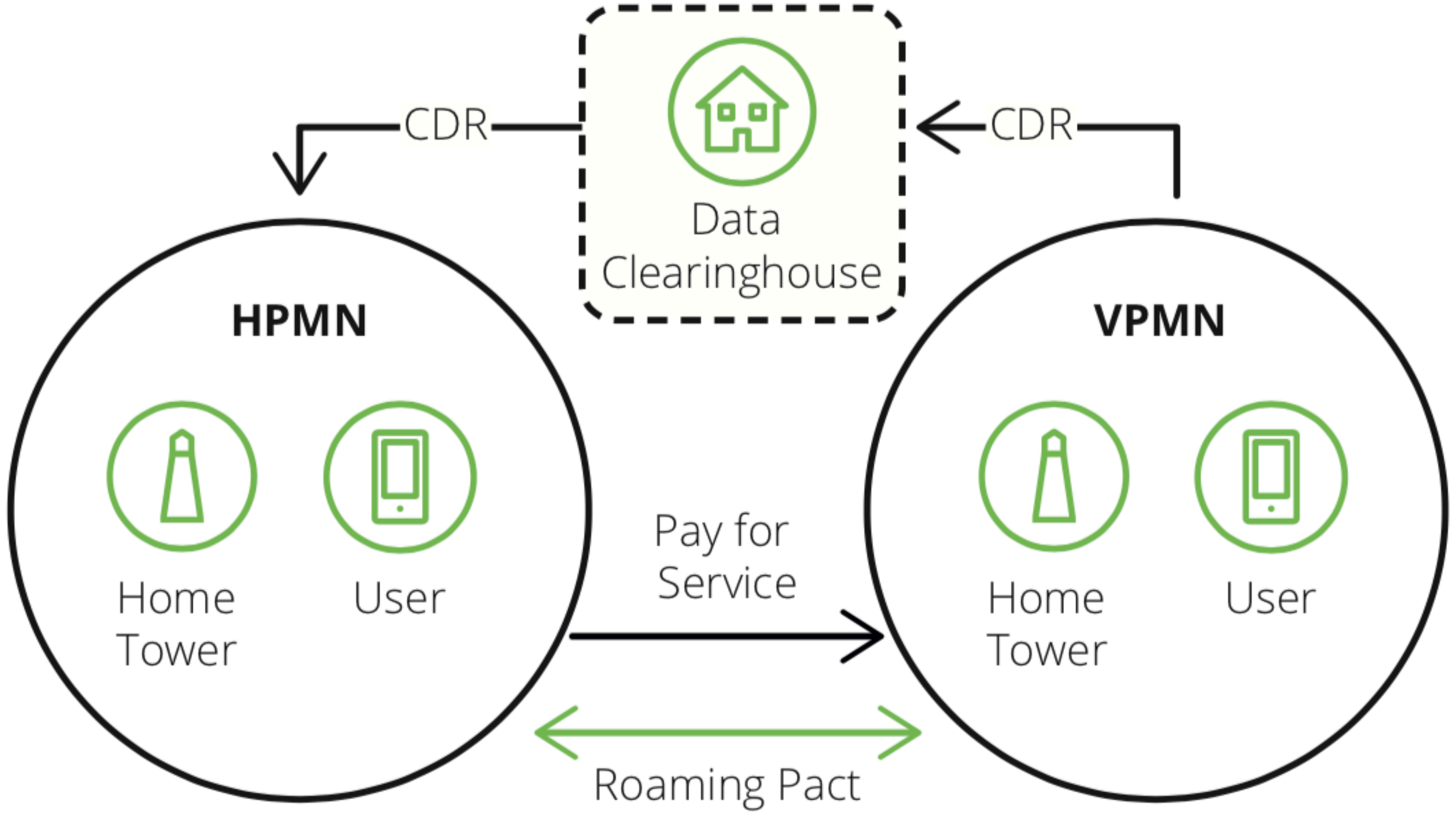
PORSCHE

Roaming Fraud Prevention

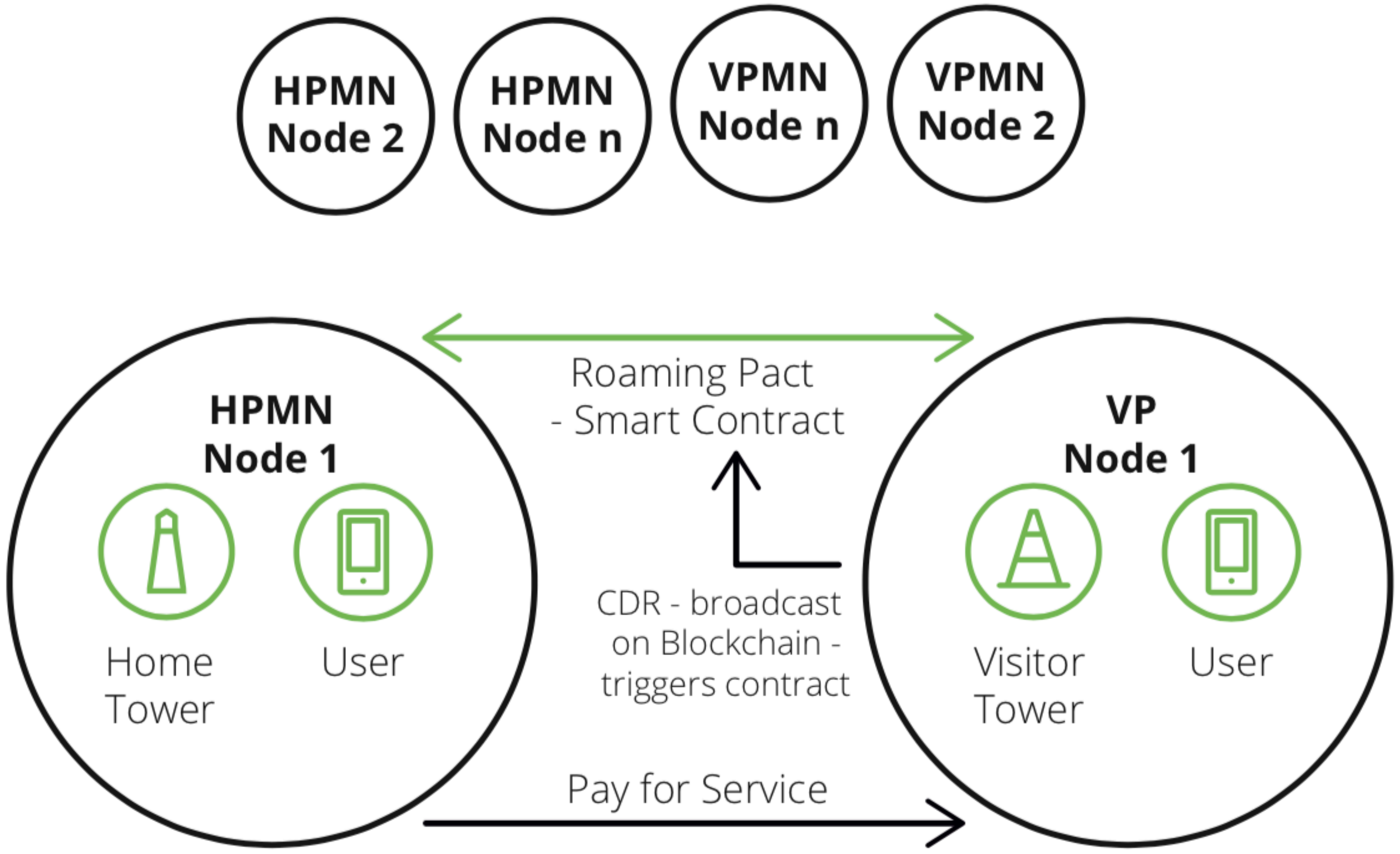
Problems: Longer detection time and longer response time

Benefits: Cost saving, smart roaming contract and easy to audit

Current System



Blockchain Alternative



Source: Blockchain @ Telco, Deloitte Monitor, 2017.

South Korean Telecoms Giant KT Has Built Its Own Blockchain

« With the launch, KT said it is now looking to employ the technology to authenticate users' identities in order to streamline international roaming services. The feature would allow users' information to be securely shared among global partners over a distributed network.

For the first stage of the plan, the telco said it will work with China Mobile and Japanese mobile operator NTT DoCoMo to start exploring the tech in international data roaming within the year.»

Source: Coindesk, Jul 24, 2018

Why not or limits

- Technologies are immature and rapidly evolving
  - Lack of interoperability
  - Lack of scalability
  - Providers are often small startups
- Megavendors are not up to speed… yet
- Not always better than existing technologies
- Regulations
- Value creation must be proven
- Lack of talents
- Code is not always law
- Code is not human

Take away: It is time to gain a deep understanding of blockchain threats and opportunities.

Technologies are overestimated in the short-term and underestimated in the long-term.

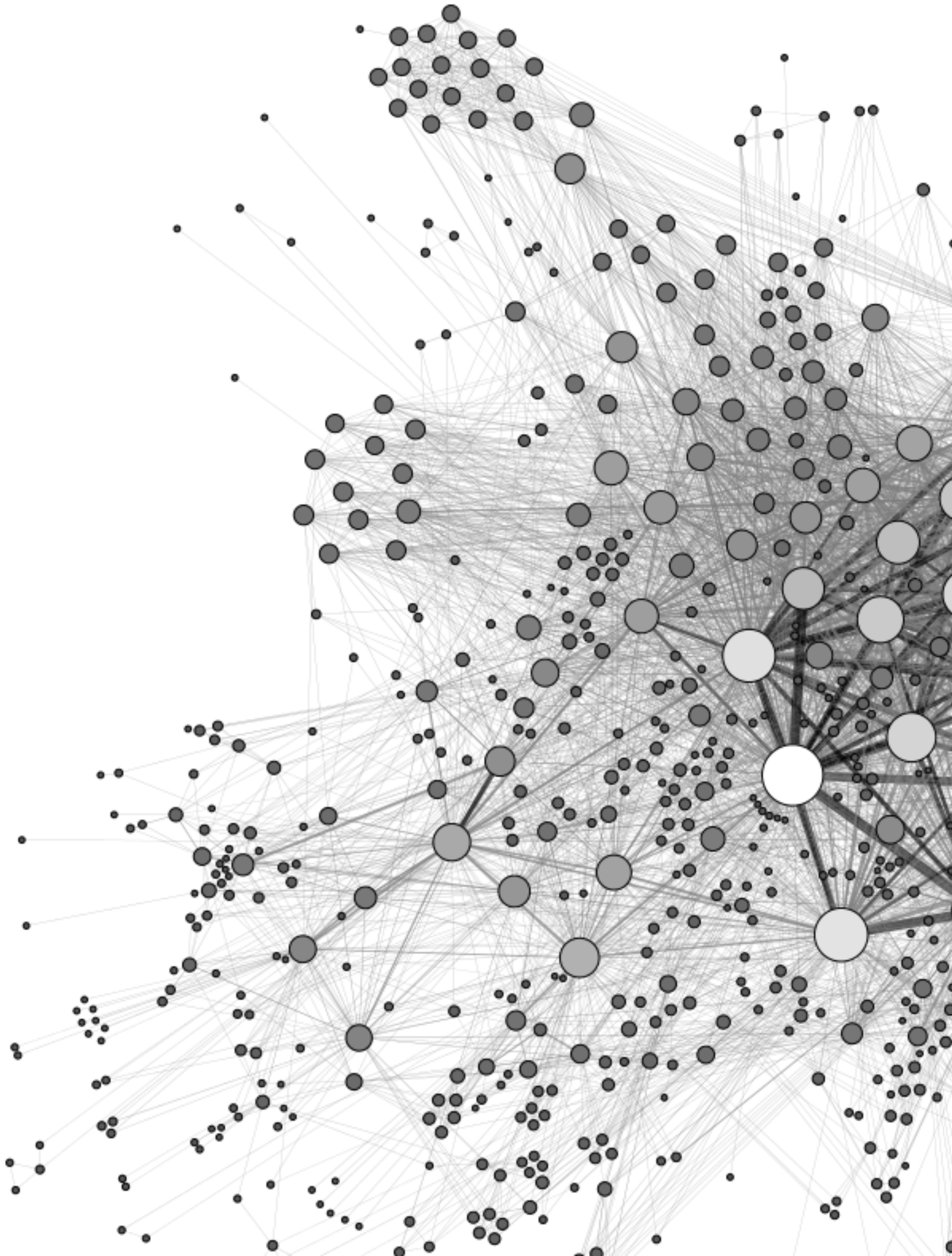
Thank you

Régis Barondeau, Ph.D.

Assistant Professeur management and technologie
ESG UQAM
barondeau.regis@uqam.ca

in linkedin.com/in/regisbarondeau

www.regisbarondeau.com



Reserve

Five critical challenges according to Gartner

- *Countering the potential threat from disruptive startups, especially if they have been able to substantiate their claims with compelling offerings and/or via significant capital support, e.g., from an ICO.*

- *Changing/influencing executives to adopt a new business mindset that centers on competing with decentralized operating and business models and thence, in particular, the redefinition of the enterprise role away from being a central intermediary in commercial activities.*

- *Filtering hype and marketing hubris from real data insights on maturity and progression by identifying business value for all needed parties in the ecosystem to stimulate investment and adoption.*

- *Stepping into blockchain evolution via an understanding and evaluation of "blockchain inspired" capabilities, e.g., those private and enterprise blockchains that lack tokenization and decentralization components.*

- *Understanding that blockchain's use as the primary system of record will be very intrusive to the current systems. Complexity in achieving that integration without any disruption to business will be challenging, and any dilution of the use will weaken the business case.*

Source: Hype Cycle for Blockchain Business, Gartner, 2018.

Functional BCP Classification Overview

BCP Class	1 - Native Utility Tokens No legal counterparty (decentralized ecosystem)				2 - Counterparty Tokens Natural/legal person as counterparty (relative right)					3 - Ownership Tokens Right in rem (absolute right)		
BCP Sub-Class	Basic Tokens	Infrastructure Access Tokens	Application Access Tokens	Application Settlement Tokens	IOU Tokens	Derivative Tokens	Fund Tokens	Equity Tokens	Membership Tokens	Joint-Ownership Tokens	Co-Ownership Tokens	Sole-Ownership Tokens
FINMA Equivalent	Payment Tokens	Payment and/or Utility Tokens			Payment, Utility and/or Asset Token	Asset Tokens			n/a	n/a		
Functionalities	Medium of exchange, unit of account and store of value providing access to an underlying technology (1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)
		Access to enhanced functionality infrastructure, i.e. SCS or burning mechanisms, without legal claim against a counterparty	Access to decentralized application or platform without legal claim against a counterparty (2)	(2)	Tokenization of a claim against a legal counterparty (e.g. right to receive funds, services or use infrastructure)	Tokenization of a claim	Tokenization of a fund share	Tokenization of a corporate membership	Tokenization of a personal membership	Joint-ownership of an asset, i.e. IP	Co-ownership of an asset, i.e. IP	Sole-ownership of an asset, i.e. IP
				Use as P2P settlement instrument on an application / platform		Value derives from an underlying on- or off-chain base value		Equity related shareholder's and financial rights				
Underlying Value	None	None	None	None	Debt / Claim	Derivative (debt)	Fund share	Equity share	Personal membership right	Ownership of an asset	Ownership of an asset	Ownership of an asset
Examples	Bitcoin, Bitcoin Cash, Litecoin, Monero, ZCash	Ether, Ether Classic, Cardano, Lisk, ICON, EOS	Wings	Siacoins, Mysterium, Filecoin	Lykke Colored Coins, "Utility Tokens" with counterparty	Modum	Blockchain Capital	Daura C-Shares	tba	tba	tba	tba

Key features

Implementation Approach

- Use cases being explored
- Cost and time to implement
- Business case
- Working partners (e.g., VCs, banks, etc.)

Overall consensus methodology

- Underlying methodology
- Nodes needed to validate a transaction
- Ownership of nodes
- Different stages of consensus and timing
- Fault tolerance
- Validator nodes – number and type
- Data storage

Tokenization (if used)

- Asset tokenization and life cycle
- Use of tokens
- Transaction signing
- Token security

Governance, risks, and control

- Enforcement of governance/controls
- Responsibilities and legal action
- Access control and admin privileges
- Types of nodes – read/write
- Risk mitigation measures
- Counterparty risk

Crytographer/ strength of algorithm

- Key generation and key life cycle
- Library and HSM integration
- System strictness
- Error monitoring

Performance

- Time to validate transactions
- Volume and value
- Scalability
- Number of fields per transaction
- Speed
- Synchronization

Privacy

- Verifiable authenticity
- Transparency and visibility into transactions
- Data encryption

Security

- Transaction activity monitoring
- Digital signatures
- Security testing and certifications
- Infrastructure hosting options and security architecture
- Preventing signature fraud
- Documentation
- Network synchronization

Figure 6: Distributed consensus evaluation framework

Consensus

1962
1970s
1976
1979
1982
1986
1987
1988
1990s
1994
1996
1997
1998
1999
2001
2002
2004
2006
2007
2008
2009
2012
2013
2014
2015
Jan 2016
Feb 2016
March 2016
Apr 2016
May 2016

"On Distributed Communications Networks", Paul Baran

Post-centralized mainframe distributed computing emerges

Public Key Infrastructure is introduced (GCHQ / Diffie Helman)

Ralph Merkle patents Merkle Tree Hashing technique

Byzantine Generals Problem paper published

Practical Byzantine Fault Tolerance (Paper Written)
– PBFT (Mechanism Developed)

Elliptic Curve Cryptography (Joseph H. Silveman)

DigiCash (David Chaum) in Netherlands first attempt at Crypto-currency based on his work on blinding formula

Viewstamped Replication

Cypherpunk movement becomes popular within parts of global Crypto community

Secure Hash Algorithm (SHA) first published by NSA

– Digital currency eGold based on Gold price

– RIPEMD encrypted hashing techniques first described in Belgium

Proof of Work consensus first discussed (Adam Back)

PayPal commences operations as global online payments platform

WebMoney digital currency attempt from Moscow

Napster, Kazaa, Limewire and BitTorrent show potential for P2P distributed computing

– Proof of Work
– (Developed)

Paxos

Sybil attack first described Brian Zill

More innovations in the field of Cryptography (Roger Heath-Brown)

Liberty Reserve is another failed attempt to create a digital currency

– Global Financial Crisis erodes trust in Financial Services

– Perfect Money yet one more attempt for a global digital currency

– August, Bitcoin.org domain name is registered

– Mencius

Bitcoin → – BNY Mellon Explores Bitcoin's Potential (Bitcoin)
– Bitshares

NXT

– Proof of Stake (Developed)

– ZAB

– Colored Coins (Paper)

– Colored Coins (Developed)

Copay

– RBFT (Redundant Byzantine Fault Tolerance)

– DAH (Digital Asset Holding) → – DAH announces plans with DTCC "to develop and test a distributed ledger based solution
– Tendermint (Founded)
– RAFT (Paper and Founded)
– Tangaroa (Paper and Founded)
– Eris → – Eris and 40 of the world's, largest and mostly systemically-important, banks join the R3 consortium
– Pebble
– DAG (Founded)
– Factom
– Chain
– Coinprism

– DPOS
– BitShares 0.X

Stellar

Ripple →

– Ethereum → – UBS begins developing blockchain implementation with Ethereum
– MultiChain
– Openchain
– CASPER

– Santander invests in Ripple

– CORDA (R3CEV Ledger) → – Barclays interest rate swap (Corda – Proof of Concept)
– Distributed Concurrence
– Derived PBFT (Hyperledger project)
– BigChainDB
– Distributed Proof of Stake
– PoET
– Juno → – JPMorgan Unveils 'Juno' Project at Hyperledger Blockchain Meeting

Evernym

– HSBC, Citibank, and other banks sign up for Distributed ledger startup R3CEV

– Sawtooth Lake → – Intel Unveils 'Sawtooth Lake' Proposal

Theoretical Papers

Actual Consensus definitions (currently being implemented)

Implementation attempts

Source: Consensus - Immutable agreement for the Internet of value, KPMG 2016