



BLOCKCHAIN 101

Demystifying the disruption beyond cryptocurrencies.

HELLO!

We are here because we love to interact with
blockheads.



“

"What the internet did for communications, Blockchain will do for trusted transactions."

-IBM Chief Executive Ginny Rometty.



Blockchain: Disruptive Innovation

Distributed digital ledger containing immutable, cryptographically secure transactions added only by peer consensus and governed with auto-triggering smart contracts, eliminating the need of third party intermediaries.

Simply put, blockchain is a

Digitally protected, de-centralised, distributed ledger.



Ledgers are everywhere

Any time we need a **consensus** about **facts**, facts underpinning the modern economy.

Why?

- Ledgers confirm ownership
- Ledgers confirm identity
- Ledgers confirm status
- Ledgers confirm authority





Source: KPMG Research

ADVANTAGES OF BLOCKCHAIN



Efficiency

Using the "if-this-then that" logic of smart contracts can reduce error reduction and increase speed.



Transparency

Get real-time insights into trades and transactions rather than just receiving reports in different formats at different times from different institutions.



Trust

The majority of participants in a blockchain system need to approve the transactions and agree upon which data is written, altered or removed.



Resilience

The larger the number of blockchain participants the more robust the data is, as it can be seen as a massively replicated database.





Banking, Financial Services & Insurance

(Fx Settlement, Cross Border Payments, Trade Finance, OTC Derivative Contracts)



Technology & Media

(Media & Usage Rights, Intellectual Property)



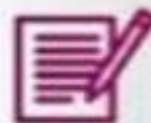
IoT



App



Authentication



Smart Contract



Transparency



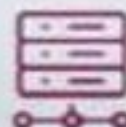
Security



Efficiency



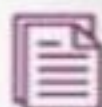
Disintermediation



Data Storage



Digital content



Document Storage & Delivery



Digital Identity



Travel & Transportation

(Loyalty point program, Bookings, Records)



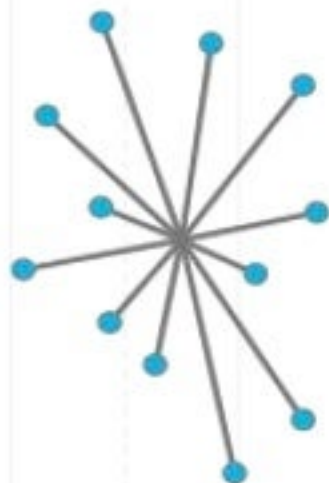
CPG, Retail & Manufacturing

(e-commerce, Marketplace, Home Automation)

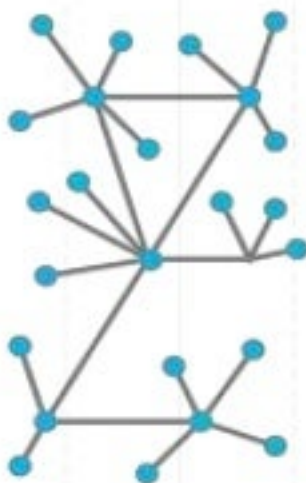
Blockchain
(Chronological & Immutable)

Understanding Networks

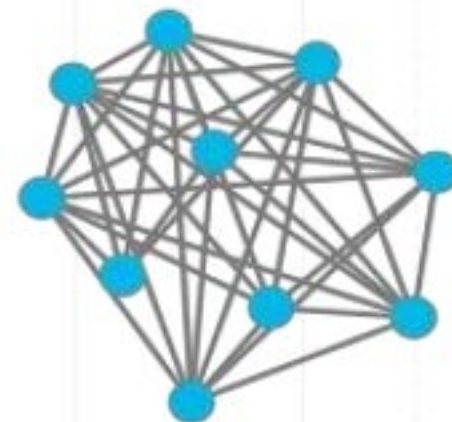
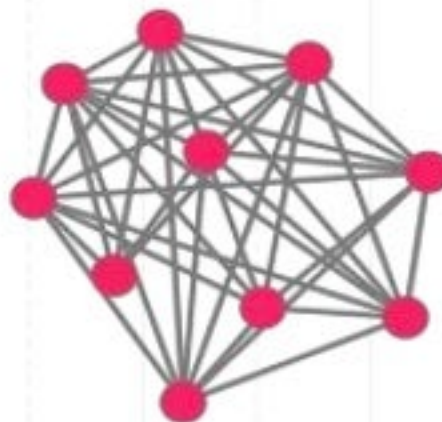
Centralized



Decentralized



Distributed Ledgers



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous
- Each user has a copy of the ledger and participates in confirming transactions independently

- Users (●) are not anonymous
- Permission is required for users to have a copy of the ledger and participate in confirming transactions



Blockgeeks

MOST IMPORTANT BLOCKCHAIN-RELATED TERMS



Validate and approve transactions, connecting the blocks to a Blockchain.

Miners

Cross-industry standard for distributed ledgers.



Hyper-ledger



centralised



decentralised



distributed

Book containing records of all transactions by all users in a network.

Distributed Ledger

Blockchain Technology terms

Cryptography

Provides proof that records in the public ledger cannot be changed. Any attempt to tamper is apparent immediately.



Mathematical scrambling (digital fingerprint) used to boil down information, like a PDF or DOC, into a code known as a hash.

Hashing

Digital Currencies



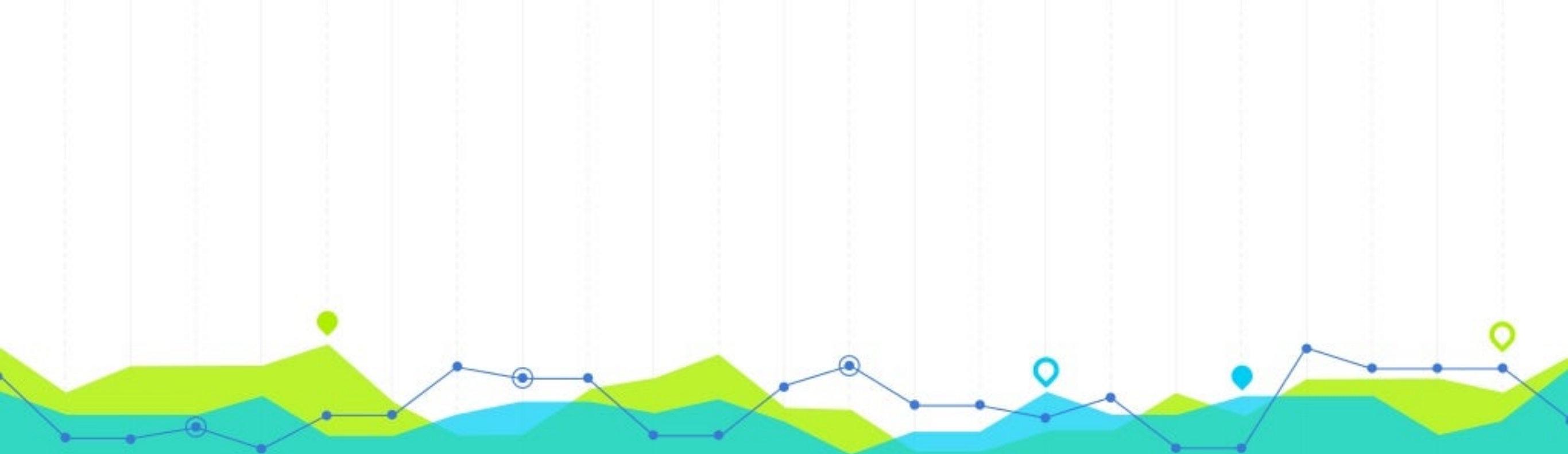
Internet-based form of money (in the form of an online code) that can be used like other currencies.

sources: Moody's Investors Service, 2016; WEF & Deloitte - The future of financial infrastructure, 2016

Myths Busted

With every new technology, there is hype and there is reality.

- Myth 1. There is a Singular Blockchain
- Myth 2. Blockchain is All About Money
- Myth 3. Blockchain and Bitcoin are the Same Thing
- Myth 4. Blockchain is the Solution to Fraud
- Myth 5. Blockchains are Immutable
- Myth 6. Blockchain is Cost Effective and Cheap
- Myth 7. Only Big Companies Can Use Blockchains



Variations of Blockchains

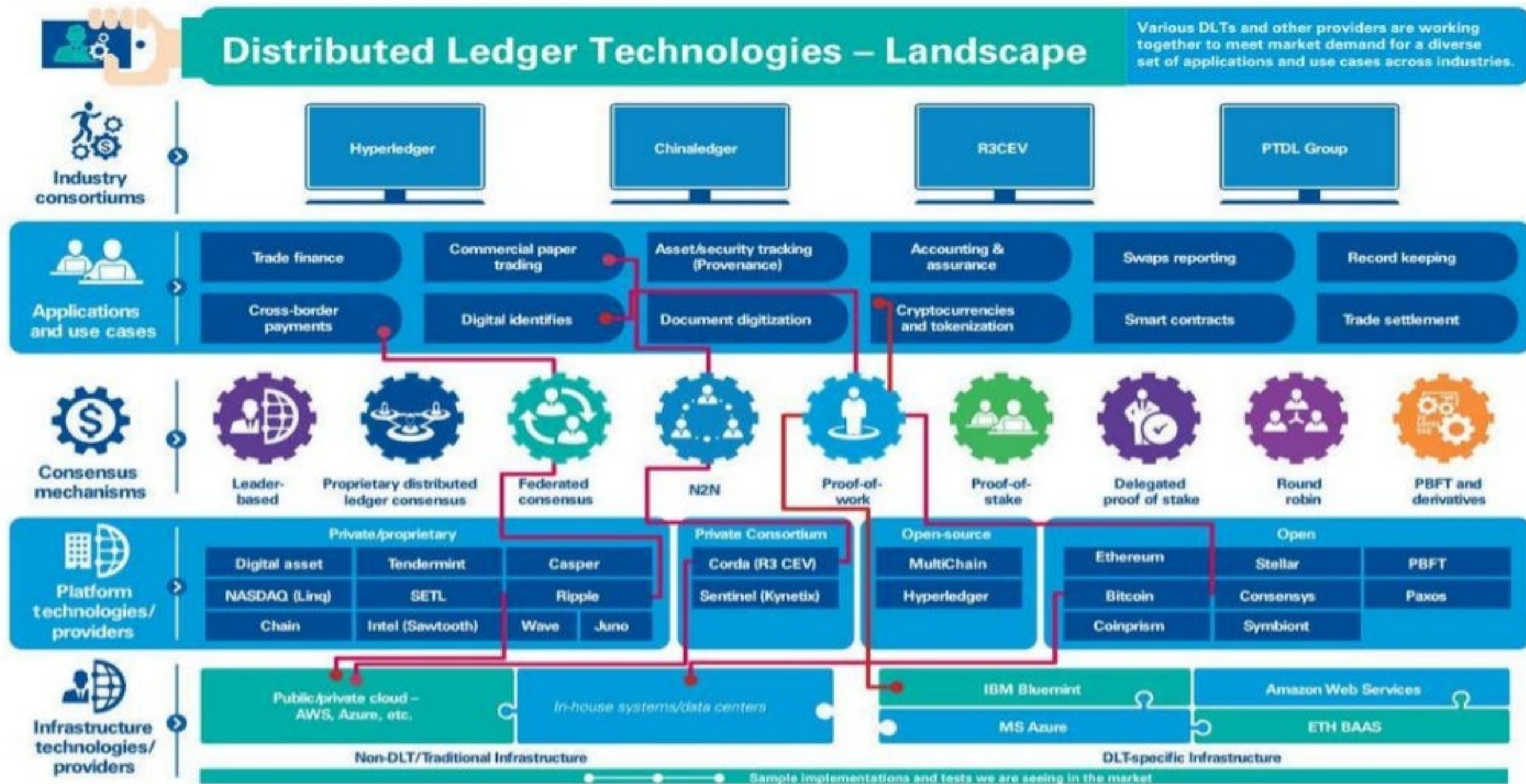


Public (open) vs. Private Blockchain (closed)

	Public	Private
Access	Open read/write access to database	Permissioned read/write access to database
Speed	Slower	Faster
Security	Proof-of-Work/ Proof-of-State	Pre-approved participants
Identity	Anonymous/Pseudonymous	Known identities
Asset	Native Assets	Any asset
Costs	Expensive	Cheaper



Figure 4: Illustrative distributed ledger technologies



Features	Bitcoin Blockchain	Hdac Blockchain	Ethereum Blockchain
Main Features	Financial Transactions (Bitcoin script)	IoT friendly blockchains, Public/Private blockchains	Smart Contracts (Solidity, Serpent etc.)
Consensus Algorithm	Proof of Work	ePoW, Trust-based	Current: Proof of Work Future: CASPER PoS
Transaction Speed	7 tx/sec	~160 tx/sec (public)* ~ 500tx/sec (private) 1000 tx/sec (target)	25 tx/sec
Block Time	10 minutes	3 minutes	12 seconds
Block Size	1MB	Dynamic (Max. 8 MB)	Dynamic
Extra Data	80 Byte (OP_RETURN)	Dynamic (Max. 4 Kb)	Dynamic (5 gas / byte)
Topology	Public blockchain	Private/Public blockchains, Permissioned blockchains	Public blockchain, Permissionless blockchain



LIMITATIONS OF BLOCKCHAIN TECHNOLOGY



Block size

The limited block size of 1MB restricts the number of possible transactions per second. A larger block will, on the other hand, increase the time taken until each block is verified before it can be added to the Blockchain.



Scalability

More computational power and stronger hardware is needed to solve the complicated mathematical problems of every transaction. It is expensive to operate with larger blocks.



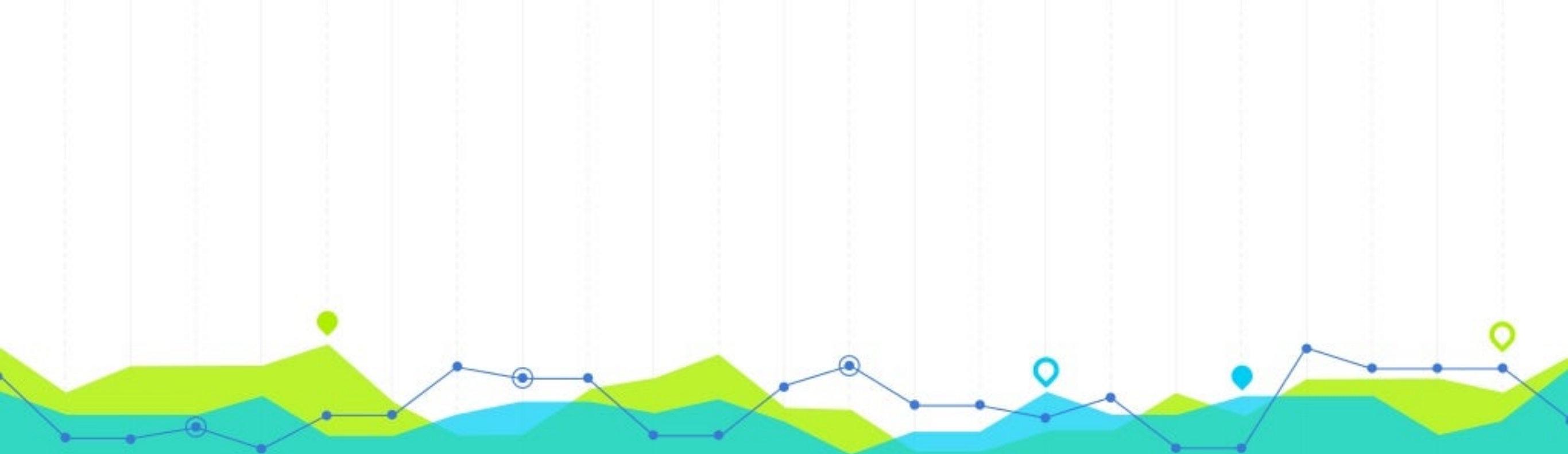
Standards

To use Blockchain on an industrial scale, there must be certain industry standards as well as legal and governance frameworks to improve robustness, overall performance and security of the technology.



Diverging interest

Replacing existing financial infrastructure will require time and investment. With competing interests between different parties, it will take time to find common ground for collective action.



Applications & Key Players

Non-Financial Use Cases

Digital Content/Documents, Storage & Delivery



BitProof, Blockcal, Ascribe, ArtPlus, ChaiLink, Stampery, Blocktech (Alexandria), Bisantium, Blockpart, The Rudimental, BlockCDN

Authentication & Authorization



The Real McCoy, Degree of Trust, Everpass, BlockVerify,

Digital Identity



Sho Card, Uniquid, Onename, Trustatom

Marketplace



Providing premium rights & brand based coins: MyPowers

Smart Contracts



Otonomos, Mirror, Symbiont, New system Technologies

Real Estate



Factom

Diamonds



Everledger

Gold & Silver



BitShares, Real Asset Co., DigitalTangible (Serica), Bit Reserve

Reviews/Endorsement



TRST.im, Asimov (recruitment services), The World Table

Blockchain in IoT



Filament, Chimera-inc.io, ken Code – ePlug

App Development



Proof of ownership for modules in app development: Assembly

Network Infrastructure & APIs



Ethereum, Eris, Codius, NXT, Namecoin, Colored Coins, Hello Block, Counterparty, Mastercoin, Corona, Chromaway, BlockCypher

Other



Prediction platform:
Augur
Election Voting: Follow My Vote
Patient Records management: BitHealth

Financial Use Cases

Currency Exchange & Remittance



Coinbase (Wallet), BitPesa, Billion, Ripple, Stellar, Kraken, Fundrs.org, MeXBT, CryptoSigma

P2P Transfers



BTC Jam, Codius, BitBond, BitnPlay (Donation), DeBuNe (SME's B2B transactions)

Ride Sharing



La'zooz

Data Storage



Storj.io, Peernova

Trading Platforms



equityBits, Spritzle, Secure Assets, Coins-e, DXMarkets, MUNA, Kraken, BitShares

Gaming



PlayCoin, Play(on DACx platform), Deckbound

Blockchain Applications by Sector (selected)

Economics and Markets

- Currency
- Payments & Remittance
- Banking & Finance
- Clearing & Settlement
- Insurance
- FinTech
- Trading & Derivatives
- QA & Internal Audit
- Crowdfunding

Government & Legal

- Transnational orgs
- Personalized governance services
- Voting, propositions
- P2P bonds
- Tele-attorney services
- IP registration and exchange
- Tax receipts
- Notary service and document registry

IOT

- Agricultural & drone sensor networks
- Smarthome networks
- Integrated smartcity, connected car, smarthome sensors
- Self-driving car
- Personalized robots, robotic companions
- Personalized drones
- Digital assistants

Health



- Universal EMR
- Health databanks
- QS Data Commons
- Big health data stream analytics
- Digital health wallet
- Smart property
- HealthToken
- Personal development contracts

Science, Art, AI

- Community supercomputing
- Crowd analysis
- P2P resourcenes
- Film, dataviz
- AI: blockchain advocates, friendly AI, blockchain learners, digital mindfile services

Crucial Blockchain Properties

- Cryptolegger
- Decentralized network
- Trustless counterparties
- Independent consensus-confirmed transactions

- Permanent record
- Public records repository
- Notarization time-stamping hashes
- Universal format
- Accessibility

- Communication (messaging)
- Large-scale coordination
- Entity ingress/egress
- Transaction security

- Universal format
- Large-scale multi-data-stream integration
- Privacy and security
- Real-time accessibility

- Large-scale infrastructural element for coordination
- Checks-and-balances system for 'good-player' access

APPLICATIONS & SOLUTIONS

Brokerage



Exchanges



Soft Wallets



Hard Wallets



Investments



Microtransactions



Capital Markets



Money Services



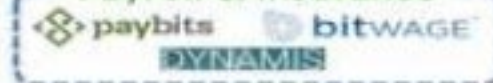
ATMs



Trading Platforms



Payroll & Insurance



Compliance



Payments



Financial Data



Trade Finance



MIDDLEWARE & SERVICES

Services



Software Development



General APIs



Special APIs



Platforms



Smart Contracts



INFRASTRUCTURE & BASE PROTOCOLS

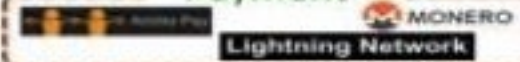
Public



Special



Payment



Miners



Banks and Other Financial Services Firms Exploring Blockchain



Central Concept Being Explored

✓ Private blockchain

✓ Semi-private blockchain

Application Areas

- Asset registries, smart contracts, smart shares, smart bonds
- Trading
- Cross-border payments and digital payment system
- Trade execution and settlement
- Digital security
- Risk management
- Post-trade processing services
- Regulatory reporting, KYC, AML
- Faster payments

Source: GrowthPraxis

Infrastructure Providers / Partners



Countries with high density activity in blockchain



Israel



U.S.A



U.K



Singapore



Australia



Sweden



Netherlands

Understanding the Application of Blockchain technology in Logistics & Supply chain Management



Six Ways Blockchain would disrupt Insurance Sector



Event-triggered smart contracts

- Automated claims
- Self-executing contracts
- Reduced fraud, improved customer experience



Increased back-end efficiency

- Decentralized, fully digital, safer markets
- Less human error, no data duplication
- Less processing delays, transaction costs



Disintermediation

- Decentralized carrier consortium
- Automatic identity validation
- Self-executed transactions



Better pricing and risk assessment

- Real-time, individualized
- Automatic data sharing for analytics and pricing
- Connected to IoT, Big Data, health trackers



New types of insurance

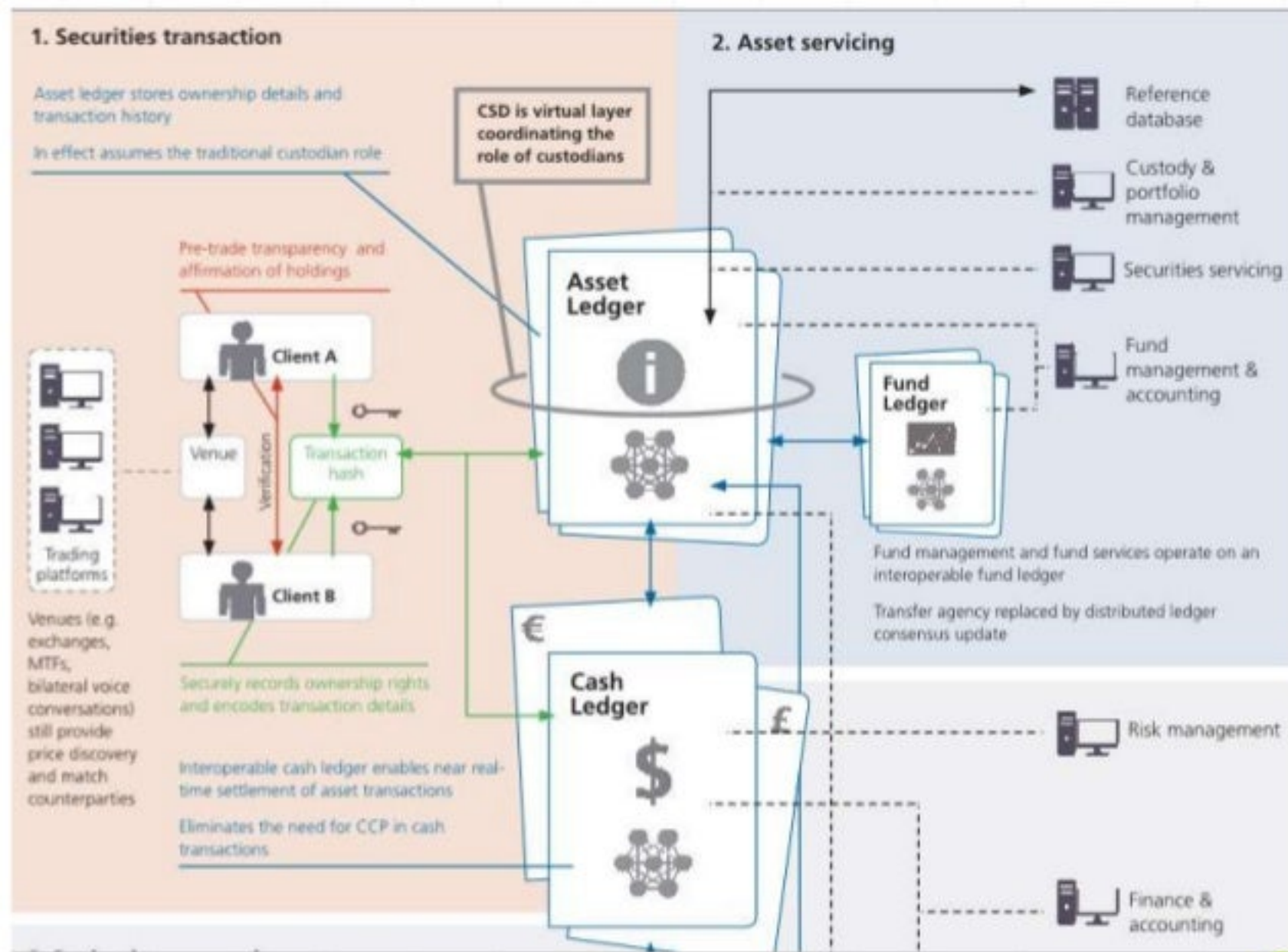
- P2P, shared economy, spot-insurance, hybrids
- More transparency, less costs
- Social media and crowdsourced oracles



Reaching the underserved

- Solves many microinsurance challenges
- Automatic construction of distributed database
- Better prices through simplicity and efficiency

Understanding the Application of Blockchain technology in securities transactions and Asset Servicing





The Blockchain Technology Framework

OTHER

R3 CEV Bank Consortium

APPLICATIONS
(Products & Services)



BITCOIN NETWORK BASED

PAYMENT PROCESSOR

BITPAY

CIRCLE

EXCHANGE

COINJAR

BITSTAMP

KRAKEN

COINBASE

MORE

TRADING PLATFORM

HEDGY

Product: Bitcoin Trading Platform

LedgerX

Product: Bitcoin Options Trading Platform

TeraExchange

Product: Bitcoin Swap Trading Platform

ISSUANCE PLATFORM

LIQ (NASDAQ)

Product: Private Issuance Platform

t5

Product: Debt & Equity Trading Platform

NON-BITCOIN NETWORK BASED



BLOCKCHAIN TOOL PROVIDERS

CHAIN

Tools: Bitcoin API's & Tools

SYMBIONT

Tools: Smart Contract API's & Tools

BLOCKSTREAM

Tools: Sidestream

MONETAGO

Tools: Bitcoin API's & Tools

CONSENSYS

Tools: API's and Tools for Ethereum, bitcoin and private permissioned ledgers

BLOCKAPPS

Tools: API's and Tools that are compatible with Ethereum

ERIS INDUSTRIES

Tools: Smart Contract apps on Eris software network using Tendermint and Ethereum compatible

DAH

(Digital Asset Holdings)
Tools: API's & Tools for Financial Services

ITBIT

Tools: API's & Tools for Financial Services using Blockchain

INFRASTRUCTURE ADD-ON

COUNTER PARTY

Infrastructure: Smart Contracts

ROOTSTOCK

Infrastructure: Smart Contracts

INFRASTRUCTURE
(Blockchain Networks)

NON PERMISSIONED PUBLIC LEDGER

BITCOIN BLOCKCHAIN

Currency: Bitcoin
Settlement Process: Proof of Work
Ledger Owner: All Users

ETHEREUM

Currency: Ether
Settlement Process: Proof of Work
Ledger Owner: All Users

TENDERMINT

Settlement Process: Consensus (Proof of Stake)

PERMISSIONED PUBLIC LEDGER

HYPER LEDGER

Settlement Process: Proof of Work
Ledger Owner: All Users

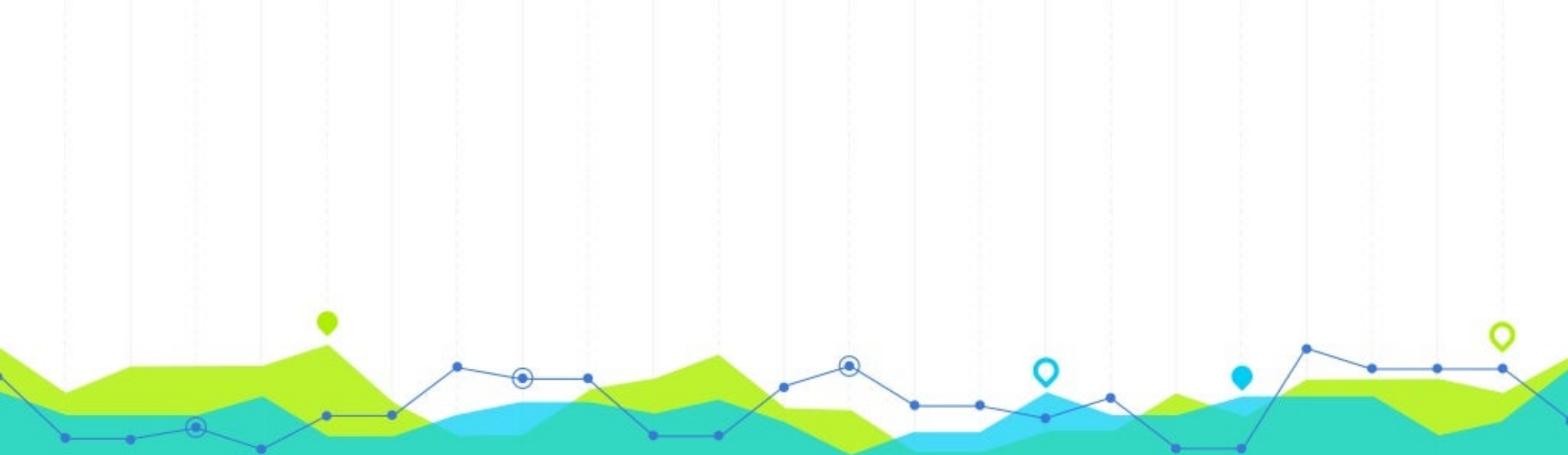
RIPPLE

Currency: XRP
Settlement Process: Consensus
Ledger Owner: Trusted Parties

PERMISSIONED PRIVATE LEDGER

BANKCHAIN

Settlement Process: Consensus
Ledger Owner: R3



The Timelines

BLOCKCHAIN TIMELINE

PIONEERS
DISCOVER



October 2008:

Bitcoin whitepaper by the nom-de-plume Satoshi Nakamoto is published.

LHVpank

June 2014:

LHVpank starts research on Blockchain and its digital security with their app "Cuber Wallet".



September 2015:

Major financial companies form R3 – a consortium of over 40 institutions committed to exploring and implementing Blockchain technology.



September 2016:

Over 40 financial service institutions have invested in a Blockchain or Bitcoin startup since 2014.

May 2010:

First Bitcoin purchase: BTC 10k for a \$25 pizza. Today BTC 10k is worth \$10m! Bitcoin is known as the first use case of Blockchain technology.



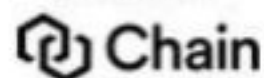
July 2014:

Ethereum Project – a Blockchain platform with the ability to build decentralized applications – is funded by a crowd sale.



September 2015:

Visa, Citi, Nasdaq, Capital One and Fiserv invest \$30m in the Blockchain startup Chain.com.



2018:

WEC estimates that 80% of all banks will initiate projects concerning distributed ledger technology – the underlying technology supporting Blockchain.



13

- Started research on blockchain with specific interest in digital security
- Developed 'Cuber Wallet', an app based on 'Colored Coins' (June 2015)
- Partnerships: Coinbase & CoinFloor

UHVbank
June 2014

- Areas of interest: Faster payments & banking services
- Partnership: Rabobank partnered with Ripple Labs

ING
Rabobank **ABN-AMRO**
Dec. 2014

- Accelerator program with Safello, Atlas Card & Blocktree
- Partnered with Safello in June 2015 to test banking services on blockchain

BARCLAYS
Mar. 2015

CommonwealthBank

- Areas of Interest: Payment settlement
- Partnership: Ripple Labs



- Research team studying Bitcoin
- May 2015

SOCIETE GENERALE **BNP PARIBAS**

- Societe Generale has started staffing employees with BTC, blockchain & cryptocurrency expertise
- BNP Paribas is exploring faster transactions with blockchain

citi

- 3 separate systems within Citi that deploy blockchain technology
 - Developed an equivalent to Bitcoin, called 'Citicoins'
- July 2015

Oct. 2013



- Areas of interest: Digital currency exchange (Oct. 2013), money transfer services (May 2014) & BTC trading (Feb. 2015)
- Partnerships: Karken, Bitcoin Deutschland GmbH, Ripple, Bitcoin.de

Sep. 2014



- Areas of interest: Risk management system & cross border payments
- Partnership: Ripple Labs

Jan. 2015



- Participated in a \$75 Mn Series C funding for Coinbase (Jan. 2015)

Apr. 2015



- Areas of Interest: Payments, trading & settlement, Smart bonds
- Partnership: Mentoring London based FinTech startups in blockchain

June 2015



- Claims 20-25 use cases for blockchain and that ~GBP 12 Bn could be saved in banks infrastructure by switching to blockchain concept.
- Areas of interest: international payments and smart contracts



- Areas of interest: Payments and Banking services
- Partnership: Ripple Labs

2017-2020:
Shared Infrastructure Emerges

2016-2018:
Proof of Concept

2014-2016:
Assess Blockchain's Value for
Financial Assets

2014-2016: Assess Blockchain's Value for Financial Assets

- Banks and other financial infrastructure intermediaries (FIs), including Central Depositories, Exchanges, & Technology Vendors, size potential efficiencies from permissioned, shared, secure distributed ledgers
- Banks and financial infrastructure intermediaries form industry groups to discuss opportunities
- R3
- Linux Hyperledger Foundation

2016-2018: Proof of Concept

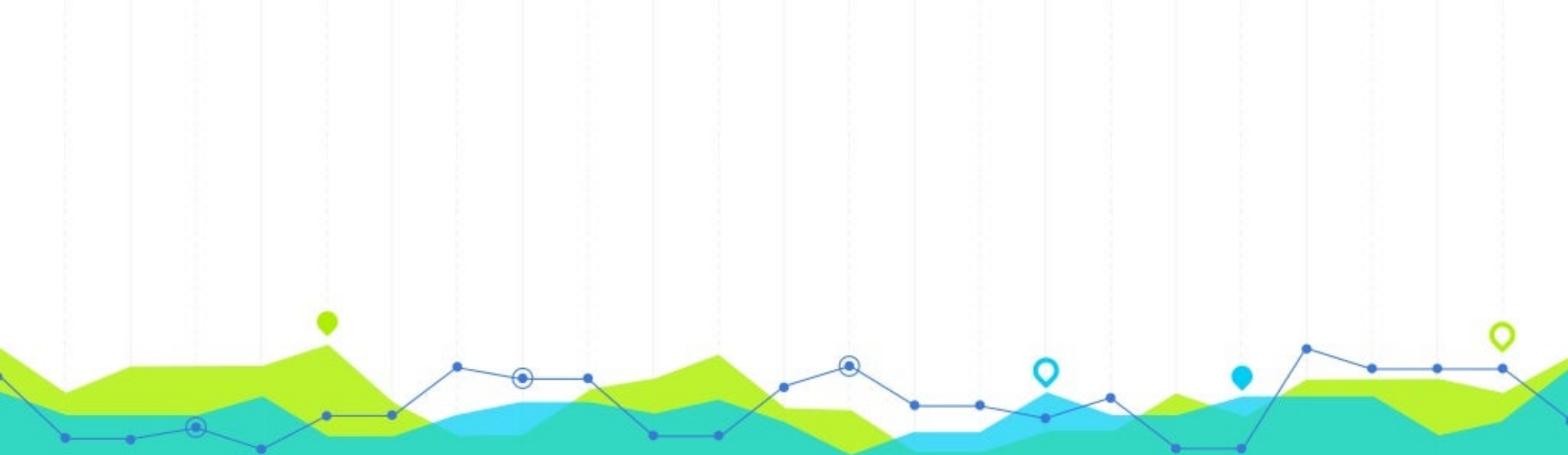
- Banks and FIs tee up specific assets as a test case for Blockchain
- CDS
- Repo settlement
- Corporate syndicated loan settlement
- Trade finance
- International currency transfer
- Exchanges for post trade settlement
- POC Goal: Assess if Blockchain can scale and reduce costs
 - 1) Does Tech work and scale
 - 2) Does the asset transact between buyer and seller smoothly
 - 3) Does it offer benefits beyond existing technologies on a performance, cost, speed, scale analysis
- Fails are de minimis
- POC Tiering: Segment into most to least important assets to address
- Focus resources on most important assets, most inefficient processes
- Engage regulators, lawyers, auditors

2017-2020: Shared Infrastructure Emerges

- Proven assets adopted well beyond initial POC group
- Develop interface for external users
- Leverage APIs
- Reduce costs with fewer heads and increased mutualization of infrastructure costs

2021-2025: Assets Proliferate

- More assets move onto Blockchain as efficiencies prove out

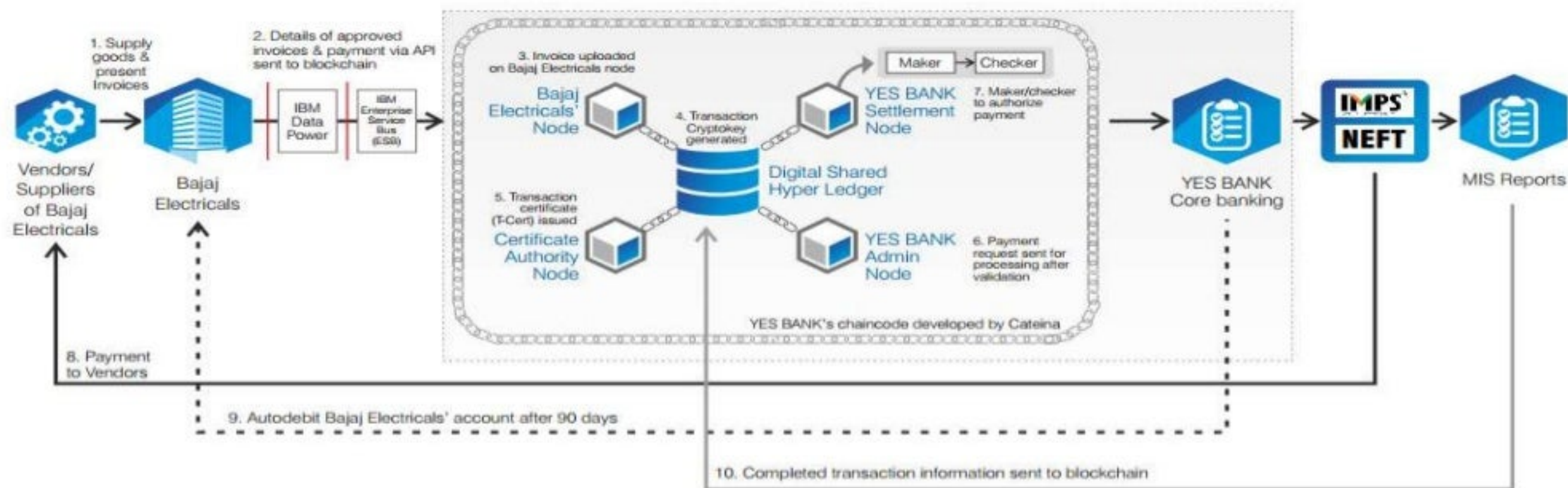


Use -Cases

How to Identify the Use - Case

- Multiple parties use the data , want to update the data
- Transactions are interdependent on each other's transactions
- CUMBERSOME TO TRACK THE progress of the requested transactions
- Risk and severity of fraudulent transactions is very high
- Intermediaries are adding cost delays complexity
- Mandatory requirement for verification of transactions
- Manual document processing and reconciling the information
- Two transaction parties only trust a third party intermediary
- Assets need to be backed up in real time

Multi-nodal Vendor Financing on Blockchain



IBM Blockchain Platform

Deliver production ready service with speed and at scale with the new IBM Blockchain Platform

- Based on Hyperledger Fabric V1 runtime optimized for enterprise requirements
- Specialized compute for security, performance and resilience
- Delivered via the IBM Cloud on a global footprint with 24x7 Integrated Support
- Full lifecycle tooling to speed activation and management of your network

Develop

Explore and accelerate development time with tools that ensure close alignment between business leaders and developers

Govern

Speed activation, customization and management of your business network with democratic, multi-party governance tooling

Operate

Deploy and operate always-on networks with production-ready enterprise performance and security for most demanding use cases



Benefits Drawn by implementation of Blockchain Technology



NASDAQ LINQ

Trade recording reduced from 3 days to 10 mins and settlement risk exposure reduced by 99 %.



Kotak Mahindra

Cross border remittance initially taking about 2 days reduced to near real time



IBM Supplychain finance

Supply chain financing solution can be reduced from 12 – 16 days to less than 2 days.



BNP Paribas Securities

Is planning to adopt blockchain for \$747bn assets.



Barklays- Wave

Trade finance transactions brought the signoff time from 10 days to 4 hours. Reduced cost added transparency and improved customer experience



Northern Trust Bank

Estimates saving of 6bn annually in streamlining and clearing and settlement cash securities.



Global Average Cost of USD \$100 Remittance

Method	Commercial Banks	Online Platforms	Blockchain
Total Average Cost (%)	10.64%	5.43%	~1.10%
Total Average Cost	\$10.64	\$5.43	\$1.10



Strengths	Weaknesses
<ul style="list-style-type: none"> ▪ Distributed resilience and control ▪ Decentralized network ▪ Open source ▪ Security and modern cryptography ▪ Asset provenance ▪ Native asset creation ▪ Dynamic and fluid value exchange 	<ul style="list-style-type: none"> ▪ Lack of ledger interoperability ▪ Customer unfamiliarity and poor user experience ▪ Lack of intraledger and interledger governance ▪ Lack of hardened/tested technology ▪ Limitation of smart contract code programming model ▪ Wallet and key management ▪ Poor tooling and poor developer user experience ▪ Skills scarcity and cost ▪ Immature scalability ▪ Lack of trust in new technology suppliers
Opportunities	Threats
<ul style="list-style-type: none"> ▪ Reduced transaction costs ▪ Business process acceleration and efficiency ▪ Reduced fraud ▪ Reduced systemic risk ▪ Monetary democratization ▪ New business-model enablement ▪ Application rationalization and redundancy 	<ul style="list-style-type: none"> ▪ Legal jurisdictional barriers ▪ Politics and hostile nation-state actors ▪ Technology failures ▪ Institutional adoption barriers ▪ Divergent blockchains ▪ Ledger conflicts/competition ▪ Poor governance

Approach to Build Your Blockchain Empire

Discover

- Develop key understanding of the technology, Identify which problems need to be addressed
- Asset gaps, re-engineering processes, Re-Align stakeholders – workshops explaining intent, approach and benefits

Analyze

- Feasibility analysis- Operational effectiveness
- Risk Assessment : Impact to existing system
- Regulatory compliance assessment

Define

- Design in house
- Start with non-permissioned public ledgers, Go private/permissioned ledgers or consortium
- Define distributed network, roles, smart contracts Speed, stability, scale, data limits, privacy for eyes

Implement

- Collaborate- design interoperability and standards, Partner with fintech and build the stack
- Sandbox tests Pocs for defined processes, Test for transaction stability security scalability and BCP

Go Live

- Rollout plan identify stable geographies
- Gap assessment immediate fixes
- Fine tune if no cost , turn around time etc gains





THANKS!

Any questions?

You can find us at

LinkedIn  Jithin Babu
Sakshi Manthanwar



Jargons.. Just for fun

- **HODL** – “HODL” was originally a typo for HOLD
- **TO THE MOON** - a crypto's upward momentum
- **ADDY** - cryptocurrency public address (or key)
- **ATH** – All time high
- **WHALE** – a trader with a fat account
- **REKT** – a misspelling of “wrecked”
- **FUD** - Fear, uncertainty, and doubt



when stop rekt?

