Lessons Learned From Industrializing Blockchain Technology

March 2019

Paul R Brody

Principal, Global Blockchain Leader
San Francisco

@pbrody
linkedin.com/ln/pbrody

Building a better working world

So Far, So Predictable

Vision Compared To What Actually Works

5 Lessons Learned

Where Blockchain Goes Next

So Far, So Predictable

Vision Compared To What Actually Works

5 Lessons Learned

Where Blockchain Goes Next

The collapse in crypto-asset prices was entirely predictable given the hype and impossible expectations

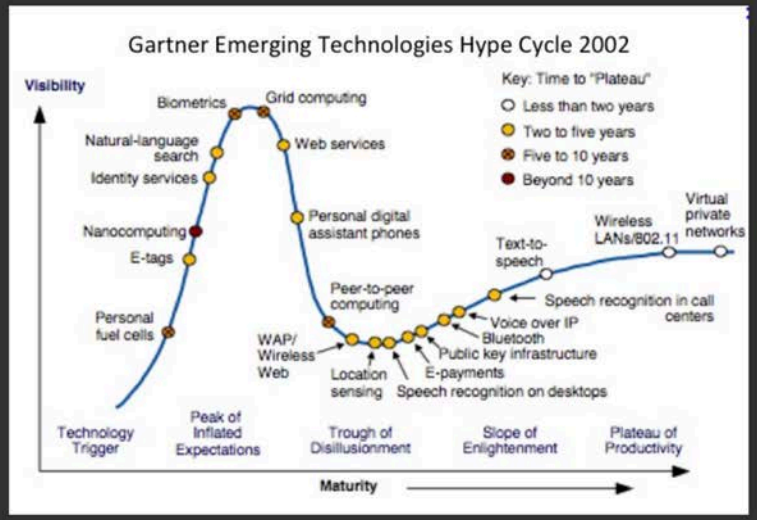
The NASDAQ from 1997 to 2002

The collapse in crypto-asset prices was entirely predictable given the hype and impossible expectations

BitCoin from Dec 2016 to Dec 2018

Fortunately, the ups and downs of the hype cycle have little impact on the eventual adoption of a technology

Yes, blockchains are way overhyped. They are still the biggest software innovation in 50 years.



- Most of the technologies that were being ”dissed and dismissed” in 2002 are standard today.
- Foundations for market success are laid after the hype but long before a market matures

Page 13 Source: Gartner Hype Cycle, 2002 – Internal EY Use Only

When we set out to build start systematically driving blockchain investment four years ago, we set expectations with our leadership team that real adoption curves are not 1-2 year programs, they take a decade or longer and the real work is done long after the hype dies down.

In relatively a short period of time, blockchain has become a truly global business for EY

What started in a couple cities is now a global network of technologists working together:

- Growing consistently year to year at around 300%
- Sharing key lessons learned around success & failures
- Investing in IP and patents that will help realize our vision

Development:

- Trivandrum, India
- San Jose, Costa Rica
- Madrid
- Cambridge, MA

Research Sites:

- London
- Paris
- Tel Aviv

Client-Facing Locations:

- London
- Paris
- Munich
- Rome
- Manila
- Tel Aviv
- Singapore
- Tokyo
- Shanghai
- Seoul
- Seattle
- San Francisco
- New York
- Toronto

So Far, So Predictable

Vision Compared To What Actually Works

Lessons Learned

Where Blockchain Goes Next

At the heart of our solution is a vision of how blockchains can become central to enterprise applications

Blockchains will do for networks of enterprises and business ecosystems what ERP did for the single company.

EY currently offers 8 major blockchain solutions, of which we have developed 7 in-house

Blockchain Applications

OpsChain for Supply Chain Management

- Tokenize & manage supply chains
- Procurement & sales

OpsChain for Food Traceability

- Wine blockchain
- Works for all food types

OpsChain Intercompany

- Enabling transactions within large enterprises

Insurwave Maritime Insurance

- Shipping insurance JV with Guardtime & others

Distributed Contracting Network

- Contract management
- Starting with X-Box

Tesseract

- Smart, connected asset management with IoT

Public Financial Management

- Accountability for public spending programs

Blockchain Analytics

Blockchain Analyzer
Audit & assurance foundation

Public Blockchain Analytics

Private Blockchain Analytics

Tax Liability Calculation

Smart Contract Testing

The origin of our blockchain business is the need to audit cryptocurrency transactions as investments

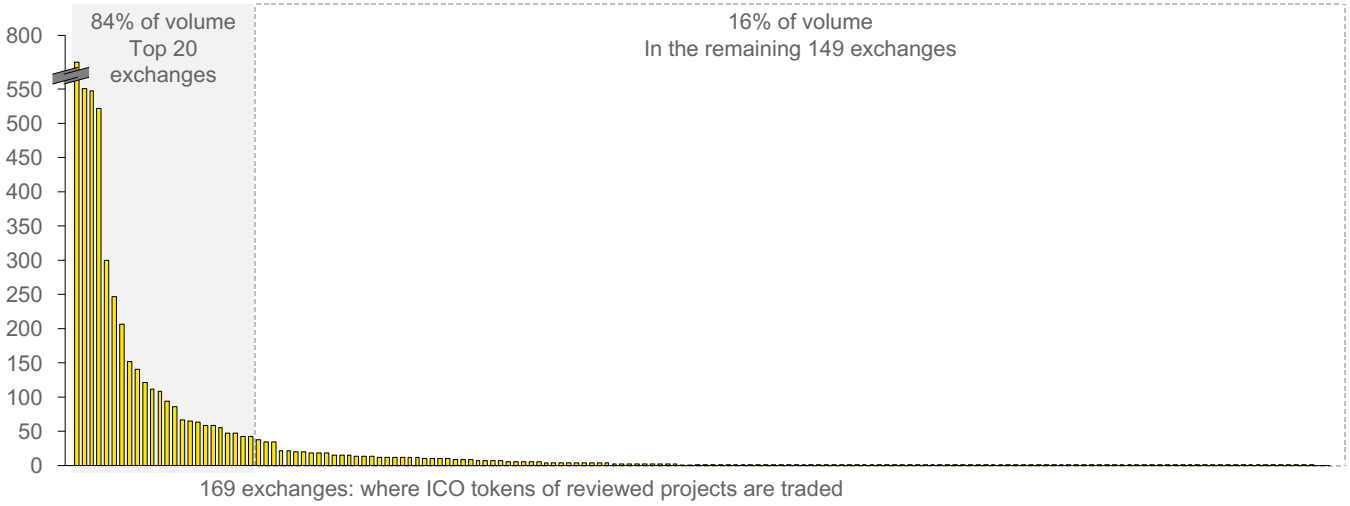
- EY Blockchain Analyzer is being built to support blockchain assurance at scale
- Matching cryptocurrency transactions between private ledgers and public blockchain records
- Technical foundation for private nodes, machine learning systems
- Multiple currencies – Bitcoin, Bitcoin Cash, Litecoin, Ethereum, Stellar

Though the overall market for crypto-assets has shrunk in the crash, the crash is consolidating the winners

84% of ICO tokens trading volume consolidates in the top 20 exchanges.

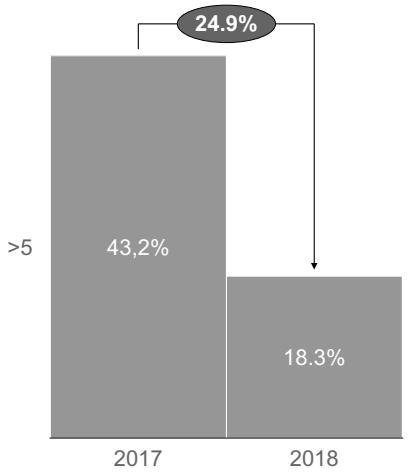
24-hour trading volume of ICO tokens

169 crypto-exchanges analyzed, where ICO tokens are traded, US$mm



Data compares 2017 with the first half of 2018/

% of ICO tokens listed on five and more crypto exchanges

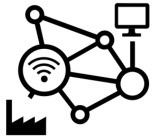


Only 18% of ICO tokens list on more than five exchanges, compared to 43% in 2017. Decline is likely due to increasing listing fees and rising KYC/AML requirements.

As blockchain transactions become more mature, the tools needed to monitor and audit will need to match that

Many Input Sources



Blockchain Analytics

- Blockchain Analyzer
  - Audit & assurance foundation
- Public Blockchain Analytics
- Private Blockchain Analytics
- Tax Liability Calculation
- Smart Contract Testing

Insights & Actions

- Transaction matching for audit
- Fraud detection & related analytics
- Tax liability
- Contract safety & on-going monitoring

Long term, we think the big application of blockchain is its power to transform business to business interactions

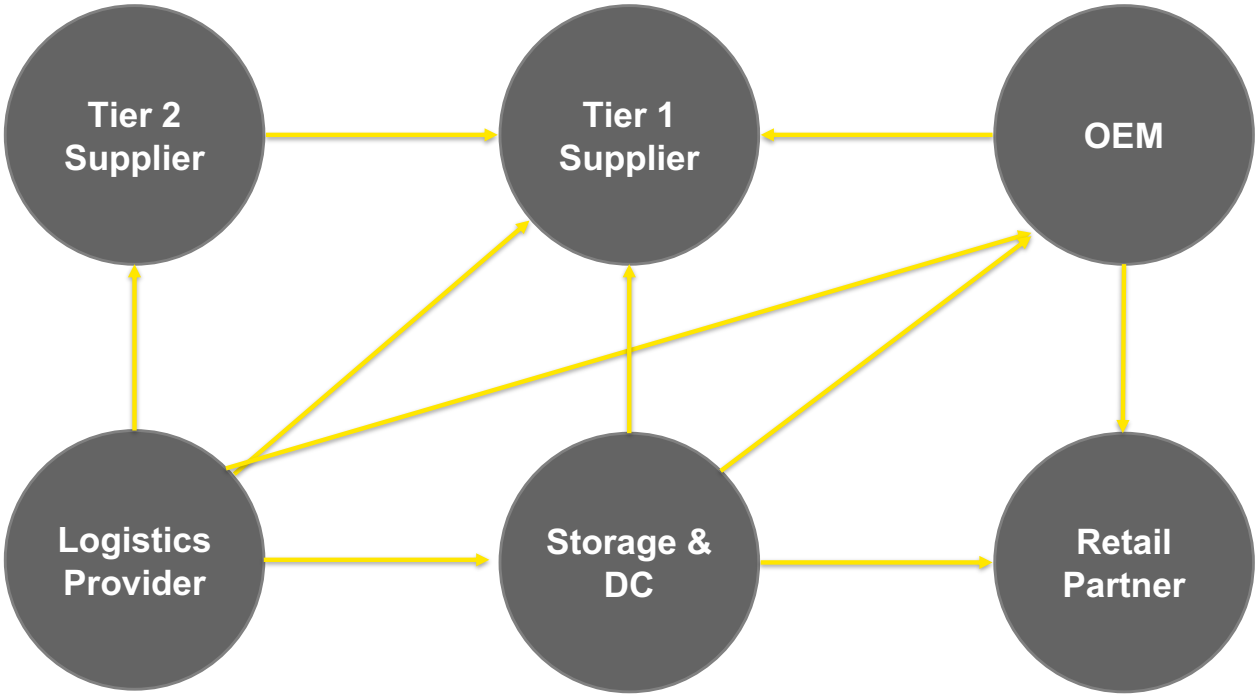
From Vertically Integrated

- *River Rouge plant for Ford*
- *Vertically integrated end-to-end car manufacturing*

To Ecosystem Partner

- *Foxconn's Shenzhen factory complex: assembly only, depending on a huge global network of suppliers*

Integration across companies has traditionally been done on a point to point basis with EDI



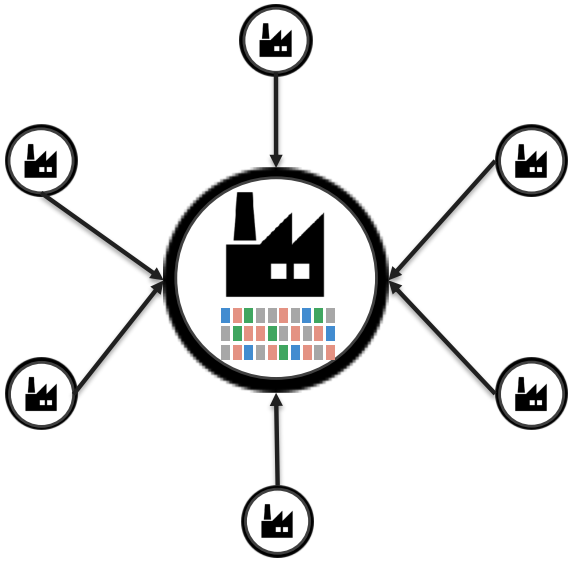
The world of business operations is awash in a flood of just-out-of-sync and non-standard EDI and XML messages.

The results are:

1. *Islands of information*
2. *Data that never propagates past one node in the network*
3. *Information that always slightly out of sync*
4. *No embedded business logic*

Centralized digital markets allow for shared information and common business process

Centrally controlled marketplaces are opaque and the flow of information as very asymmetrical…



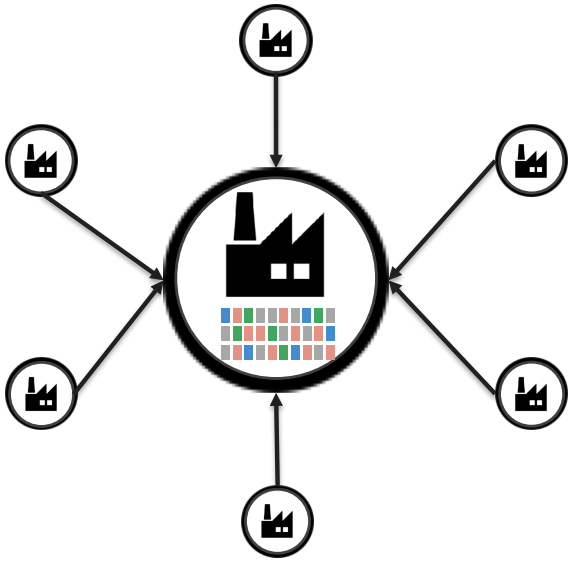
Market operators quickly become market dominators if their power is unregulated:

- *Market operators can see accounts and activity*
- *Market operators can create and maximize the value of information asymmetry*
- *All marketplaces are different and require unique technology integrations*

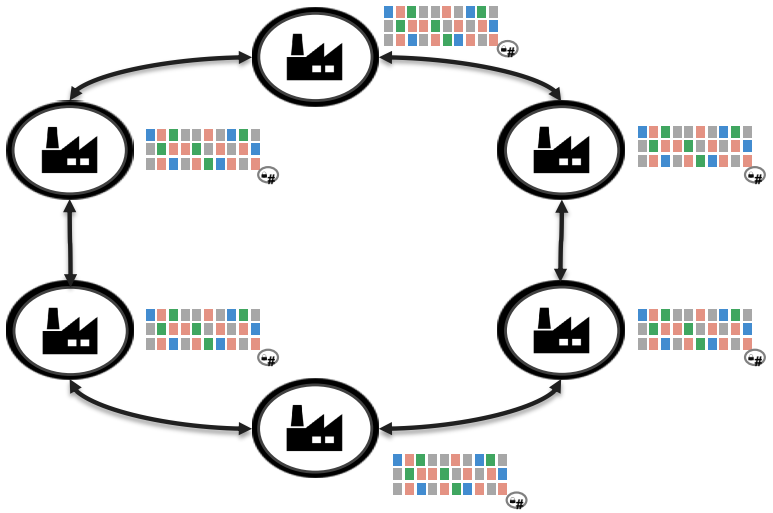
Consumers have embraced digital markets, but larger enterprises are much more reticent to join digital markets that will commoditize their business.

Blockchains are a game changer because they allow for shared information & process without a central authority

Centrally controlled marketplaces are opaque and the flow of information as very asymmetrical…

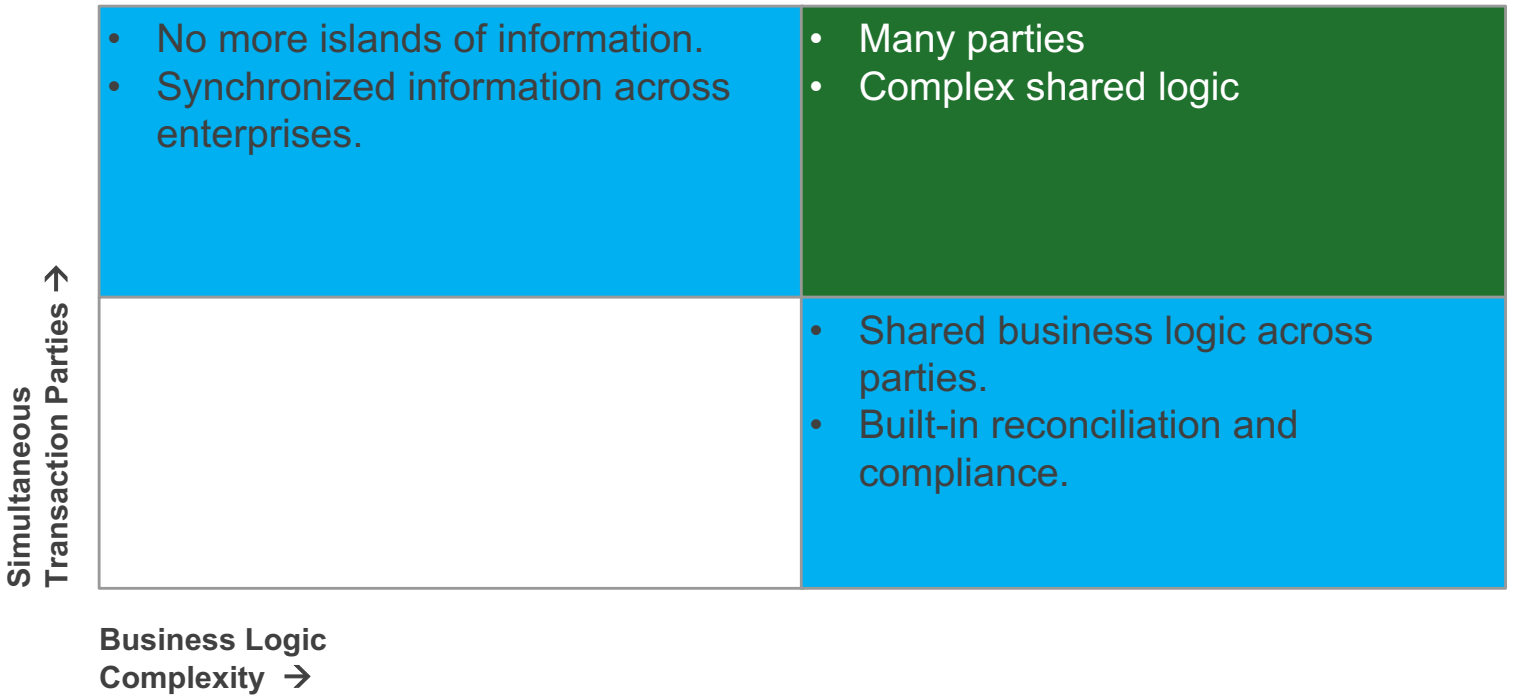


Blockchains have identical information and business logic that is transparent.



With blockchains and standard tokens and contracts, digital markets with shared information and process are possible with far fewer risks.

The sweet spot for blockchain technology is at the intersection of shared information and shared logic



This is the solution space that traditional ERP systems fail at very badly or don't do at all: complex business logic that is differentiated at very large scale across many players.

Before we get to really sophisticated digital markets, we have to start with what can create value now: process integration

Contract	Order	Fulfill	Invoice	Pay
Paper contracts with complex terms	Purchase orders sent by EDI against contract	Shipment tracking information by EDI or Email	Invoice upon receipt by email	Paper check after 60 days





All running in a single, public blockchain…

Smart contracts on a blockchain → Pull signal through blockchain → Tokens created & moved on the blockchain → Automatic based on the smart contract → Paid through the blockchain.

Our most famous solution is the Distributed Contracting Network for the Microsoft X-Box platform

- Digital contracting infrastructure running in Quorum on the Microsoft Azure infrastructure
- Sophisticated software and content licensing contracts can be managed at scale in near-real time.
- Easy on-boarding for any client including both blockchain and web access options
- In early production now with Ubisoft and Electronic Arts and several others

The appeal of blockchain processes is their ability to handle complexity at scale and to do so efficiently and fairly

Case Example: Microsoft's expected benefits from implementing a blockchain for digital rights & royalties:

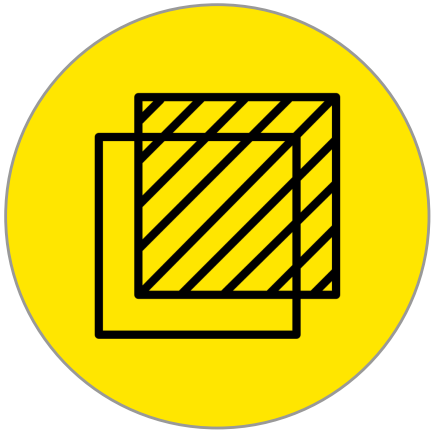
Less time needed to calculate rights & royalties owed.

- From 45 days to <4 minutes to complete statements of account

Less cost to administer the entire system.

- Reduction in the cost to administer the system

Full transparency for all leading to less litigation.



- Increased trust from all parties being allowed to examine the transaction logs & business logic in detail

Whether it's software licenses or truck leases, our goal is to tokenize and model business relationships on a blockchain

Take enterprise assets (real & virtual)

…and represent them as tokens in a blockchain.

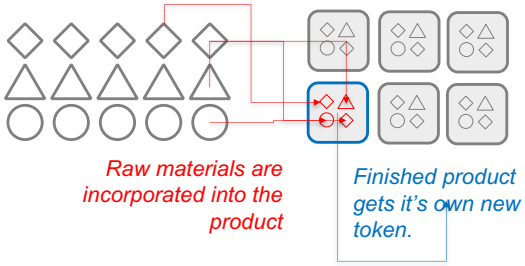
Contracts govern the exchange of products or services for money. These can all be represented as smart contracts and tokens.

A seller (truck maker) is exchanging a physical product with a buyer. On the blockchain, it's an exchange of truck token for a set of financial tokens.

The result is the ability to represent complex business processes end-to-end using a blockchain

Raw Materials

- Purchase raw materials
- Create digital tokens to represent those assets

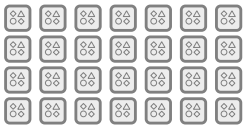


Manufacture

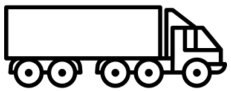
- Integrate items together into manufacturing output
- New digital token incorporates the materials

Transport

- Put finished in to an in-transit status

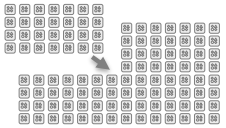


- In a container on a truck (also tokenized on a blockchain)



Warehouse

- Move into warehouse with a distributor
- Unload container & truck



- And in a warehouse (also tokenized on a blockchain)

Sell

- Transfer to a retailer
- Transfer ownership first to retailer and then to end customer

- Stocked in a stores in a region

Support

- Build true end-to-end traceability for product history

Blockchains reconcile any token movement with the same discipline as banks, a powerful asset for supply chains

Transport

- Put finished in to an in-transit status

On The Truck:

100

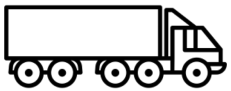
Move to Warehouse:

-100

- In a container on a truck (also tokenized on a blockchain)

Left On Truck

0



2 In order to add inventory to a warehouse, it must come from somewhere: in this case, In-Transit inventory.

1 On a blockchain with tokenization, inventory moves must be balanced between locations

Warehouse

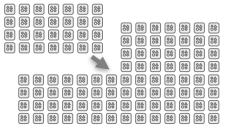
In Warehouse:

0

- Move into warehouse with a distributor
- Unload container & truck

Added to Warehouse:

+100



Total In Warehouse:

100

- And in a warehouse (also tokenized on a blockchain)

Using tokenization on a blockchain means that inventory moves between locations are handled with the same precision as bank transfers.

Tokenizing an asset makes traceability simply, but also lays the foundation for more sophisticated applications.

- End to end wine traceability for thousands of customers
- Direct relationship opportunity with the client
- Lays foundation for deep insights into gray market and distribution behavior
- Lays the foundation for retail promotion management with business partners

So Far, So Predictable

Vision Compared To What Actually Works

Lessons Learned

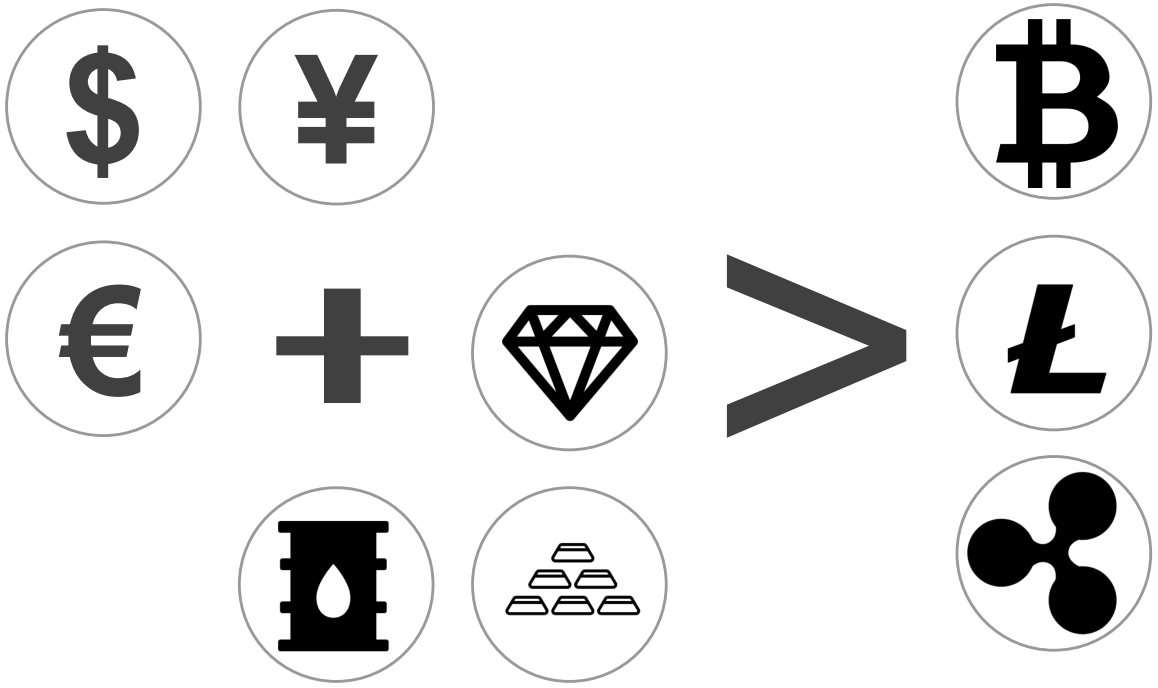
Where Blockchain Goes Next

Lesson #1

Trust is most mis-used and misunderstood concept in the world of blockchain.

The future of blockchain transactions are the exchange of assets for money, most of it based on the real-world.

Our experience shows an overwhelming preference by investors and enterprise users for widely accepted currencies and real-world assets over crypto-currencies:



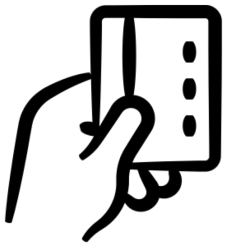
- Don’t confuse the value of public blockchains with demand for cryptocurrency
- The future of business contracts is the exchange of product & service tokens for money tokens
- There is huge demand for fiat currencies and all kinds of real world assets
- Efficient, reliable tokenized fiat currency is critical to bring enterprises into the public blockchain ecosystem

Lesson #2

If it ain’t broke, you’re not going to make any money fixing it.

Payments, stock-exchanges and other regulated, digital financial systems aren't broken (enough)

Payments are not broken.



Stock exchanges are not broken.

- Billions of transactions per day
- Global reach
- Completely digital settlement systems
- Robust regulatory and compliance systems

It's rare that "rip and replace" occurs in the world of technology:

Centralized systems will ***always*** be faster & cheaper.

Regulators limit the power of intermediaries in finance.

Slightly better isn't enough to offset big risks and investments.

Lesson #3

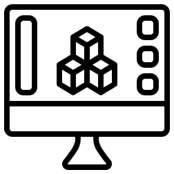
Operations before finance.

For most enterprises, getting the operational side of things right is necessary before jumping into payments

Many big players are starting on the operations side of things

- Food traceability but not procurement

- Contract management
- Payments through ERP



- Calculate licensed owed
- Payments through ERP

- Verifying that inventory levels and pricing are correct before commitment to payments
- Checking on smooth integration with existing ERP and accounting first

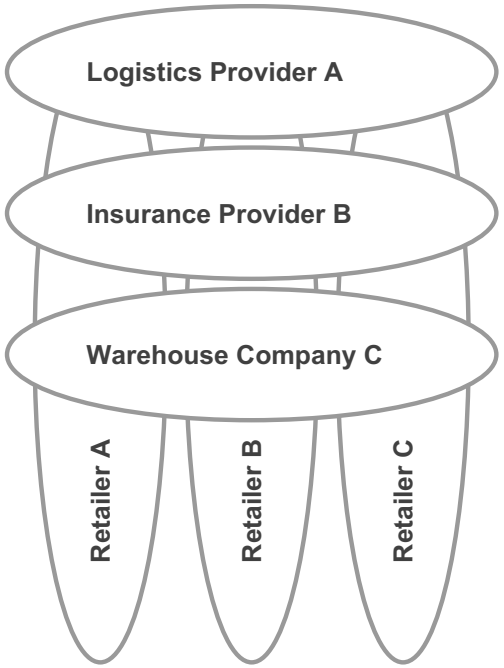
- Payments are just harder to reverse than it is to fix inventory errors
- Operations before payments allows companies to test and get comfortable with blockchain without risk of “irrevocable” payments to partners
- Once they are comfortable, the value proposition of closing the loop will be compelling

Lesson #4

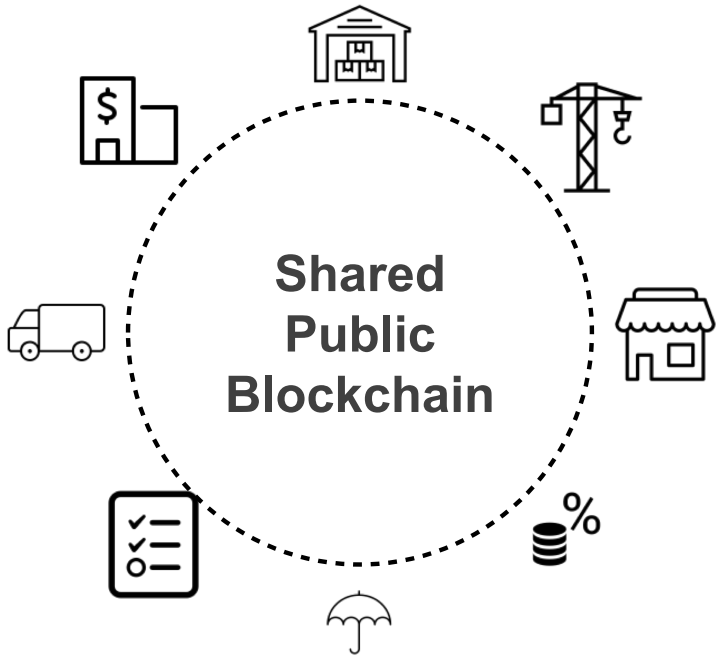
Private blockchains are only a temporary solution.

Private blockchains work for small networks of close partners, but company or industry solutions usually need many interactions to be useful

Current model of siloed and parallel private networks is unsustainable:



A future or large, regional or sector-specific networks that are public is more likely:



Lesson #5

There will be only one blockchain (to rule them all)

Economics and network effects mean that it is very unlikely that we will see a world of many different platforms

Social Networks

Smartphones

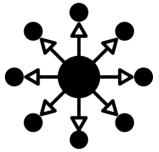
PCs

Mainframes

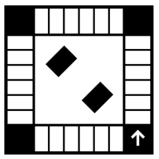
Networking Standards

Software Economics

Network Effects



Monopoly



So what kind of future would you like to have?

Open & Decentralized


FTP: 1971

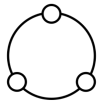

TCP/IP: 1974


SMTP: 1981


IMAP: 1986

Closed & Proprietary


DRM


Token Ring


AOL IM


Social Media

So Far, So Predictable

Vision Compared To What Actually Works

Lessons Learned

Where Blockchain Goes Next

We are still early on in the development of this technology, and much must be done for blockchain to deliver it's full potential

We are here 

Proof of Concept	Specialized Applications	Universal Business Infrastructure
Public Blockchains Bitcoin & other cryptocurrencies Ethereum applications	**Public Blockchains** Cryptocurrencies Initial Coin Offerings Distributed Applications Decentralized Storage Capital Markets **Private Blockchains** Managed Business Networks - Food & wine traceability - Shipping insurance - Digital Rights - Procurement Interbank Payments	**Public Blockchains** Decentralized applications Decentralized storage Business contracts: - Supply chain traceability - Multi-enterprise procurement - IoT integration - Global shipping & logistics - Cross-border VAT & taxes Tokenized Fiat Currency **Private Blockchains** High security managed networks - Healthcare - National security

Three things have to happen for public blockchains to triumph in the long run.

Secure, Private Transactions on Public Networks

Robust & Reliable Links To The Off-Chain World

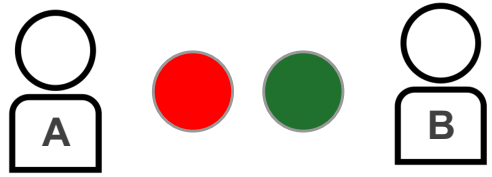
Regulatory Compliance Without Centralization

Zero Knowledge Proofs will allow secure, private transactions over public blockchains.

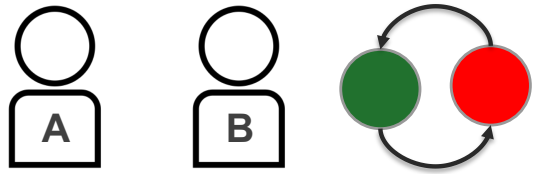
Using ZKPs, you can prove a statement is true without ever revealing the underlying data:

Alice has two colored balls. Bob is color-blind. How can Alice convince Bob that this is true?

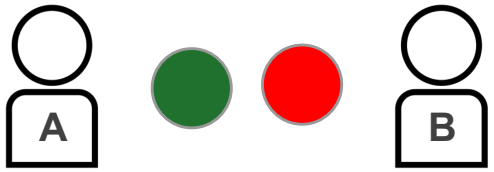
Bob cannot tell the difference between these two:



Bob takes both balls and switches them behind his back. (Or doesn't)



Alice correctly tells Bob that he switched (or not) the balls, confirming her knowledge.



Repeat 7 times to achieve >99% certainty.

A Zero Knowledge proof must satisfy three key conditions:

Completeness: if the statement is true, a honest verifier must be satisfied.

Soundness: if the statement is false, no cheating is realistically possible.

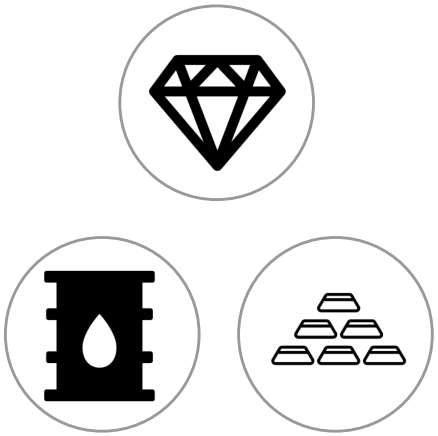
Zero Knowledge: The verifier cannot ever know or learn anything other than that statement is true.

With ZKPs we can have the privacy needed by enterprises and governments delivered on shared, open access public infrastructure.

Verifiable linkages to the world of off-chain assets is another area of rapid growth.

Fiat currency token attestation will the first link to off-chain assets that is systematically verified:

The attestation of other real-world assets will follow, though may be more challenging:



Instrumentation and attestation will be the keys to enabling scalable, trustworthy off-chain integration

Instrumentation means multiple forms of digital connectivity that verify asset production and status:

Manufacturing Execution Systems

Warehouse Management

Wireless Connectivity

Attestation means that an independent third party has reviewed those links and found them reliable & truthful:

Continuous testing & monitoring

Periodic spot checks & other verifications

Algorithm and/or software connectivity review

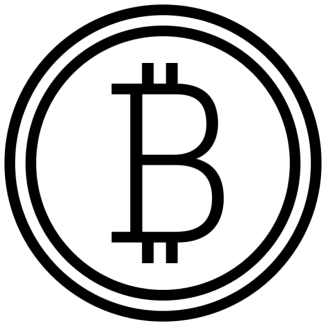
Smart Contract Testing & Analytics

We don't yet know what all shapes this will take as this capability matures over time.

Frictionless Transactions On The Blockchain

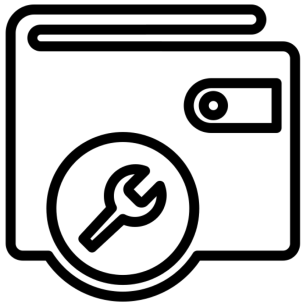
Despite the wild-west image, blockchains lend themselves to robust regulatory compliance. It's coming fast.

Tokens



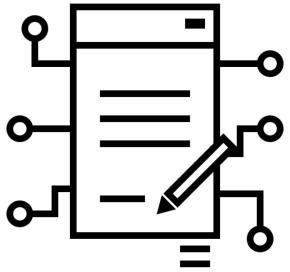
- Assets that come with rules
- Transfer restrictions
- Full history of ownership

Wallets



- Identity and access controls that can be tied to business rules and payments

Contracts

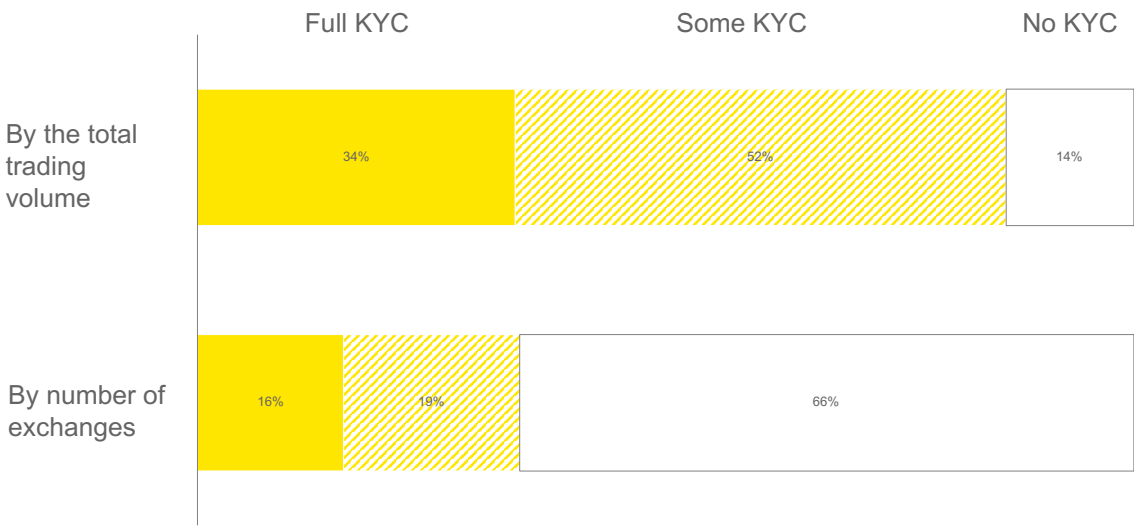


- Identity and access controls that can be tied to business rules and payments

In the world of ICO tokens and cryptocurrencies, compliance, though still weak, is tightening very quickly

While there are still many exchanges that have weak or no KYC requirements in place, they account for a rapidly diminishing share of the total market. We expect implementation of KYC and other anti-money laundering (AML) requirements to continue to spread in 2019.

KYC information requested by crypto-exchanges selling ICO tokens*
By volume and number of exchanges



*For 33 selected crypto-exchanges (87% by trading volume) out of 169 where ICO tokens are traded

Exchanges are classified into three categories by the level of KYC information requested:

1. No KYC: anyone can trade any amount without an ID. An email is usually enough for registration.
2. Some KYC: anyone can trade below certain amount without an ID. Official/state issued IDs only required to trade with fiat currencies and/or above certain limit.
3. Full KYC: an exchange requires bank level identification (state issued ID, phone, address)

Even when KYC is in place, it is still possible to evade restrictions. When there are value thresholds below which no identity information is required, it is possible to split funds across many accounts and or move them through a transit account before attempting to trade. To detect this KYC procedures should take advantage of public blockchain transaction analytics.

Our strategy is to make our vision come true.

Blockchains will do for networks of enterprises and business ecosystems what ERP did for the single company.

If the cloud is any guide, it's a 10 year journey that is just getting started.

2006

The year Amazon Web Services Launched.

2017

The year the majority of ERP installs shifted to the cloud.

Source: Panoroma Consulting, 2018

Paul R Brody

Principal, Global Blockchain Leader
San Francisco

@pbrody
linkedin.com/ln/pbrody

Building a better working world