CRYPTO EVOLUTION OF REGULATORY CAPITAL MARKETS AND FINANCE

Michael Hiles

THIS SESSION

- Who Am I?
- Basics of Blockchain
- Operational Risks Posed to Banks
- How to Mitigate Risks to Find Business Opportunities

MICHAEL HILES

- Founder/CEO of 10XTS
- GP in Cincinnati Crypto Fund & Tax Smart Crypto Fund
- Information Governance, Risk & Compliance Architect
- Decades of work in compliance and government workflow automation
- Smithsonian Laureate Award for 1st to connect a judicial management system to the WWW
- Deployed the 1st biometric device on a judge's bench to e-sign official records into public record

10XTS

- Governance, Risk & Compliance for Digital Assets & Markets
- XDEX, GRC oracle layer
- Tokenization of real-world assets
- Decentralizing programmable securities management & clearing
- Embedded compliance

COMMERCIUM BANK

- Incubated the team and launched Commercium Bank
- State chartered bank in Wyoming under new Special Purpose Depository Institution (SPDI) regulations
- Non-lending charter to provide fee-based services
- Provide cash accounts, escrow, custody and clearing of digital assets & tokenized securities in capital markets
- Custodied digital assets are off balance sheet
- Provide Banking-as-a-Service to other Community Banks & Credit Unions

COMMERCIUM BANK

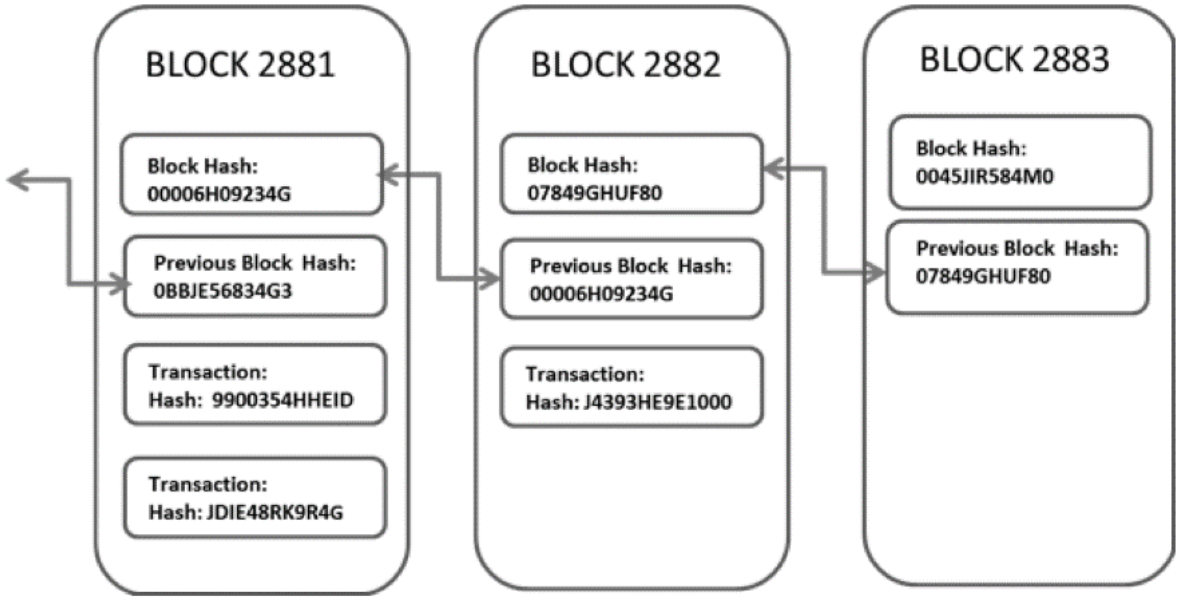
BASICS OF BLOCKCHAIN

TRUST THROUGH INTERMEDIARIES & HIDING INFORMATION

- We entrust intermediary 3rd parties with our data and trust them to HIDE it properly, keep it safe from hackers.
  - What happens when they fail? Equifax? Anthem? Target?
- Transactions can be modified and reversed, by somebody for any reason.
  - It is relatively easy to rewrite information
- We expect the 3rd party to protect our interest.
  - What happens if it conflicts with theirs?

BLOCKCHAIN: TRUST THROUGH TECHNOLOGY AUTOMATION

- Cryptographic technology to automate & democratize trust
- Distributed Ledger (“WRITE-ONCE” database) copied across the internet, nobody “owns” it
- Stores Transactions (From => To, How Much) that are “chained” to each other using cryptographic links called “hashes”
- Chaining ensures that nobody can modify ledger’s “history”
- Adding transactions comes at a “cost” (requires computing power)
- “Miners” or data block producers hold an identical copy of the blockchain and maintain it by adding transactions (and are paid if they succeed)

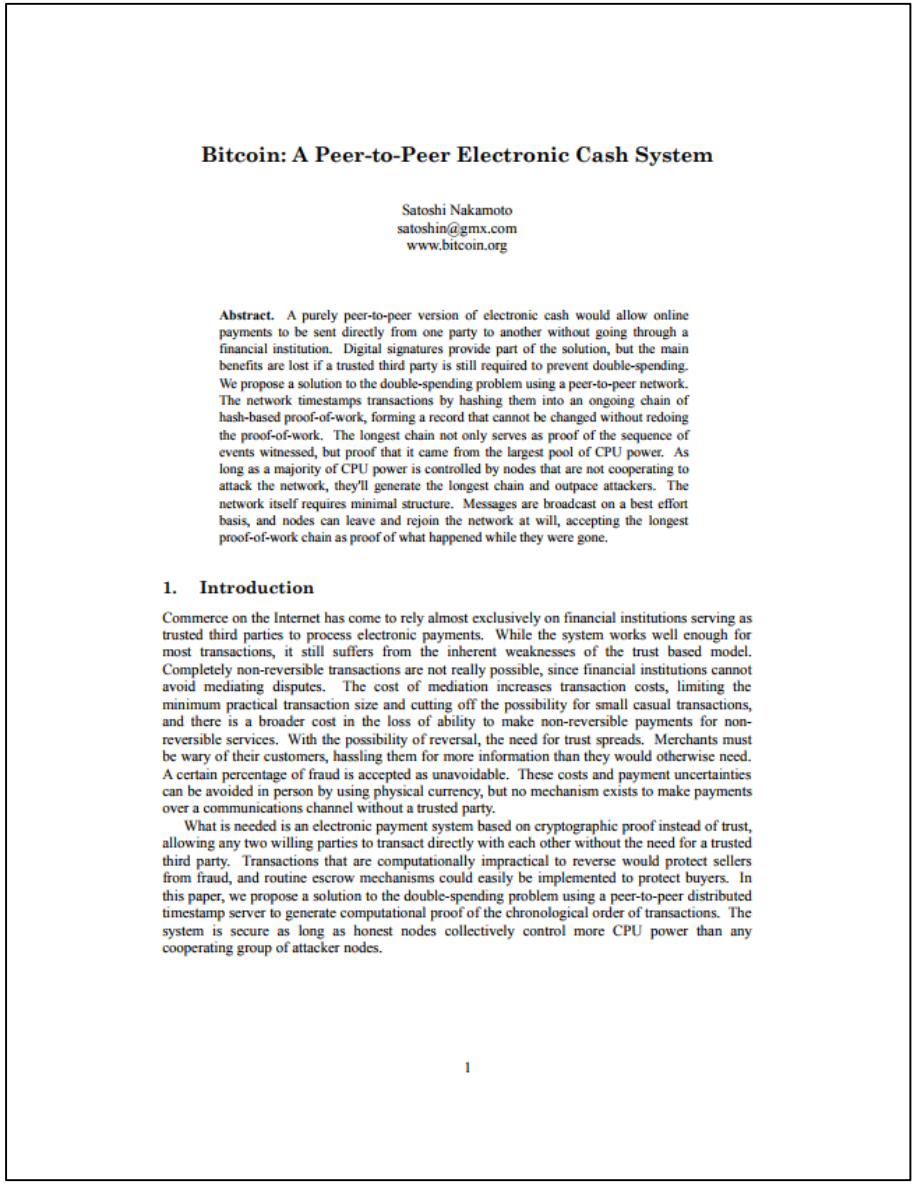


BLOCKCHAIN AS A SYSTEM OF TRUTH

- Reduces the cost to coordinate transactional information and data through automation between organizations
- Value of a coordination system > cost to coordinate
- Value of information shared > cost to share that information
- RESULT: We are likely to see the effective tokenization (and by extension, the introduction of markets) of almost everything

BITCOIN

- Satoshi Nakamoto released in 2008
- Open-source network launched in 2009



Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. 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. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

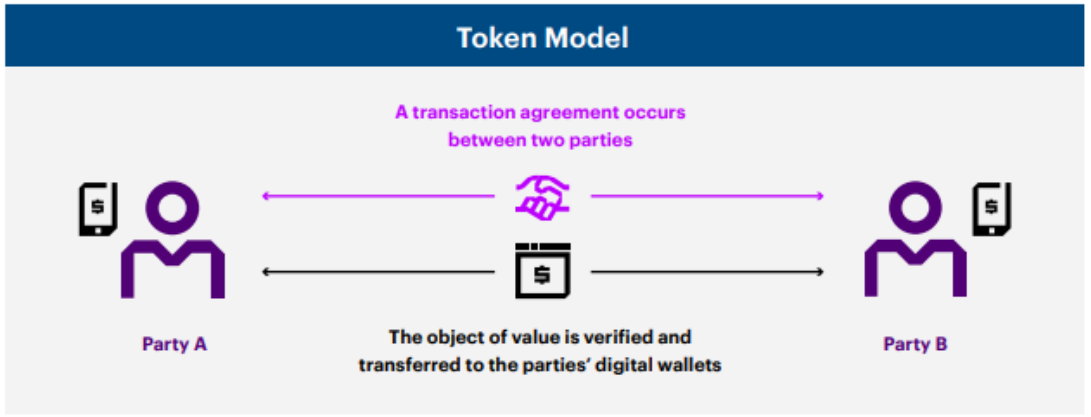
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

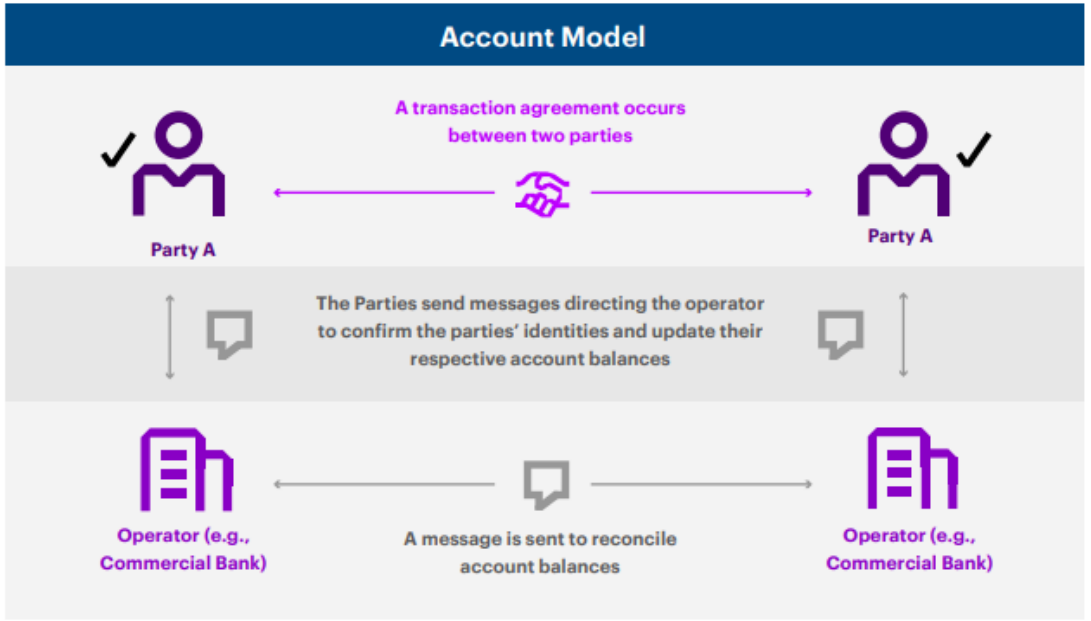
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

TRADFI ACCOUNT MODEL VS. TOKEN MODEL

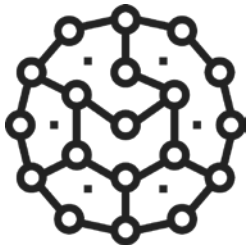
- Replacing account-based information exchanged between intermediaries with direct, peer-to-peer transactions





COMPONENTS OF A BLOCKCHAIN

Cryptography

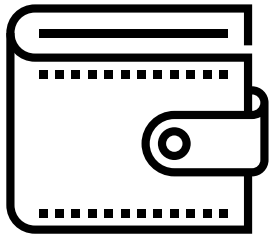


Computer Network

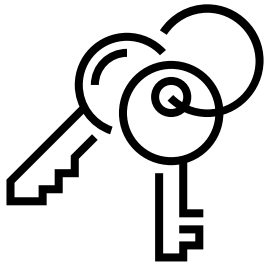
Consensus Mechanism

Ledger

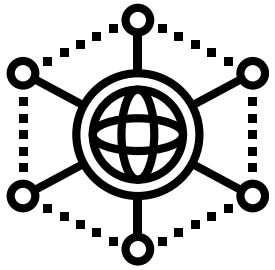
Validity Rules



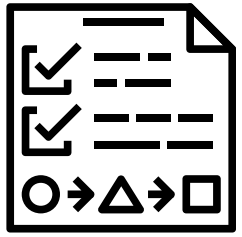
Wallets



Keys



Tokens



Smart Contracts

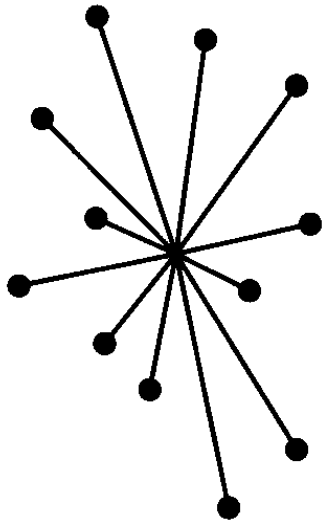
CRYPTOGRAPHY

- The practice and study of techniques for secure communication in the presence of adversarial behavior
- Modern cryptography uses mathematical algorithms to encrypt data
- Security Certificates (SSL)
- Many types of cryptographic algorithms, SHA-265
- Hashing information creates a “fingerprint” of the data

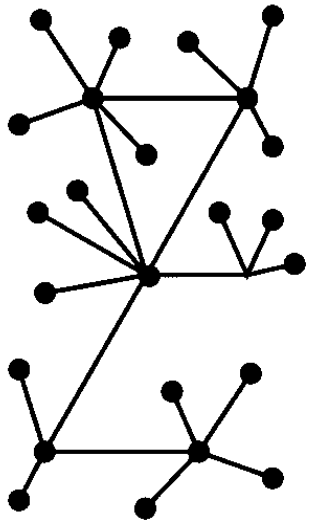
INPUT DATA	HASH OUTPUT (SHA-256)
My name is Toby	cacb5418163039b016be9746818a2926f68fd1e4bad1b04f6791f6aabb5e8c52
My name is Tony	9cd2444dc56929bdb97123add1f007643effa88bf1ed061eee1eead4e15ac7f9
My name is Toby and this is my project	9abbaa0c54fcd028ac51bede2608d06e8d3a026784e34adfac14fadd143d212c

COMPUTER NETWORKS

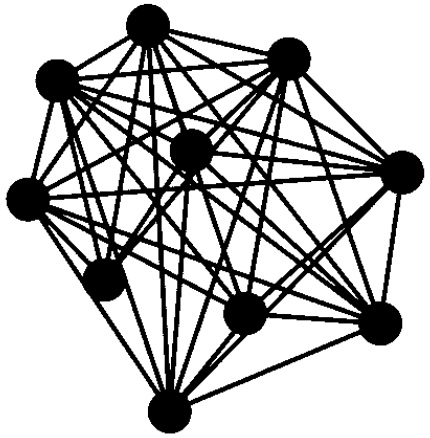
- Computers communicating with each other using standard protocols
- Networks have evolved over the years
- The value of a network increases proportionately to the number of users of the network



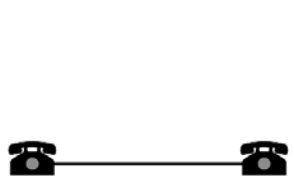
Centralized

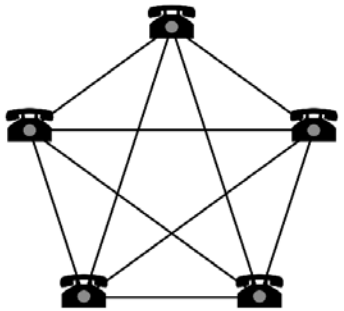


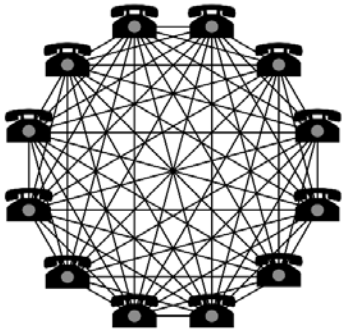
Decentralized



Distributed



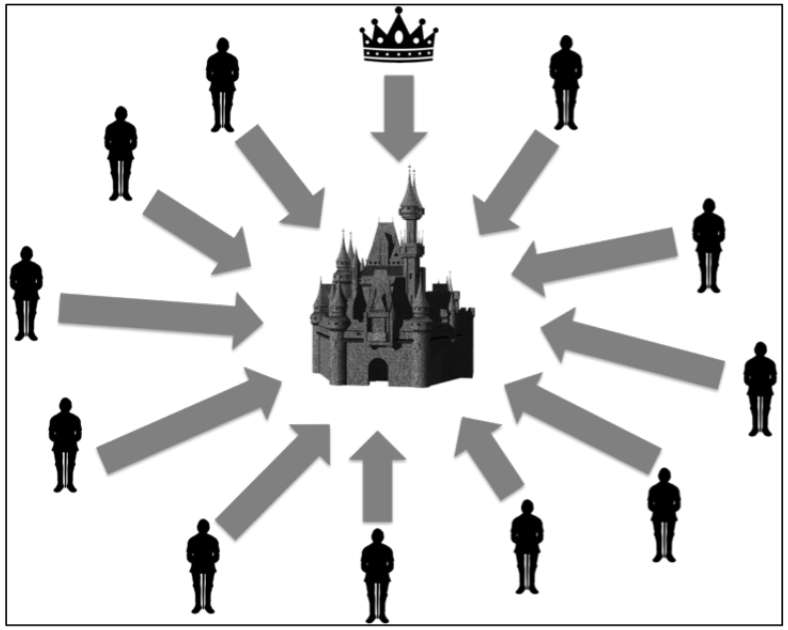




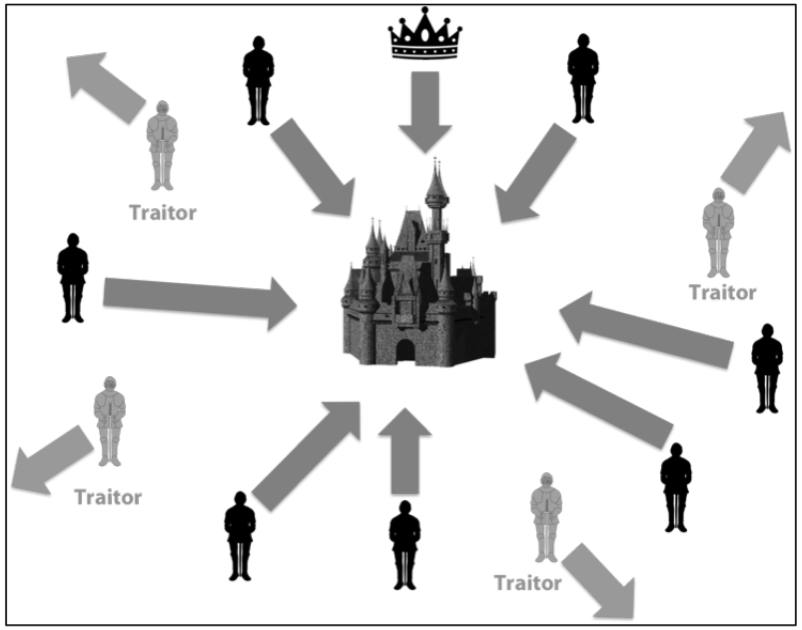
$$\sum_{i=1}^{n+1} V_{i,j} > \sum_{i=1}^{n} V_{i,j}$$

CONSENSUS MECHANISM

- Byzantine Generals Problem -> Byzantine Fault Tolerance (BFT)
- A method of communicating agreement
- Algorithmic math to ensure consistency and proof
- Proof of Work, Proof of Stake, Delegated Proof of Stake, …



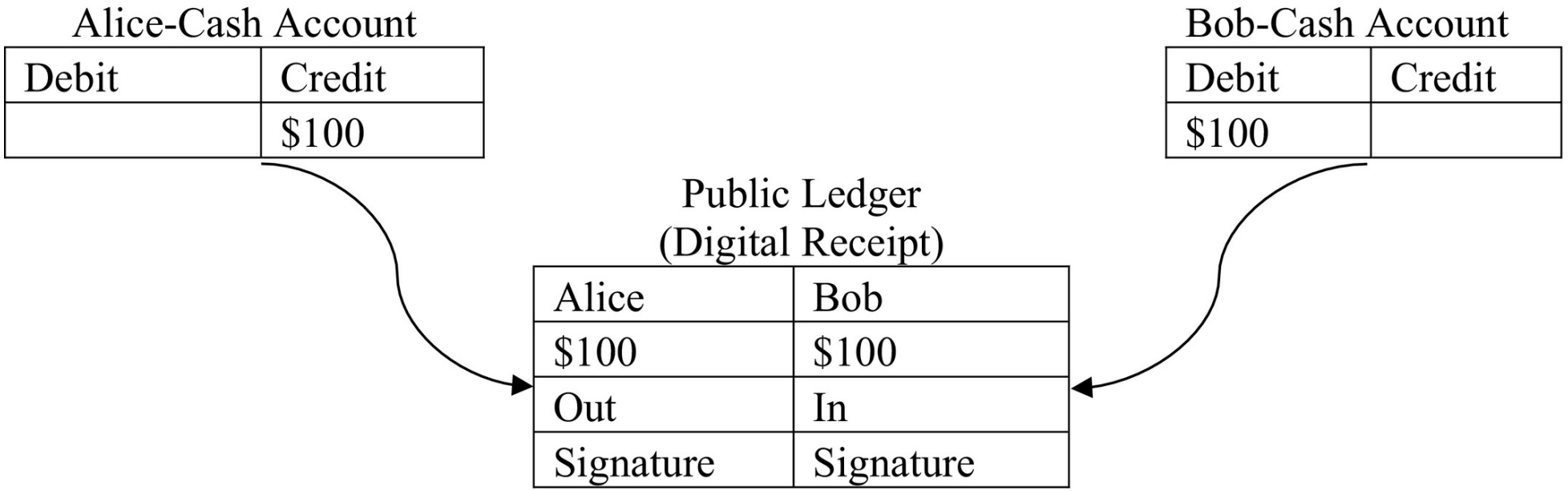
Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

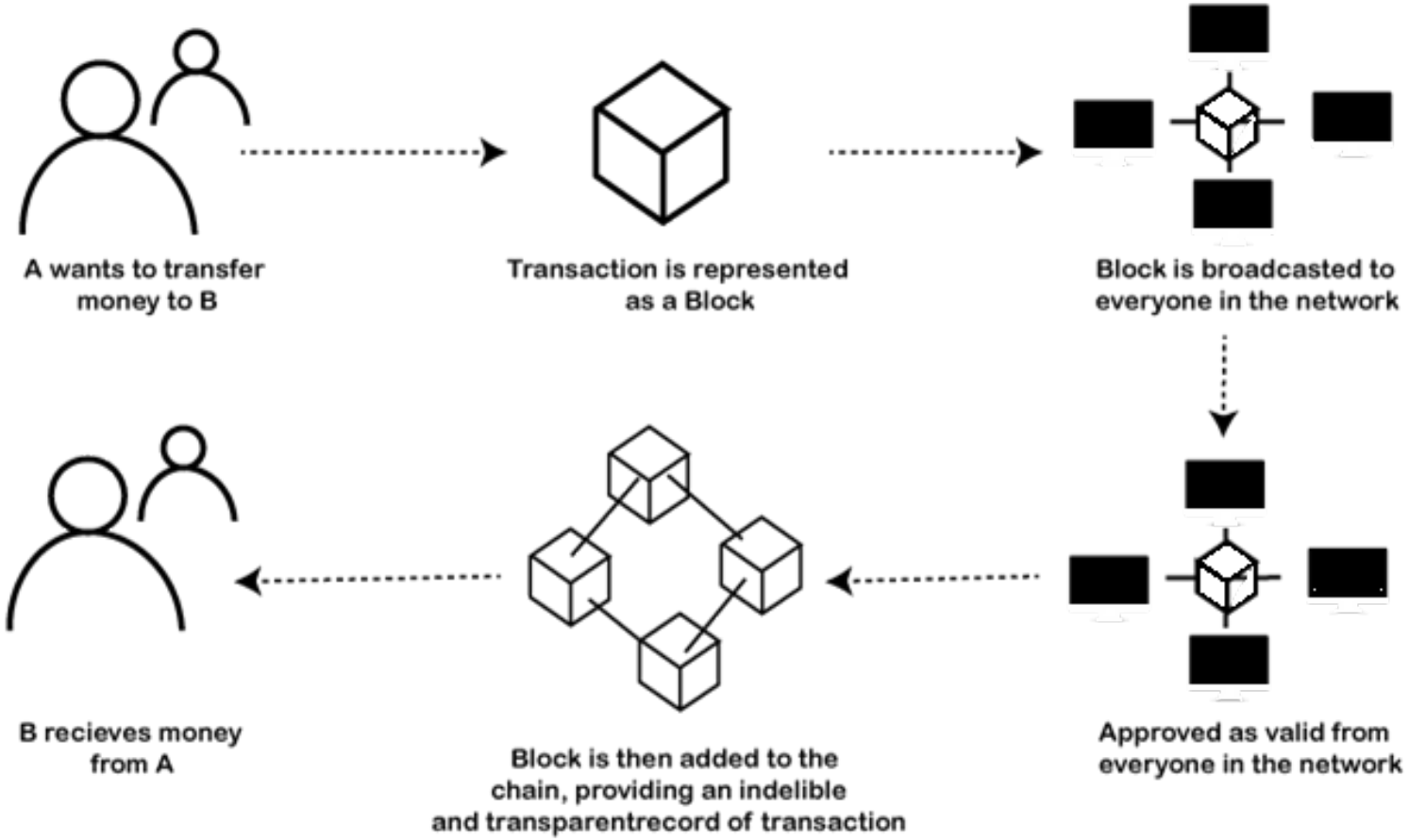
LEDGER

- Blockchain is a form of triple entry ledger
- The ledger is synchronized across the nodes on the network



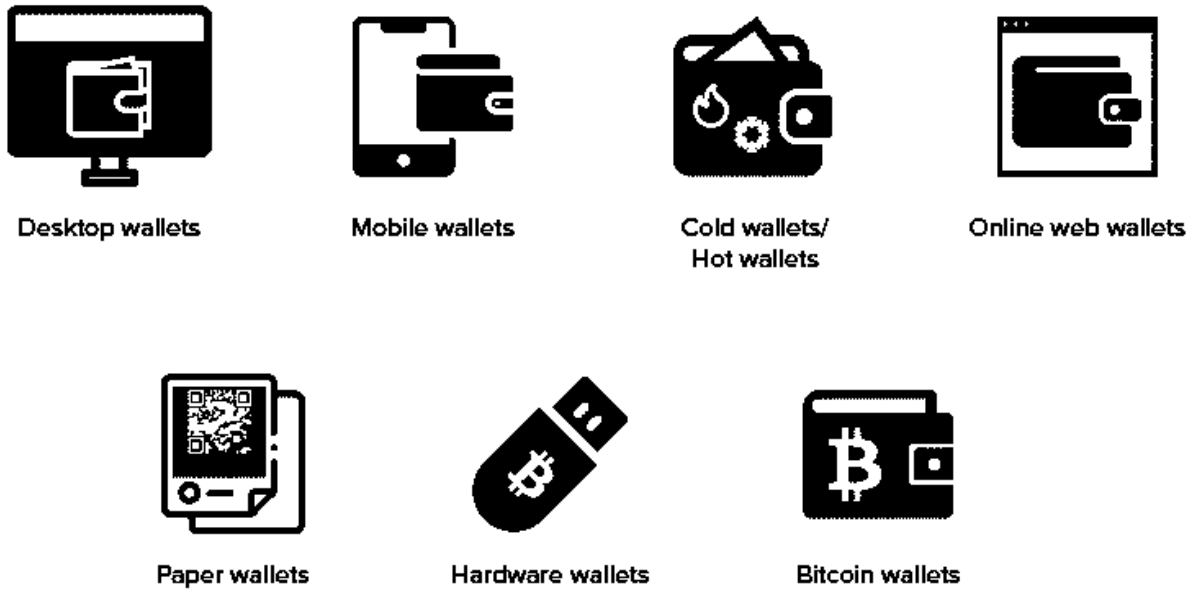
VALIDITY RULES

- How a transaction is validated and written to a blockchain



WALLETS

- Called a wallet because it started with currency
- Just a software “client” (application to talk to the blockchain)
- Only contains Private Key + Blockchain Address not the actual assets, which remain on the network
- Multi-signature Wallet requires multiple parties to approve transactions
- Often targeted by Hackers to steal cryptocurrency
- Whose wallet is it? The question of custody



KEYS

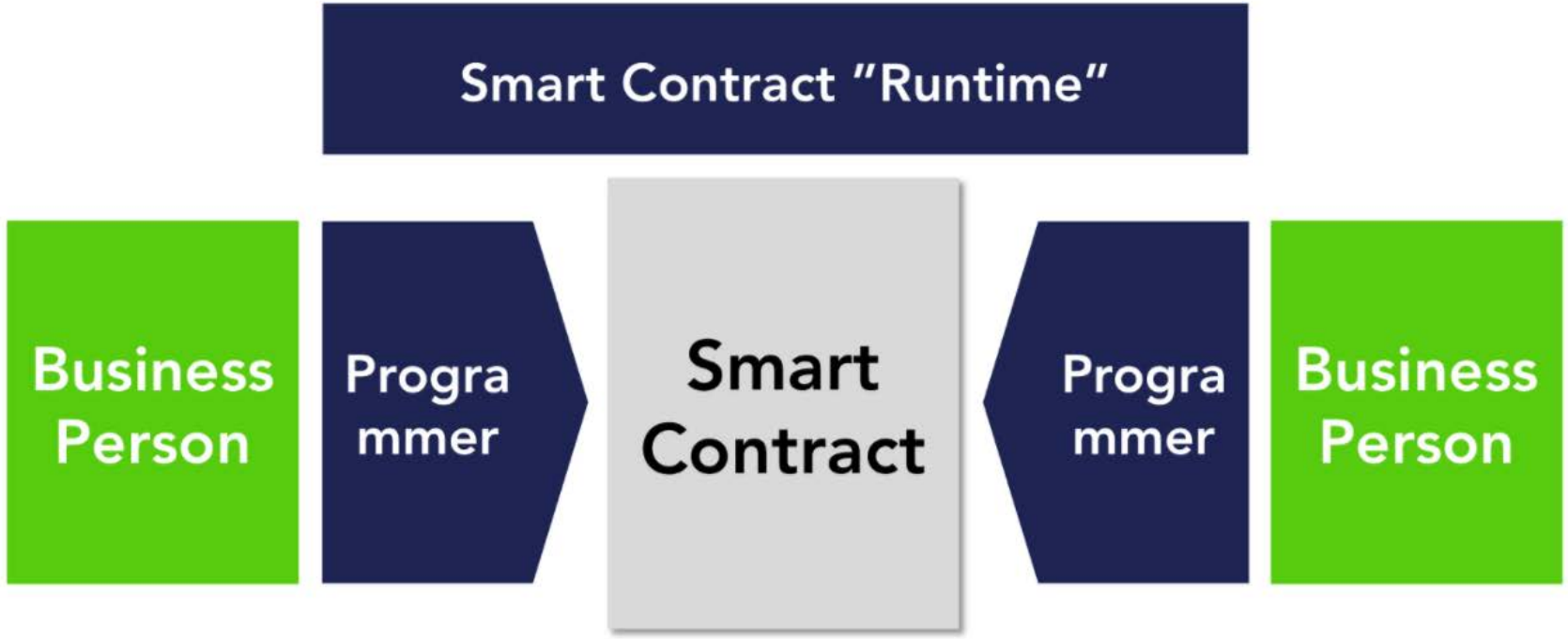
- Public Key -> The “Address” of the wallet
- Private Key -> The “Password” of the wallet
- Who has access to the key? Question of custody

TOKENS

- Units of account like Bitcoin
- Fungible vs. Non-fungible tokens (NFTs)
- Can have extended logic through “Smart Contract” functionality

SMART CONTRACTS

- Replace “attorney” with “programmer” and “legal system” with “runtime code” and we have smart contracts



SMART CONTRACT EXAMPLE

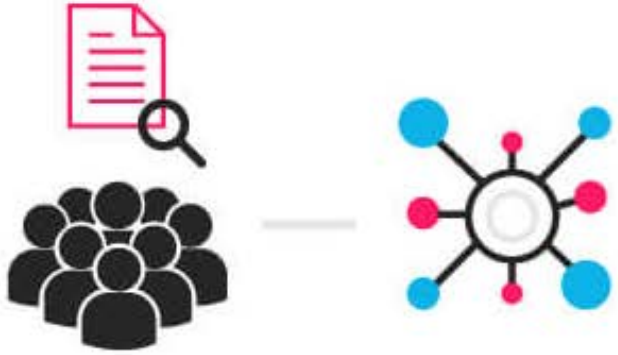
1

An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

2

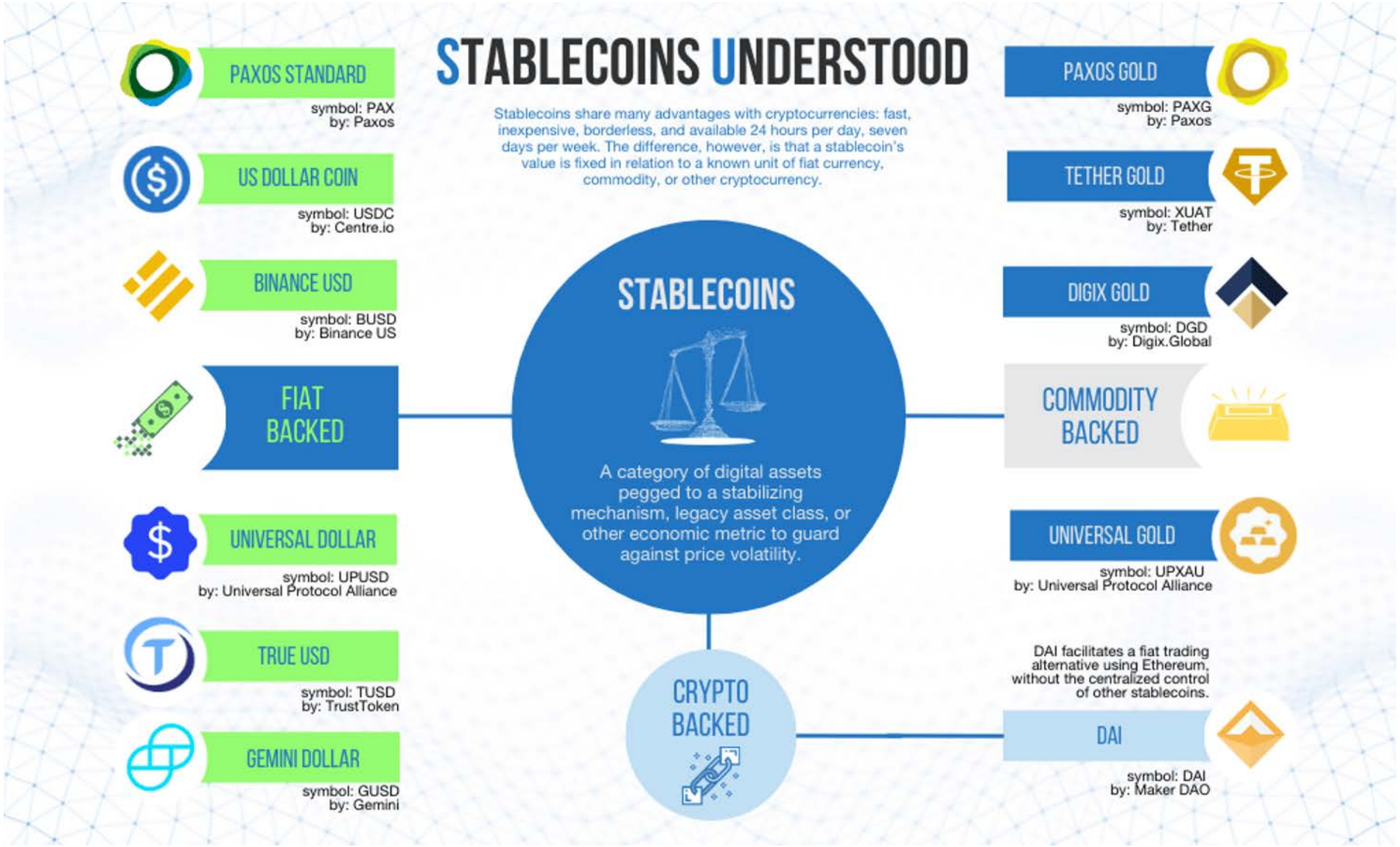
A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3

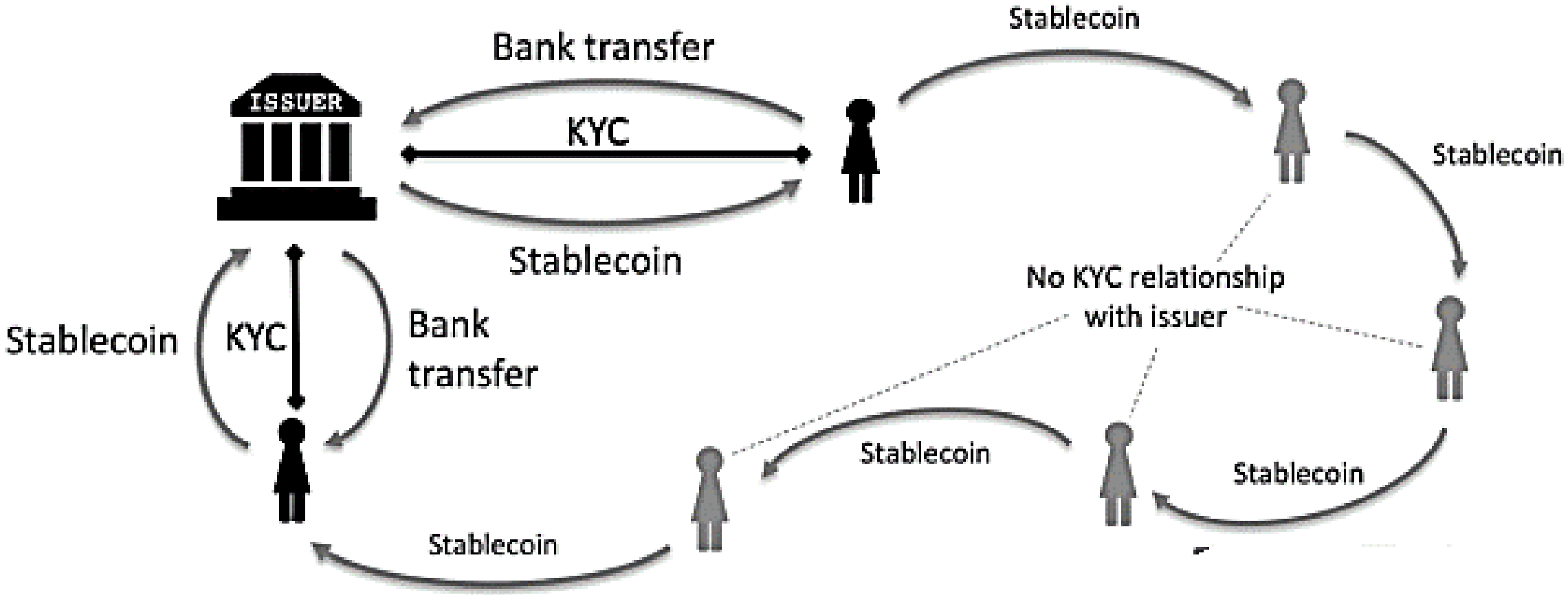


Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

STABLECOINS



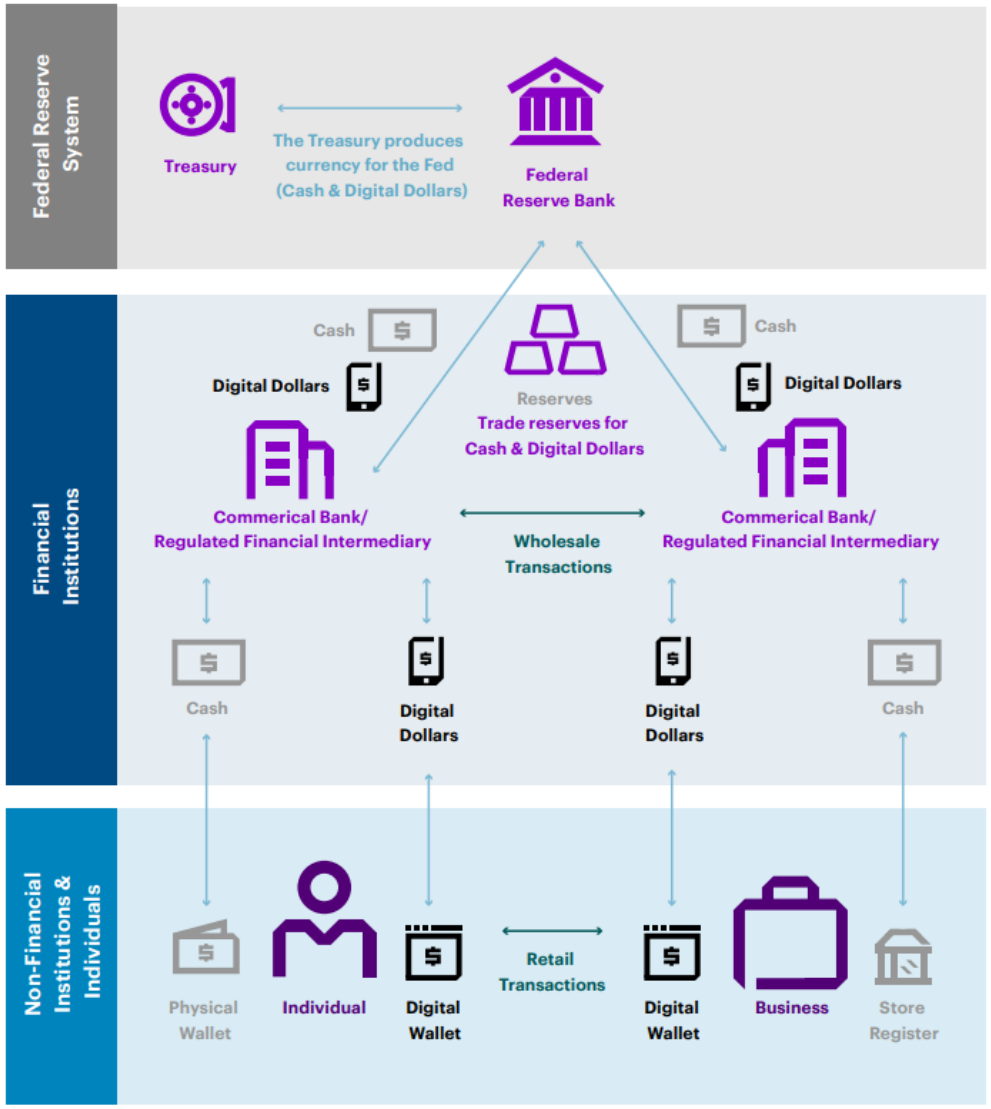
STABLECOIN PSEUDONYMITY AS ELECTRONIC CASH



TWO-TIERED DISTRIBUTION OF U.S. DIGITAL DOLLAR

Christopher Giancarlo
Former CFTC Chair

THE
DIGITAL DOLLAR
PROJECT



COMPETING GLOBAL NARRATIVES - BITCOIN AND CRYPTOCURRENCIES VS CENTRAL BANK DIGITAL CURRENCY

"……..cryptocurrencies must not circulate and ….overseas exchanges are barred from providing services to China-based investors. It also barred financial institutions, payment companies and internet firms from facilitating cryptocurrency trading nationally." (Analysts say China also sees cryptocurrencies as a threat to its sovereign digital-yuan, which is at an advanced pilot stage.)

- People's Bank of China, (September 24, 2021)

"France has used digital assets and blockchain technology in a series of bond transactions, marking one of the most significant trials to date of cryptocurrencies in a leading established market. The consortium of banks included BNP Paribas, Credit Agricole, CIB, HSBC and Societe Generale. The groups traded the government bonds as securities "tokens" and settled them with cryptocurrencies supplied by the central bank."

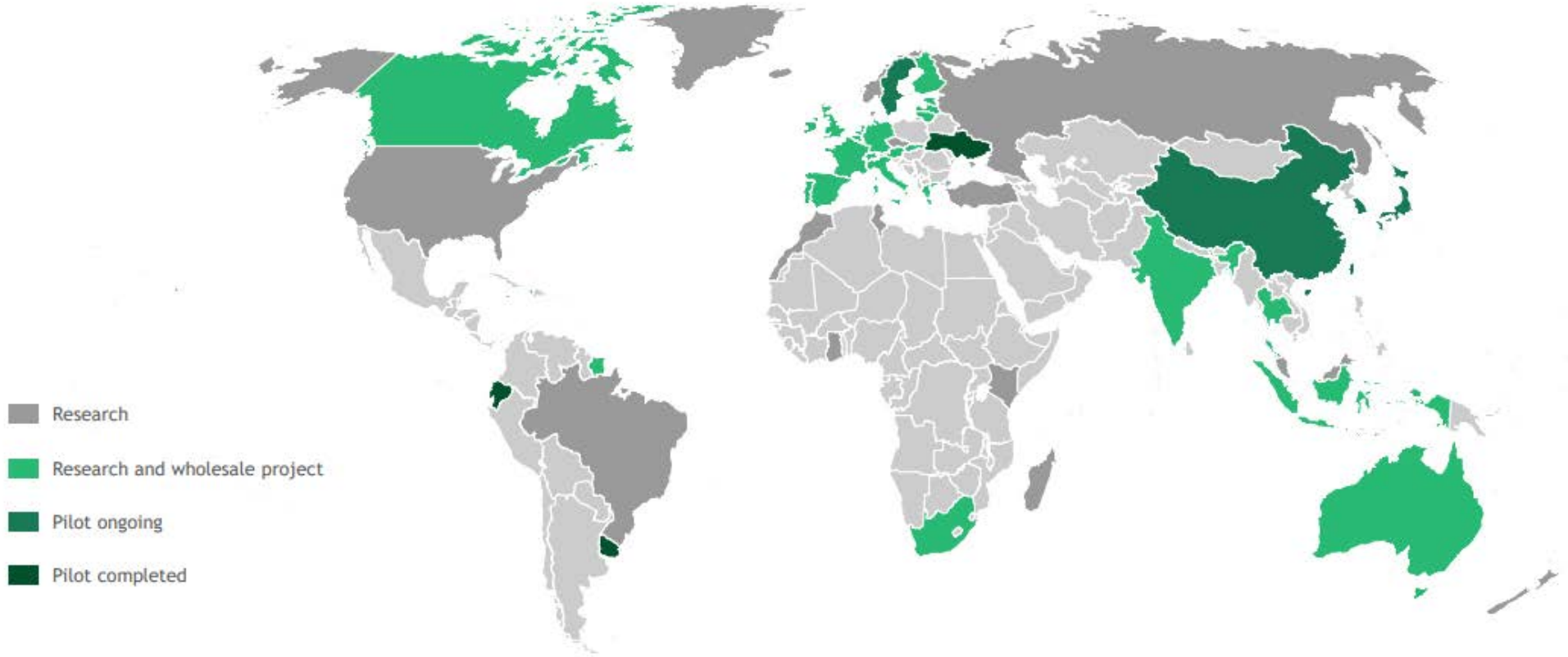
- Philip Stafford, Financial Times (October 19, 2021)

"I have no intention to ban or limit the use of cryptocurrencies." "….the development of a U.S. central bank digital currency (CBDC) could undercut the need for private crypto and stablecoins."

- Jerome Powell, Chairman of the Federal Reserve (September 30, 2021)

CENTRAL BANK DIGITAL CURRENCIES (CBDCS)

Status of central-bank digital currencies, retail projects[1], April 2021



1. Retail CBDCs are for the public; wholesale CBDCs for financial institutions

DECENTRALIZED FINANCE (DEFI)

- Finance that does not rely on central financial intermediaries to offer traditional financial instruments:
  - Lend or borrow funds from others
  - Speculate on price movements on a range of assets using derivatives
  - Trade cryptocurrencies
  - Insure against risks
  - Earn interest in savings-like accounts
- Controversial due to licensing & KYC/AML verification
- Extremely high yields

ASSET TOKENIZATION

- Digital securities are digitized investment contracts that provide investors with a contractual claim on an underlying asset. This could be in the form of economic interest tokens, equity tokens, debt tokens or convertible tokens.
  - Digital Securities are NOT cryptocurrencies
  - Digital Securities are regulated by governing bodies and must be issued and traded on licensed platforms
  - Digital Securities are able to embed smart features into their programming contracts, such as receiving voting rights and dividends

INEFFICIENT INFORMATION AND PROCESSES CREATES A MASSIVE DRAIN ON GLOBAL CAPITAL MARKETS EFFICIENCY

In 2017, OECD reported that regulatory divergence alone costs capital markets $780 billion annually in reconciliation of assets and transactions between global jurisdictions.

This hurts capital efficiency, flow, and returns on investment across all global financial markets and asset classes.

BLOCKCHAIN-POWERED CAPITAL MARKETS ARE ALREADY A REALITY

Traditional institutions are scrambling to implement the technology-based efficiencies that power fintech challengers.

Blockchain token-based, regulatory-compliant, programmable digital securities are already here with licensed intermediaries in every category of market infrastructure.

Technology-native institutions are rapidly building new market infrastructures. Crypto-friendly traditional market players are also showing signs of paving the way for mainstream adoption.

Broker Dealers

Propellr, uphold, ATOMIC, ENTORO, coinbase, DALMORE GROUP

ATS / Trading Venues

stellarx, LATOKEN, tZERO, SLICE, SIX, EMPLUM, FLUIDITY, SECURRENCY, AIRSWAP, GBX, MERJ, OpenFinance Network, AlphaPoint, SHARESPOST, Bancor, OASIS PRO MARKETS

Transfer Agents

VERTALO, SECURITIZE, SECURRENCY, TOKENSOFT, LEDGER LAB

Fiduciary Trust Companies

KINGDOM TRUST, KOMAINU, PrimeTrust, bakkt, Fidelity DIGITAL ASSETS, GEMINI

Chartered Banks

silvergate BANK, ANCHORAGE, PAXOS

Wyoming Special Purpose Depository (SPDI) Banks

kraken, AVANTI FINANCIAL GROUP, WDT Financial, Commercium Bank

PROGRAMMABLE DIGITAL SECURITIES TOKENS ARE SEEING EXPLOSIVE GROWTH

The early issuers in the space were experimental projects based on the growing adoption of blockchain technology itself.

By 2020 there was still a market cap of less than $60 million USD total in the market.

By the end of 2020, that grew to $366 million USD.

2021 saw that number swell to over $1 billion with multiple billions presently under development.

2020 Digital Securities Token Market Summary	
2020 Opening Market Cap	$59,339,362
2020 Closing Market Cap	$366,100,103
2020 Cap Change	+516.96%
2020 Total Trading Volume	$69,660,511
2020 Volume Change	+1,105.23%
2020 tZero Return ($TZPROP)	+205.26%
2020 Overstock Return ($OSTKO)	+195.00%
2020 Tokenized Real Estate Securities Market Cap	$27m

TOKENIZATION SERVICE PROVIDERS ARE HELPING ISSUERS CREATE AND LIST PUBLIC CHAIN-BASED TOKENIZED SECURITIES

BLOCKDATA

ASSET TOKENIZATION PROVIDERS COMPARED

DATE OF PUBLICATION: 25-10-2021

NAME	TZERO	CONSENSYS CODEFI	SECURITIZE	ADDX	POLYMATH	SECURRENCY	BITBOND	TOKENY SOLUTIONS	TOKENSOFT
HQ	US, NEW YORK	US, NEW YORK	US, SAN FRANCISCO	SINGAPORE, SINGAPORE	CANADA, TORONTO	US, WASHINGTON	GERMANY, BERLIN	LUXEMBOURG, LUXEMBOURG	US, SAN FRANCISCO
YEAR OF ESTABLISHMENT	2014	2017	2017	2017	2017	2015	2013	2017	2017
TOTAL FUNDING (IN $M)	$330.3M	$82.5M	$73M	$60M	$58.7M	$49.4M	$7.6M	$5.6M	$4M
TEAM SIZE	~84	~5	~90	~88	~44	~71	~19	~27	~20
TOKENIZED VOLUME (PUBLIC DATA)	-	-	$500M+	-	$2.2B+	-	€210M+	€8.5B+	$360M+
# TOKENIZED ASSETS	4	-	115	15	225	-	5	45	50
USED BLOCKCHAIN	ETHEREUM, TEZOS, ALGORAND	ETHEREUM, QUORUM	ETHEREUM, ALGORAND, AVALANCHE	ETHEREUM (PRIVATE)	POLYMESH, ETHEREUM	ETHEREUM, STELLAR, RIPPLE, GOCHAIN, EOS	STELLAR	ETHEREUM, POLYGON	ETHEREUM, STELLAR, CORDA, HYPERLEDGER
TOKEN	TZROP	-	-	-	POLYX	-	BB1	-	TSFT
TOKEN STANDARD	ERC-20	UNIVERSAL TOKEN	DS TOKEN PROTOCOL	ERC-20	POLYMESH, ERC-1400	CAT-20, CAT-721	STELLAR ASSETS	ERC-3643	ERC-1404
OPEN SOURCE	✓	✓	✓		✓		✓	✓	✓
KYC / AML COMPLIANT	✓	✓	✓	✓	✓	✓	✓	✓	✓
OPERATES A (SECONDARY) MARKETPLACE	✓	✓	✓	✓					✓
NOTABLE PARTNERS	OVERSTOCK	SOCIÉTÉ GÉNÉRALE	MORGAN STANLEY, ARCA	SGX, DEVELOPMENT BANK OF JAPAN	MARKETLEND, REDSWAN	U.S. BANK, STATE STREET	STANDARD CHARTERED, VONOVIA	PRINCIPALITY OF MONACO, EURONEXT	SEBA, CELO

BLOCKDATA IS A CB INSIGHTS COMPANY

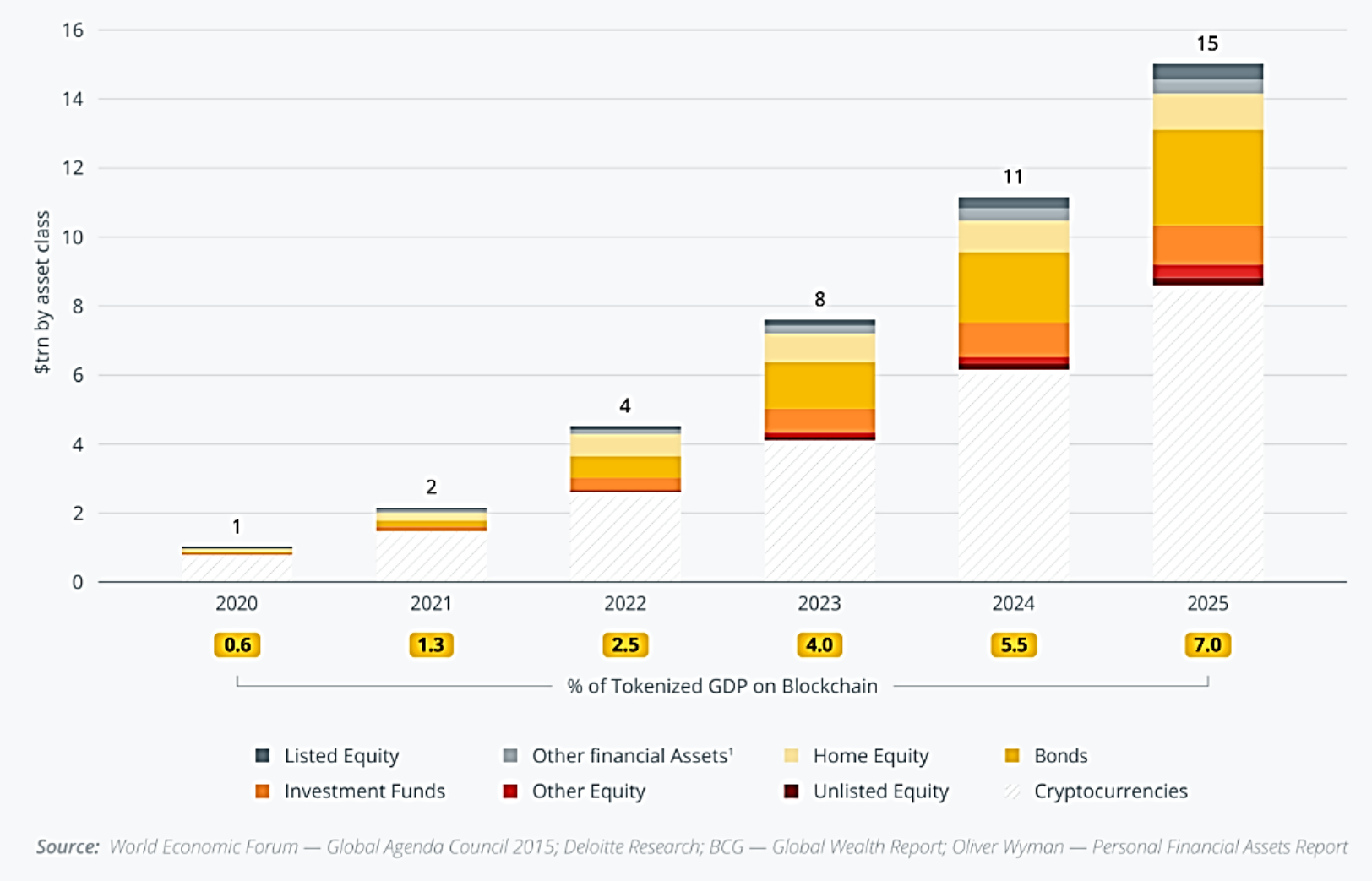
WWW.BLOCKDATA.TECH | INFO@BLOCKDATA.TECH

TODAY OVER $1 BILLION IN SECONDARY MARKET CAP IS TRADING ON REGISTERED EXCHANGES

Total Market Cap **$1,140,940,855.20**

Token	Market Cap	Price	Change %	24H Volume	Exchange	Price Trend
INX Limited INX	$372,279,599	$3.01	5.94%	$66,046	INX Securities	
Overstock OSTKO	$270,503,000	$61.90	4.03%	$19,746	tZERO	
tZERO TZROP	$115,819,891	$5.50	0.92%	$23,309	tZERO	
Blockchain Capital BCAP	$104,376,105	$14.86	0%	$0	INX Securities	
Exodus EXOD (EXIT)	$76,530,412	$28.00	6.67%	$46,984	tZERO	
FirstShot Centers LLC FST	$39,114,665	$1.93	0%	$0	CryptoSX	
Science SCI2	$31,023,487	$1.90	0%	$0	INX Securities	
SPiCE VC SPiCE	$24,124,364	$2.85	0%	$0	INX Securities	
MERJ Exchange MERJ-S	$23,852,343	$2.65	0%	$0	MERJ	
AspenCoin (St. Regis) ASPD	$18,900,000	$1.05	7.08%	$1,154	tZERO	
Tokensoft TSFT	$16,024,618	$1.99	0%	$0	Tokensoft	

THE VOLUME OF TOKENIZED ASSETS IS PROJECTED TO REACH $15 TRILLION BY 2025



Source: *World Economic Forum — Global Agenda Council 2015; Deloitte Research; BCG — Global Wealth Report; Oliver Wyman — Personal Financial Assets Report*

HOW BIG CAN IT EVENTUALLY GET? $866.9 TRILLION

The World Economic Forum estimates the size of the global market for digital asset disruption to eventually be **$866.9 trillion USD**.

- Equity markets: $95 trillion
- Debt markets: $106 trillion
- Securitized products: $10 trillion
- Derivatives: $560 trillion
- Securities financing: repurchase agreements $4 trillion securities lending $2.9 trillion
- Asset management/fund administration: $89 trillion

http://www3.weforum.org/docs/WEF_Digital_Assets_Distributed_Ledger_Technology_2021.pdf

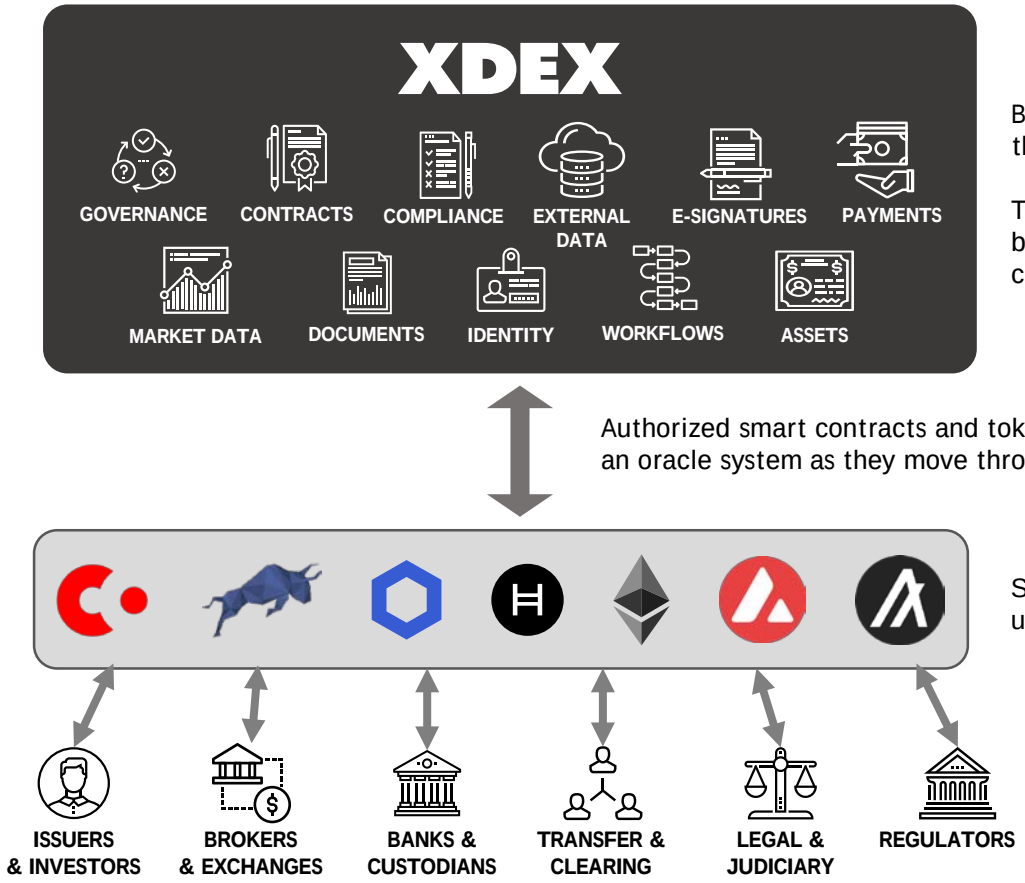
XDEX, THE EXTENDED INDEX

For capital market securities offering issuers, investors, broker dealers, exchanges and alternative trading systems, custodians, banks, and regulators who need common information to process regulatory-compliant digital token-based securities transactions, XDEX provides an immutable information layer to connect with disconnected, siloed enterprise line of business information systems.

Unlike other solutions that simply create smart contracts and tokens on a blockchain, XDEX adds the essential business information translation layer as an “oracle” to smart contracts and tokens to embed compliance at the core.

HOW DOES XDEX WORK?

XDEX is a Web3 information governance, risk, and compliance oracle solution that provides API-based access to real-world business information across a distributed network.



Business metadata and governance is captured and stored in a single source of truth repository and then hashed as cryptographic information within XDEX.

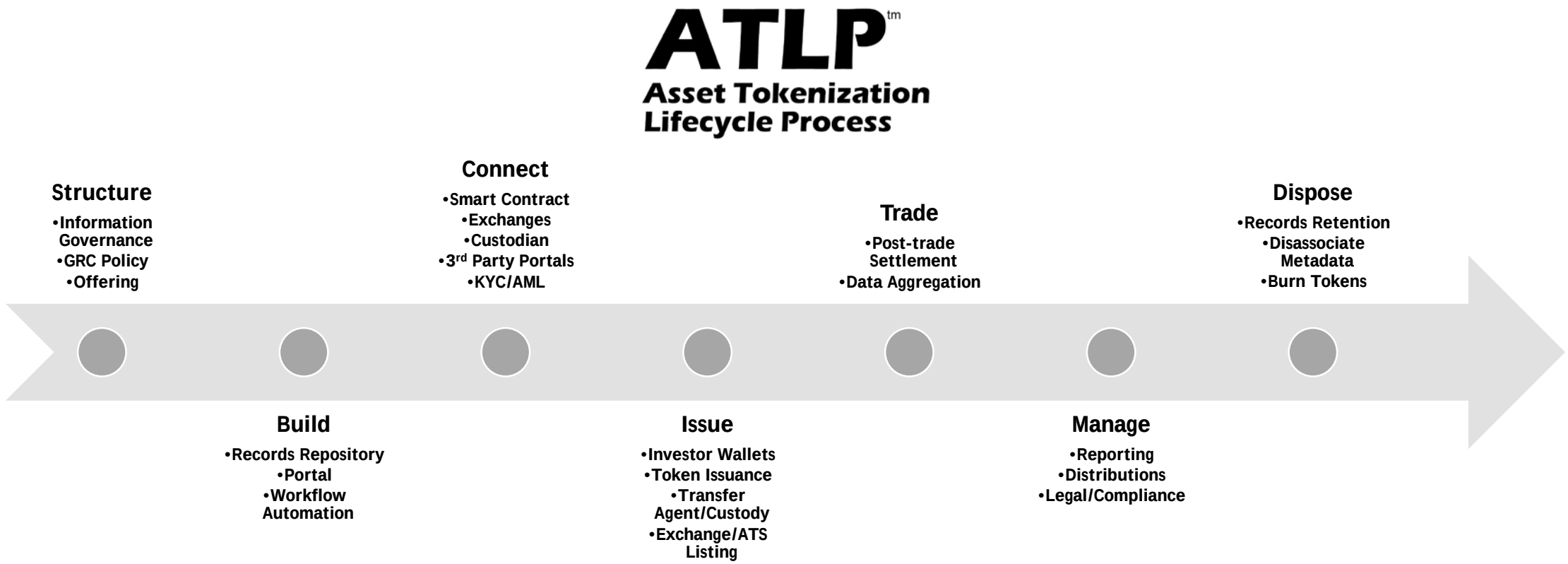
The body of metadata is indexed and categorized as a standard, taxonomy-based system that can be further exposed to public blockchains via an API to be consumed by smart contracts on the chain.

Authorized smart contracts and tokens on public chains can send and retrieve data to and from XDEX through authorized API calls as an oracle system as they move throughout the global, decentralized market ecosystem.

Smart contracts and tokens can be generated on any common public chain network ecosystem for use across the global capital market infrastructure.

All parties related to any market activity may utilize the smart contract or token within their own business process while ensuring business documents, metadata, workflows, and governance remain consistent and intact across post trade market settlement across any jurisdiction.

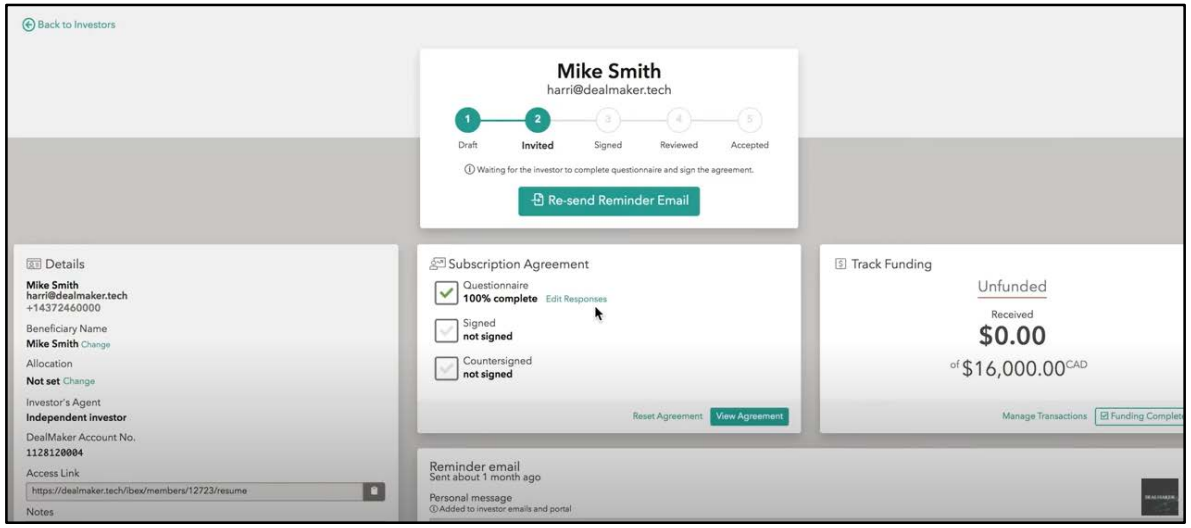
TOKENIZING ASSETS FOR SECURITIES OFFERING ISSUERS



SECURITIES ISSUERS CAN AUTOMATE THEIR TOKENIZED OFFERING AND SUBSCRIPTION PROCESS

XDEX helps issuers automate their offering process by providing a seamless investor experience for subscription, KYC/AML, accredited status verification, and payments.

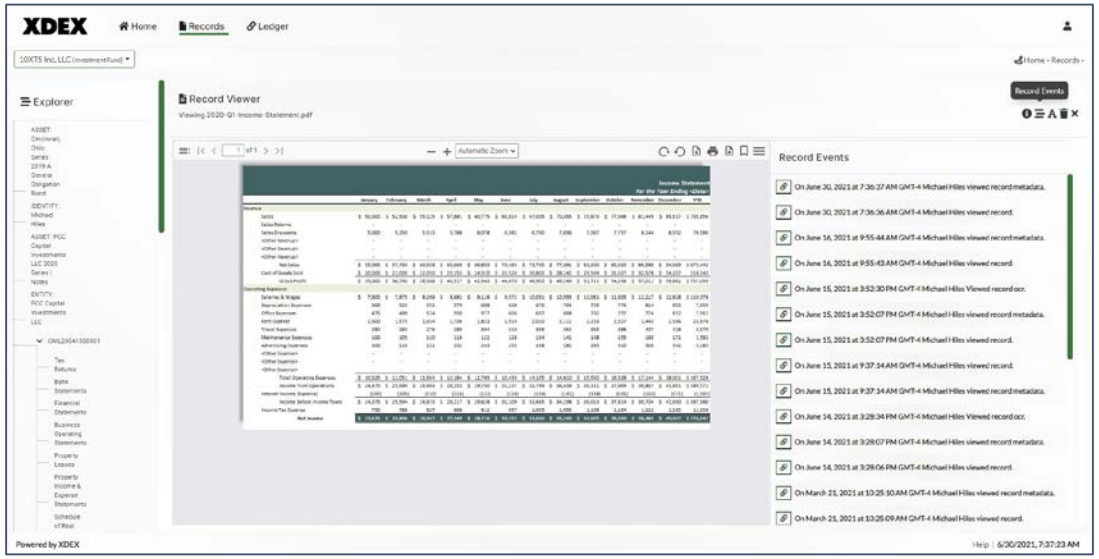
The investor data and documents are ingested into XDEX to then provide downstream integration into broker dealer networks and trading exchanges.



OWN AND CONTROL DATA WITH XDEX CLOUD SAAS PORTAL

Users can access XDEX records and data through the cloud-based SaaS portal that can be branded as a white label solution for offering sponsors.

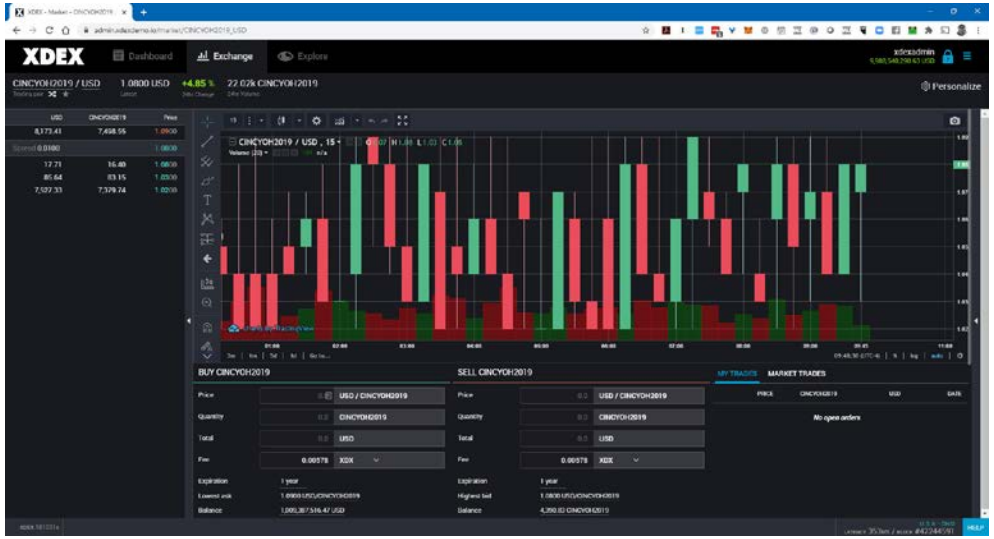
- **Records Management System** – Hashing of documents, metadata, workflows, and logging
- **Information Governance** – Role-based permissions and granular action event logging for comprehensive auditing
- **Issue Digital Securities Tokens** – Digitized assets on a decentralized data ledger.
- **Digitized Asset Metadata** – Connect to XDEX Entity, Asset& Transaction
- **OCR (Optical Character Recognition)** – Automatically scans and converts documents into ASCII text, which is further hashed and encrypted



SECONDARY MARKET INTEGRATION

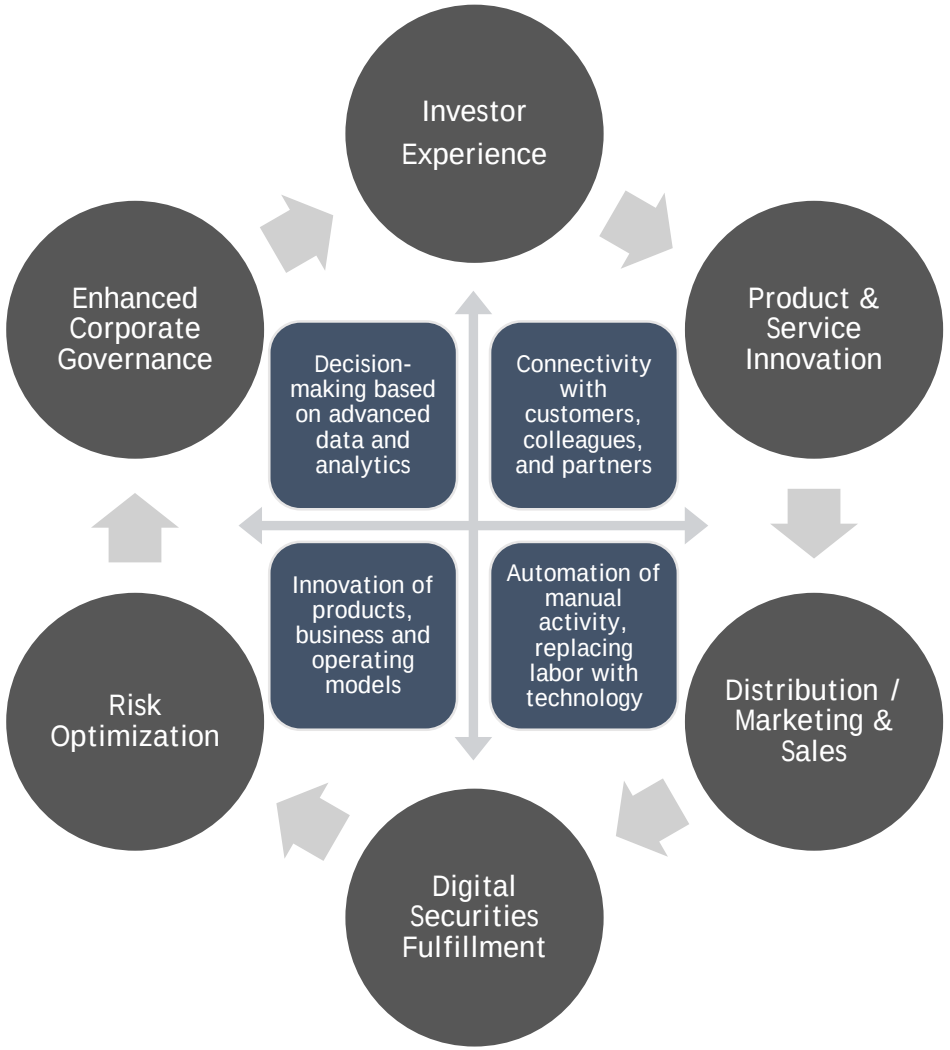
XDEX can connect to secondary markets to provide issuers with trade data about their listed security actively trading in multiple liquidity pools for real-time price discovery.

- **Asset Portfolio** – Show account-based asset portfolio holdings.
- **Issue Digital Securities Tokens** – Digitized assets on a decentralized data ledger.
- **Digitized Asset Metadata** – Connect to XDEX Entity, Asset & Transaction
- **Secondary Market Trade Settlement** – System of record for all secondary market transactions & trades on exchanges (manual or integrated).
- **External Trading Platform / Exchange Integration** – Connect to other trading platforms to force tracking of asset
- **Market & Asset Analytics** – Capture entire data set for deep analysis, ML, AI.
- **Trade Chart Visualization** – Present market data with traditional chart models and popular indicators.
- **Aggregated price settlement feeds** – connect price feeds from multiple trading platforms, ATS, exchanges, broker dealer networks.
- **Fully-functioning Decentralized Order Book** – matching orders as a decentralized network for regulatory-compliant exchanges, ATSs, private capital markets.



WHAT ARE THE BENEFITS?

- **Confidential** – Sensitive, contractual information is only ever shared with parties entitled to see it. Parties can be assured that they are notified of all events affecting them.
- **Auditable** – Institutions and their regulators can comply with reporting and compliance requirements in real-time, rather than days or weeks after transactions are completed.
- **Programmable / Extensible** – XDEX serves as a common foundation which can be extended with additional functionality, entirely new product lines or even to power other markets.
- **Zero Reconciliation** – Continuous and distributed data integrity removes the need and cost of reconciling between multiple parties automatically and in real-time.
- **Common Workflows** – Market rules and common business workflows can be captured and independently verified by every party involved in an agreement to ensure systems are never out of sync.
- **Lower Costs** – Reduce administrative costs for audits, filings, and transactions. In the event of litigation, can radically reduce pre-trial eDiscovery and records hold costs.
- **Automated Regulatory Compliance** — Reduce reconciliation costs, provide transparency and automated regulatory compliance, create a full window into all market data and transactions.

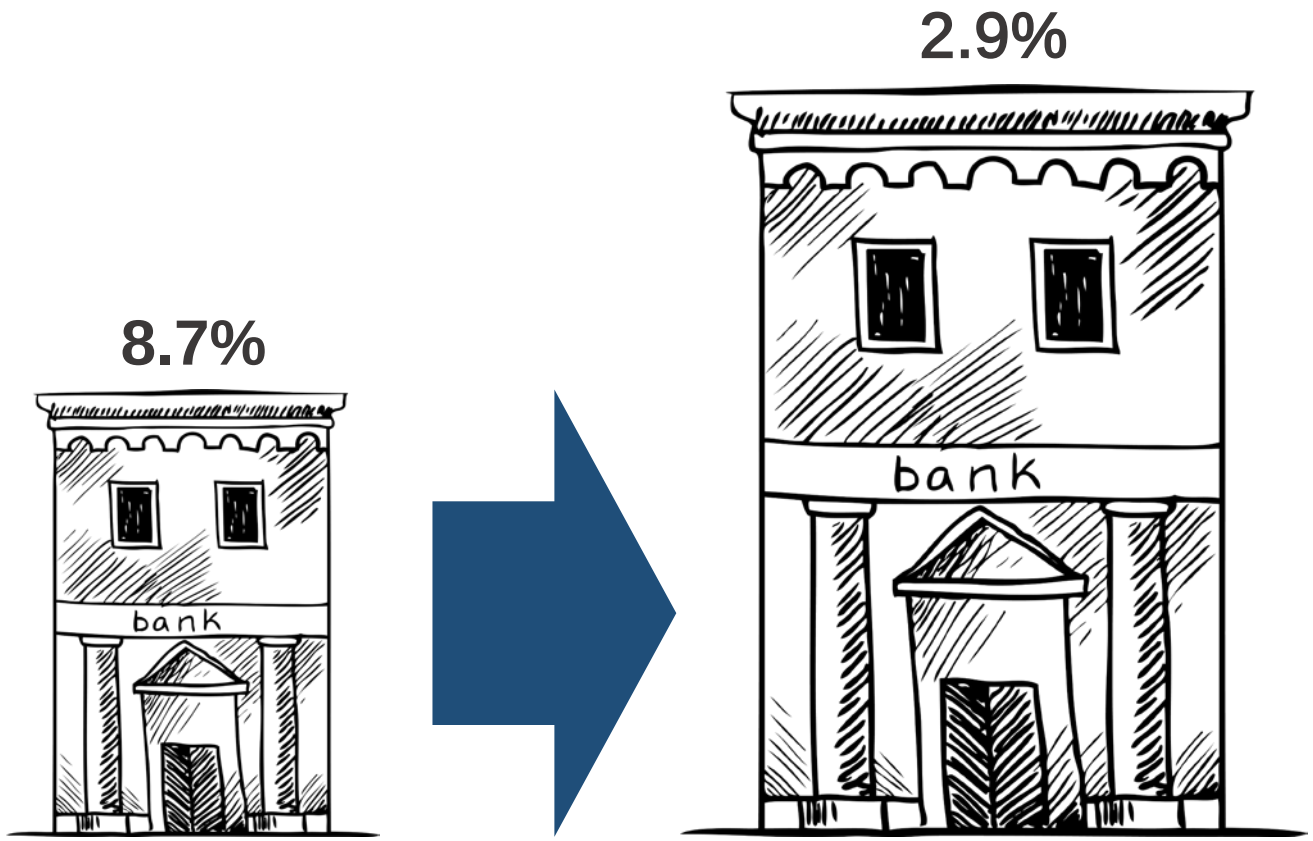


HEAVY COMPLIANCE COSTS DISPROPORTIONATELY HURTS SMALLER FINANCIAL INSTITUTIONS

In a 2018 study released by Gartner, by 2030, 80% of traditional financial services firms will fold, become commoditized, or exist but will not compete effectively in the market.

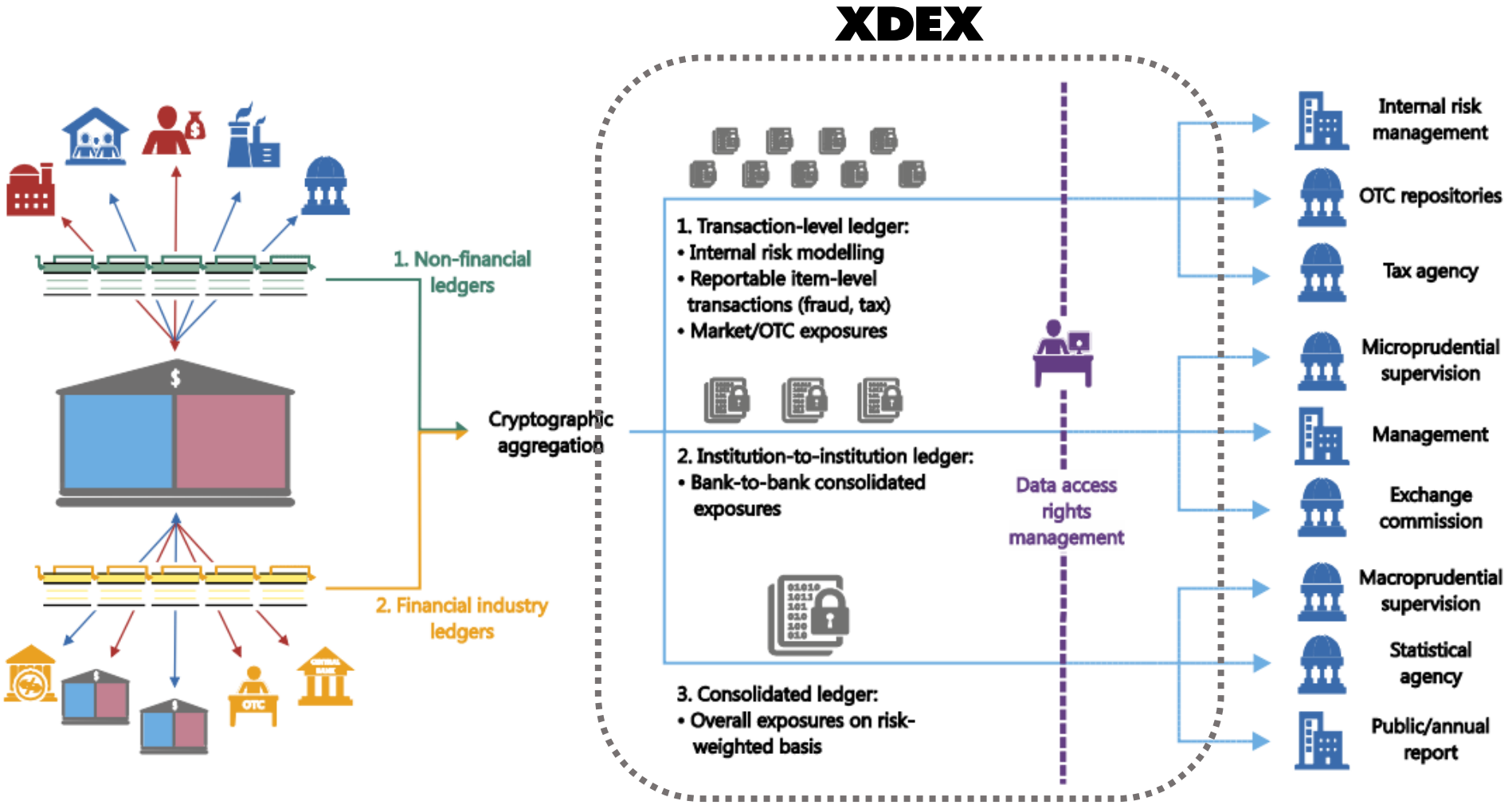
Banks with under $100M in assets reported that total compliance costs represented an average of 8.7% of their non-interest expense.

Meanwhile, banks with $1-10 billion in assets reported compliance costs represented an average of 2.9% of their non-interest expense.



SOURCE: Gartner & St. Louis Federal Reserve Bank

POWERING EMBEDDED COMPLIANCE AND GLOBAL SUPERVISION MONITORING



Q&A

michael@10xts.com

@michaelhiles