

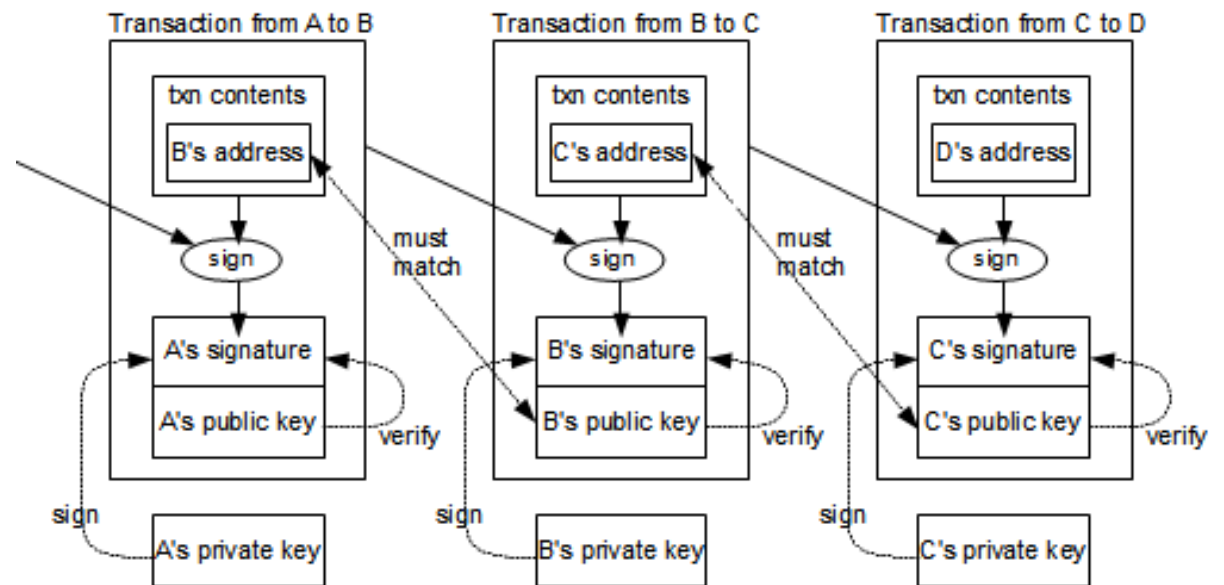
What is Blockchain?

Xin Yu, PhD CFA
Presentation for WSFC Webinar Meeting
Thursday, May 04, 2017

BLOCKCHAIN **ESSENTIALS**

Google says

A blockchain is a public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as 'completed' blocks are added to it with a new set of recordings. The blocks are added to the blockchain in a linear, chronological order."



Transaction is an assets transferring

- Anything that is capable of being owned or controlled to produce value, is considered **an asset**
 - can be tangible or intangible
 - value can be converted into cash.
- Cash also an asset.
- Asset examples:
 - Cars, value clothes (physical)
 - Bonds, securities, repurchase agreements (intangible)
 - Licenses & patents (intangible assets)
 - Music, video, games (intangible, digital)



Participants, Transactions & Contracts

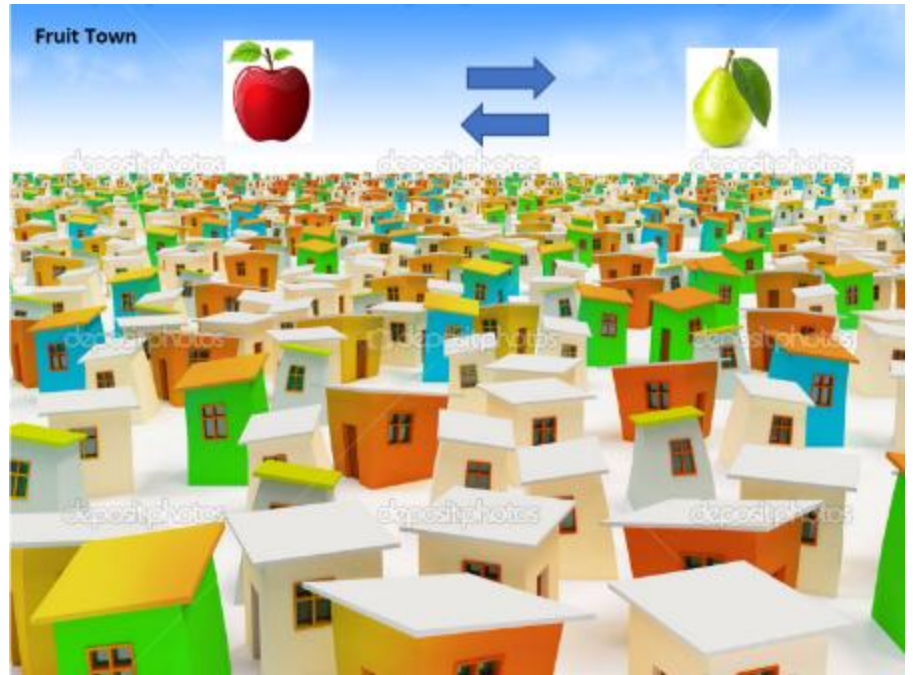
- A **participant** is a member of a business network
 - Customer, Supplier, Government, Regulator
 - Usually reside in an organization
 - Have specific identities and roles
- A **transaction** is an asset transfer between two or more participants, for example
 - John gives a car to Anthony (**simple**)
 - John gives a car to Anthony, Anthony gives money to John (**more complex**)
- A **contract** is set of conditions under which transactions occur, for example
 - If Anthony pays John money, then car passes from John to Anthony (simple)
 - If car won't start, funds do not pass to John (as decided by independent third party arbitrator)



Transaction 1000 years ago

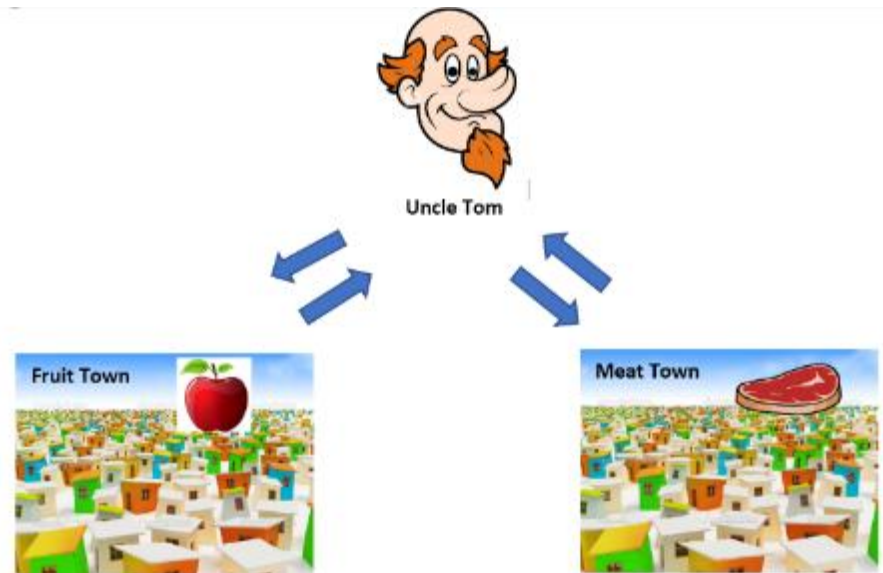
Transaction in a town

A gentleman Peter, who lived in a tiny little town "Fruit town" a thousand years ago. He has nothing more than apples (his asset). Peter wanted to exchange his apples for some pears and knows only Julie in his town has pears.



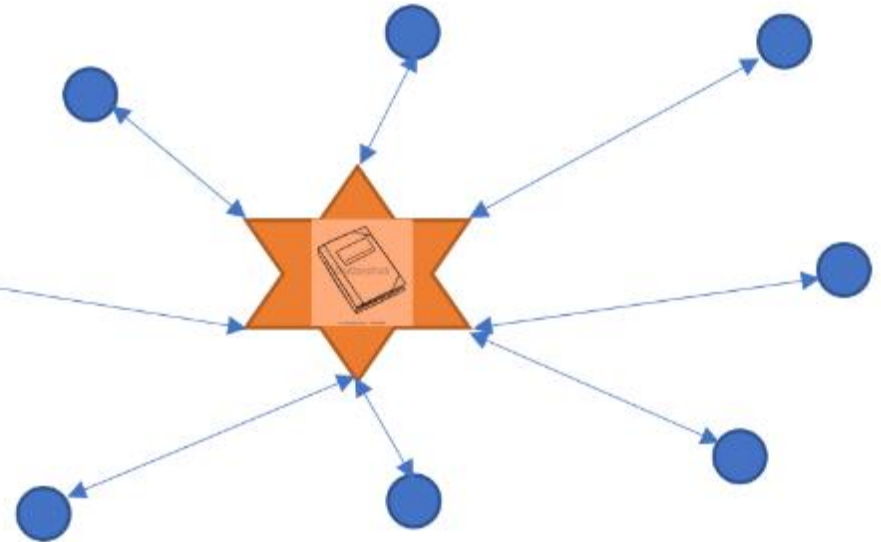
Transaction between two towns

Peter wanted to exchange his apples for some beef. However, Peter is living in a “fruit” town and he has to go to a “meat” town to make the exchange. Since Peter knows little about the meat town and also does not want to travel to the town to explore by himself, Peter asked help from Uncle Tom, who is well known by people in both towns.



More and More Transactions

Uncle Tom gets more and more requests like this, Tom felt he cannot rely only on his brain memory to do the verification. He needs to keep some records about who the transaction parties are (identity) and where the goods come from and go (change of ownership).



What if?



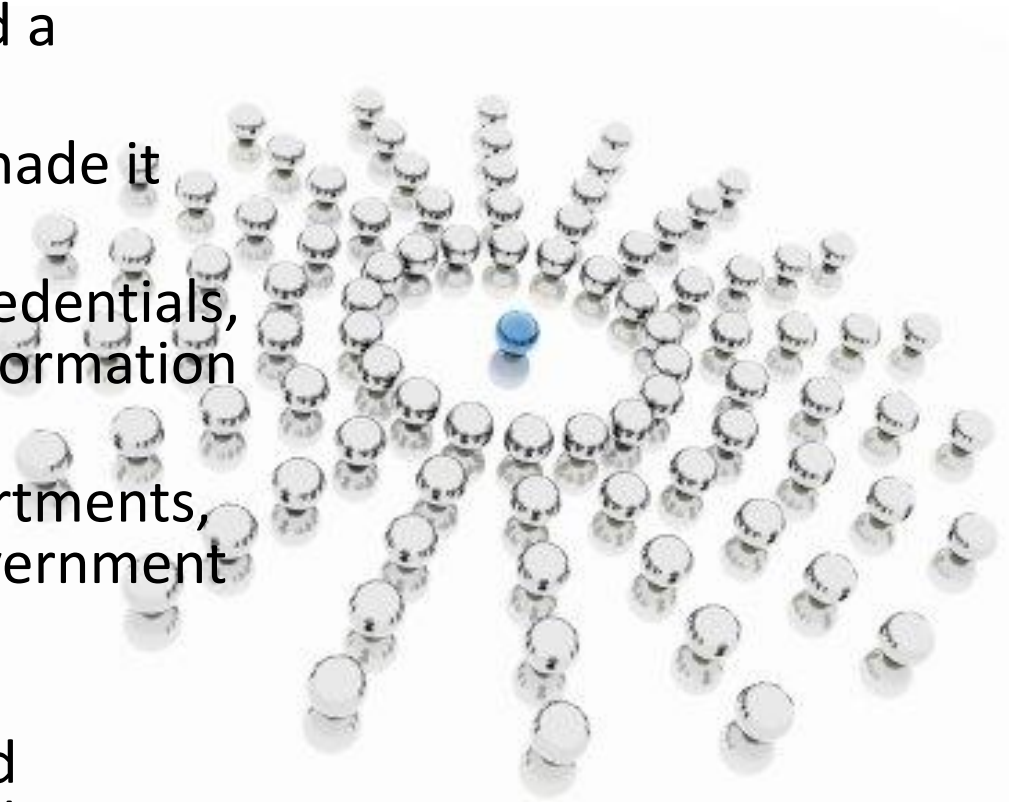
- What if Tom made some wrong records,
- What if Tom just adds some apples to his best friends
- What if someone tempers with Tom's records?
- Maintain the centralized records and the authority of Uncle Tom
- But add some regulatory audit and examination on the records
- Wstablish some rules and laws to penalize any fraud and dishonesty.



Transaction Today

Nothing Really Changed

- The way people do business is almost the same as they did a thousand years ago,
- The modern technologies made it more complicated.
- Record and maintain the credentials, identity, and transaction information (ledger)
- Centralized corporate departments, regulatory institutes, or government organizations now).
- A comprehensive auditing, regulatory examination, and enforcement system to do the error check and fraud punishment.



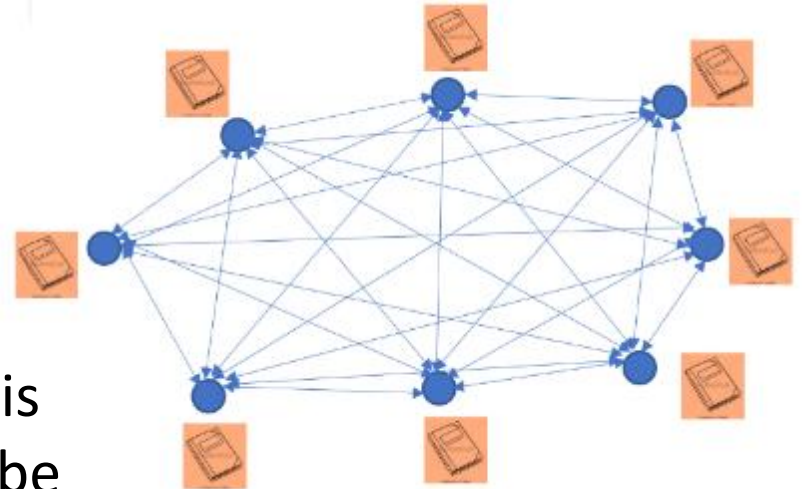
Problems of centralized census

- Only have the big audit and regulatory examination system to minimize the risk.
- The centralized points of vulnerability are difficult to control
- Especially in the digital era, as anonymous computer hackers can easily exploit any central point of failure.



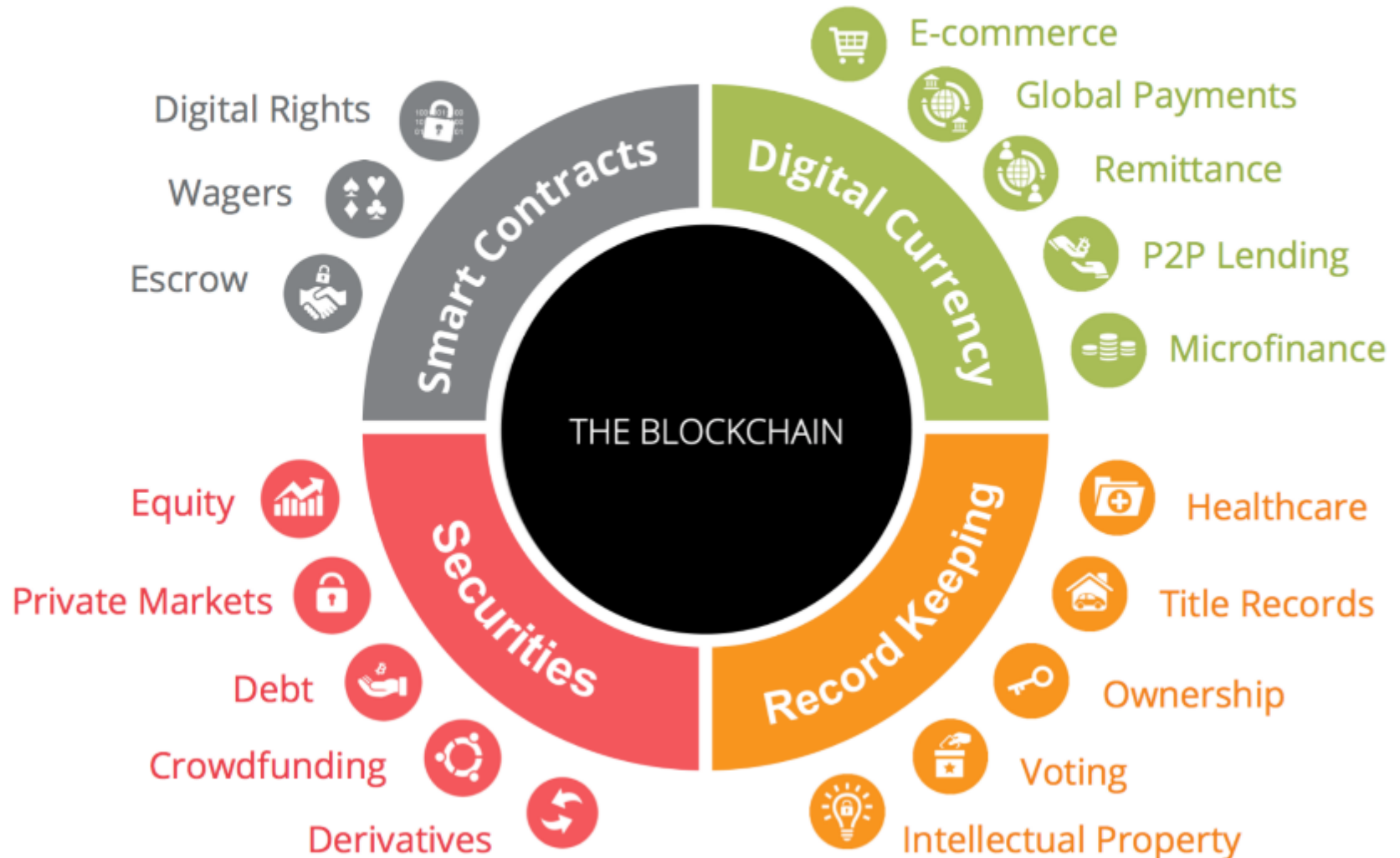
What if...Blockchain

- What if we gave the ledger of everyone's transaction related information to everyone?
- The information are updated synchronously and any new transactions will be recorded in everyone's book
- This network system described is named "blockchain". Block can be viewed as the "transaction database" and Chain is the connector linking every block in the system.



Blockchain Potential Applications & Disruption

The blockchain is radically changing the future of transaction based industries



Challenges



Versus



- A revolutionary design with relatively mature technologies.
- Challenging to be implemented and customized for business practices.
- The needs of computing power, network infrastructure, and energy

- The shortfalls of technological advancement
- can be easily turned into a real world application and business practice once available

BLOCKCHAIN **For Financial Services**

Silos of the Financial Services Industry

Financial Services

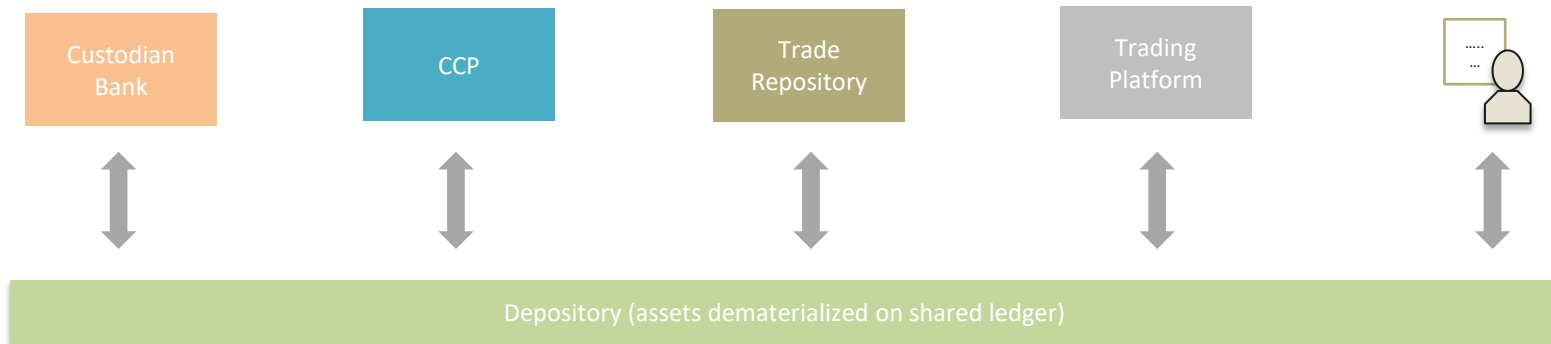
Retail/Commercial Banking	Investment Banking	Markets Infrastructure	Asset Management	Insurance
Depository	Investment Banking	Exchanges	Mutual Funds	Life
Lending	Sales & Trading	Custody/Clearing	Mandates	Property & Casualty
Non-Depository Credit Institutions	Underwriting	Stocks	Alternatives	Accident & Health
Domestic Payments	Structured Finance	Commodities	Wealth Management	Specialty
International Payments	Prime Brokerage	Foreign Exchange	Trust Services	Reinsurance
Remittances		Futures & Options		Brokerage

Reduce costs and complexity

Blockchain technology offers a way for market participants to access dematerialized assets **directly** without always going through other participants needlessly



Centralized Repository (today's system): most participants are disconnected from their asset depository, settling transaction would require participants to collaborate in a flow that is **slow**, **inefficient**, and **expensive**



Shared Repository: all participants can interact with depository directly without going involving third parties, potentially making post trade operations **cheaper** and **faster**

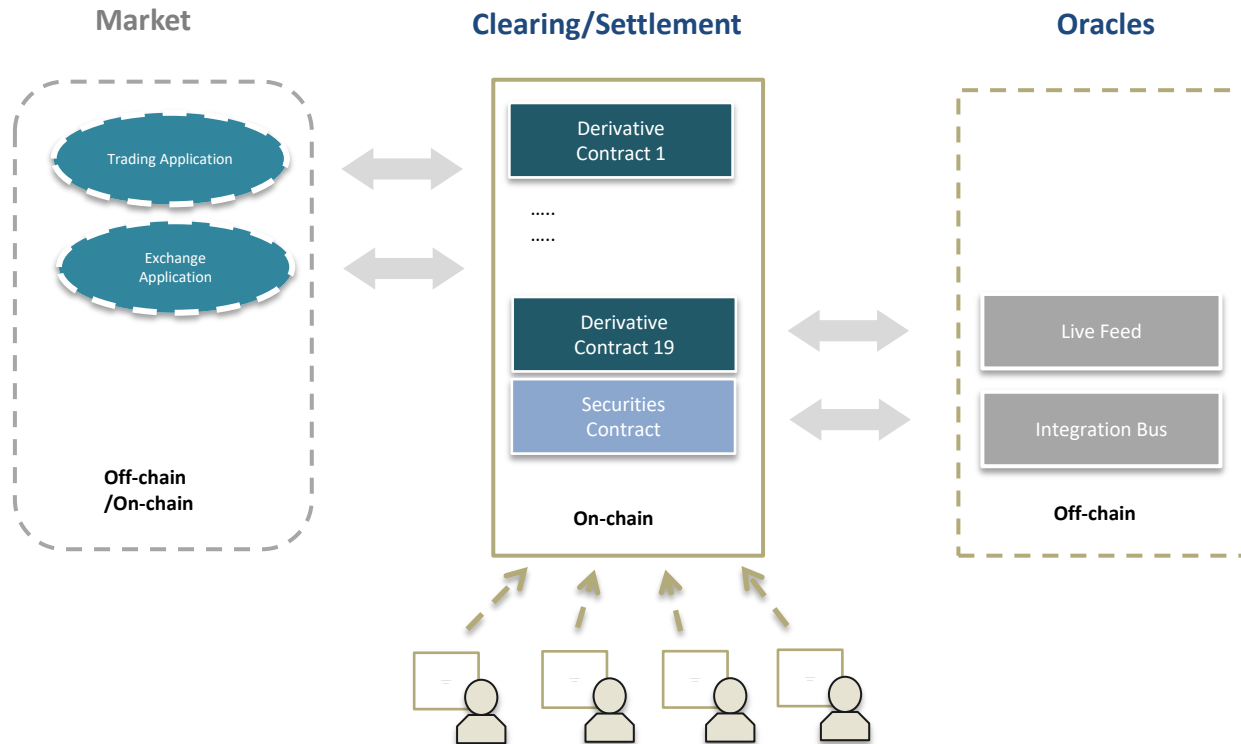
Financial Industry Applications best suited for Blockchain

- Financial Instruments
 - Payments – Cross Border, P2P, Corporate and Interbank
 - Private Equity
 - Bonds
 - Derivative commodities
 - Trading records
 - Spending records
 - Mortgage/Loan records
 - Microfinance
 - Servicing records
- Stack of Processes
 - Clearing Networks
 - International Transfers
 - Clearing and Settlement
 - auditing, reconciliation, reporting, settlement
 - Asset Ownership

BACK UP

Blockchain for Financial Market

Trading, clearing, and settlement functions can all be automated on a blockchain network using smart contracts and oracles.



Market

Trading/exchange applications can live either on-chain or off-chain (i.e. off-chain applications are often more centralized, but likely offer better latency).

Clearing/Settlement

Final clearing/settlement of financial assets can be automated through smart contracts, which have direct access to assets defined on chain.

Oracle

Oracles are off chain services that integrate on-chain contracts with existing systems; network participants do not interact with oracles directly.

IBM – Financial Services use cases for Blockchain

Blockchain for Banking

Letters of Credit

As a bank handling letters of credit (LOC) for my clients, I need a common ledger that allows me and all counter-parties to have the same validated record of transaction and fulfilment of conditions, so that we can increase trust and speed of execution from 4 days to <1 day. If we can drive out 99% of the time and cost, we can offer innovative LOC solutions for a wider range of clients, including start-ups that are “born global.

Corporate Debt

As a bank handler of corporate debt, I need a Blockchain based system so that I can pay vendor invoices for my corporate client immediately and win the highest NET discount while immediately letting my client validate that the invoice was executed and the money paid, and also so that I don't need to build another system for innovative factoring use cases and government oversight measures — one API for all. I want to do this at a market-level, so that I don't have to build one for each of my client relationships, and so that I can spread the cost of building and maintaining the system.

Repurchase Agreements

As a repurchase agreement trader, I need a transparent marketplace of bids and asks, so that I can discover, trade, and execute agreements with relative assurance that there will be no repudiation or other issues. I don't want to have to be subject to the string of counterparties exerting control over the market; rather, I want to be an equal partner in the network, trade directly, and spread the costs/risks.

Supply Chain and Self-Executing B2B Contracts

As a corporate buyer, I want to be able to submit my purchase contract to a network I share with the supplier, which will convert the agreement into a validated, trusted, self-executing process, so that when the PO is appended to the ledger, supply has been received, and other events occur, the terms of the contract are automatically executed, and both the supplier, me (the buyer), our banks, logistics partners and other stakeholders all can have visibility and be assured of proper completion of the transaction.

IBM – Financial Services use cases for Blockchain

Blockchain for Banking Consortia	
Security Services	<p>Security Settlement: Once financial assets are dematerialized on a shared ledger, all stakeholders will have direct access to the asset depository and the power to settle trades, without always going through intermediaries needlessly.</p> <p>Post Trade Operation: Post trade processes such as trade capture, enrichment, confirmation/affirmation, clearing, and settlement can be automated on shared ledger, potentially reducing post trade operation time from days to seconds.</p> <p>Trade Repository: By design, Blockchain is a secure record repository of ordered collection of financial transactions. It records the history of asset control and state changes, reducing the need of maintaining a separate trade repository for record keeping.</p>
Capital Market	<p>Derivative Trading: Connect potential buyers and sellers on a decentralized network. Offers placed on Blockchain network can be automatically seen by all participants, the network will be cheaper and potentially bigger than ECNs today because the risk and cost of maintaining the network is spread across all participants (there will not be a single owner charging premium for maintaining the service).</p> <p>Derivative Post-Trade Management: Derivatives contracts can be managed and automated through smart contracts on shared ledger, significantly cutting down the management cost and time while reducing the intra-day risk.</p> <p>Syndicated Loan: Help borrowers and arrangers to broadcast their offers to all potential investors on a Blockchain network, and to automate the syndication process.</p>
Trade Finance	<p>Cross-Currency Payment: Automatically connecting market makers and bypassing intermediaries to significantly reduces time taken for cross currency payment from days to seconds.</p>
Card Operation	<p>KYC: Creditor card issuers can record customer credit histories on a shared ledger so that customer information can be easily shared (or sold) between companies.</p>