Enterprise Blockchain Solutions for Financial Services: Techniques and Challenges

Dr. Ziyuan Wang
Senior Research Fellow - Blockchain
Swinburne University of Technology
About Us

Using digital technology to enable businesses and industries beyond traditional boundaries

Application Areas
- Environment
- Healthcare
- Education
- Urban Development
- Food

Application Areas
- Finance
- Manufacturing
- Marketing
- Retail
- Transport

Technology Drive

Digital Research Innovation Capability Platform

Data Analytics  Cybersecurity  Visualization  IoT  Blockchain  AI
Outline

• Part I: Blockchain & core techniques

• Part II: Enterprise Applications & Blockchain Platforms

• Part III: Key lessons we learnt in practice
Blockchain Impact

10% of Global GDP will be stored on blockchains or blockchain related technology by 2025.

$360 Billion The business value added by blockchain by 2026, then to exceed $3.1 trillion by 2030.

$20 Billion Estimated revenue of the blockchain technology market by 2024.

30% of Banks Blockchain can offer a reduction in banks’ costs by up to 30%, or $12 Billion.

Source: World Economic Forum; ITWeb; Cision; IBM; Gartner; MarketandMarkets
Why Blockchain

• Enable exchange of value without trusting intermediaries.

• Maintain a single source of truth and a shared set of rules across entities without anyone being able to alter them and control the system.

• Anything that is capable of being owned or controlled to produce value, is an asset

Blockchain shift the cost of trust

Two fundamental types of asset

– Tangible, e.g. a house
– Intangible, e.g. a mortgage

Intangible assets subdivide

– Financial, e.g. bond
– Intellectual, e.g. patents
– Digital, e.g. music

Cash is also an asset

– Has property of anonymity
Problem...

... inefficient, expensive, vulnerable
Shared Ledger...

... with consensus, provenance, and immutability
Blockchain Benefits

Saves time
Transaction time from days to near instantaneous

Removes cost
Overheads and cost intermediaries

Reduces risk
Tampering, fraud & cyber crime

Increases trust
Through shared processes and recordkeeping
Core Techniques

- Asymmetric Cryptography
- Digital Signature
- Hash Functions
Asymmetric Cryptography

• Uses a pair of keys for encryption
  • Public key for encryption
  • Private key for decryption
• Messages encoded using public key can only be decoded by the private key
  • Secret transmission of key for decryption is not required
• Every entity can generate a key pair and release its public key
Digital Signature: Authentication

• A digital signature is a way to prove that a message originates from a specific person and no one else.
  • A guarantee of the source of the data
  • Proof that the data has not been tampered with

• Your public key is how others are able to identify you. Your private key gives you the power to digitally sign and authorize different actions on behalf of this digital identity when used with your public key.
Hash Functions

• A *hash function*, takes any input, and produces an output of a fixed size.

• The process of applying a hash function to some data, is called *hashing*.

• The output of a hash function is called a *hash*.

• digital fingerprinting: It verifies and confirms that the output produced from hashing has not been meddled

• e.g. SHA256 is one example of hash function (Bitcoin uses). It outputs 256 bits of 1s and 0s.
Properties of Hash Function

- **Deterministic**: same input yields same output. This can be used to verify that two documents are the same.
- **One-way**: Given the hash, hard to discover the input.
- **Collision resistant**: it is hard to find two inputs that yield the same hash.

Example: SHA256 hashes of ‘hello’ compared to ‘Hello’

- **hello**: Hash 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824 (Hexadecimal)
- **Hello**: Hash 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969 (Hexadecimal)
What is Blockchain

• Establish trust among unfamiliar or unknown partners by cryptographic protocols.

• Made up of sequentially grouped, verified blocks of transactions. Blocks are chained together, creating a shared record of all transactions.

• Verify and store information in peer-to-peer networks by consensus with no central authority or intermediary.

• Immutable record of transactions dating back to the first transaction.
How does Blockchain Work?

Someone requests a transaction.

The requested transaction is broadcast to P2P network consisting of computers, known as nodes.

Validation

The network of nodes validates the transaction and the user's status using known algorithms.

A verified transaction can involve cryptocurrency, contracts, records, or other information.

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
Common Misconceptions

• There is no privacy/ Everything is shared and open
• It is lack of regulation
• It is not secured, many hacks and lost cryptocurrencies
• Blockchain consumes intensive energy for mining
Requirements of Blockchain for Business

Business Network decides the assets to share on the ledger. Rules set by smart contracts

Choosing what to share

Transaction endorsement

Transactions provably endorsed by relevant participants. e.g. sender bank, receiver bank, payments provider

Knowing who you're dealing with e.g. KYC, AML, CFT

Identity

Privacy and Confidentiality

Transaction visibility is need-to-know.
Part II: Enterprise Applications for FS

• Current Status & Challenges
• Enterprise Applications
• Platforms for Enterprise Solutions
Rising Problems with Traditional FS

Antiquated and Inefficient Processes

- 4+ million faxes received by syndicated loan custodians in 2012

Settlement Delays

- Average settlement time for a syndicated loan in the US: 20+ days
- In Europe: 48 days

Fraud

- $40+ billion per year
  - The FBI estimate for the total cost of non-health insurance fraud

Overheads

- $4-$5 billion
  - ASX estimate of end-to-end costs in Australian equity markets which are ultimately paid for by the issuers and end-investors

Concentration of Risks

- £277 billion per day
  - Volume handled by UK’s RTGS payment system that went offline for ten hours in 2014, delaying deals worth billions

Source: Smart Contracts in Financial Services: Getting from Hype to Reality, Capgemini
Existing Use Cases for FS

### Capital Markets and Investment Banking
- Corporate Finance:
  - Initial Public Offers (IPOs),
  - Private equity
- Structured Finance: Syndicated loans, leveraged loans
- Stock exchange market infrastructure

### Commercial and Retail Banking
- Trade Finance:
  - Supply-chain documentation, invoicing and payments
- Mortgage Lending
- Loans and crowdfunding for startups and small and medium enterprises

### Insurance
- Automated claims processing in motor insurance, crop insurance, etc.
- Fraud prevention in luxury goods
- New products: insurance for the sharing economy, autonomous vehicles, peer-to-peer insurance, cyber insurance

Source: *Smart Contracts in Financial Services: Getting from Hype to Reality*, Capgemini
Key Metrics about Using Blockchain

• Identifying a good blockchain use-case is not always easy
  • However there should always be:

  • A **business problem** to be solved that cannot be more efficiently solved with other technologies
  • An identifiable **business network** with Participants, Assets and Transactions
  • A need for **trust** with Consensus, Immutability, Finality or Provenance

Applications:
• Shared KYC
• Bank Guarantee
• Micro-Insurance
• Document and Workflow Management for Trade and Logistics
What is Shared-KYC?

• Know Your Customer (KYC) identifies a set of processes that financial institutions implement when onboarding a new customer for any of the services they provide, in order to comply with existing regulations. KYC is just a portion of what is comprehensively called Customer Due Diligence (CDD).

• While this process is rather simple for single individuals, it can be quite complex for when on-boarding corporate organizations.

Our Goal with Shared KYC

• To provide a technical solution for Corporate KYC that is faster, more accountable, and eventually cheaper.
Corporate KYC Paint Points

**Corporate Customers**
- Poor customer experience
  - Changing requirements from bank to bank
  - Long on-boarding times

**Regulators & Auditors**
- Lack of standardisation
- Effectiveness of audits
  - Information access
  - Post-mortem vs real-time

**Financial Institutions**
- Expensive*
  - $60M on average in CDD/KYC spending per bank
  - 10% > 100M
  - 3% > 500M
  - Lost revenue opportunities

- Time Consuming
  - 5-100 documents per KYC
  - ~24 days to on-board a new client
  - KYC refresh takes 20 days

- Reputational & Regulatory Risk
  - Fines and shutdown for non-compliance
  - Brand damage
Corporate customer on-boarding is today heterogeneous, rather manual, and directly affects the business of both customers and financial institutions.

We imagine a future where corporate KYC is performed on top of an integrated platform, which not only makes it more effective but also develops new business opportunities.
Benefits of Shared KYC on Blockchain

By having a single integrated platform, based on a distributed shared ledger, where KYC data is securely stored, we expect to:

**Increase speed**  from 3~4 weeks of on-boarding time, to 1 week or less by compressing data gathering and automating processes

**Reduce costs**  decrease significantly costs to at least 20% less by eliminating duplication through shared services

**Reduce risk**  via a redundant, distributed and shared ledger that acts as in immutable, assured audit trail of all the corporate KYC processes

**Enhance experience**  via instant visibility across all shared information by a customer, secured through a consent-based mechanism, which controls information access
Shared KYC Scenario

Customer
Could be an individual or a corporate customer, who has an identity in the Blockchain.

KYC Portal
It is the point of access for the customer to manage its information in the network.

Fulfilling Bank
The first bank (Bank A) to establish a relationship with customer.

Requesting Bank
Another bank (Bank B) onboarding the customer and requiring the KYC information.

Regulator
To verify compliance, performs investigations and audits by inspecting the Blockchain.

The parties form a consortium to share KYC information while respecting business constraints. They use Blockchain as the shared permissioned network where information is exchanged.
## Business Constraints

<table>
<thead>
<tr>
<th>Anonymity of Relationships</th>
<th>The relationship between a customer and a bank is confidential. Therefore, when sharing/requesting information bank’s identity must be hidden.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>The access to a customer profile (and corresponding documentation) must be explicitly granted by the customer (consent).</td>
</tr>
<tr>
<td>Dynamic Permissions</td>
<td>Consent is granted and revoked in accordance with the evolution of the customer-bank relationship.</td>
</tr>
</tbody>
</table>
Model for Privacy and Consent

Consent Model
Defines how access to profile and sensitive information is managed and granted or revoked by preserving the confidentiality of the relationship.

Document Share Model
Allows for anonymous but verifiable share of documents based upon consent.

14 May 2019
ICBC 2019 Tutorial
Bank Guarantees for Commercial Property Leasing
What is Bank Guarantee?

Bank guarantee is a bank’s unconditional undertaking to pay one party in the event of another’s default. They are used across many industries to secure contracts, be it in the trade of goods and services, financial transactions, industrial projects, the development of property, or the leasing of assets.
Issues in the Current System

• **Physical document management**
  • Significant costs associated with management of a paper-based guarantee
  • Guarantees as a digital asset will simplify guarantee lifecycle management

• **Fraud risk**
  • Tenant (applicant) fraud arising from the provision of forged or duplicated paper guarantees
  • A shared ledger as a single source of truth will eliminate document forgery

• **Inefficient reporting & management**
  • Storing, tracking and reporting large numbers of documents is highly inefficient
  • Analysis of digital data will greatly improve the ability to make decisions from aggregate data

• **Non-standard T&Cs and formats**
  • Variations in the articulation of contract terms and guarantee formats between banks, landlords and tenants result in a large manual review effort
  • Blockchain can embed industry standards into the business rules of the platform to drive standardization
Why Blockchain?

• Bank Guarantees are offered by multiple institutions, and many different applicants and beneficiaries require their use – A single network managing all of these provides a single point to manage all guarantees a particular user is party to

• The strong security offered by DLT technologies, and the nature of being a single source of truth greatly reduces the risk of fraud or lost documents

• Bringing guarantee providers into a single network creates a platform to drive standardisation
Scope of Proof-of-Concept

4 core capabilities are involved in implementing:

- Issue a new guarantee
- Amend an existing guarantee
- Demand payment on a guarantee
- Cancel a guarantee

2 additional user stories improve on the usability of the solution:

- Search for a specific guarantee
- Report across multiple guarantees
System Architecture

Application Server

- REST API
- Notifications Manager
- Business Application Logic
- Fabric SDK Node

Hyperledger Fabric

OrdererOrg

Org1

- Membership Service Provider
- Peer + CouchDB (x2)

Org2

- Membership Service Provider
- Peer + CouchDB (x2)

Chain Code (Deployed on Peers)

- Guarantee Lifecycle Manager
- Request Lifecycle Manager
- Query Manager

Web Application

14 May 2019

ICBC 2019 Tutorial
AI Driven Micro Insurance Marketplace on Blockchain
Empowering users and insurance providers
Global Market Opportunity

Customers

Large numbers of drivers in developing countries without insurance:

- 65% to 70% in South Africa\(^1\)
- 60% in India\(^2\)

Insurers

Usage-based auto Insurance (UBI) is expected to grow globally\(^3\): 12 million in 2015 → 142 million in 2023

---

\(^1\) [11.4 million cars on SA roads not insured](http://example.com), 2016.
\(^2\) [60% of vehicles on Indian roads don’t have insurance](http://example.com), 2017
\(^3\) IHS Automotive, [Auto Tech Report: Usage Based Insurance 2016](http://example.com)
Value Proposition

Customers

• Lower premiums 5-30%[^4]
• Increased transparency
• Make purchasing of policies easier
• Reduce complexity of the claim process

Insurers

• Innovate products and services
• Automate underwriting and claims handling by use of smart contracts
• Improve customer experience
• Reduce customer’s privacy concerns on personal and sensitive data

Project Outline

• Provide dynamic Pay-As-You-Go (PAYG) insurance for automobile drivers:
  • Link insurance cost to route, driving duration and other factors such as weather conditions, road conditions, driving behavior, etc.
  • Dynamic cost calculation gives customers more accurate quotes, allowing customers to choose which factors are most important to them

• Provide a shared ecosystem for insurance companies to share customer history:
  • For instance, this data sharing can enable insurers to build more accurate risk models for customers
  • Insurance providers can leverage dynamic quotes to adjust price based on dynamic variables, such as weather, time and demand, etc.
AI-Driven Insurance Marketplace

• Lots of useful analytics can be derived from the data we are storing in the blockchain (e.g. driver risk profile, trip and claim history etc.)

• However, much of these analytics are not part of the core business of insurance companies, therefore there is a potential for these analytics to be offered via a marketplace

• This marketplace could include analytics such as:
  • Fraudulent claims identification
  • Route adherence to micro insurance policy
Why Blockchain

• Insurance companies have no basis for trusting each other, yet must also work together in the marketplace to ensure the allocation of policies for driver trips.

• A shared ledger is important because there is no obvious central authority that is not also an ecosystem participant.

• Insurance companies collaborate in sharing driver and driving data, yet also must compete in the marketplace, so it is reasonable to expect the insurance companies to work together ensuring the completeness and integrity of the shared ledger.

• Insurance regulators are also expected to participate in the marketplace, and a shared, permissioned ledger aids auditing and traceability of policies as assets, and regulatory oversight.
Insurance Company Portal

- Leverage collected data and gain insights to increase claim resolution and reduce time going over a claim’s data.
- The analytics will overlay a trip’s timeline, bringing to the front crucial aspects for the insurer to better judge a claim.
- View active trips in real time to understand market demand in a micro-insurance world – so that rates/rewards can be adjusted (think high surcharge according to demand/location/risk profile).
Micro-Insurance Driver App

- A blockchain marketplace for insurance consumers PAYG micro-insurance
- Integrated with real-time weather forecasting (dynamic quoting)
- Insurance companies can adjust rewards based on demand, customer risk, time, etc.
System Architecture

Driver App

Insurer A Dashboard

Insurer A Backend

Insurer B Dashboard

Insurer B Backend

API

Insurance Service

Quotes Aggregator

Claims Service

Trip Data Handler (GPS series)

Driver Profile Service

Insurance Blockchain

Hyperledger Fabric
Document and Workflow Management in Trade and Logistics
Value Proposition

• More than $16 trillion in goods are shipped across international borders each year

• 80% of the goods consumers use daily are carried by the ocean shipping industry

• By reducing barriers within the international supply chain, global trade could increase by nearly 15%, boosting economies and creating jobs[^1]

Pain Points

Global trade is highly inefficient and burdened by paper-based processes

- Data trapped in organizational silos
- Disparate perspectives on transaction state
- Manual and time-consuming processes
- Clearance processes subject to fraud
Digitizing the Global Supply Chain

• **Connects the ecosystem**
  • Brings together all parties in the supply chain - including traders, freight forwarders, inland transportation, ports and terminals, ocean carriers, customs and other government authorities, and others - onto a Blockchain-based platform with a secure permission and identity framework

• **Drives true information sharing**
  • Provides for the seamless, secure sharing of real-time, actionable supply chain information across all parties to a trade - encompassing shipping milestones, cargo details, trade documents, the structured data embedded in trade documents, customs filings, sensor readings, and more

• **Fosters collaboration and trust**
  • Enables the digitization and automation of the cross-organization business processes integral to global trade, including import and export clearance, with Blockchain ensuring secure, auditable, and non-repudiable transactions
Why Blockchain

Blockchain addresses the underlying challenges inherent in collaborating across a distributed, fragmented supply chain ecosystem.

**SHARE LEDGER**
Append-only distributed system of record shared across business network
A network of industry participants maintains a distributed, permissioned ledger with copies of document filings, relevant supply chain events, authority approval status, and full audit history; every change results in a new, immutable block.

**SMART CONTRACT**
Shared business logic governing what transactions may be written to the ledger
Cross-organizational business processes, such as import and export clearance, are pre-programmed and built into Blockchain and distributed to and executed on the network, preventing any member from changing the business logic.

**PRIVACY**
Ensuring appropriate visibility; transactions are secure, authenticated and verifiable
Cryptography enables permissioned access so only the parties participating in a specific shipment can submit, edit or approve related data.

**TRUST**
Transactions are endorsed by relevant participants
Information such as documentation filings and authority approvals can only be changed if endorsed by the parties taking part in the shipment; full audit history maintained on the Blockchain.
Workflow and Payments in Current Systems

**Workflow of Documents direct to Buyer**

**Workflow of Documents via Banks “Cash Against Document”**

**OPTION 1**
- Buyer’s Bank only forwards BoL once Buyer has made payment
- Option 2 of Original copies of BoL & other docs where banks are required to exchange docs with buyer

**OPTION 2**
- Buyer’s Bank only forwards BoL once Buyer has made payment
- Option 2 of Original copies of BoL & other docs where banks are required to exchange docs with buyer

Buyer
- Buyer
- Sales Contract
- Certificate of Origin
- Phyto Certificate
- Quality Certificate
- BoL
- Buyer’s Bank
- Buyer’s Bank

Seller
- Seller
- Original copies of BoL & other docs
- Verifies and signs BoL
- Scans BoL & emails to Seller for verification of docs
- Seller’s Bank
- Seller’s Bank

Vessel Owner
- Vessel Owner
- BoL
- Copies of BoL & other docs

Discharge Port Agent
- Discharge Port Agent
- BoL
- Copies of BoL & other docs
The Blockchain System Design

Workflow event mapping to notification

1. CREATE_SHIPMENT
2. BUYER_VERIFICATION
3. MATES_CERT
4. VESSEL_OWNER_SIGN
5. PAYMENT_NOTIFICATION
6. TRANSFER

Part II-b: Platforms for Enterprise Solutions

• Hyperledger Fabric
• R3 Corda
Hyperledger: A Linux Foundation project

• A collaborative effort created to advance cross-industry blockchain technologies for business

• Founded February 2016; now more than 230 member organizations

• Open source, open standards, open governance

• Five frameworks and five tools projects

www.hyperledger.org
An implementation of blockchain technology that is a foundation for developing blockchain applications

- Emphasis on ledger, smart contracts, consensus, confidentiality, resiliency and scalability.

- V1.4 released
  - focus on stability and production operations

- IBM is one of the many contributing organizations

http://hyperledger-fabric.readthedocs.io/
Hyperledger Fabric v1 – Design Goals

• Better reflect business processes by specifying who endorses transactions
• Support broader regulatory requirements for privacy and confidentiality
• Scale the number of participants and transaction throughput
• Eliminate non deterministic transactions
• Support rich data queries of the ledger
• Dynamically upgrade the network and chaincode
• Support for multiple credential and cryptographic services for identity
• Support for "bring your own identity"
Hyperledger Fabric Overview

**Peers** are the networked services that maintain ledger state and run smart contracts.

**Channels** are defined subsets of the peer network that share a single ledger.

**Certificate authorities** provide identity services to participants on the network.

**Smart contracts** constitute the transaction logic whose output is agreed by the peer network.

**Consensus** is the process by which agreement is obtained on the peer network.

The **Ordering Service** agrees transaction sequence and distributes blocks to peers.
Fabric V1 Architecture

Client Application

SDK (HFC)

External-CA

optional

Membership Services

Fabric-CA

optional

Peer

Admin

Endorser

Committer

Ledger

Chaincode

Events

Ordering-Service

Hyperledger Fabric Network

14 May 2019
How Applications Interact with the Ledger

Client Application

SDK

Smart Contract

Ledger

World state

Blockchain

Peer

Blockchain developer

develops

develops

develops

submits

emits

accesses

recorded

‘get’, ‘put’, ‘delete’

14 May 2019
Fabric Ledger

• The Fabric ledger is maintained by each peer and includes the blockchain and world state
• A separate ledger is maintained for each channel the peer joins
• Transaction read/write sets are written to the blockchain
• Channel configurations are also written to the blockchain
• The world state can be either LevelDB (default) or CouchDB
  • LevelDB is a simple key/value store
  • CouchDB is a document store that allows complex queries
• The smart contact decides what is written to the world state
R3 and Corda

• R3 leads a consortium of more than 80 of the world's biggest financial institutions.

• Consortium started in 2015 with 9 financial companies (CBA, JPMC, Goldman ...).

• Some of the key members, JPMC, Goldman, Morgan Stanley, Santander have since left the consortium.

• The consortium seems to have taken a requirements driven approach to designing a DLT that is suited specifically for FSS.

• Built Corda based on these requirements and open sourced it in late 2016.
Corda Design Principles

• No blockchains

• No broadcast: all communication is point-to-point
  • Rejects the notion that data should be broadcast to all participants – or to predefined groups
  • Data is shared on a need-to-know basis and peers only see what they need to see
  • Not sending is preferable to sending and encrypting
  • Message senders need to know the identity of recipients

• Unspent Transaction Output (UTXO) for recording states (like Bitcoin) i.e. Does not use an account model like Ethereum, Fabric etc.

• Platform is JVM-based, written in Kotlin (can use Java, Clojure, etc)

• Supports industry-standard protocols: AMQP, JDBC, PKIX, etc.
Legal Agreements as a Foundational Concept

Elements of a Legal Agreement (State)

Issuer: Australia and New Zealand Banking Group
Beneficiary: Scentre Group
Applicant: Smith Co.

Effective date:
- From: May 10th 2018
- To: May 10th 2020

Amount: $...
Interest: ..%

Amount payable to be computed based on share price as of ....

Lifecycle of an Agreement

Creation → Amendment, Novation, Renewal etc. → Execute Agreement → Exit

Time (Time Windows)
- Before (Expiry)
- After (Maturity date)
- Within period

External facts and conditions that govern the contract (Oracles)
Corporate Action, Interest rates, share price, bankruptcy, FX conversion etc.

Witness (Notaries, Observers)

Terms and Conditions (Legal Prose)

Supporting documentation (Attachments)
The Corda Peer-to-Peer Network

No global broadcast ensures data received and stored only by parties with a legitimate need to know.

The doorman enrolls the entity by initiating the issuance of a TLS (identity) cert from the permissioning service.

The Corda Node

Network Map Service

Oracle

Notary

Peer-to-peer TLS-encrypted messages sent over AMQP/1.0

JVM

AMQP Message Queue

Corda Service

Corda Service

CorDapps

Transaction flow

Contract

Alice

Bob

Charlie

Permissioning Service

Issues identity certs to participating entities

Doorman

The doorman enforces KYC on all entities before admitting to the network.

ICBC 2019 Tutorial
Shared facts are represented by states using a UTXO state-machine model.

States are similar to Bitcoin transactions, but can represent arbitrary data.

States are immutable and represent a shared fact at specific point in time.

States evolve by allowing new states to replace old states, resulting in a state sequence.
Transactions

• Transactions reference zero or more input states and create zero or more output states.
• The newly created output states replace the inputs states which are marked as historic.

• There are three broad types of changes which can be facilitated by transactions:
  • Issuances
  • Updates
  • Exists
    Models the life-cycle of legal agreements
Transactions

• Transactions reference zero or more input states and create zero or more output states.

• The newly created output states replaces the inputs states which are marked as historic.

• There are three broad types of change which can be facilitated by transactions:
  • Issuances
  • Updates
  • Exists

Models the life-cycle of legal agreements

Input state references are comprised of a pair of: (Transaction ID, Index)
Transactions

- Transactions reference zero or more input states and create zero or more output states.
- The newly created output states replaces the inputs states which are marked as historic.

- There are three broad types of change which can be facilitated by transactions:
  - Issuances
  - Updates
  - Exists

Models the life-cycle of legal agreements
Part III: Key Lessons We Learnt

• Challenges related to moving from PoCs to production
• Governance and business models to accelerate the adoption
Barriers to Making it Mainstream

• Unwilling to share organizational data
• Privacy and Regulatory compliance
• Security challenges
• Limited transaction speed
Path to Enterprise Adoption

Think big, but start small. Prove value with iterative bursts of design, build, and review to quickly learn from results—and adjust.

Source: Deloitte, Blockchain for Finance, 2018
Path to Enterprise Adoption

Enterprise Impact and Industry Impact

Meaningful issues should revolve around significant costs to enterprise and industry

Existing business process is distilled down to blockchain-based model
Reinventing the business based on a trust system

Technology to align with the business imperatives
Technology design decisions and deployment options

Integration with downstream transaction systems
Reflecting on critical business systems

Source: IBM, Making Blockchain Real for Business, 2018
Key Lessons Learnt

• Governance
  • Setting and maintaining good governance is imperative for steady progress
  • Early agreement on a RACI matrix are critical for a smooth transition to operation

• Scope and Method
  • Jointly agree both the Functional and Non-Functional MVP scope early
  • Locking down what is considered ‘done’ in Agile is not obvious for large programmes

• Estimation
  • Estimate wisely and calibrate the initial story points extremely accurately

• Solution
  • Do not underestimate user onboarding along with identity and access management
Building Blocks of Governance Model

Industry and use case-specific which need to factor various facets and evolution of the industry itself.

- Common/shared services management, such as KYC, audits, reporting, etc.
- Product and business network evolution
- Enforcement of legal and regulatory frameworks

Focused on IT infrastructures, performance, cost structures, and business risk.

- A distributed IT management structure
- Model for distributed maintenance – software/HW updates, upgrades, path management
- Technology adoption and assessment – leads to keeping up with technology evolution and economic deployment models

An equitable cost structure that is fairly spread based on participant activity.

- Membership onboarding/off-boarding
- Data ownership structure – for business entities joining and leaving the network
- Network support services – include business network SLA enforcement, and membership services
Business Models

**Founder-Led Network**
Single company driving the initial project then others join the network
eg. UC4: Trade & Logistics

**Joint Venture Network**
2 or more create a JV to govern the initial network
eg. UC2: Bank Guarantee, Maersk-IBM

**Consortium Network**
A consortium as the initial network and governance in a specific industry or sector
eg. UC1: Shared KYC

**Business Ecosystem**
A Consortium Network working across multiple industries or sectors
eg. UC3: Micro-Insurance
Total Economic Impact

Source: Forrester, Emerging Technology Projection: The Total Economic Impact Of IBM Blockchain, 2018
Our Solutions

• Application and impact-driven research
  • Decentralized identity management
  • Consumer Data Rights for open banking
  • Anti-Money-Laundering with AU Regulator
  • Interoperability of public and permissioned blockchain

• Production-level development
  • ArtChain: a blockchain-based platform for artwork registration, tracking, and authentication.

• Professional training
  • Short courses
Our Partners
Takeaways

• Rethink on the notion of trust
  • Enable exchange of value without trusting intermediaries.
  • Maintain a single source of truth and a shared set of business rules across separate entities without anyone being able to alter them and control the system.
  • Shift the cost of trust

• More value-added when combined with other technologies (AI and IoT)

• We look forward to exploring these opportunities with you
Thank you!

Contact
Dr. Ziyuan Wang
Senior Research Fellow - Blockchain
ziyuanwang@swin.edu.au