A practical look at how decentralization with blockchain and DLTs can transform today’s financial scenarios

Vito Chin
“The thing I remember distinctly is that I was sitting in the living room when I thought of it the first time and then I went downstairs to get a Coke and I almost lost it," he says. "I mean, there was this moment when - I was thinking about something. What was it? And then I got it back and didn't forget it.”

Whitfield Diffie

As told to Steven Levy
Public key cryptography

Alice
- Bob's Public Key
- Alice's Private Key

Combine keys -> 751A696C 24D97009

Alice and Bob's shared secret

Bob
- Alice's Public Key
- Bob's Private Key

Combine keys -> 751A696C 24D97009

Alice and Bob's shared secret
Hash functions

Input
- Fox
- The red fox jumps over the blue dog
- The red fox jumps over the blue dog
- The red fox jumps over the blue dog

Digest
- DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
- 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
- 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
- FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
- 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C
Digital Signature

**Signing**

Data

Hash function

Hash

101100110101

Encrypt hash using signer's private key

Certificate

111101101110

Signature

Attach to data

Digitally signed data

**Verification**

Digitally signed data

Data

Hash function

Hash

101100110101

Digitally signed data

111101101110

Signature

Decrypt using signer's public key

? = 101100110101

Hash

If the hashes are equal, the signature is valid.
Transaction Chain
Blockchain

Previous Hash

Nonce

Previous Hash

Nonce

Tx  Tx  Tx  ...

Tx  Tx  Tx  ...

Microsoft DIGITAL TRANSFORMATION SUMMIT
## Ledger

<table>
<thead>
<tr>
<th>FROM</th>
<th>TO</th>
<th>PROPERTY</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td>Katie</td>
<td>Payment</td>
<td>$500</td>
</tr>
<tr>
<td>Jim</td>
<td>Sally</td>
<td>Payment</td>
<td>$300</td>
</tr>
<tr>
<td>Alex</td>
<td>Garth</td>
<td>Asset</td>
<td>Car</td>
</tr>
<tr>
<td>Katie</td>
<td>Tony</td>
<td>Payment</td>
<td>$100</td>
</tr>
<tr>
<td>Molly</td>
<td>Paula</td>
<td>Message</td>
<td>I love you</td>
</tr>
</tbody>
</table>
Decentralized
Public Networks
Enterprise blockchain
Benefits

Eliminates Intermediaries
Allows industries to redefine or create new business models.

Reduces Fraud
Highly secure and transparent, making it nearly impossible to change historical records.

Increases Efficiency and Speed
Simplifies transactions and enables T+Zero settlement time.

Increases Revenue and Savings
Potential savings and new revenue opportunities through more efficient processes and reduced costs.
Trust
Project Ubin

**PHASE 1**
Use of digital currency in RTGS

**PHASE 2**
Achieved gridlock resolution and LSM on a decentralised system without compromising on privacy (focus of this report)

**FUTURE PHASES OF PROJECT UBIN**

- **Domestic Delivery vs Payment (DvP)**
  Securities settlement

- **Target Operating Model**
  Processes & policy impact

- **Payment vs Payment (PvP)**
  Cross-border settlement

- **Cross-border settlement of payments and securities (DvPvP)**

Microsoft DIGITAL TRANSFORMATION SUMMIT
Gridlock resolution

Bank 1
- Begin Balance: $50k
- End Balance: $0

Bank 2
- Begin Balance: $100k
- End Balance: $70k

Bank 3
- Begin Balance: $20k
- End Balance: $100k

$100k $130k $50k

$50k $30k $50k
Functional scope

Decentralisation of Processing
- Account Management

Digitalisation of Payment
- Balance Enquiry
- Redeem
- Pledge
- Fund Transfer

Payment Queue Handling
- Queue Mechanisms
- Queue Reprioritisation

Liquidity Optimisation
- Gridlock Resolution

Privacy of transactions
- Privacy

Settlement finality
- Transaction Validation

Versioning
Platform

- Hyperledger
- Quorum
- Azure
Trade Finance
Opportunities for “standard” digital transformation

- **People** – All four parties involved would need similar IT skill competencies to build and operate a digital system.
- **Process** – Transformation would relocate the pain from manual entry to reconciliation whenever one counterparty updates.
- **Technology** – All counterparties would require compatible technology stacks and then allow access into their networks.

**Digital Transformation**

- Counterparty IT staffs have to maintain network connections and provide operational cybersecurity.
- SBLC latency is reduced moving from paper to digital but still exists due to counterparty synchronization.
- Which counterparty maintains the authoritative system of record?
- The underlying databases are still subject to data entry errors.
Opportunities for Blockchain-enabled digital transformation

Blockchain enables near real-time collaboration among all participants when...

...it needs to be **Secure**
Authenticated counterparts digitally sign SBLC requests, updates and claims.

...it needs to be **Shared**
Applicants and beneficiaries collaborate in near real-time using standardized templates.

...it needs to be **Distributed**
Each member of the network can use the blockchain to validate the other counterparts.

...it needs to be **Authoritative**
Each immutable SBLC entry is written once thereby increasing visibility and auditability while reducing error rates.
Initiatives
KYC – Current State Pain Points

1. Customer has a poor experience, being forced to submit information multiple times with each new registration, often with subtle differences.
2. Manual reviews of information are inefficient and costly. In the field of retail banking, this can take 37 days for corporations and 12 days for an individual.
3. Storage – whether on disk or in a system – has the potential to be compromised.
4. Legacy system design and implementation may limit agility to address changing regulatory requirements.
Private documents are selectively shared by a customer with a trusted party (regulator, government entity, or licensed partner.)

The trusted party reviews and verifies the authenticity of the documents, then produces a digital signature from the documents’ cryptographic proofs, which is then notarized onto a blockchain.

A cryptographic token is generated for the customer, which can be used to verify the authenticity of the trusted party’s signature, the documents, and thus the validity of each step of the KYC process.

As documents become obsolete or invalid, a workflow is introduced and updates are timestamped into a public blockchain to prove the validation of these documents by a trusted party.
When a customer begins a registration process with an institution, she can share an identity token instead of the original documents.

Reducing redundancy in the verification of registration requests coupled with reporting can reduce the costs of participating parties.

Increased transparency provides regulators the ability to easily and quickly validate KYC verification activity stored on the ledger.
Maersk Uses Blockchain to Secure and Streamline Marine Insurance Process

**Challenge**
- Duplication, inefficiency, lack of transparency, lack of data, fraud, and errors across lots of parties interacting in marine insurance
- Change is hard due to multiple regulators and jurisdictions
- Rates are under pressure and costs are becoming unmanageable
- Compliance is challenging

**Strategy**
- EY, Maersk, Guardtime, and Microsoft developed a real-time blockchain enabled platform for marine insurance
- The solution streamlines claims and settlement processes, while reducing errors.

**Results**
- Real-time visibility into the location, condition and safety of high-value assets moving around the world
- Accurate, dynamic and fair underwriting and pricing based on that visibility
- Streamlined regulatory reporting and compliance
- Accurate and transparent data sharing among all relevant stakeholders with audit trail
- Capital freed from poor credit system

“It is a priority for us to leverage technology to streamline and automate our interaction with the insurance market. Insurance transactions are currently far too tedious and frictional. The distance between risk and capital is simply too far.”

— Lars Henneberg, VP, Head of Risk and Insurance of A.P. Moller-Maersk
Bank Hapoalim Uses Blockchain to Streamline the Bank Guarantee Process

**Challenge**
- Bank guarantees are a guarantee from a lending institution, like a bank, that ensure the liabilities of its customers are met.
- Required for large purchases like real estate.
- Currently customers must visit a branch multiple times to move through the application process.

**Strategy**
- Bank Hapoalim and Microsoft Services developed a real-time blockchain enabled platform to collaborate on documents with customers.
- The solution lets customers and banks update documents securely without in person verification.

**Results**
- Blockchain technology improves the customer experience and confidence in the banking system by enabling them to receive automated, digital documents without the need to go to a physical bank branch.
- The solution creates a competitive advantage and cost savings for Bank Hapoalim by streamlining existing systems and services.

“The use of Blockchain technology will significantly improve the customer experience and the level of trust in the banking system.”
— Arik Pinto, Chief Executive Officer of Bank Hapoalim
Utilidex Reimagines Energy Trading with Blockchain

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Strategy</th>
<th>Results</th>
</tr>
</thead>
</table>
| • The sector is becoming increasingly complex, with new suppliers entering the market.  
• Markets have also suffered from increased volatility, while generation trends have shifted significantly towards renewable sources such as solar power.  
• Changing dynamics of the market, and increasing value in energy flexibility. | • Help customers buy, sell and optimise their energy in an open, transparent way.  
• Worked with Microsoft to trial blockchain technology and prove the technology’s application in buying and selling energy. | Utilidex’s blockchain technology will:  
• Let users analyse data on plants.  
• Make billing easier.  
• Show real-time market data.  
• Predict energy production.  
• Feature a personal digital assistant that offers instant alerts. |

“This work is part of our broader ambitions to help customers buy, sell and optimise their energy in a very different way”

- Richard Brys, Chief Executive Officer of Utilidex
Microsoft Azure

Marketplace

Blockchain

What's new

Corda Single Ledger Network R3
Hyperledger Fabric Single Member
Quorum Single Member
Waves Node
Parity Ethereum Fallback Kovan

Single node ledgers

Corda Demo R3
Quorum Demo
Chain Core Developer Edition Chain
Emercoin Blockchain Engine
Syscoin Full Node
Parity Ethereum Fallback Kovan

Multi-node ledgers

Ethereum Consortium Microsoft
Ethereum Consortium Microsoft
Hyperledger Fabric Single Microsoft
Corda Single Ledger Network R3
Quorum Single Member Enterprise Ethereum
Ethereum Consortium Microsoft
Deploy in the topology of your choice

1. Dev/Test: Enable developers to get started
   Single node (virtual machine)

2. Single Member: Simulate production for multiple divisions within a single organization
   Multi-node across single region

3. Multi-member: Collaborate between multiple divisions and organizations
   Multi-node across multiple regions, Azure subscriptions, and/or organizations
POCs
- Healthcare
- Retail & CPG
- Government
- Discrete Manufacturing
- Banking, Capital Markets

Professional Services & Support

Industry Solutions
- Horizontal SaaS & Adapters
  - 1st Party
  - 3rd Party

Middleware
- Distributed Ledger Gateway Services
- Identity & Key Services
- Encryption Services
- ML & BI Services

Crypto services & architecture (secure containers, attestation, etc.)

Base Platform
- Smart Contract-Based Distributed Ledger Stacks
  - Blockchain Virtual Machine
  - 1st party DL Stack
  - 3rd party DL stack A
  - 3rd party DL stack B

- UTXO + others
  - Adapter
  - 3rd party DL stack C

Azure – Blockchain resource provider

Crypto services & architecture (secure containers, attestation, etc.)
Overcome technology gaps with Coco Framework

**Scalability**
Database-like speeds for transaction throughput and latency

**Confidentiality**
Richer and more flexible confidentiality models

**Consortium Governance**
Configurable constitution to govern membership
Simplifying Blockchain app development

Smart contracts plus config file stands up an app with UI

---

Smart contract (business logic)

```
pragma solidity ^0.4.4;

contract IfairTradeProperty {
    //Smart contract (business logic)
}
```

Metadata

```
{"Role": {
   "Firm": {
      "Role": "Participant",
      "Actions": [
         "AcceptOffer",
         "RejectOffer"
      ]
   }
},
"Buyer": {
   "Manufacturer": {
      "Role": "Participant",
      "Actions": [
         "PurchaseCocoa"
      ]
   }
},
"Manufacturer": {
   "Marketplace": {
      "Role": "Initiator",
      "Actions": [
         "Full"
      ]
   }
}}
```

Blockchain application

---

Microsoft DIGITAL TRANSFORMATION SUMMIT
What it provides

• Admin experience (manage business workflows, user assignments)
• Simulation apps (simulate end-to-end workflow UX through generated web, iOS and Android apps)
• REST-based APIs (abstract APIs generated which can be used for all scenarios)
• Queue Messaging Hub
• Easy Deployment (via Azure Marketplace)
• Identity Management (leveraging AAD)
• Off-Chain Transaction Synching (synchronized transaction to off-chain storage)
Accelerate your development with an upcoming tool

- **Reduce Cost and Time**
  Build Blockchain apps faster and easier and reduce costs of development

- **Get Off the Island**
  Automatically connect Blockchain applications to services you care about

- **Move towards production**
  Move towards production faster with automatically built scaffolding
Do you have a blockchain scenario?

- Do multiple parties share data?
- Do multiple parties manipulate the same data?
- Is there a requirement for verification?
- Can intermediaries be removed?
For Partners

• We have 3 fundamental missions to accelerate your growth as a Microsoft partner:
  • Help you build solutions and business with our “Build With” team.
  • Help you differentiate yourself and connect with customers via our “Go-to-Market” team.
  • Help you win opportunities and support our customers with the “Channel Management” sales team.
Learn more

- Sign up for an Azure account and join our Blockchain Preview Program
- Visit our Azure Blockchain Page
- Visit the Azure Blockchain Blog and our Blockchain User Voice
- Connect with the Microsoft Tech Community
- Join the conversation on Azure Advisors
Sources and references

• Images in slide 2 - 6 from Wikipedia
  • https://upload.wikimedia.org/wikipedia/commons/5/58/Hash_table_4_1_1_0_0_1_0_LL.svg
  • https://en.wikipedia.org/wiki/Electronic_signature#/media/File:Digital_Signature_diagram.svg

• Images in slide 13-16 from Reimagining AS, ABS, Accenture (Singapore)

• Image in slide 18, from World Economic Forum

• Image in slide 21 https://www.marcopolo.finance/