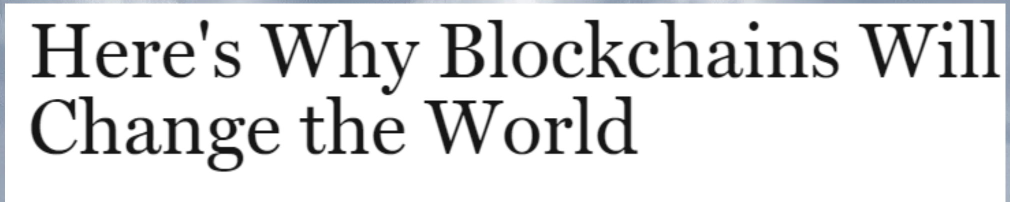
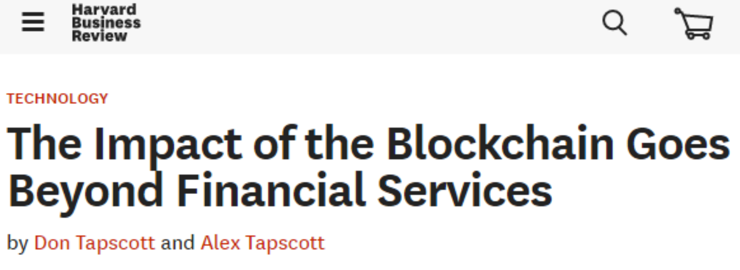
Regional Forum on Cybersecurity in the Era of Emerging Technologies
&
the Second Meeting of the “Successful Administrative Practices”-2017
Cairo, Egypt 28-29 November 2017

An Introduction to Blockchain

Dr. Ashraf Abdelwahab
Chief Technology Officer (CTO),
Africa Initiatives, Microsoft
asab@microsoft.com



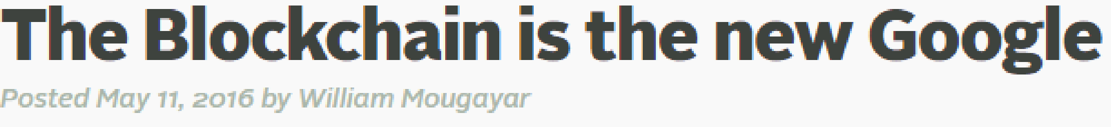
Here's Why Blockchains Will Change the World



TECHNOLOGY

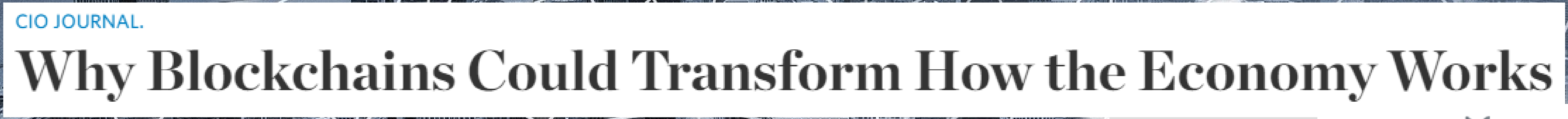
The Impact of the Blockchain Goes Beyond Financial Services

by Don Tapscott and Alex Tapscott



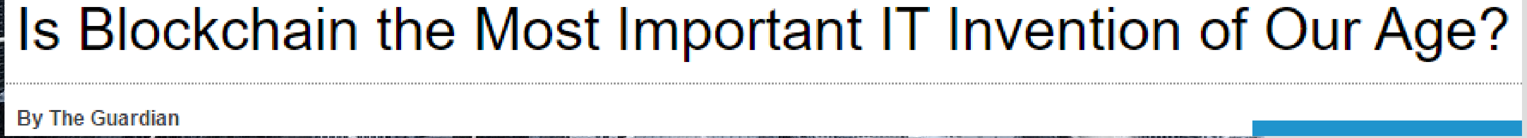
The Blockchain is the new Google

Posted May 11, 2016 by William Mougayar



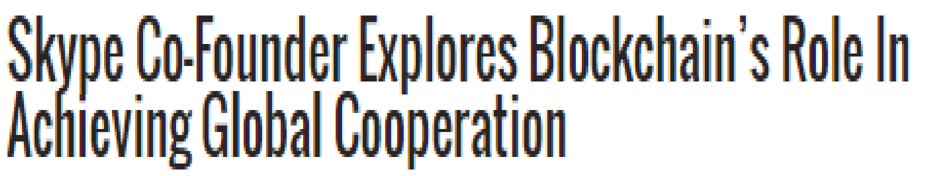
CIO JOURNAL.

Why Blockchains Could Transform How the Economy Works

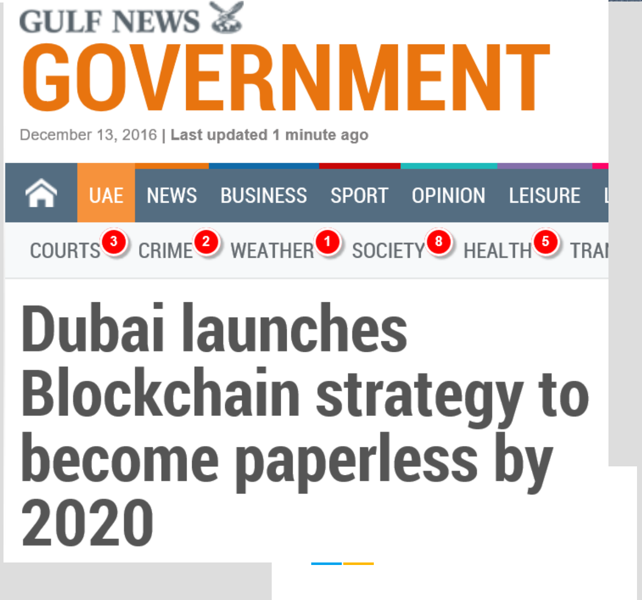


Is Blockchain the Most Important IT Invention of Our Age?

By The Guardian



Skype Co-Founder Explores Blockchain's Role In Achieving Global Cooperation



GULF NEWS

GOVERNMENT

December 13, 2016 | Last updated 1 minute ago

Dubai launches Blockchain strategy to become paperless by 2020

Blockchain by the numbers

2008: Technology started with bitcoin

90+ **Central Banks**

involved in blockchain discussions worldwide
(source WEF)

1.4B

Investments

t 3 years

00+ patents

in last 3 years

90+ **organizations**

Joined blockchain consortia

80%

of Banks will initiate blockchain projects by 2017

(Source: WEF)

Source: World Economic Forum, August 2016

Some Governments already investin in Blockchain:

UK, USA, Estonia, Russia, Georgia, Sweder Netherlands, UAE, Ghana, South Korea, Singapore

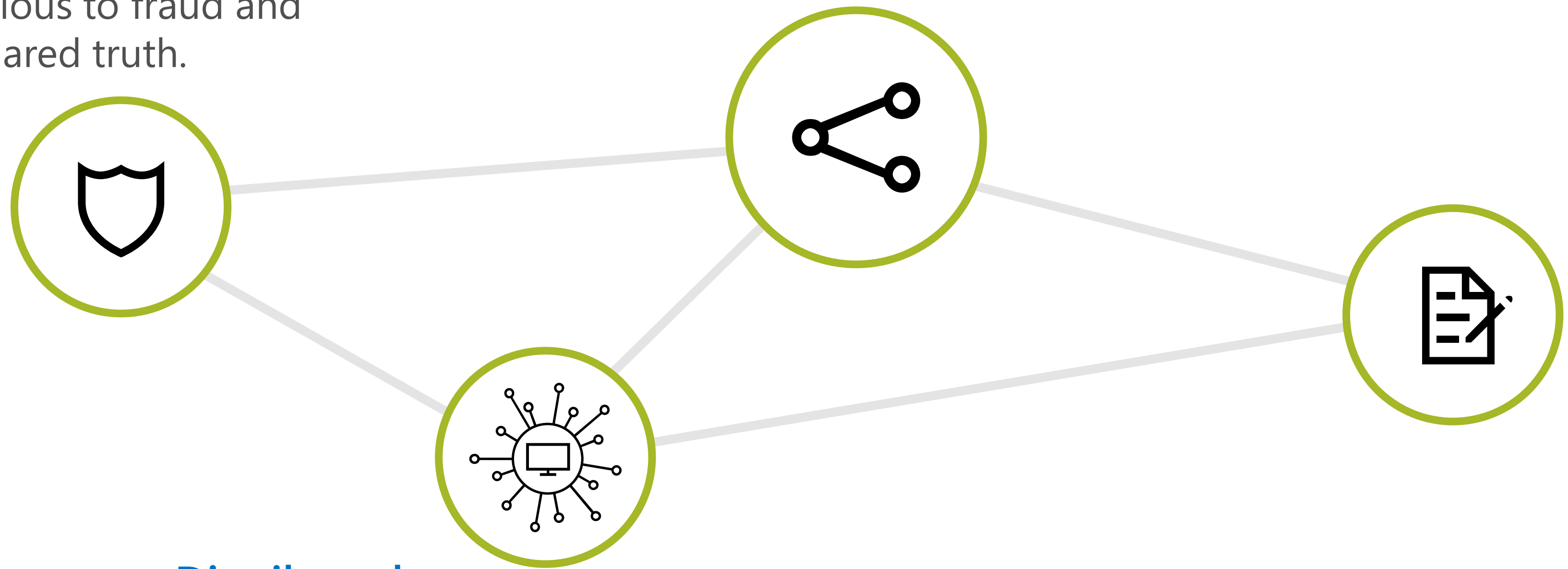
Blockchain is a secure, shared, distributed ledger

Secure

Uses cryptography to create transactions that are impervious to fraud and establishes a shared truth.

Shared

Blockchain value is directly linked to the number of organizations or companies that participate in them. There is huge value to even the fiercest of competitors to participate with each other in these shared database implementations.



Ledger

The database is "write once" so it is an immutable record of every transaction that occurs.

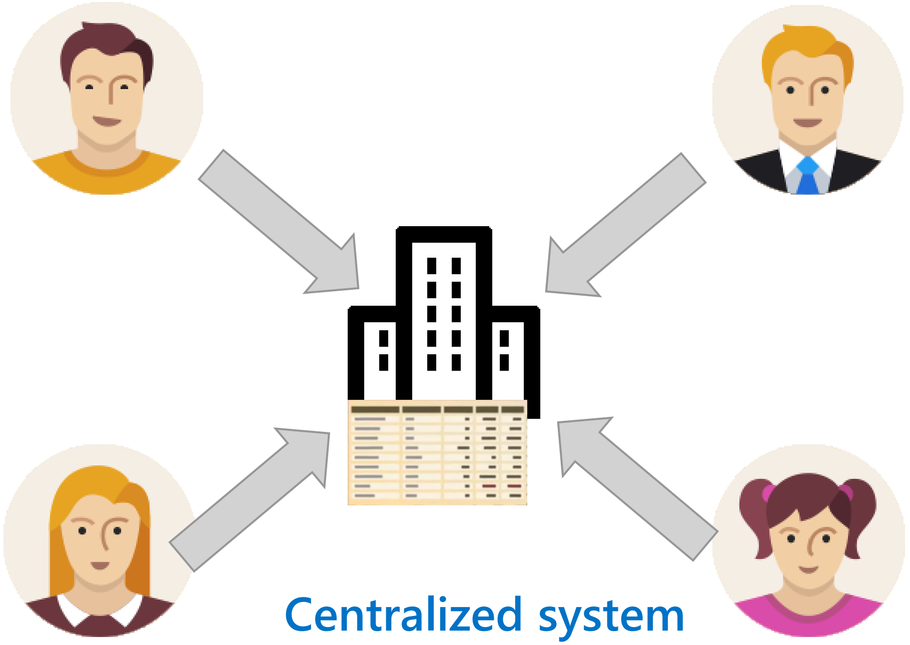
Distributed

There are many replicas of the blockchain database. In fact, the more replicas there are the more authentic it becomes.

That decentralizes data in a trustless environment

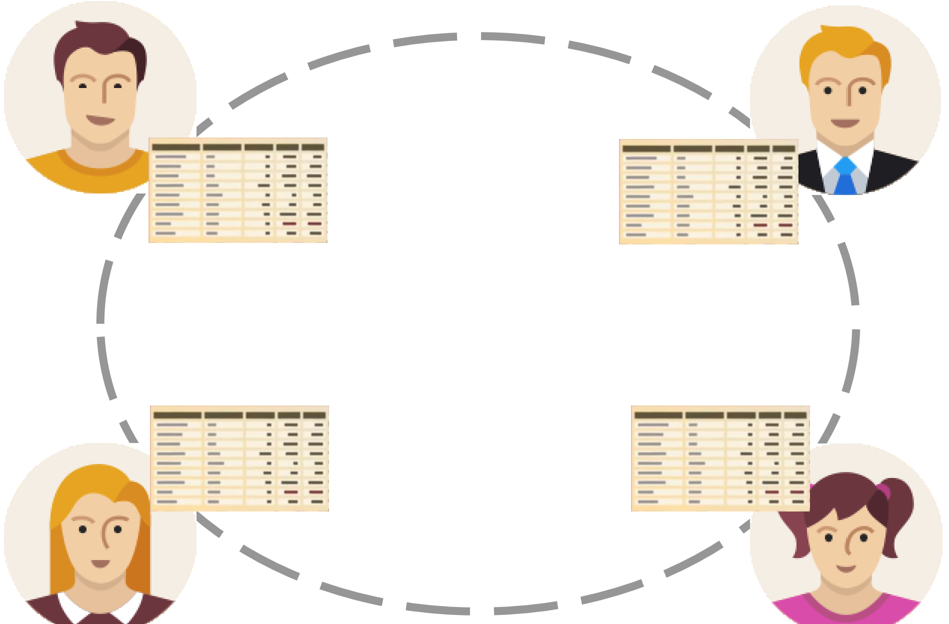
- Traditional ledgers are centralized and use 3rd parties and middlemen to approve and record transactions
- Blockchain safely distributes ledgers across the entire network and does not require any middleman
- The technology maintains multiple replicas like p2p torrent file sharing

Traditional System



Centralized system with stored ledger

Blockchain System



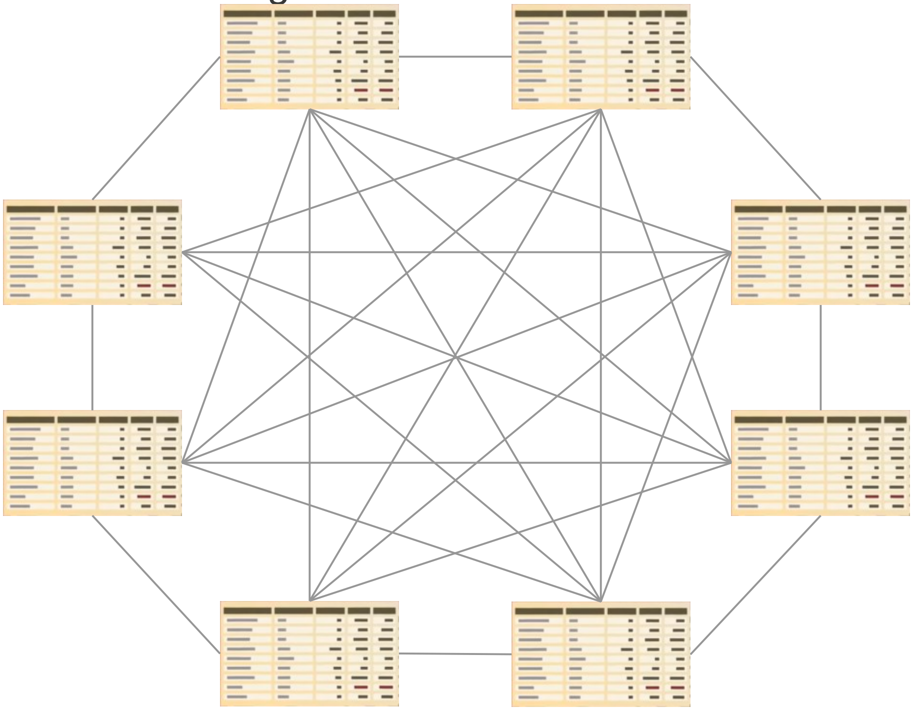
Distributed system with distributed ledger

Blockchain uses a distributed ledger for tracking

- A ledger is a write only database most commonly used in accounting
- The digital distributed ledger creates the same copy of the data across all the participating nodes
- All new transactions are digitally signed and then broadcast across the blockchain network to be added to the system
- Participants in the blockchain verify the transaction is valid and then writes it to the ledger
- This is the technology originally designed to power the bitcoin currency

FROM	TO	PROPERTY	VALUE
Alex	Katie	Payment	$500
Jim	Sally	Payment	$300
Alex	Garth	Asset	Car
Katie	Tony	Payment	$100
Molly	Paula	Message	I love you

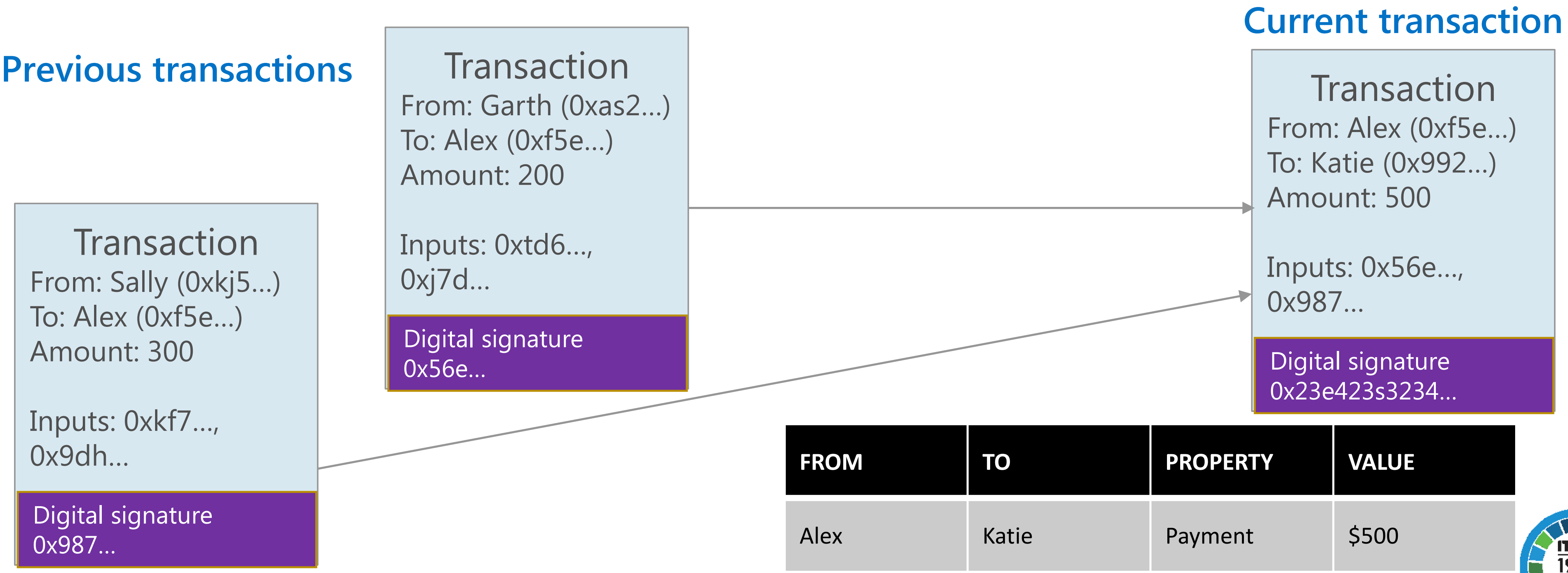
Example ledger



Entire network has same ledger

Blockchains create a transaction chain with history

- The ledger itself does not keep track of digital asset account balances, it simply records transactions
- Instead of balances, ownership of digital assets is verified by links to previous transactions, using the immutable history inherently available in a blockchain solution
- For example. For Alex to send $500 to Katie, he must reference previous transactions where he has received $500 or more to prove that he, indeed, has that much money to send. These reference transactions are called previous input transactions. The current transaction(s) is called output transaction(s)
- Validity of each transaction is based on the validity of previous transactions, which is shared.



Previous transactions

Transaction
From: Sally (0xkj5...)
To: Alex (0xf5e...)
Amount: 300

Inputs: 0xkf7...,
0x9dh...

Digital signature
0x987...

Transaction
From: Garth (0xas2...)
To: Alex (0xf5e...)
Amount: 200

Inputs: 0xtd6...,
0xj7d...

Digital signature
0x56e...

Current transaction

Transaction
From: Alex (0xf5e...)
To: Katie (0x992...)
Amount: 500

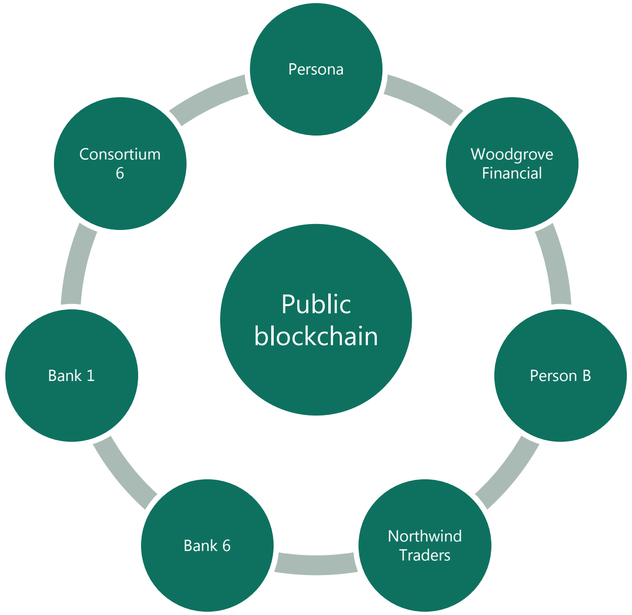
Inputs: 0x56e...,
0x987...

Digital signature
0x23e423s3234...

FROM	TO	PROPERTY	VALUE
Alex	Katie	Payment	$500

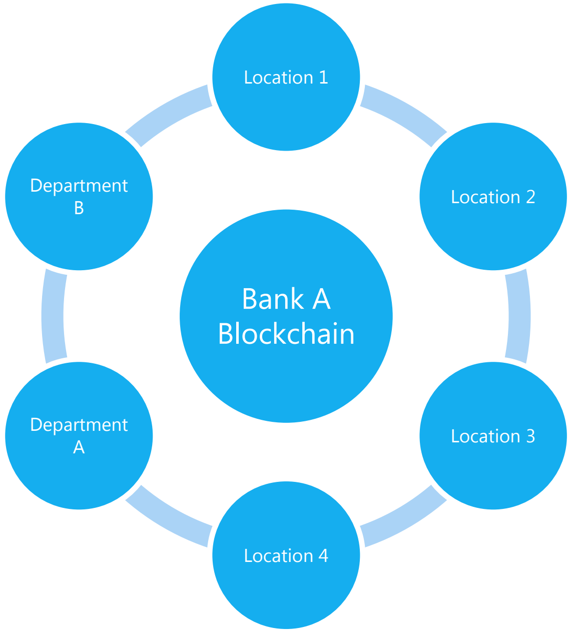
Blockchain | Network Types

Public



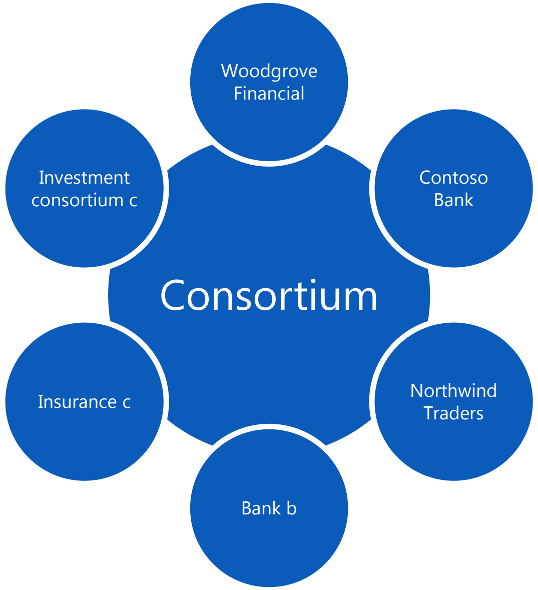
- Many, unknown participants
- Writes by all participants
- Reads by all participants
- Consensus by Proof of Work

Private



- Known participants from one organization
- Write permissions centralized
- Reads may be public or restricted
- Multiple algorithms for consensus

Consortium



- Known participants from multiple organizations
- Writes require consensus of several participants
- Reads may be public or restricted
- Multiple algorithms for consensus

Source: Ethereum blog by Vitalik Buterin https://blog.ethereum.org/author/vitalik-buterin/

Decentralization: changing fundamental processes & models

Simplify Operations
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.

Reduces Risk and Improves Trust
Challenges the need to trust counterparties to fulfill obligations as agreements are codified and executed in a shared immutable network.

Regulatory Efficiency
Enables real-time monitoring of financial activity between regulators and regulated entities.

Partial Source: World Economic Forum – The future of financial infrastructure – August 2016

When is blockchain relevant?

Answering a few questions can determine if blockchain is appropriate

Is this a business process that crosses trust boundaries?

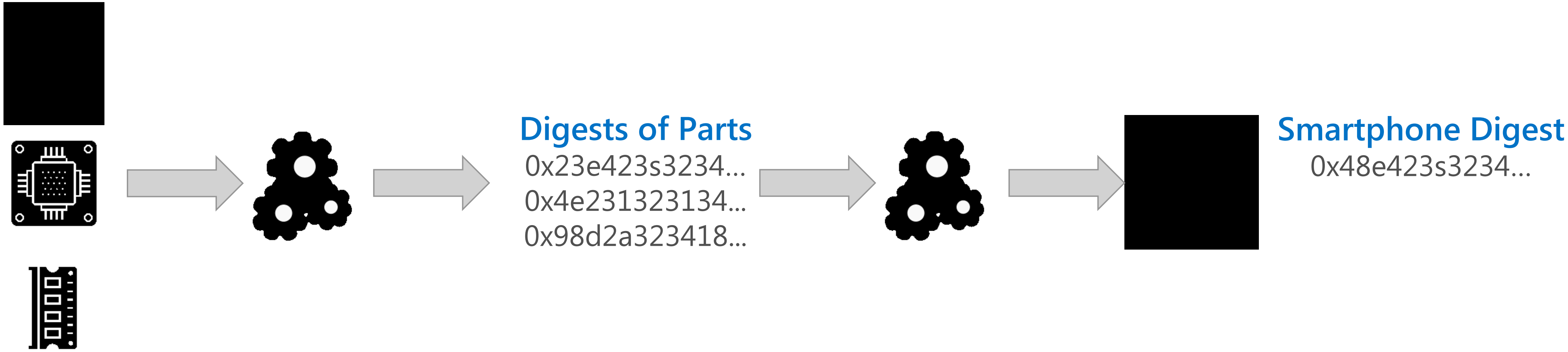
Do multiple parties manipulate the same data?

Are there any intermediaries that control the single source of the truth?

Does the process involve low-value, manual verification steps?

More complex example: Blockchain to track assets

- In this example, a smartphone and all of its components are captured in a blockchain system used to track products
- A unique identifier for the smartphone is created based on all the parts of the smartphone
- This unique identifier for the smartphone can be used to track that unique item within a blockchain

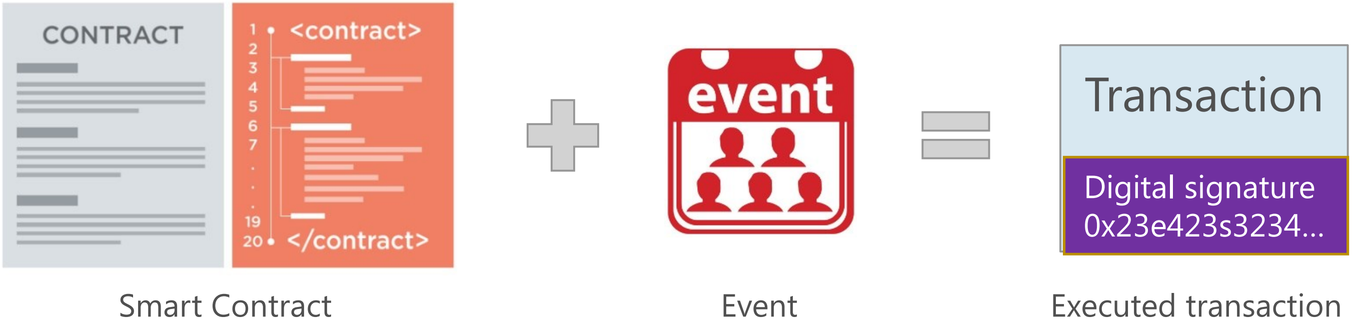


All parts get a hash (digest) based on product serial number + manufacturer

All digests of parts are combined into one unique digest for the phone

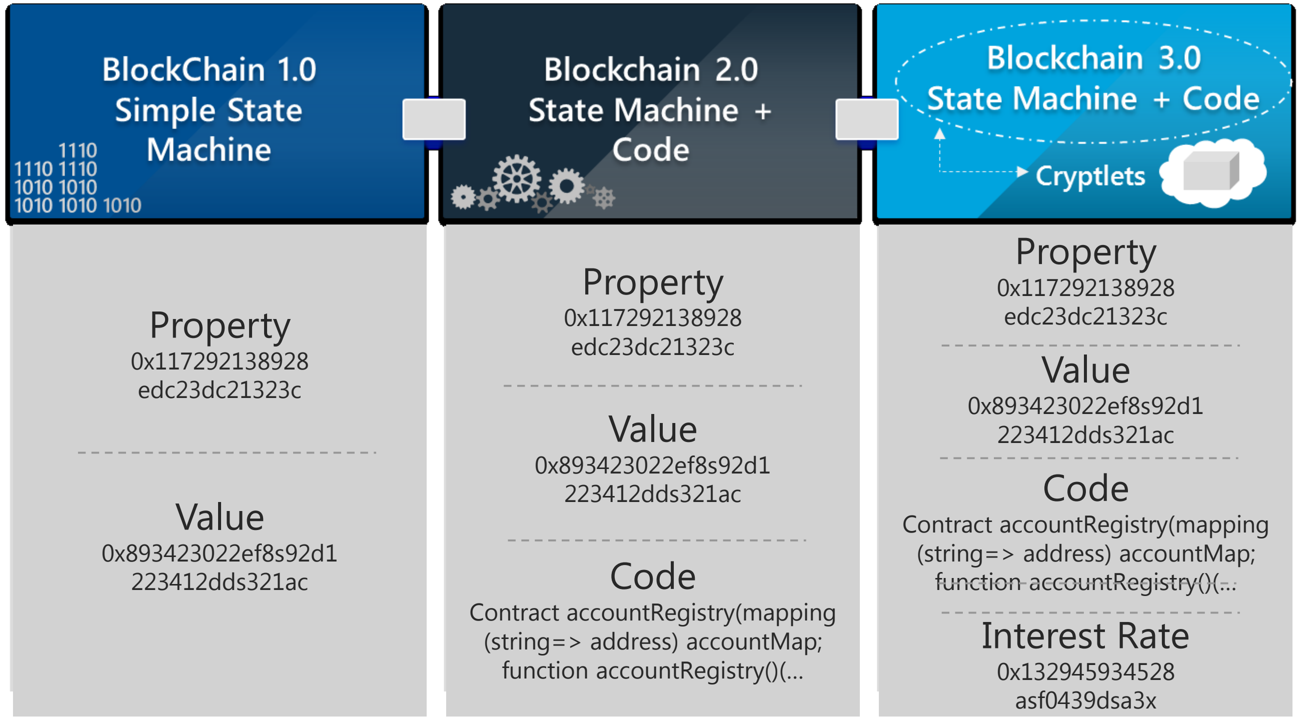
More complex example: Blockchain 2.0 & Smart Contracts

- Blockchain 1.0 is a simple ledger that records transactions in sequence. It represents the state of the network at any given moment. Blockchain 1.0 was focused on transacting payments. However, folks quickly realized that you could encrypt pretty much anything and put it on the blockchain. There are marriage proposals written to the blockchain, photographs stored, etc.
- What if you stored whole agreements on the blockchain, what would that look like?
- Blockchain 2.0 expands the power of the ledger to include additional logic (code) through Smart Contracts
  - Smart Contracts contain code and execute various terms written in that contract
  - Like normal contracts, these Smart Contracts are based on reaching agreed-upon conditions
  - Smart Contracts are now stored on and exist within Blockchain 2.0’s distributed ledger
  - Think of Smart Contracts as the computer code representation of a legal contract
- Examples: Contracts can be as simple as recording a loan and making payments on that loan or as complex as swaps.



Blockchain 3.0, Project “Bletchley,” “cryptlets” innovation

- Blockchain 2.0 introduced the power of Smart Contracts…
- …but Smart Contracts are unable to access external data or events based on time or market conditions
  - Calling code or data outside of a Smart Contract or blockchain breaks the general trust barrier and authenticity of transactions
- Cryptlets will allow the blockchain to access external data securely, while maintaining the integrity of the blockchain
- Cryptlets are a Microsoft innovation and solve a significant hurdle to enterprise blockchain adoption



BlockChain 1.0
Simple State Machine

Property
0x117292138928
edc23dc21323c

Value
0x893423022ef8s92d1
223412dds321ac

Blockchain 2.0
State Machine + Code

Property
0x117292138928
edc23dc21323c

Value
0x893423022ef8s92d1
223412dds321ac

Code
Contract accountRegistry(mapping (string=> address) accountMap;
function accountRegistry()(...

Blockchain 3.0
State Machine + Code

Property
0x117292138928
edc23dc21323c

Value
0x893423022ef8s92d1
223412dds321ac

Code
Contract accountRegistry(mapping (string=> address) accountMap;
function accountRegistry()(...

Interest Rate
0x132945934528
asf0439dsa3x

Popular scenarios where Blockchain adds value

Financial
Trading
Deal origination
POs for new securities
Equities
Fixed income
Derivatives trading
Total Return Swaps (TRS)
2nd generation derivatives
The race to a zero middle office
Collateral management
Settlements
Payments
Transferring of value
Know your client (KYC)
Anti money laundering
Crowd Funding
Peer-to-peer lending
Compliance reporting
Trade reporting & risk visualizations
Betting & prediction markets

Insurance
Claim filings
MBS/Property payments
Claims processing & admin
Fraud detection/prediction
Telematics & ratings
Digital authentication
Asset management
Automated underwriting
Self-administered insurance

Media
Digital rights mgmt
Game monetization
Art authentication
Purchase & usage monitoring
Ticket purchases
Fan tracking
Ad click fraud reduction
Resell of authentic assets
Real time auction & ad placements

Computer Science
Micronization of work (pay for algorithms, tweets, ad clicks, etc.)
Expanse of marketplace
Disbursement of work
Direct to developer payments
API platform plays
Notarization & certification
P2P storage & compute sharing
DNS

Medical
Records sharing
Prescription sharing
Compliance
Personalized medicine
DNA sequencing

Asset Titles
Diamonds
Designer brands
Car leasing & sales
Home Mortgages & payments
Land title ownership
Digital asset records

Government
Voting
Vehicle registration
WIC, Vet, SS, benefits, distribution
Licensing & identification
Copyrights

Identity
Personal
Objects
Families of objects
Digital assets
Multifactor Auth
Refugee tracking
Education & badging
Purchase & review tracking
Employer & Employee reviews

IoT
Device to Device payments
Device directories
Operations (e.g. water flow)
Grid monitoring
Smart home & office management
Cross-company maintenance markets

Payments
Micropayments (apps, 402)
B2B international remittance
Tax filing & collection
Rethinking wallets & banks

Consumer
Digital rewards
Uber, AirBNB, Apple Pay
P2P selling, craigslist
Cross company, brand, loyalty tracking

Supply Chain
Dynamic ag commodities pricing
Real time auction for supply delivery
Pharmaceutical tracking & purity
Agricultural food authentication
Shipping & logistics management

Build development environment consisting of blockchain protocol clients and network infrastructure

Build Blockchain Network on premises/cloud providers: 3 weeks

1. Review blockchain protocol specific network documentation
2. Determine topology for a consortium network
3. Map topology to IT resources
4. Manually deploy
5. Configure blockchain clients via Linux BASH scripts to support private network (peering, isolate mining nodes, etc.)
6. Configure other blockchain protocol properties (consensus algorithms, max peers, etc.)
7. Trial and error to make above steps work
8. Configure IT networks and firewall ports to permit blockchain protocol traffic
9. Test, debug, and repeat

VS

Deploy Blockchain Network in Azure using BaaS Bletchley Framework: 15 minutes

1. Activate Azure subscription
2. Search Azure Marketplace for desired blockchain
3. Click on blockchain image of choice
4. Provide 10 user parameters
(number of consortium members, number of blockchain VMs, admin usernames and passwords, etc.)
5. Deploy and wait 15 minutes
(+/- depending of nodes selected)

ITU

ITUWTDC
BUENOS AIRES 2017
9-20 October

Thank You

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

ITU-D
1992
2017
CELEBRATING
25YEARS
OF ACHIEVEMENTS