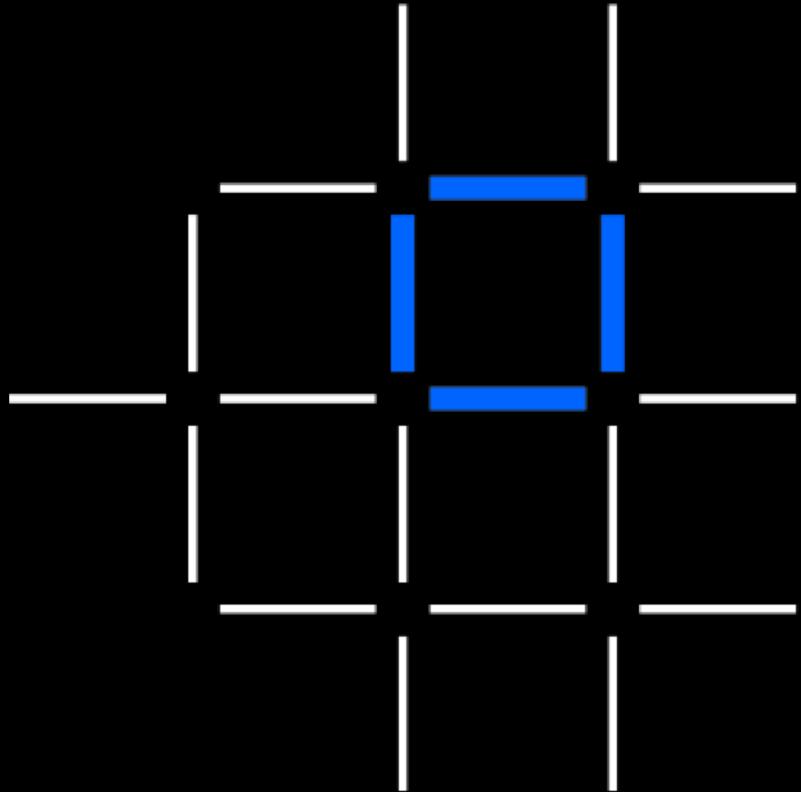


Integrating Blockchain into your business

Session E07

Mark Parzygnat
@MeetMarkP
 twitter





What is Blockchain?

A brief description

]



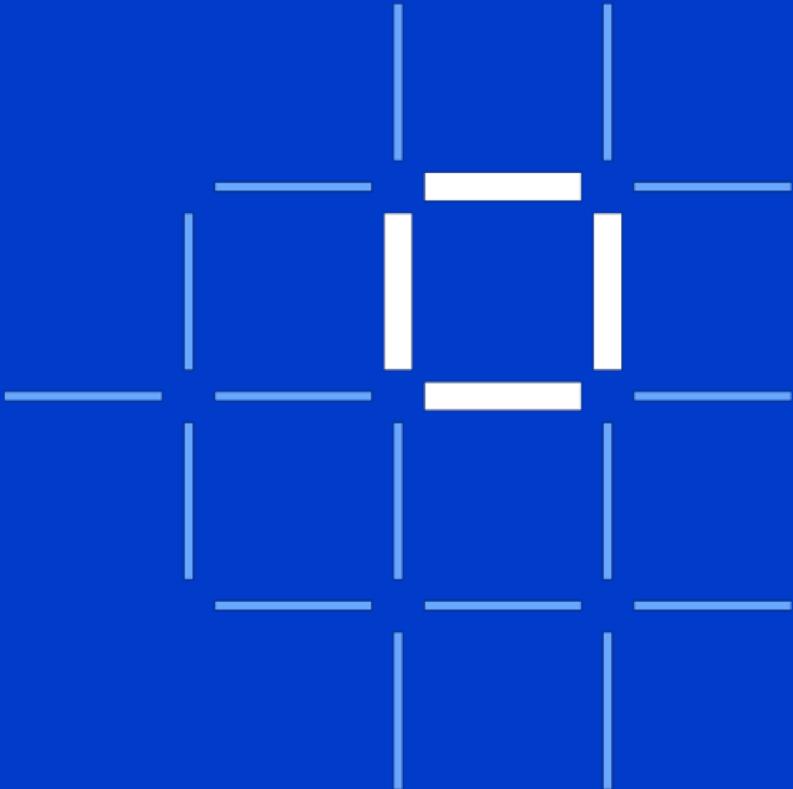
Essence of Blockchain

*Describing why blockchain is
just a piece of the puzzle*

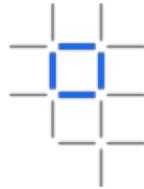


Blockchain Integration

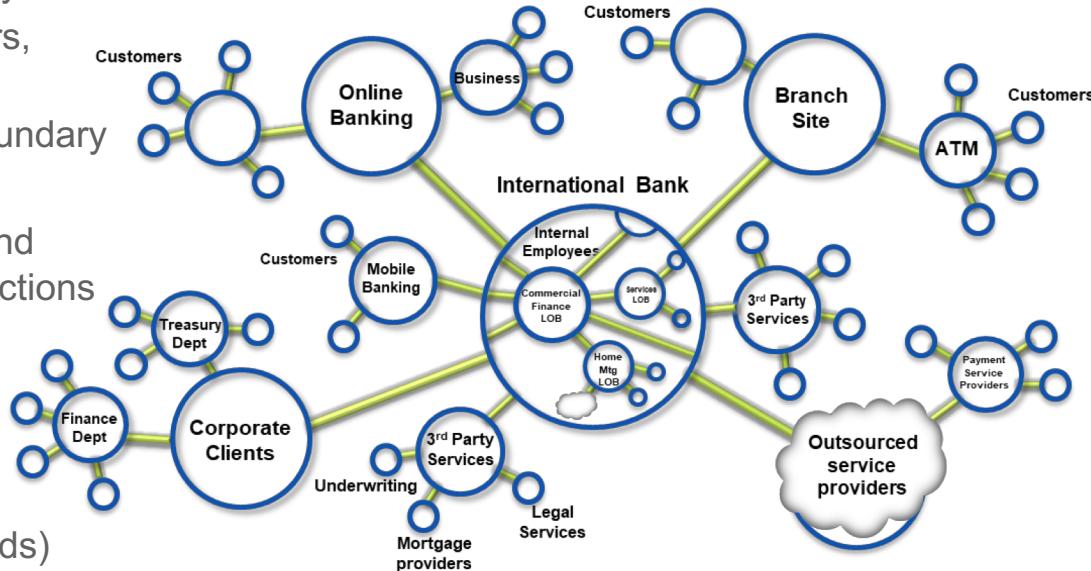
*Deriving value by leveraging
other tools*

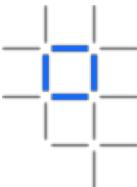


Business networks, wealth and markets



- **Business Networks** benefit from connectivity
 - Participants are customers, suppliers, banks, partners
 - Cross geography and regulatory boundary
- **Wealth** is generated by the flow of goods and services across business network in transactions and contracts
- **Markets** are central to this process:
 - Public (fruit market, car auction), or
 - Private (supply chain financing, bonds)





Transferring assets, building value

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



Two fundamental types of asset

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

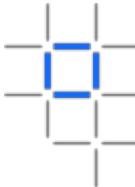
Intangible assets subdivide

- Financial, e.g. bond
- Intellectual, e.g. patents
- Digital, e.g. data

Cash is also an asset

- Has property of anonymity

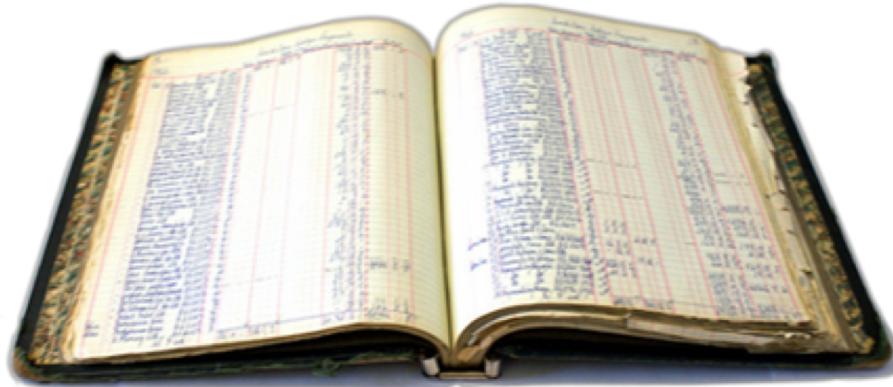
Ledgers are key

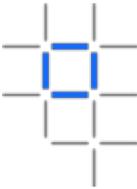


Ledgers are THE system of record for a business.

Businesses will have multiple ledgers for the multiple business networks in which they participate.

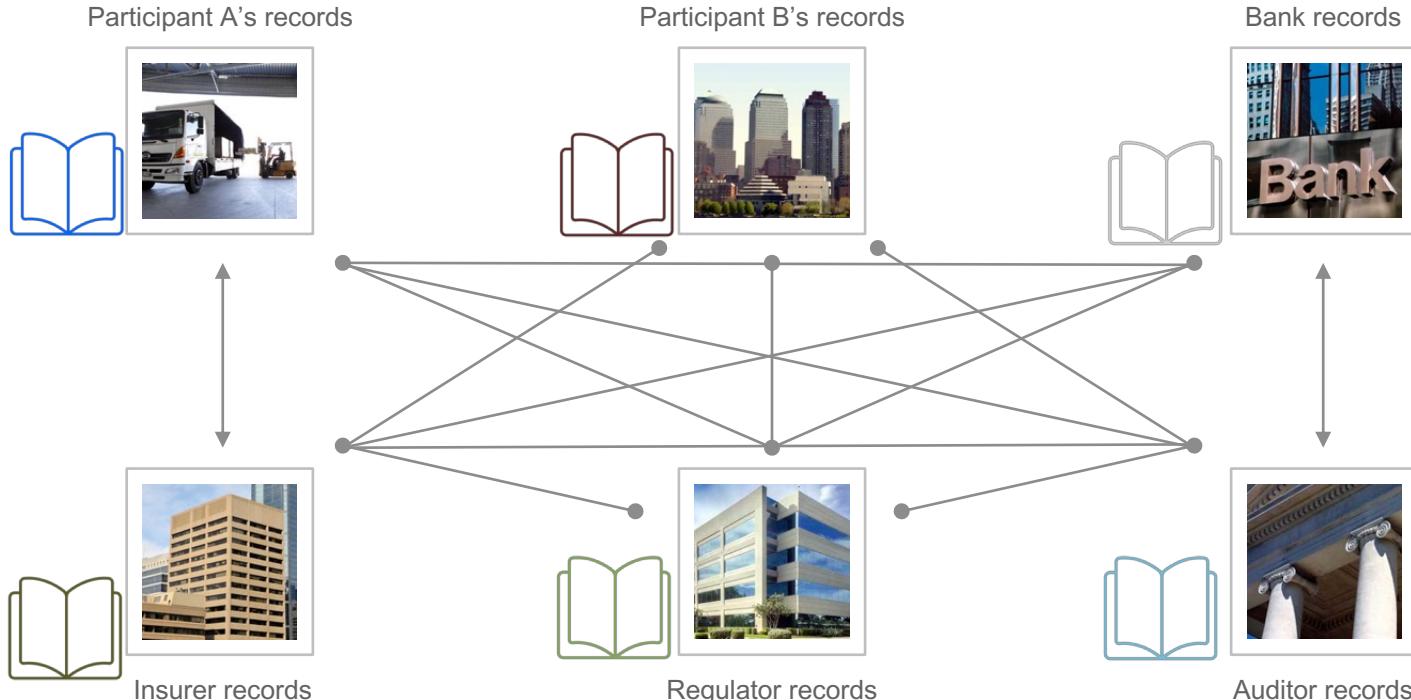
- **Transaction:** an asset transfer onto or off the ledger
 - John gives a car to Anthony (simple)
- **Contract:** the conditions for a transaction to occur
 - If Anthony pays John money, then car passes from John to Anthony (simple)
 - If car won't start, funds do not pass to John (as decided by third party arbitrator) (more complex)





Problem

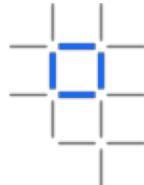
inefficient, expensive, vulnerable



Solution

A shared, replicated, permissioned ledger...

...with consensus, provenance, immutability and finality



Participant A's records



Participant B's records



Bank records



Blockchain



Insurer records

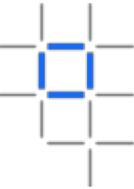


Regulator records



Auditor records

Different types of blockchain



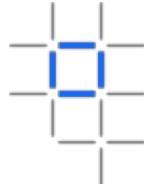
- All blockchains aim to provide **irrefutable proof** that a set of transactions occurred between participants
- Different types of blockchain exist:



is an example of an unpermissioned, public blockchain

- The first blockchain application
 - Defines a shadow-currency and its ledger
 - Resource intensive
-
- Blockchains for business generally prioritize
 - **Assets** over cryptocurrency; **Identity** over anonymity; **Selective endorsement** over proof of work





Requirements of blockchain for business



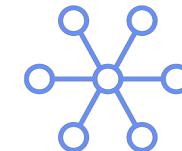
ASSETS

Participants decide which assets to share



IDENTITY

Participants know who they are dealing with; information shared is need-to-know



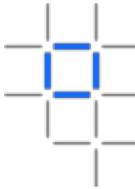
ENDORSEMENT

Participants give provable endorsement

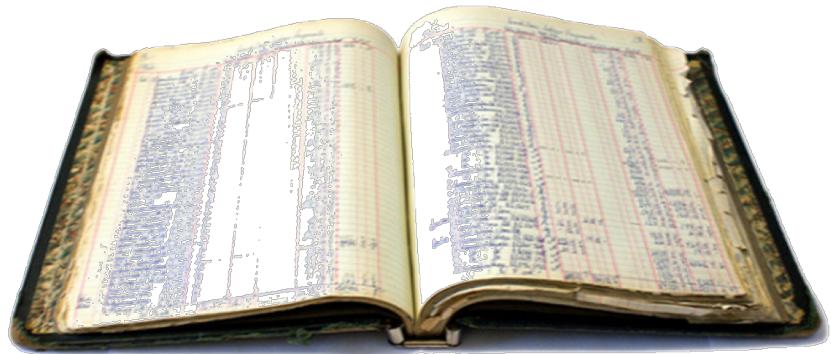


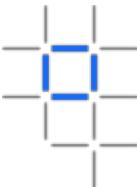
Assets

The business network decides what to share on the ledger



- **Assets** are anything of value
 - On the blockchain, these are represented digitally using a pre-agreed format
- **Transactions** change the state of an asset and are provably recorded on the blockchain
 - e.g. transfer ownership, change color
- Transactions are underpinned by **smart contracts**
 - Verifiable business rules that cause the asset to change state



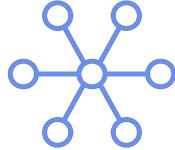


Identity

Knowing who you're dealing with

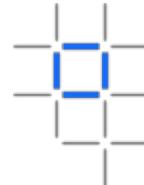
- Various regulations applied to businesses require them to know who they are dealing with
 - e.g. KYC, AML, CFT
- Identity is used to ensure business networks are kept **private** and individual transactions **confidential**
 - With transparency for the regulator
- There are established methods for obtaining and asserting identity
 - Cryptography is central to these
 - Identity allows transactions to be signed and encrypted





Transaction Endorsement

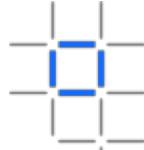
Provable verification by relevant participants



- Endorsement is the process in which a transaction is verified as “good”
 - Ensures that participants are happy to accept the transaction and prevents (e.g.) double spending
- Endorsement can be expensive in public blockchains
 - Without identity, transactions are thrown to the whole network for endorsement
 - Proof of work is particularly CPU intensive
- In the real world, transactions are endorsed by a **smaller number of participants**
 - e.g. sender bank, receiver bank, payments provider
 - Must be completed in an appropriate timeframe

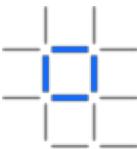


Common blockchain use cases

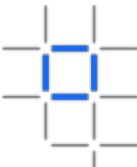


Banking	Trade Finance	<ul style="list-style-type: none">• Lending against Invoice<ul style="list-style-type: none">• Banks (Fraud)• Banks, Buyer, Seller (Fraud and Dispute Management)• Lending against Purchase Order (working capital)• Supply chain Financing<ul style="list-style-type: none">• Equipment financing• Logistic financing• Dealer Financing
	Bank Guarantee	<ul style="list-style-type: none">• Letter of guarantee for service acquisition
	KYC/KYS	<ul style="list-style-type: none">• Convert research assets to offering
	World Wire	<ul style="list-style-type: none">• Cross border Payments
Insurance	Cross Industry <ul style="list-style-type: none">• Life Insurance• Casualty & Property• Healthcare etc	<ul style="list-style-type: none">• Claims Processing• Dispute Resolution• Directors and Officers multi country policy• Healthcare information collection and sharing
Financial Markets	Cross Industry	<ul style="list-style-type: none">• Short Selling• Custody and asset tracking• Post Trade settlement• FX netting• Loans against securities• Private equity management and administration

Common blockchain use cases



Enterprise	Enterprise Asset Management	<ul style="list-style-type: none">Single source of asset inventory and contract management
	Contingent Labor	<ul style="list-style-type: none">Time and Contract dispute management
	Inter-department chargeback	<ul style="list-style-type: none">Chargeback and dispute management
	Account Payable	<ul style="list-style-type: none">Invoice dispute management
Distribution	Track & Trace	<ul style="list-style-type: none">IoT enabled Track and Trace shipment
	Cold Chain	<ul style="list-style-type: none">IoT enabled Track and Trace perishable goods
	Reverse supply chain	<ul style="list-style-type: none">Track returned goods
Travel & Transportation	Airline Baggage Tracking	<ul style="list-style-type: none">Reduce lost baggage and increase customer satisfaction
	Airlines Cargo Solution	
	Airline Loyalty	<ul style="list-style-type: none">Loyalty program includes airlines and merchandiser
	Maintenance Record Management	<ul style="list-style-type: none">Track certification and maintenance recordsTrack Pilot and crew certification
Automotive	Parts Provenance	<ul style="list-style-type: none">Track and trace parts from raw material through manufacturing and supply chain
	Conflict Mineral Management (RCN)	<ul style="list-style-type: none">Track and trace minerals and raw materials used in electronics to identify source and avoid conflict minerals
	Commerce Platform	<ul style="list-style-type: none">Frictionless payment system across multiple entities e.g. Gas, Toll, Towing, Service etc



Common blockchain use cases

Media & Entertainment	Telco – Don't Disturb	<ul style="list-style-type: none">Prevent the problem of Unsolicited Commercial Communication
	Number Portability	<ul style="list-style-type: none">Cross Telco company number portability
	Asset Inventory & Contractor Management	<ul style="list-style-type: none">Move, Add and Change asset movement and contractor dispute management
	Reverse supply chain	<ul style="list-style-type: none">Track returned goods
Life Sciences	Healthcare Records	<ul style="list-style-type: none">Create and promote a secure, efficient and scalable exchange of patient health data
	Counterfeit drugs	<ul style="list-style-type: none">Track and Trace drug supply chain
Public Sector	Notary	<ul style="list-style-type: none">Notarized document management
	Motor Vehicle	<ul style="list-style-type: none">Vehicle registration record management
	Citizen Identity	<ul style="list-style-type: none">Create single source of citizen identity as a repository for citizen services
	Benefits Payment	<ul style="list-style-type: none">Reduce fraud in benefits payment
	Corporate Registry	<ul style="list-style-type: none">Create single source of corporate registry as a repository for corporate services
Energy & Utilities	Carbon Credit	<ul style="list-style-type: none">Exchange for carbon credits and settlements
	Asset Inventory & Contractor Management	<ul style="list-style-type: none">Move, Add and Change asset movement and contractor dispute management



What is Blockchain?

A brief description



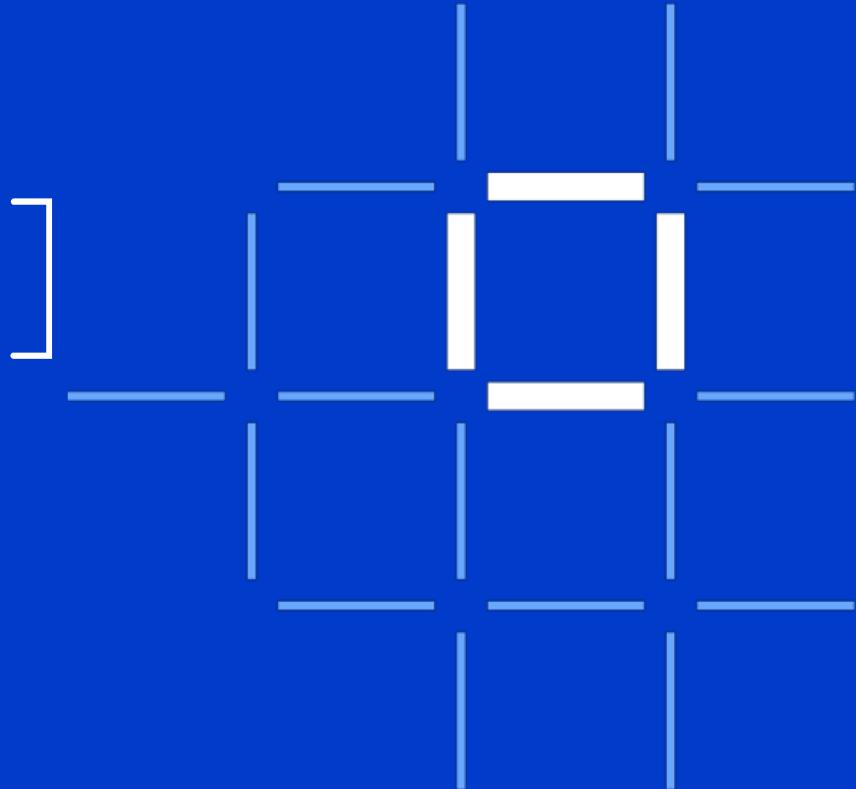
Essence of Blockchain

Describing why blockchain is just a piece of the puzzle



Blockchain Integration

Deriving value by leveraging other tools



IBM Blockchain Platform is the core of IBM's **blockchain strategy**



Garage & Lab Services

Collaborate with experts on from ideation all the way to production



Ecosystem

Tap into our diverse ecosystem to develop strategic partnerships and create your competitive advantage



Solutions

Solve critical industry challenges by building and joining new business networks and applications



IBM Blockchain Platform

Build, operate and grow blockchain networks in heterogeneous environments



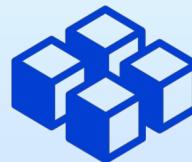
HYPERLEDGER

A founding, premier member of Hyperledger, IBM is committed to open source, standards & governance



IBM Blockchain Platform

Advanced
tooling
& capabilities



Build



Operate



Grow

Open
technology



Deploy
anywhere

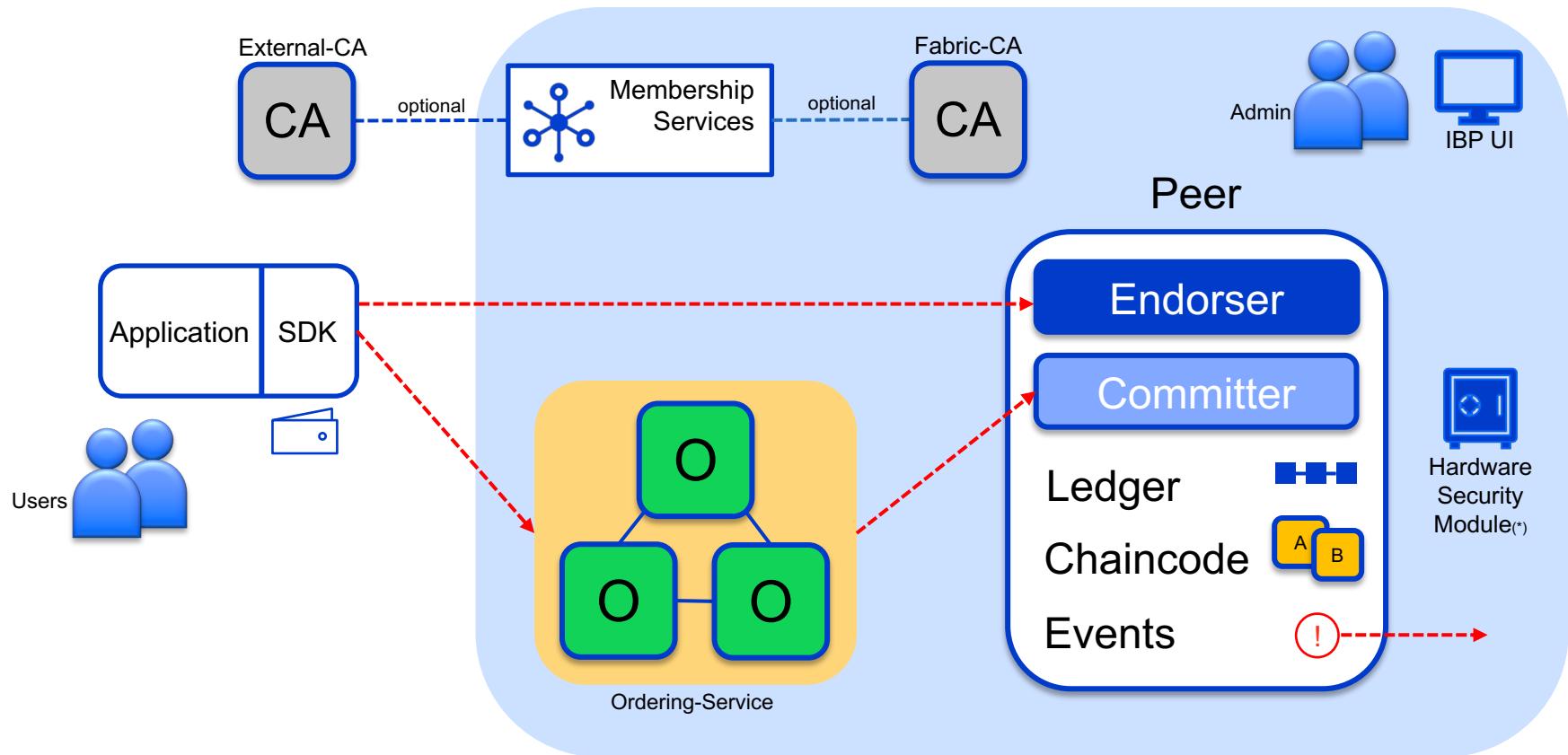
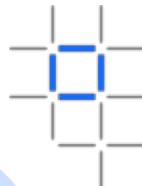


IBM Cloud

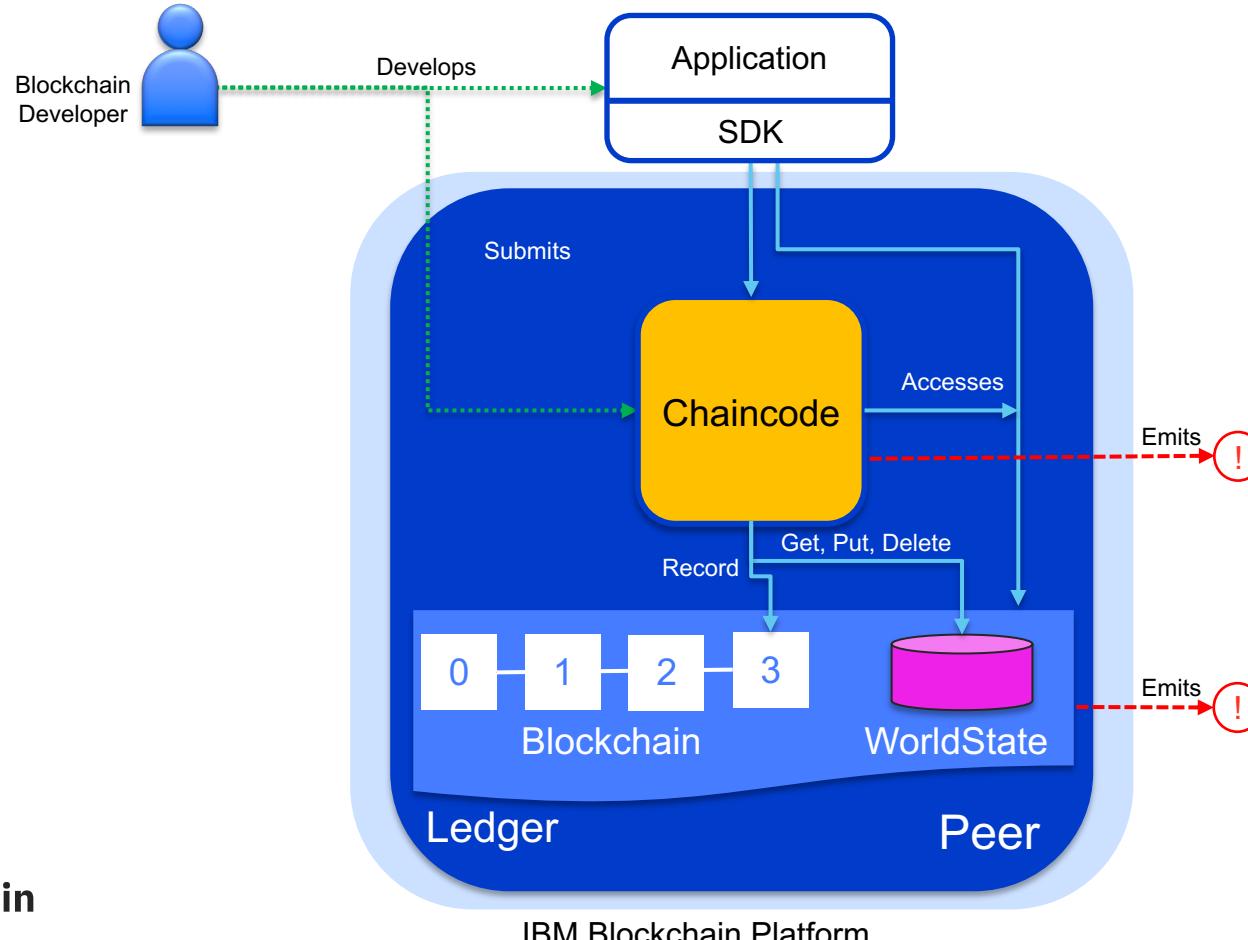
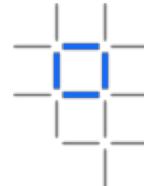
On-Premises

Other clouds

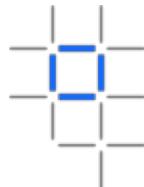
Platform Architecture Overview



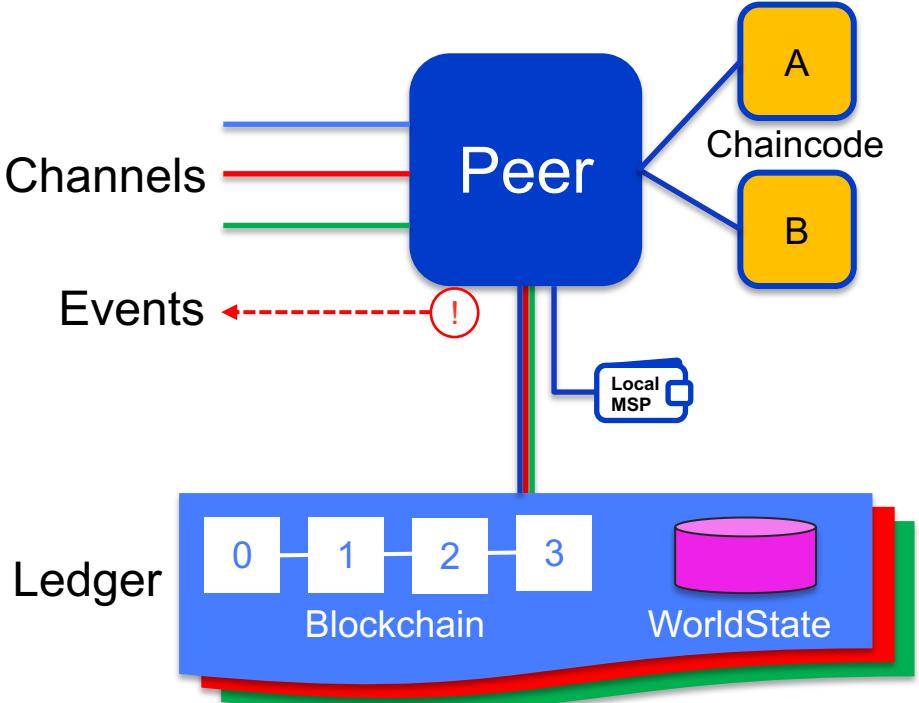
How applications interact with the IBM Blockchain Platform



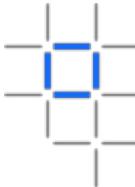
IBM Blockchain Platform - Peer



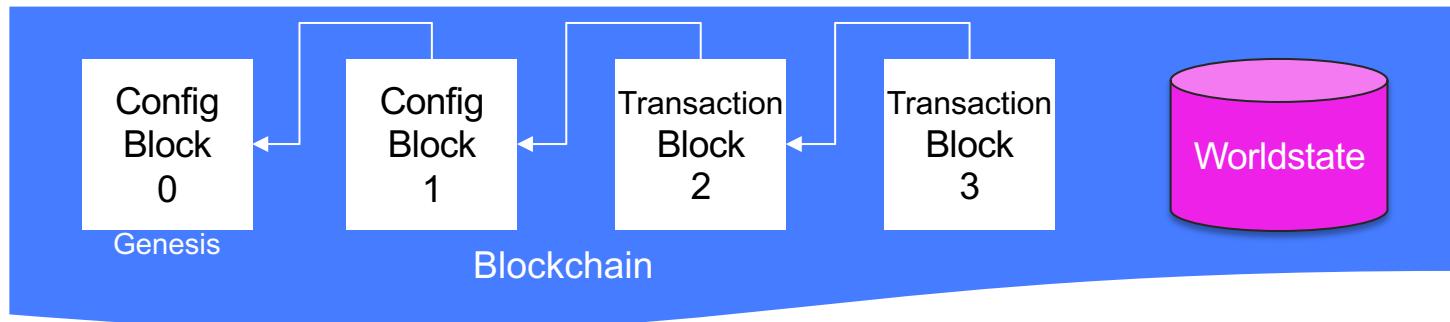
- With the IBM Blockchain Platform each peer:
 - Connects to one or more **channels**
 - Maintains one **ledger** per channel
 - Maintains **installed chaincode**
 - Manages **runtime docker containers** for **instantiated chaincode**
 - Chaincode is instantiated on a channel
 - Runtime docker container shared by channels with same chaincode instantiated (no state stored in container)
 - Has a local MSP (Membership Services Provider) that provides **crypto material**
 - Emits **events** to the client application



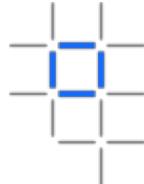
IBM Blockchain Platform - Ledger



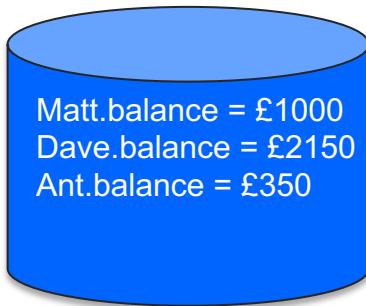
- The [ledger](#) is maintained by each peer and includes the [blockchain](#) and [worldstate](#)
- A separate ledger is maintained for each channel the peer joins
- Transaction [read/write sets](#) are written to the blockchain
- [Channel configurations](#) are also written to the blockchain
- The worldstate 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 worldstate



World State

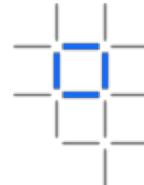


- It is clearly not feasible to reparse the entire transaction log to complete a new transaction
- Blockchains often include an associated database (world state) – e.g. Hyperledger Fabric
- Transactions become a set of creates, reads, updates and deletes of records in this data store

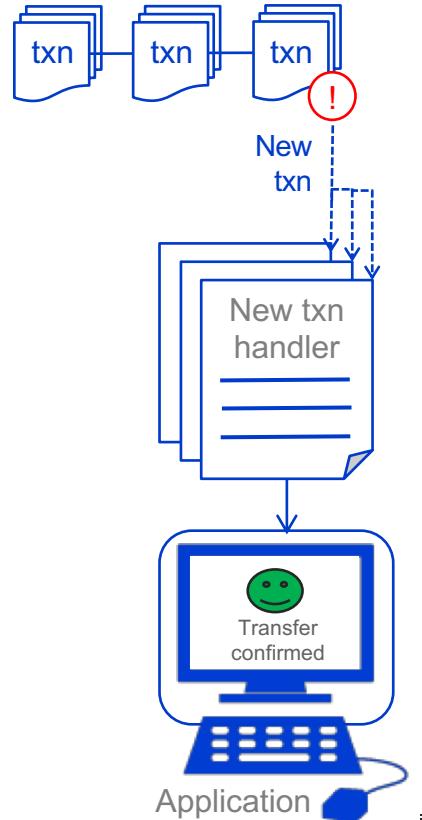


#	Transaction	Initiator	Receiver	Amount
1	Create a/c	Cash	Matt	£1000
2	Create a/c	Cash	Dave	£2000
3	Transfer	Matt	Dave	£100
4	Create a/c	Cash	Ant	£500
5	Transfer	Ant	Matt	£50
6	Transfer	Ant	Dave	£200
7	Transfer	Dave	Matt	£100
8	Transfer	Dave	Ant	£50
9	Transfer	Matt	Ant	£50

How Events are Used in Blockchain



- In computing, an **event** is an occurrence that can trigger handlers
 - e.g. disk full, fail transfer completed, mouse clicked, message received, temperature too hot...
- Events are important in asynchronous processing systems like blockchain
- The blockchain can emit events that are useful to application programmers
 - e.g. Transaction has been validated or rejected, block has been added...
- Events from external systems might also trigger blockchain activity
 - e.g. exchange rate has gone below a threshold, the temperature has gone up, a time period has elapsed...





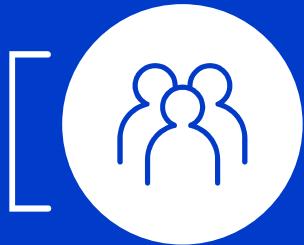
What is Blockchain?

A brief description



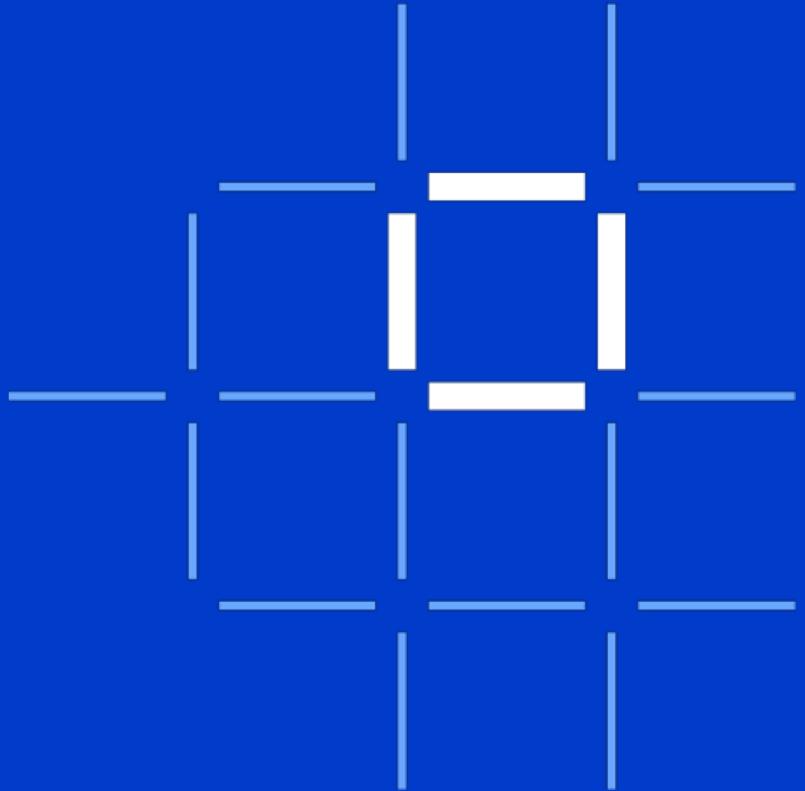
Essence of Blockchain

Describing why blockchain is just a piece of the puzzle

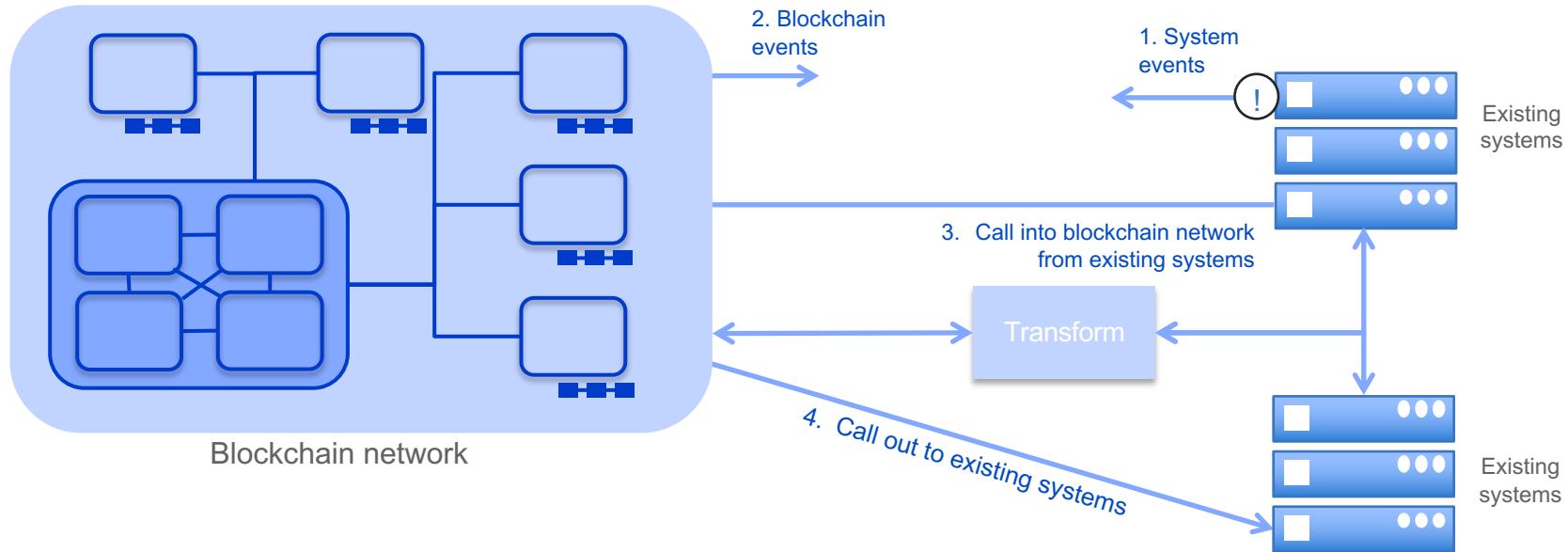
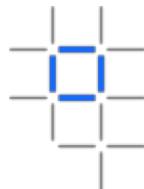


Blockchain Integration

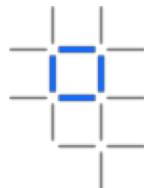
Deriving value by leveraging other tools



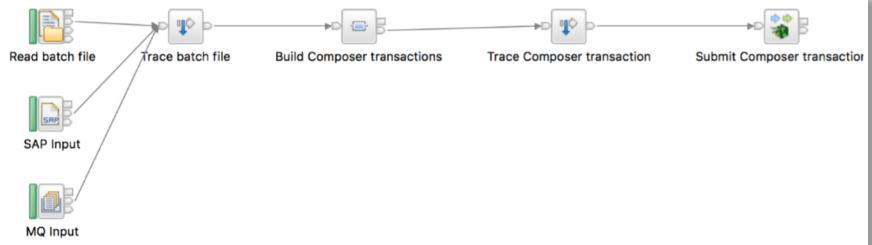
Integrating with Existing Systems – Possibilities



Integrating with Existing Systems – Using Middleware



- Blockchain is a network system of record
- Two-way exchange
 - Events from blockchain network create actions in existing systems
 - Cumulative actions in existing systems result in Blockchain interaction

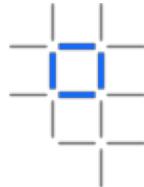


- Transformation between blockchain and existing systems' formats
 - GBO, ASBO is most likely approach
 - Standard approach will be for gateway products to bridge these formats
 - Gateway connects to peer in blockchain network and existing systems

- Smart contracts can call out to existing systems
 - Query is most likely interaction for smart decisions
 - e.g. all payments made before asset transfer?
 - **Warning: Take care over predictability: transaction must provide same outputs each time it executes...**



Non-determinism in blockchain



- Blockchain is a distributed processing system
 - Smart contracts are run multiple times and in multiple places
 - As we will see, smart contracts need to run deterministically in order for consensus to work
 - Particularly when updating the world state
- It's particularly difficult to achieve determinism with off-chain processing
 - Implement oracle services that are guaranteed to be consistent for a given transaction, or
 - Detect duplicates for a transaction in the blockchain, middleware or external system

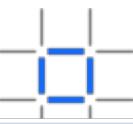
random()

getExchangeRate()

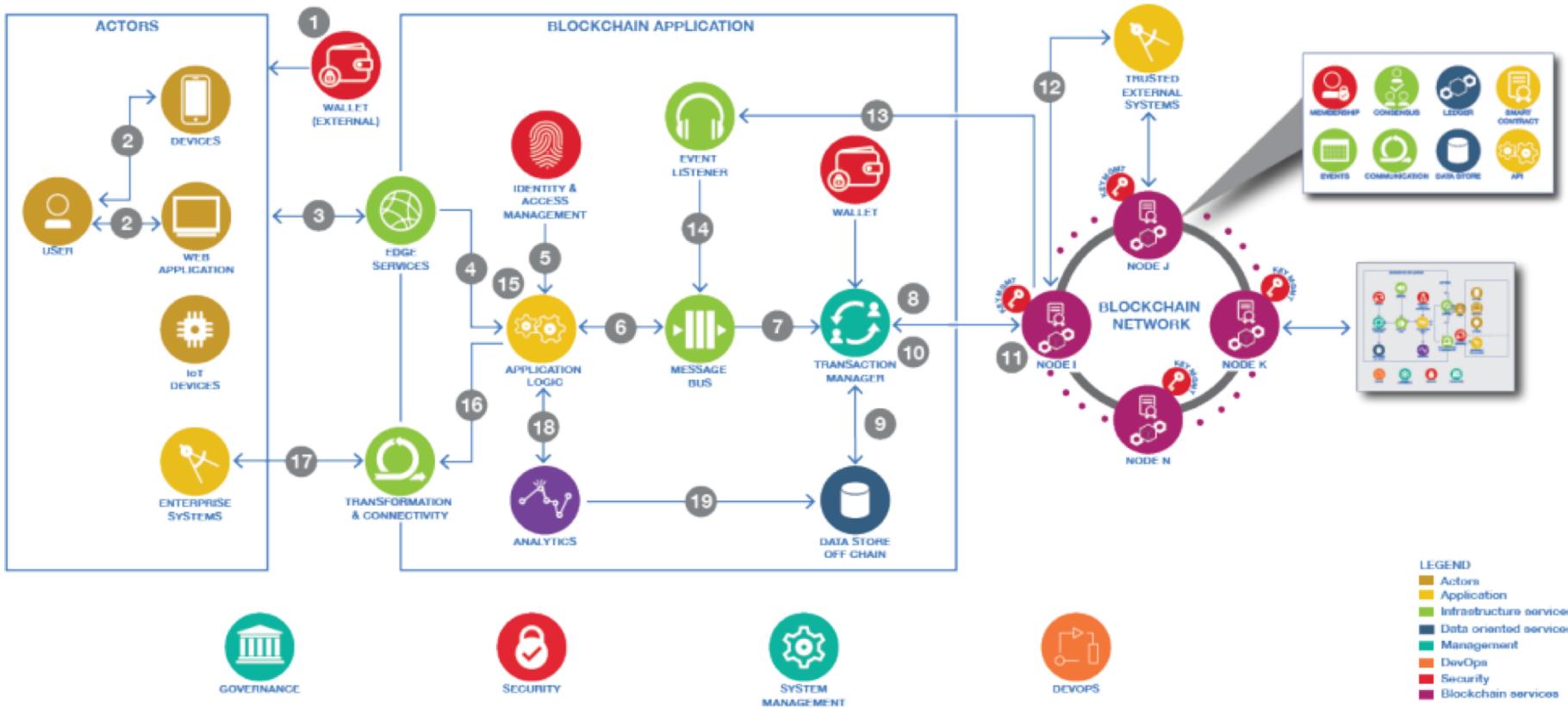
getDateTime()

getTemperature()

incrementValue
inExternalSystem(...)



Reference Architecture



Thank you

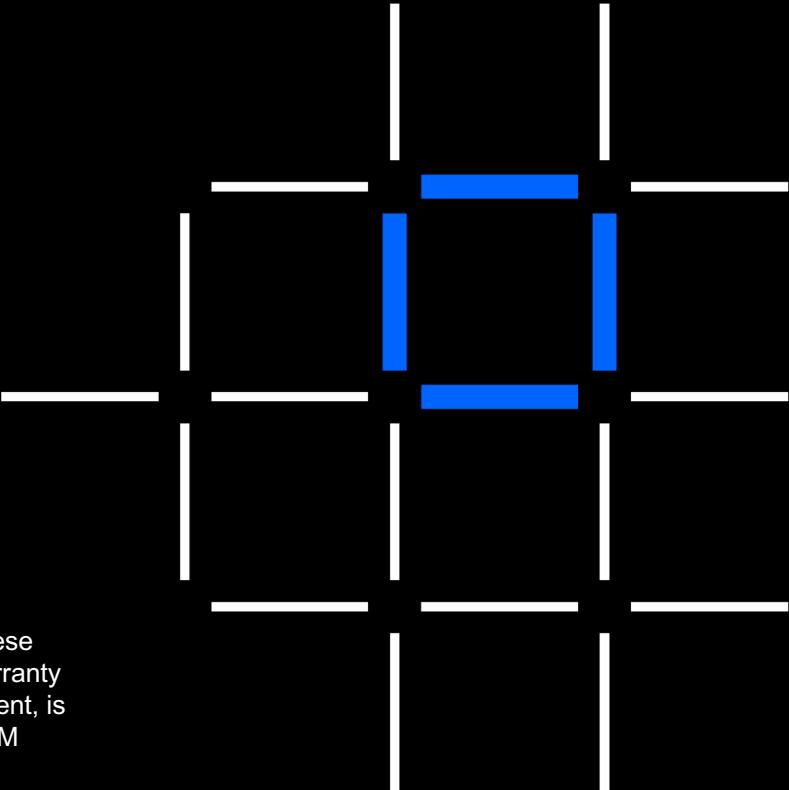
Mark Parzynat
Session E07

IBM Blockchain

www.ibm.com/blockchain

developer.ibm.com/blockchain

www.hyperledger.org



© Copyright IBM Corporation 2017. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represents only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.



