Blockchain

IMPLICATIONS AND USES

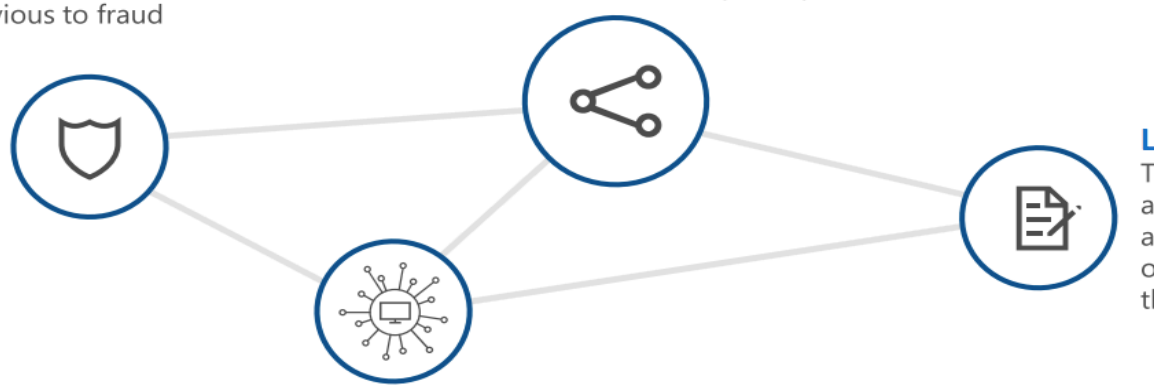
What is Blockchain?

So What is Blockchain?

Blockchain is a secure, shared, distributed ledger

Secure
Uses cryptography to create transactions that are impervious to fraud

Shared
Blockchain value is directly linked to the number of organizations or companies that participate in them.



Ledger
The database is append only so it is an immutable record of every transaction that occurs.

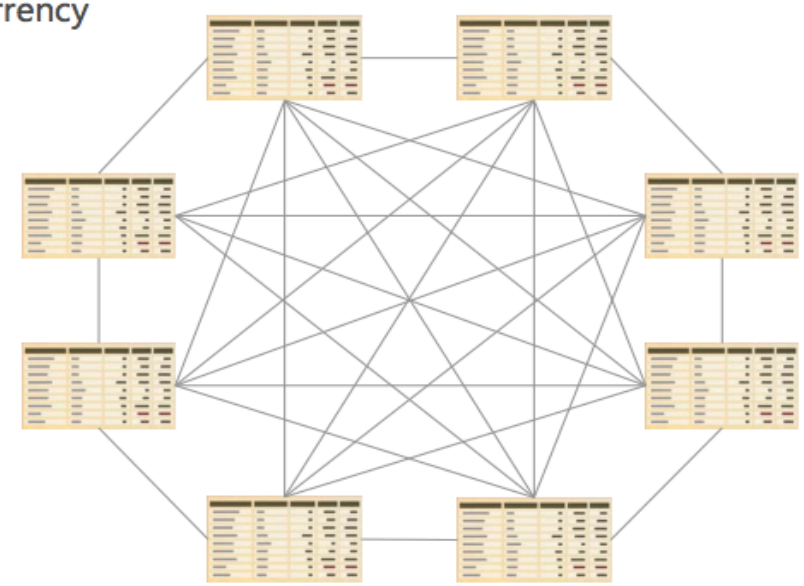
Distributed
There are many replicas of the blockchain database.

Blockchain uses a distributed ledger to track transactions

- A ledger is a write only database most commonly used in accounting
- Same copy of the data distributed across all the participating nodes
- All new transactions are encrypted 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

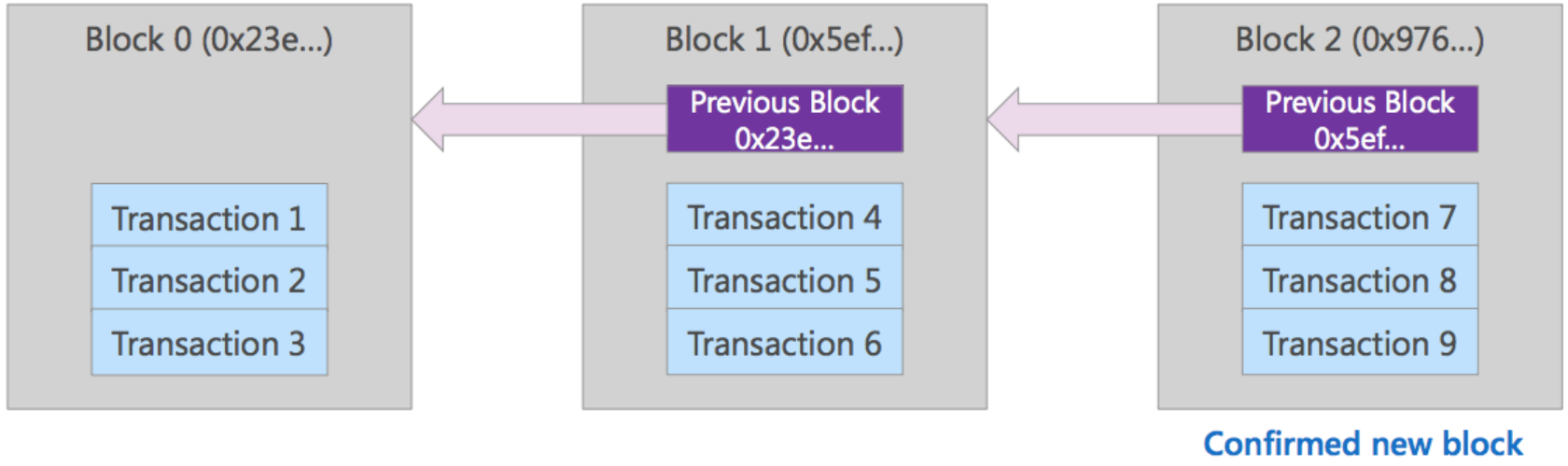
Example ledger



Entire network has same ledger

Transactions are connected within a chain of blocks

- Transactions are grouped together in blocks.
- Blocks are linked to previous blocks, which make the blockchain
- The transaction chain tracks how ownership changes, while the block chain tracks the order of transactions
- Transactions within the same block are considered to occur at the same time



The Bitcoin Blockchain

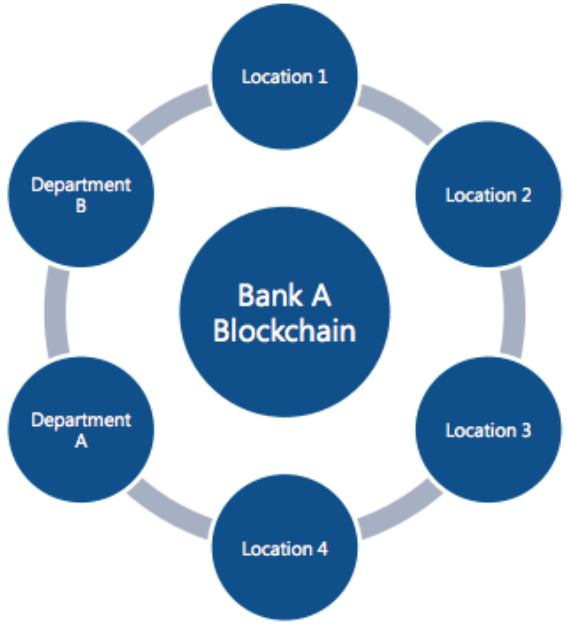
The Bitcoin Blockchain Breakthrough: the first iteration of a successful blockchain in 6 steps

1. New transactions are **broadcast** to the bitcoin network (all nodes).
2. Each participant **collects new transactions into a block** and time stamps them (aka 'hash').
3. Each node works on finding a **difficult proof-of-work for** its block, called mining
4. When a participant finds a proof-of-work, it **broadcasts** the block to all nodes.
5. The individual nodes accept the block only if all transactions in it **are valid and not already spent.**
6. Nodes express their acceptance of the block by working on **creating the next block** in the chain.

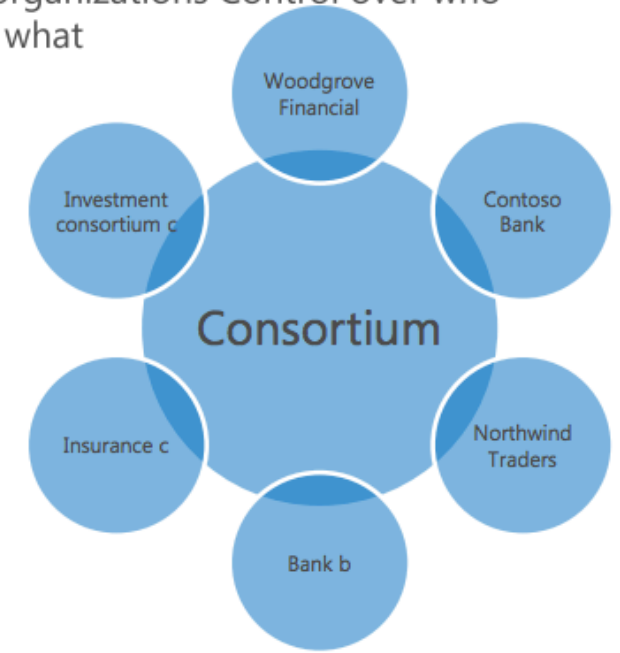
Types of blockchain networks

Public
Such as bitcoin, ethereum

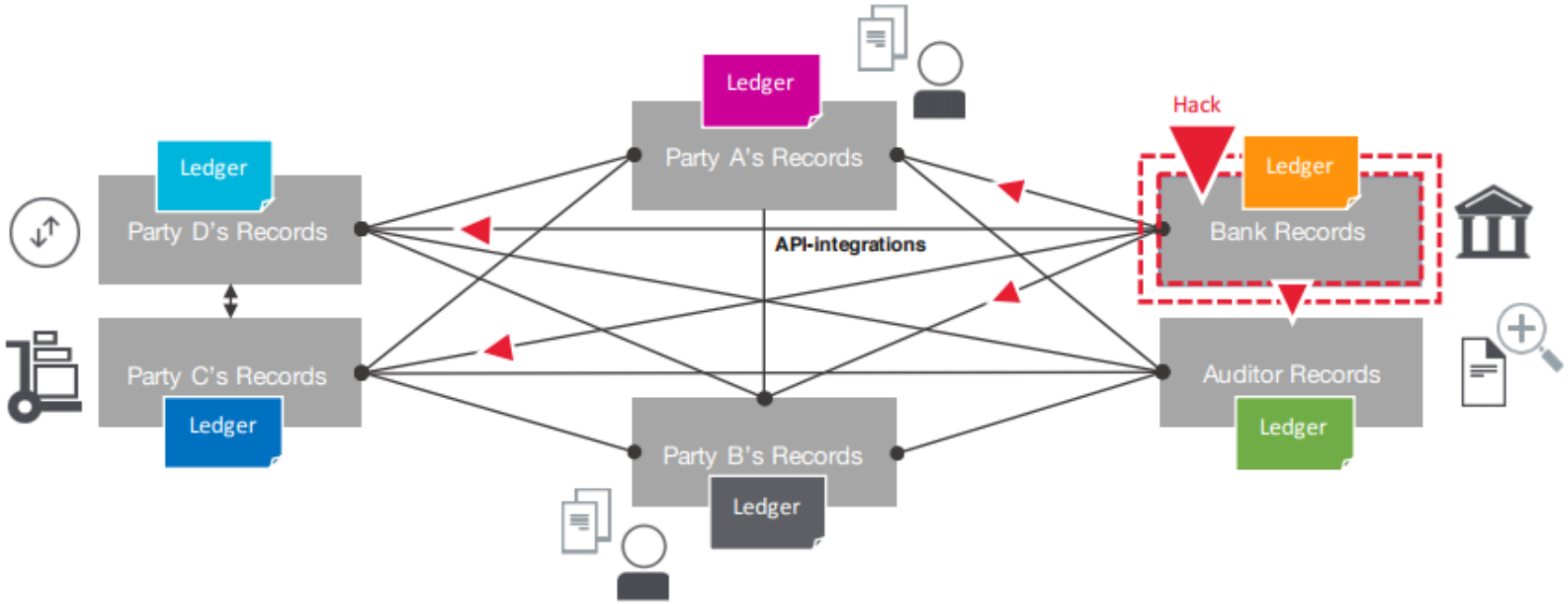
Private
For one organization



Consortium
Set of organizations Control over who can do what

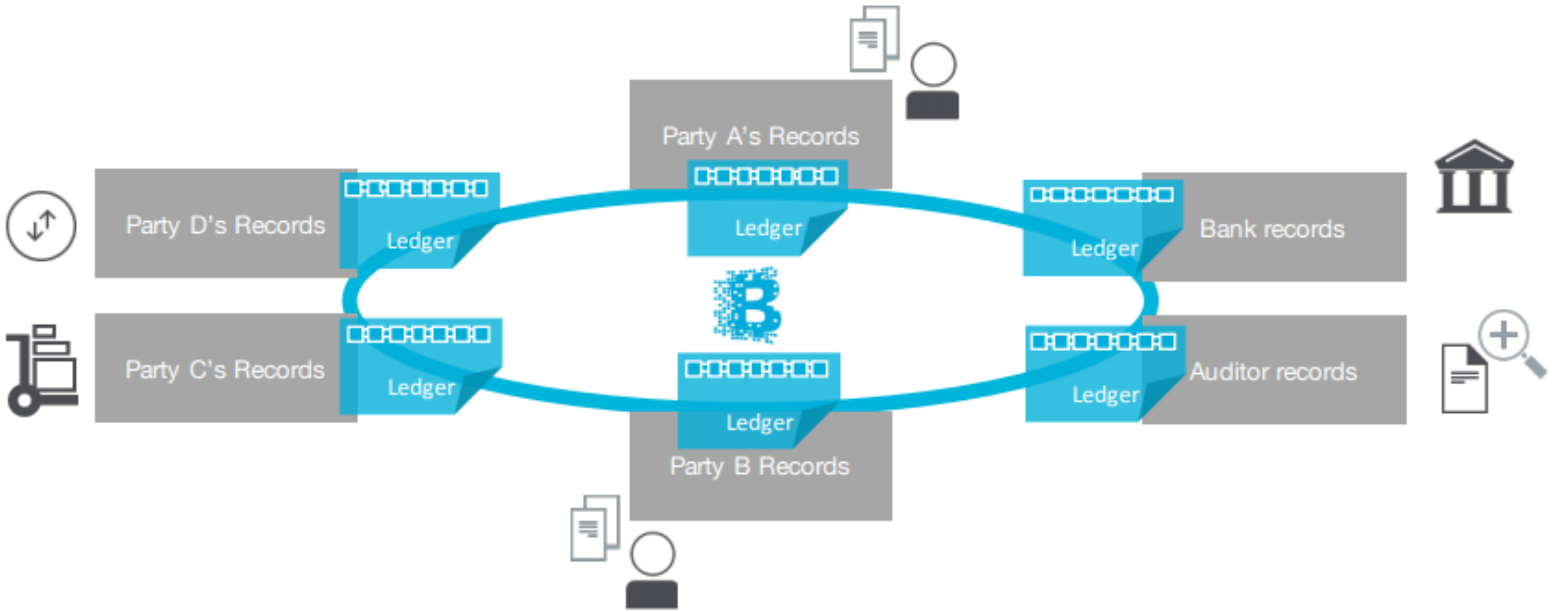


Information & Asset Exchange in business networks – Separate Ledgers



Inefficient, expensive, error sensitive and vulnerable

Information and Asset Exchange in Business Networks – Shared Ledger



Consistent, efficient, secure and resilient

4 key concepts

- - Distributed Shared Ledgers
- - Cryptography
- - Consensus
- - Smart Contracts

Distributed Shared Ledgers

- - type of database that is shared, replicated, and synchronized among the members of a network
- - every recorded transaction has a unique cryptographic signature and timestamp, thus making the ledger an auditable history of all transactions in the network
- - A Node refers to a ‘full’ client - a client that owns the block chain and that is sharing blocks and transaction across the network – all nods hold all transactions

BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Jun 14 2015 14:01:53 GMT+0200.

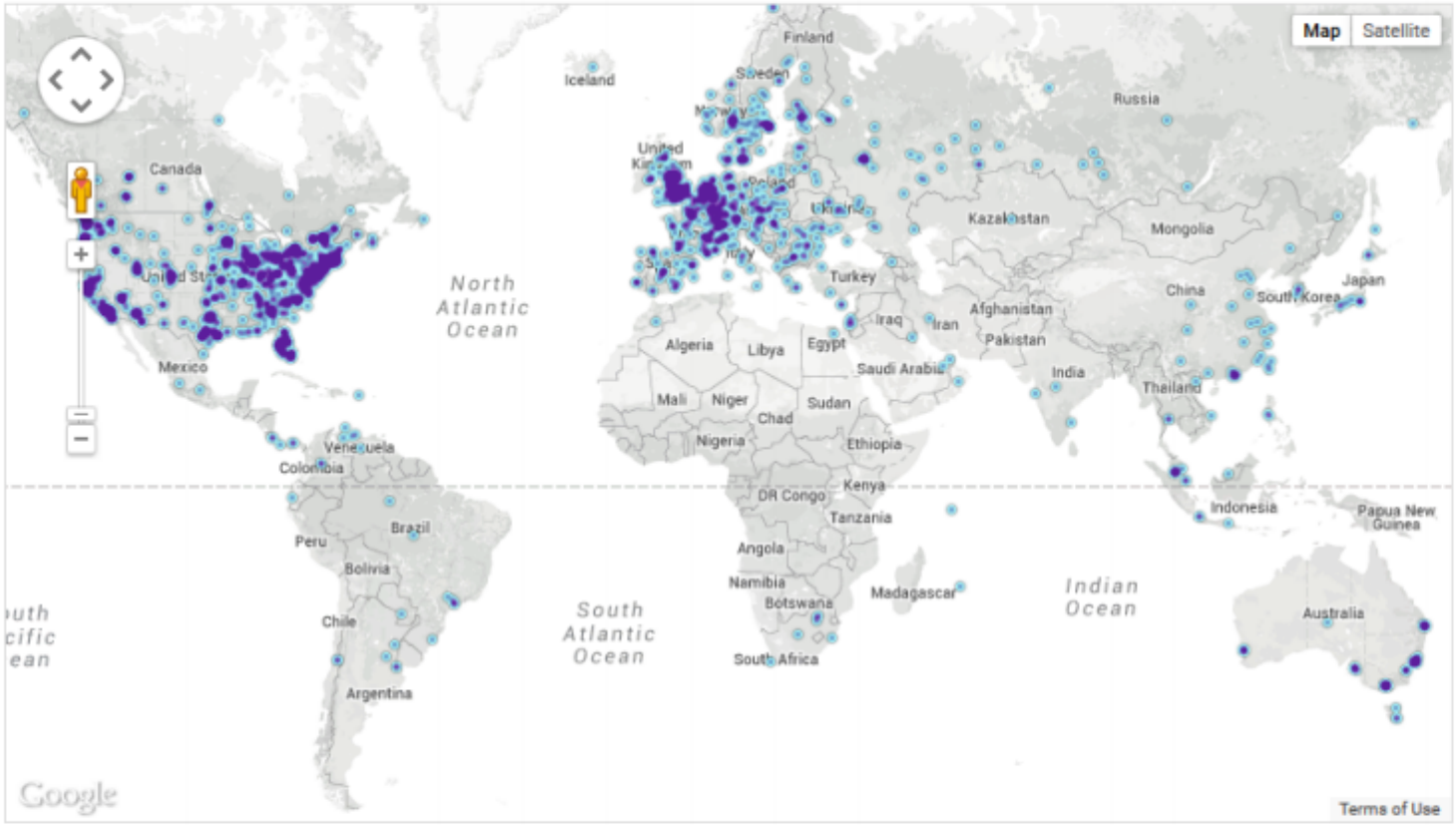
5987 nodes

24-hour charts »

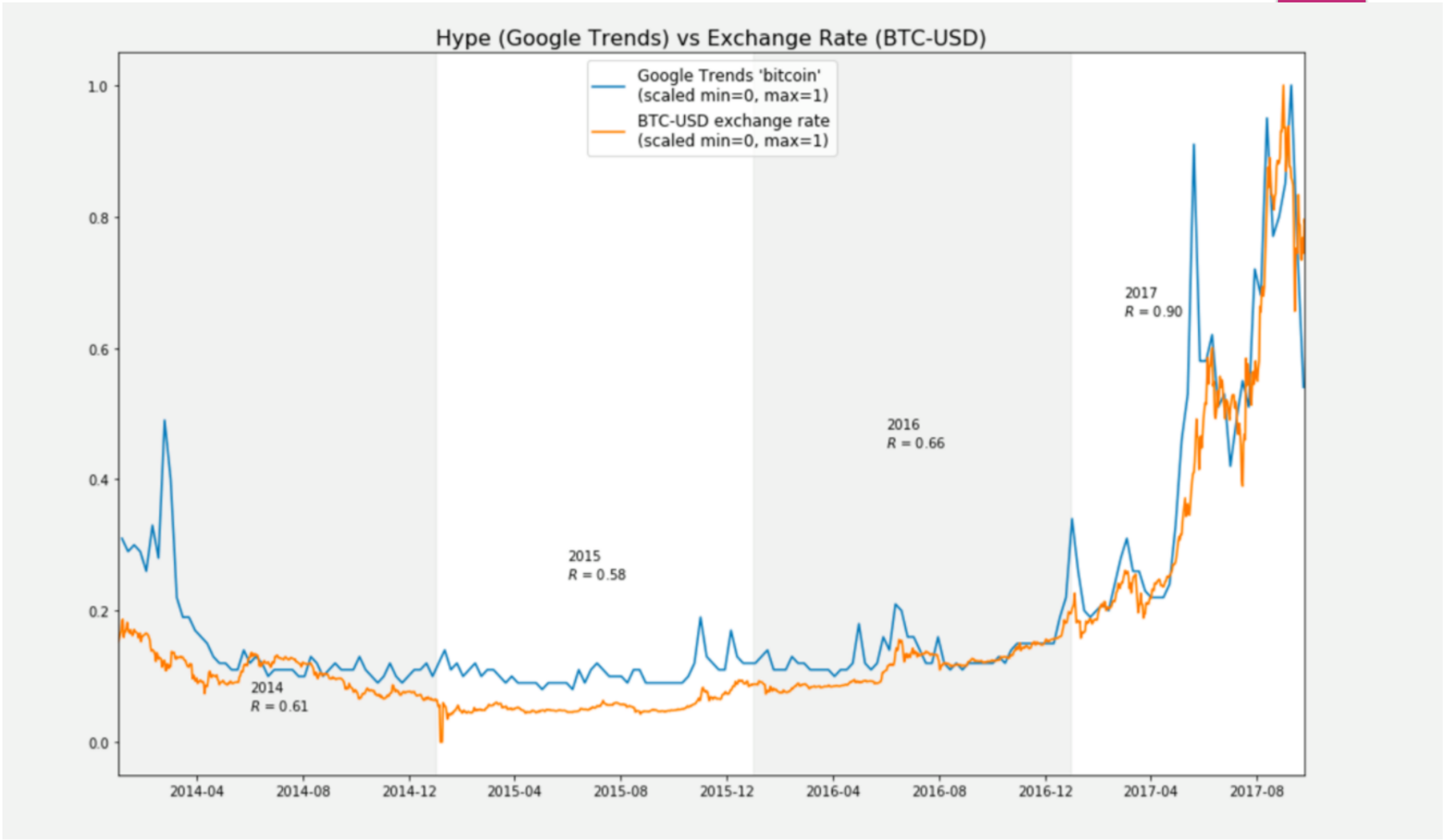
Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2161 (36.09%)
2	Germany	626 (10.46%)
3	France	442 (7.38%)
4	United Kingdom	375 (6.26%)
5	Netherlands	307 (5.13%)
6	Canada	302 (5.04%)
7	Russian Federation	187 (3.12%)
8	Australia	136 (2.27%)
9	Sweden	116 (1.94%)
10	China	102 (1.70%)

More (85) »

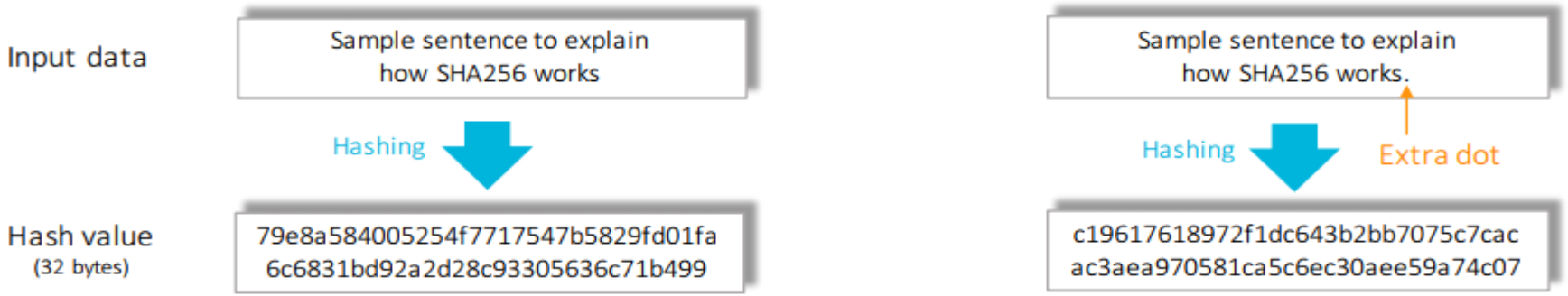


Map shows concentration of reachable Bitcoin nodes found in countries around the world.


Hype (Google Trends) vs Exchange Rate (BTC-USD)
Google Trends 'bitcoin'
(scaled min=0, max=1)
BTC-USD exchange rate
(scaled min=0, max=1)
2014
R = 0.61
2015
R = 0.58
2016
R = 0.66
2017
R = 0.90
1.0
0.8
0.6
0.4
0.2
0.0
2014-04
2014-08
2014-12
2015-04
2015-08
2015-12
2016-04
2016-08
2016-12
2017-04
2017-08

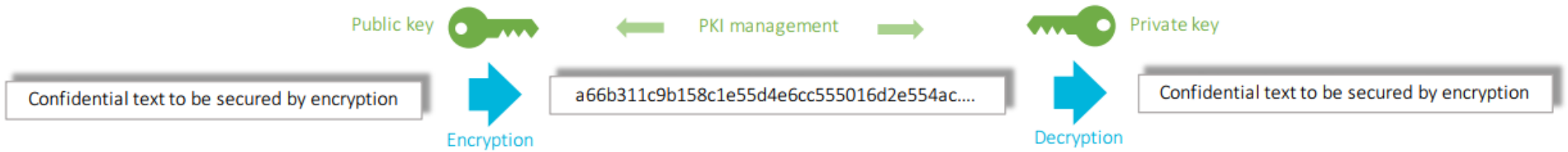
Cryptography

- Hashes – Creation of a bit string representing integrity of content other string
- Cryptographic hashes, such as the SHA256 computational algorithm, ensure that any alteration to transaction input — even the most minuscule change — results in a different hash value being computed, which indicates potentially compromised transaction input



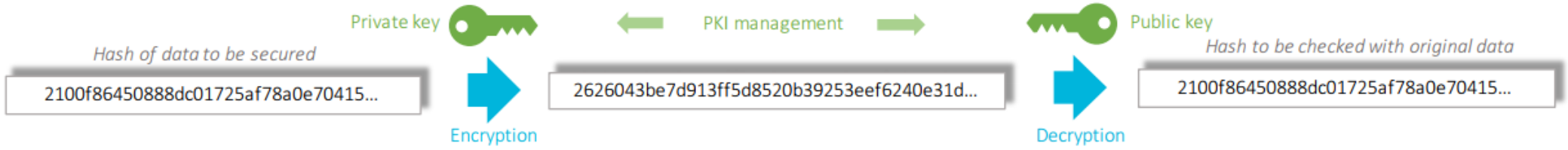
Cryptography

- Keys and Wallets – A string encrypted with one key can only be decrypted with the other. One key needs to be kept private, the other one can be made publicly known so that it can be used by other parties to exchange data with you in a secure manner. Private keys need to be stored either on a personal device or remotely with a service provider (wallet) so that it is only accessible for the owner
- Encryption – The scrambling of clear text with the public key of the recipient so that the holder of that private key is the only one that can descramble the message. This is used to guarantee the confidentiality of the data exchanged.



Cryptography

- Digital signature – Encryption of hash representing of original data to be secured with the private key of the sender that is decrypted by the recipient with the public of the sender. If the decrypted hash matches the content of the original data it implies two things. First, the encryption can only be performed with the private key corresponding with public key and secondly, the original data can't be tampered with.
- Digital signatures ensure that transactions originated from senders (signed with private keys) and not imposters

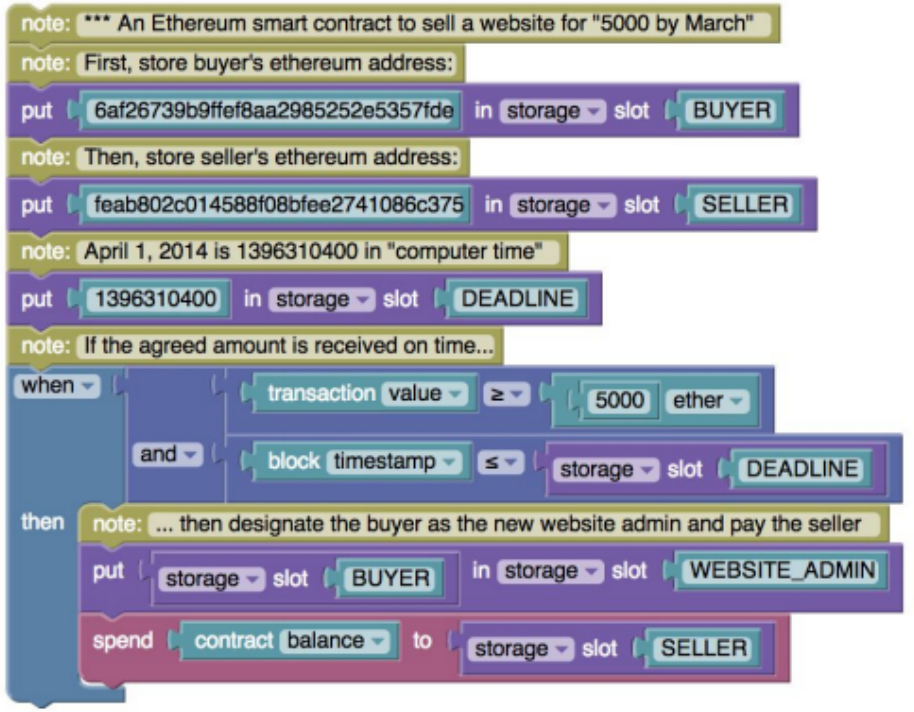


Consensus

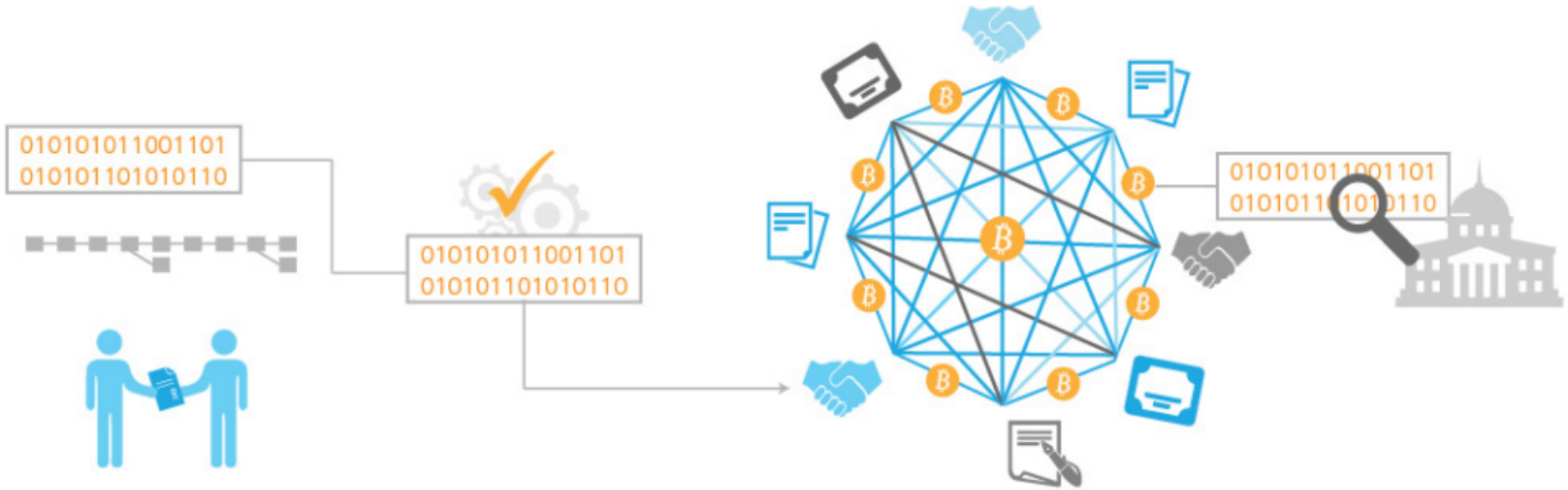
- Consensus – majority of nodes agree on the validity of transactions
- Consensus ensures that the shared ledgers are exact copies, and lowers the risk of fraudulent transactions, because tampering would have to occur across many places at exactly the same time

Smart Contracts

- A business logic that can be assigned to a transaction on the blockchain
- Acts as a notary of blockchain transactions
- It holds conditions under which specified actions can/must be fulfilled
- Cannot be modified without predefined permissions
- When a triggering event occurs the contract executes itself



Smart Contracts



1. An option contract between parties is written as code into the block chain. The individuals involved are anonymous, but the contract is in the public ledger.
2. A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.
3. Regulators can use the block chain to understand the activity in the market while maintaining the privacy of individual actors' positions.

What is blockchain used for?

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
Client and product reference data.
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 prediction
Telematics & ratings

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

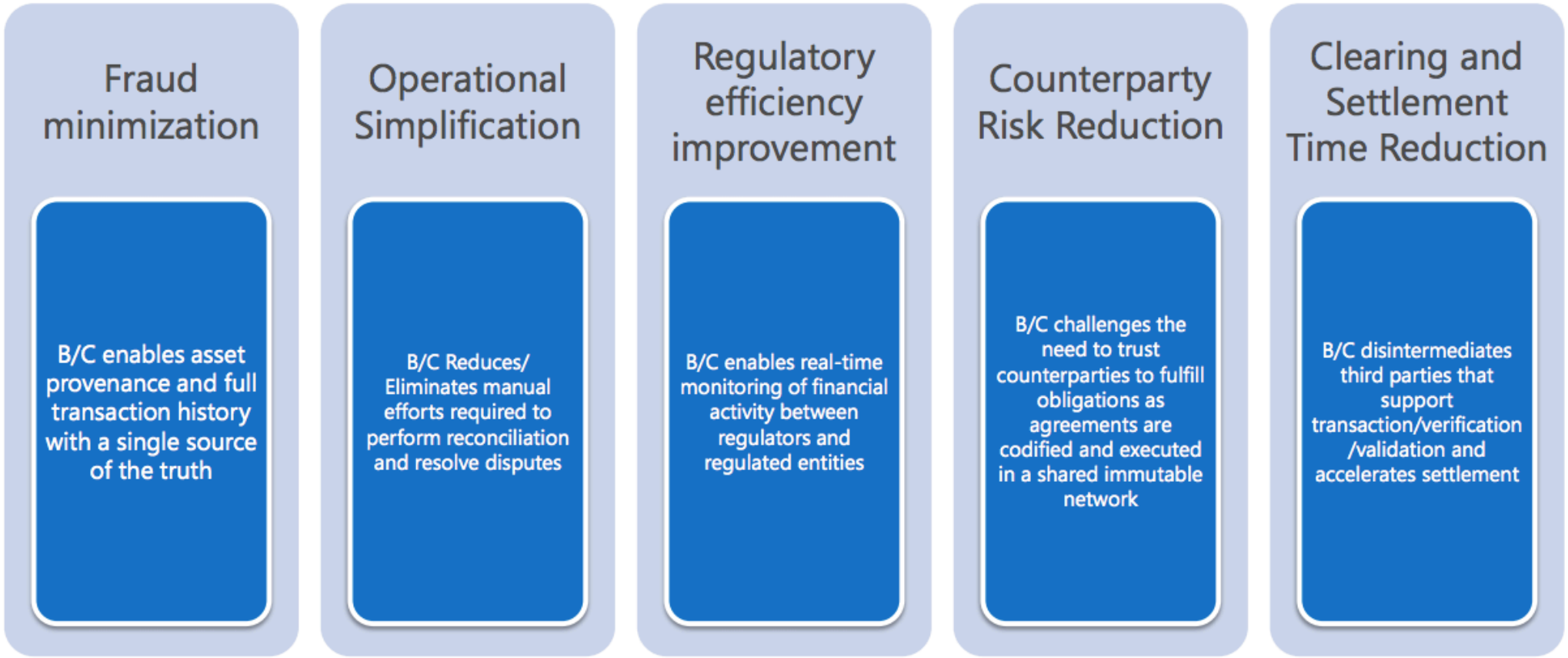
IoT
Device to Device payments
Device directories
Operations (e.g. water flow)
Grid monitoring
Smart home & office management
Cross-company maintenance markets

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

Blockchain Benefits



- Any Questions?