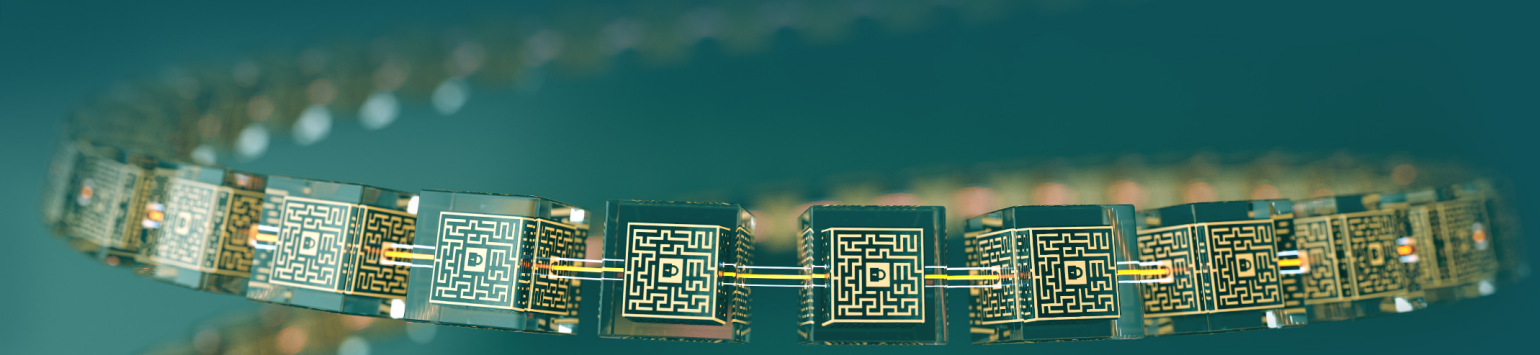
New Kids on the Block[chain]:

Blockchain 101



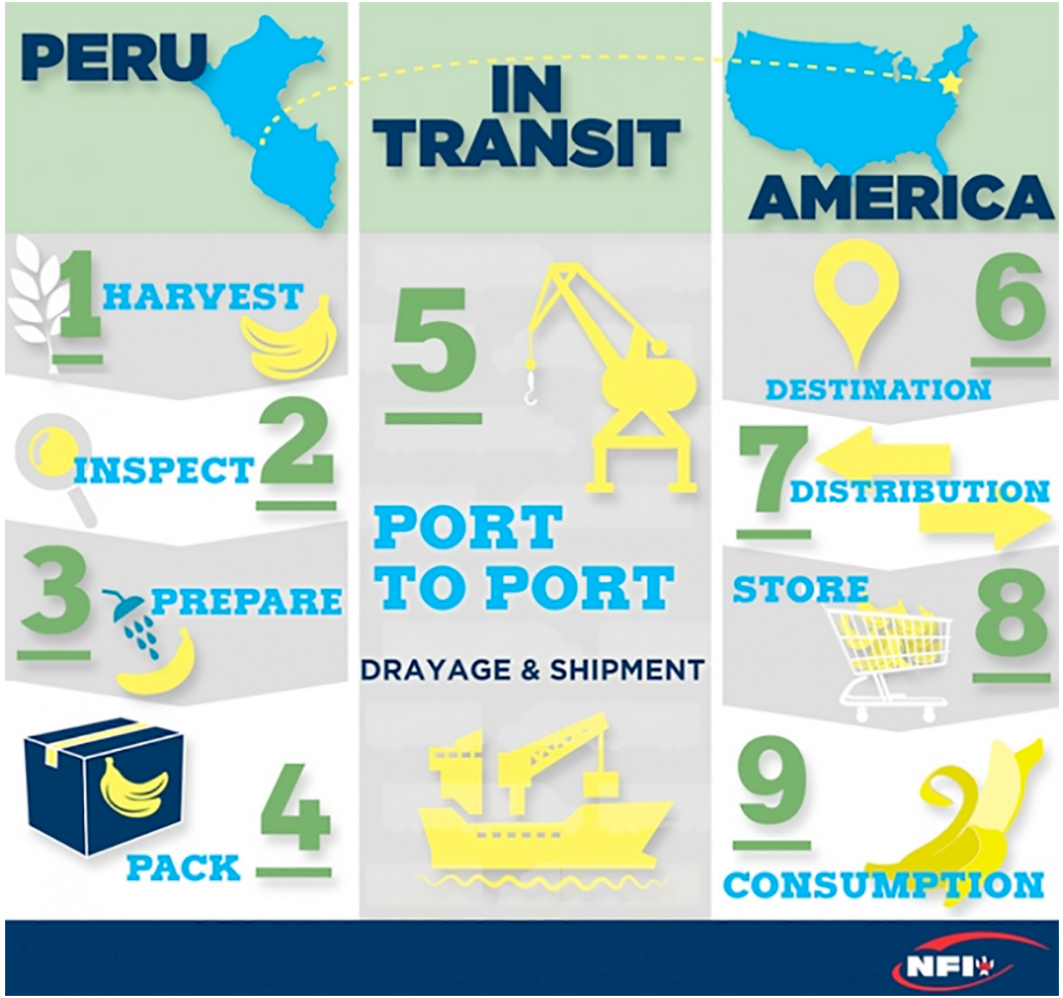
Gerhard Dinhof, gerhard.dinhof@at.ibm.com / gerhard.dinhof@iot-austria.at, @gdinhof
"Blockchainers Vienna" Meetup – sektor5, August 14th 2017

Interrupt && Discuss

Source: http://plannersweb.com/2013/02/what-does-a-discussion-look-like/

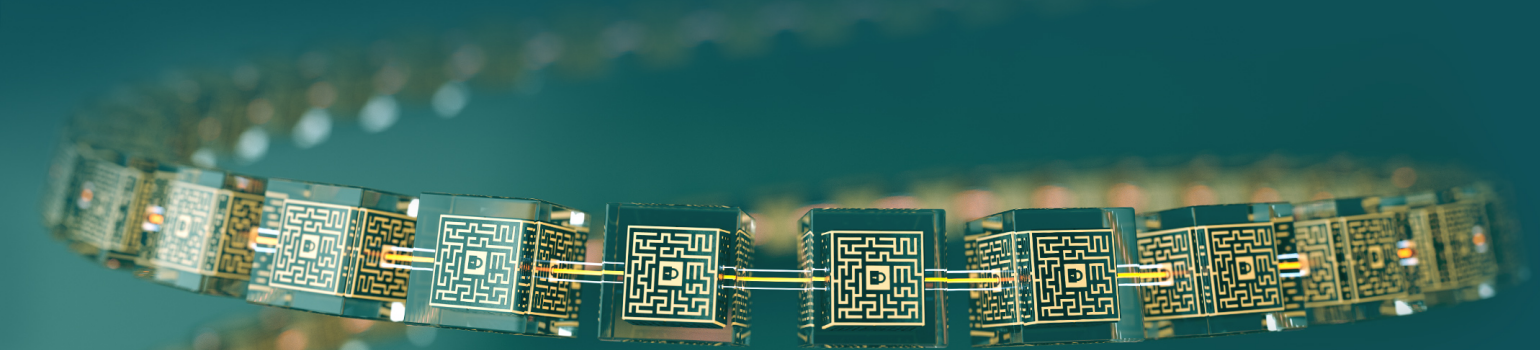
The Life of a … banana!

Source: Gerhard Dinhof / Personal



Source: NFI http://www.nfiindustries.com/wp-content/uploads/2015/08/international-shipping-produce.jpg

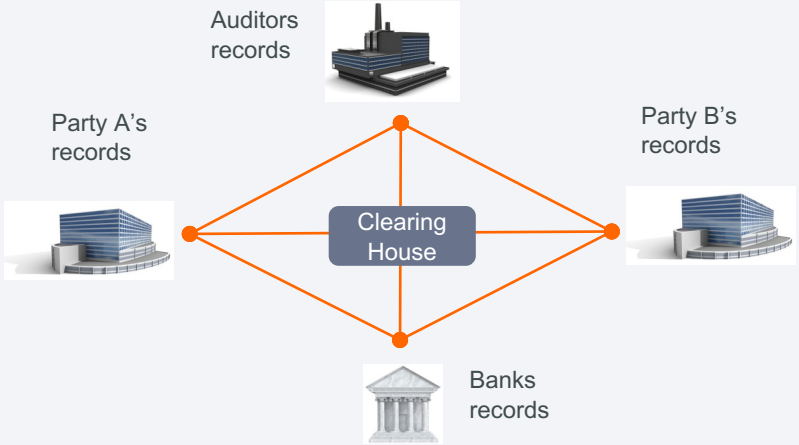
Why do we need it?



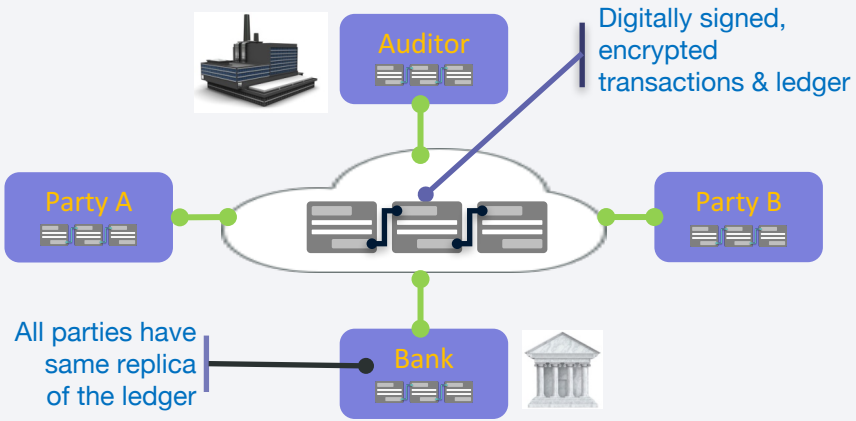
Gerhard Dinhof, gerhard.dinhof@at.ibm.com / gerhard.dinhof@iot-austria.at, @gdinhof
“Blockchainers Vienna” Meetup – sektor5, August 14th 2017

Blockchain will fundamentally change business processes

Traditional

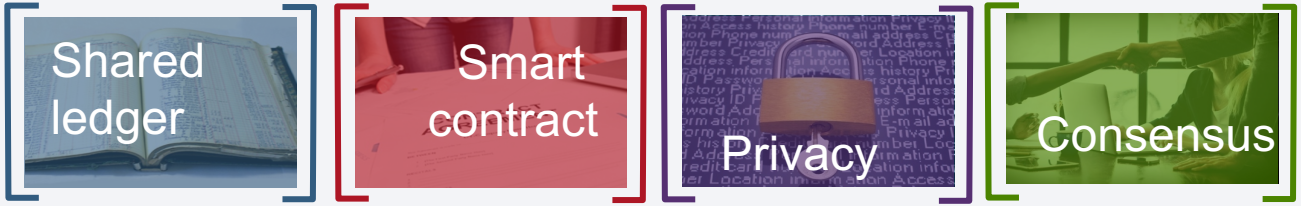


With Blockchain



…inefficient, expensive, vulnerable

…provenance, immutability, finality



The world is complex…

The Future of Transactions

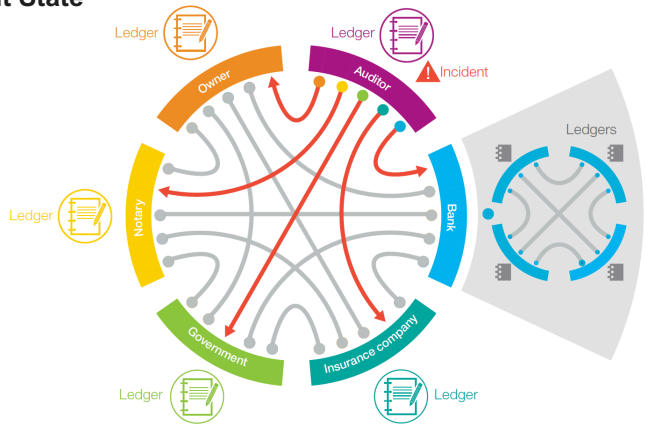
Current State:

- Transactions are recorded in multiple ledgers.
- They don't record what happens next, what came before, or the role of others – partners, suppliers, consumers – in the transaction.
- Prone to human error and vulnerable to tampering.

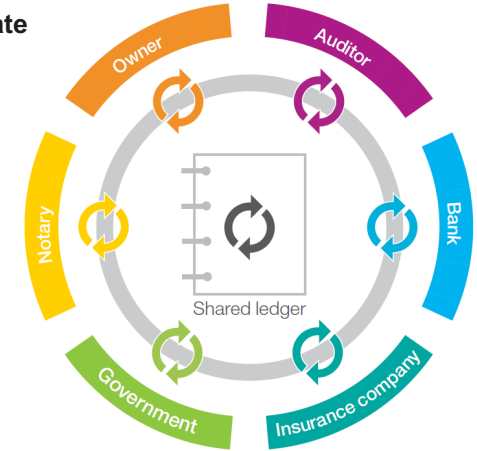
Future State:

- Distributed ledgers can be shared and updated in near real-time.
- Every transaction becomes part of the permanent record.
- Relevant information can be shared with others based on their roles and access privileges.

Current State



Future State



A Blockchain for business enables new business models

Saves time

Transaction time from days to near instantaneous

Removes cost

Overheads, paper-intensive processes and cost intermediaries

Reduces risk

Tampering, fraud & cyber crime caused by single-party system control

Increases trust

Through shared processes and recordkeeping via new digital economy built on blockchain applications

- **High Value Assets**
- **Intermediated Services**
- **Multi-Party Transactions or Flows**
- **Unique Trust Requirements**

Blockchain underpins Bitcoin…

bitcoin is:

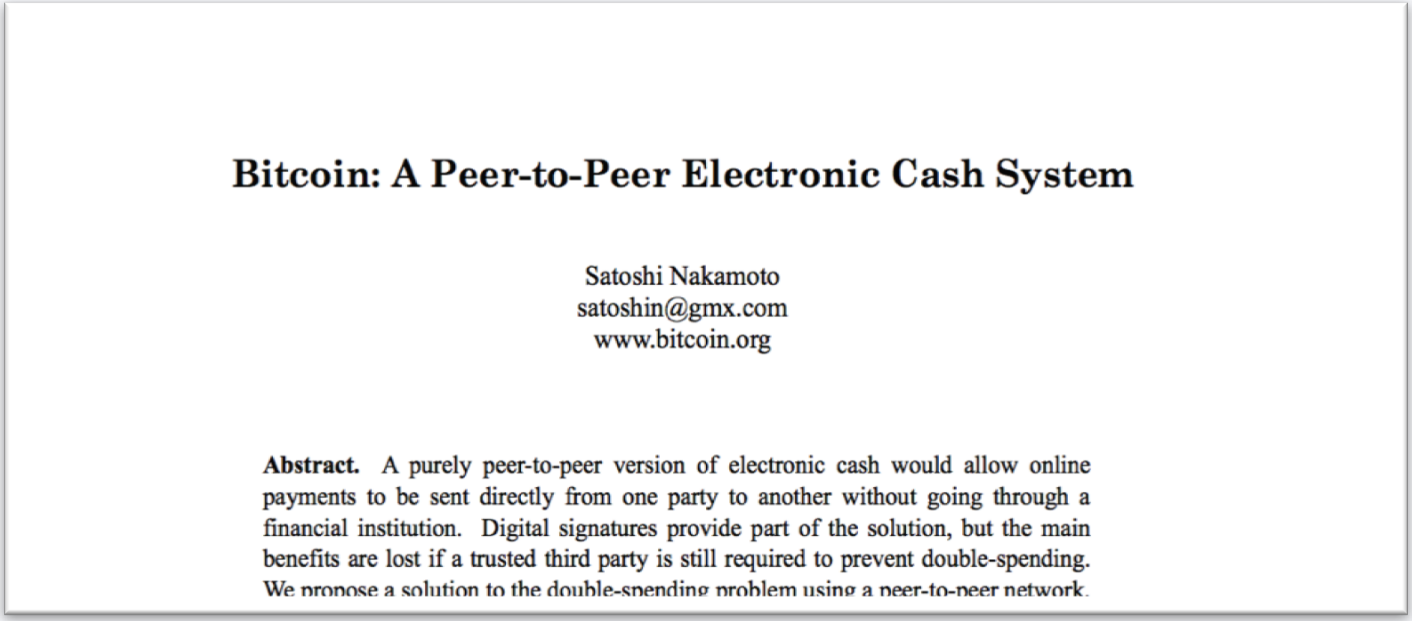
- An unregulated shadow-currency
- The first blockchain application
- Resource intensive

Blockchain for business differs in key areas:

- *Identity* over anonymity
- *Selective endorsement* over proof of work
- *Assets* over cryptocurrency

10

How it all began…



Bitcoin: A Peer-to-Peer Electronic Cash System

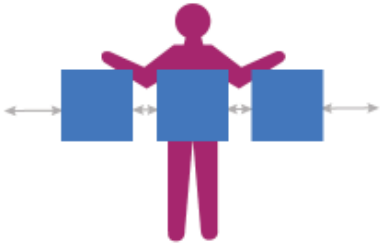
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

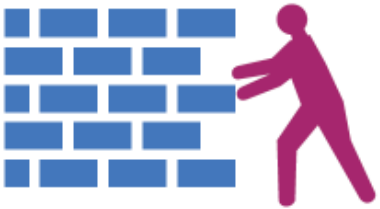
Building a blockchain.

As each transaction occurs, it's put into a block.

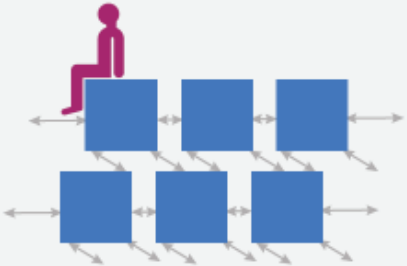
Each block is connected to the one before and after it.



Transactions are blocked together.



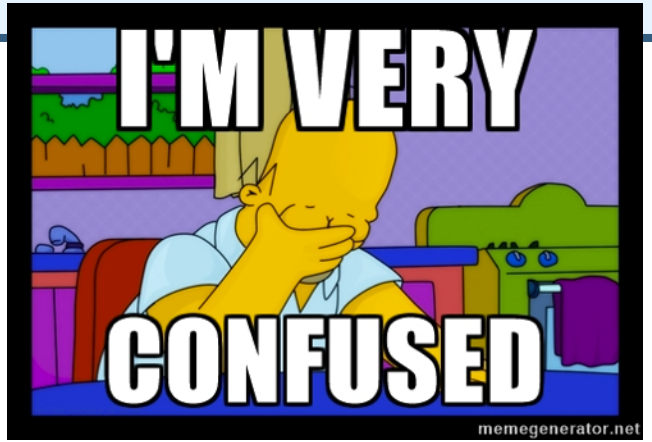
Each block is added to the next in an irreversible chain.



Source: https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XI912346USEN

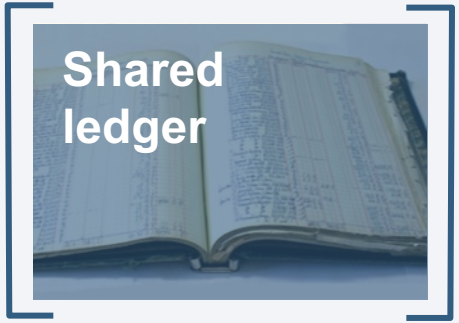
But wait…

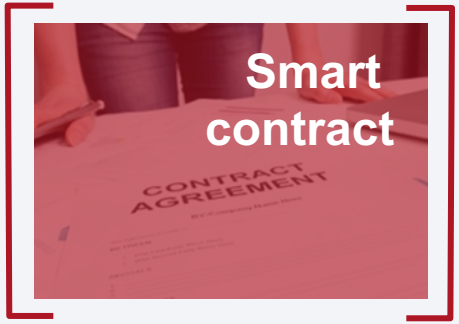
BTC, ETH, XRP, BCH, IOTA, LTC, NEO, NEM, DASH, Hyperledger... (fill in 200+ DTLs)



Requirements of blockchain for business

Append-only distributed system of record shared across business network



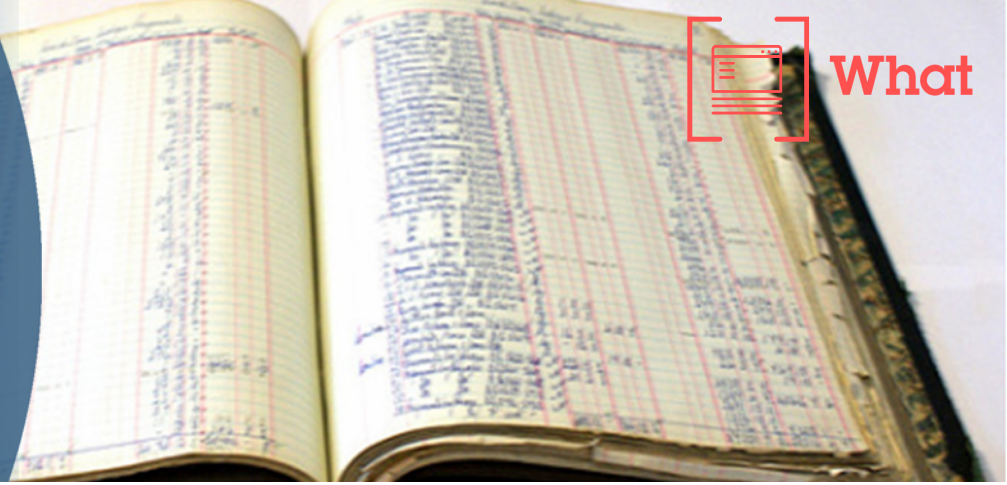


Business terms embedded in transaction database & executed with transactions

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

Transactions are endorsed by relevant participants

Shared ledger



What

Records all transactions across business network

- Shared between participants
- Participants have own copy through replication
- Permissioned, so participants see only appropriate transactions
- THE shared system of record

Smart contract

What

Business rules implied by the contract … embedded in the Blockchain and executed with the transaction

- Verifiable, signed
- Encoded in programming language
- Example:
  - Defines contractual conditions under which corporate Bond transfer occurs

Privacy

What

The ledger is shared, but participants require privacy

- Participants need:
  - Appropriate confidentiality between subsets of participants
  - Identity not linked to a transaction
- Transactions need to be authenticated
- Cryptography central to these processes

Trust

What

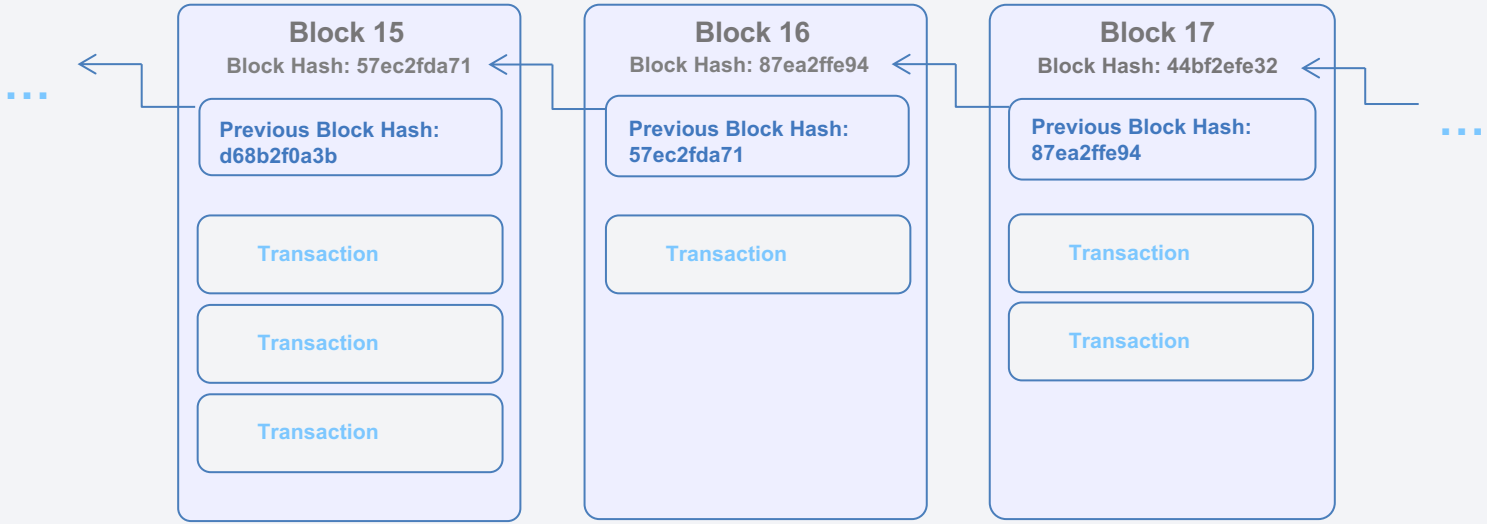
The ledger is a trusted source of information

- Participants **endorse** transactions
  - Business network decides who will endorse transactions
  - Endorsed transactions are added to the ledger with appropriate confidentiality
- Assets have a verifiable audit trail
  - Transactions cannot be modified, inserted or deleted
- Achieved through consensus, provenance, immutability and finality

Under the hood…

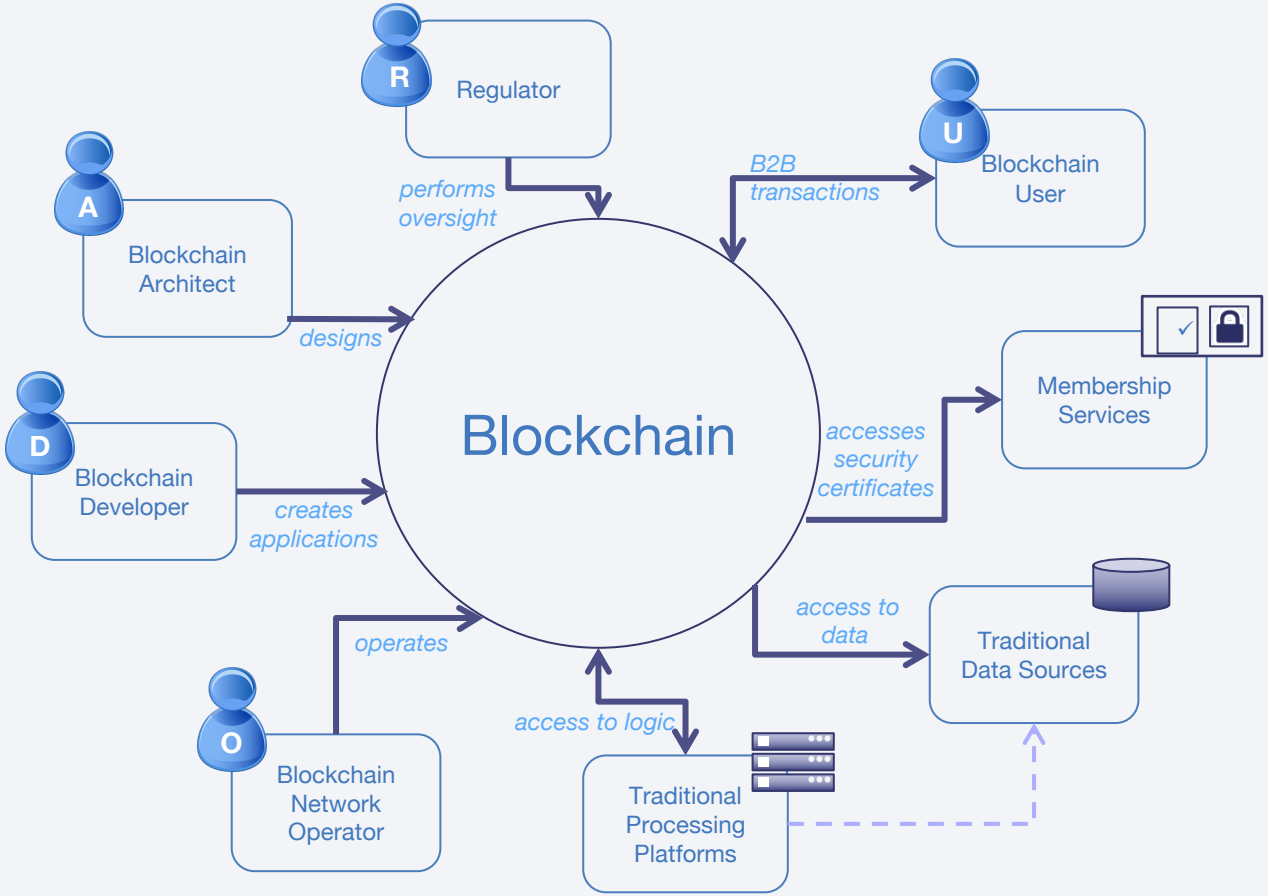
Gerhard Dinhof, gerhard.dinhof@at.ibm.com / gerhard.dinhof@iot-austria.at, @gdinhof
“Blockchainers Vienna” Meetup – sektor5, August 14th 2017

Block detail



- A blockchain is made up of a series of blocks with new blocks always added to the end
- Each block contains zero or more transactions and some additional metadata
- Blocks achieve immutability by including the result of a hash function of the previous block
- The first block is known as the “genesis” block

Actors in a blockchain solution



Some examples of consensus algorithms

Proof of work

Proof of stake

Solo

Kafka / Zookeeper

Proof of Elapsed Time

PBFT based

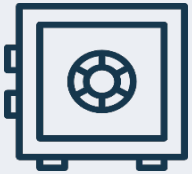
Recommended: "Blockchain Consensus Protocols in the Wild"

Use Cases

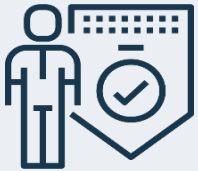
Gerhard Dinhof, gerhard.dinhof@at.ibm.com / gerhard.dinhof@iot-austria.at, @gdinhof
“Blockchainers Vienna” Meetup – sektor5, August 14th 2017

Everledger traces and tracks the supply of diamonds from mine to market

everledger is a permanent digital global ledger…



…that protects items of value…



…providing insurance companies, owners, claimants…

… with an immutable history of item's authenticity, existence and ownership.

Maersk 1/2

The paper trail of a shipping container

How blockchain will help manage and track the paper trail of tens of millions of shipping containers across the world

The ocean freight industry accounts for **90%** **of goods in global trade.**

But transport remains highly dependent on a flood of paper that is never digitized.

Shipping flowers overseas: the journey from grower to retailer is complex

The value of the global flower trade industry is nearly **USD 105 billion.**[1]

700,000 **metric tons** of cut flowers are shipped each year.[2]

Shipping information must pass through many hands, increasing potential for delays in transport.

One shipment can require sign-off from **30 unique organizations** and up to **200 communications.**

One **lost form or late approval** could leave the container stuck in port.

The entire process can take more than one month.

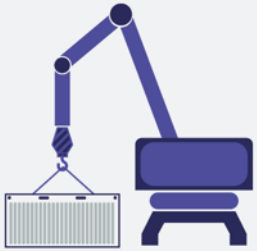
Maersk 2/2

Imagine if the same process were digitized and using blockchain technology

Blockchain—a shared, distributed ledger—can trace the container's path through the supply chain with exceptional transparency and security.

The flower grower readies the product for international shipment. Shipment information is added to the blockchain.

As the container awaits transfer to port, officials submit approvals electronically. Blockchain confirms the transaction and executes a smart contract, releasing the shipment.



The container is loaded onto the ship.

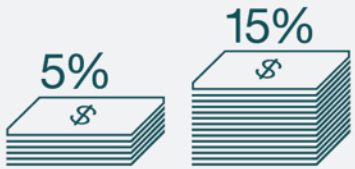
All parties have end-to-end visibility of the container's progress through the supply chain.

The container arrives at the destination port and clears customs.

Retailer receives the flowers on time and signs electronically. Information is relayed back to the blockchain.

With blockchain, delays will be reduced, resulting in significant cost savings for all parties.

Blockchain helps enable unprecedented, secure transparency across the global supply chain.



This could increase worldwide GDP by almost **5%** and total trade volume by **15%.**[3]

Blockchain can help all parties involved in a shipment:

Reduce or eliminate fraud and errors

Improve inventory management

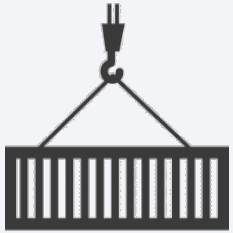
Minimize courier costs

Reduce delays from paperwork

Reduce waste

Identify issues faster

Maersk: Complex Global Distribution



Banks	Importers and Exporters	Carriers	Forwarders	Ports	Authorities
Manual, paper-based processes Lack of Real-Time information	Excess Inventory Manual, paper-based processes Duplication of Administrative Process	No single version of "the Truth" Manual, paper-based processes	Manual Data Collection Manual, paper-based processes	Collection and Delivery Black Holes Sub-optimal stack placement Manual Data Collection	False Positives Lack of visibility pre-manifest Lack of visibility into land movement before/after ocean transport

Root Causes:

Multiple data formats *Point-to-point interactions* *Absence of messaging standards*

Food Traceability in China

What?

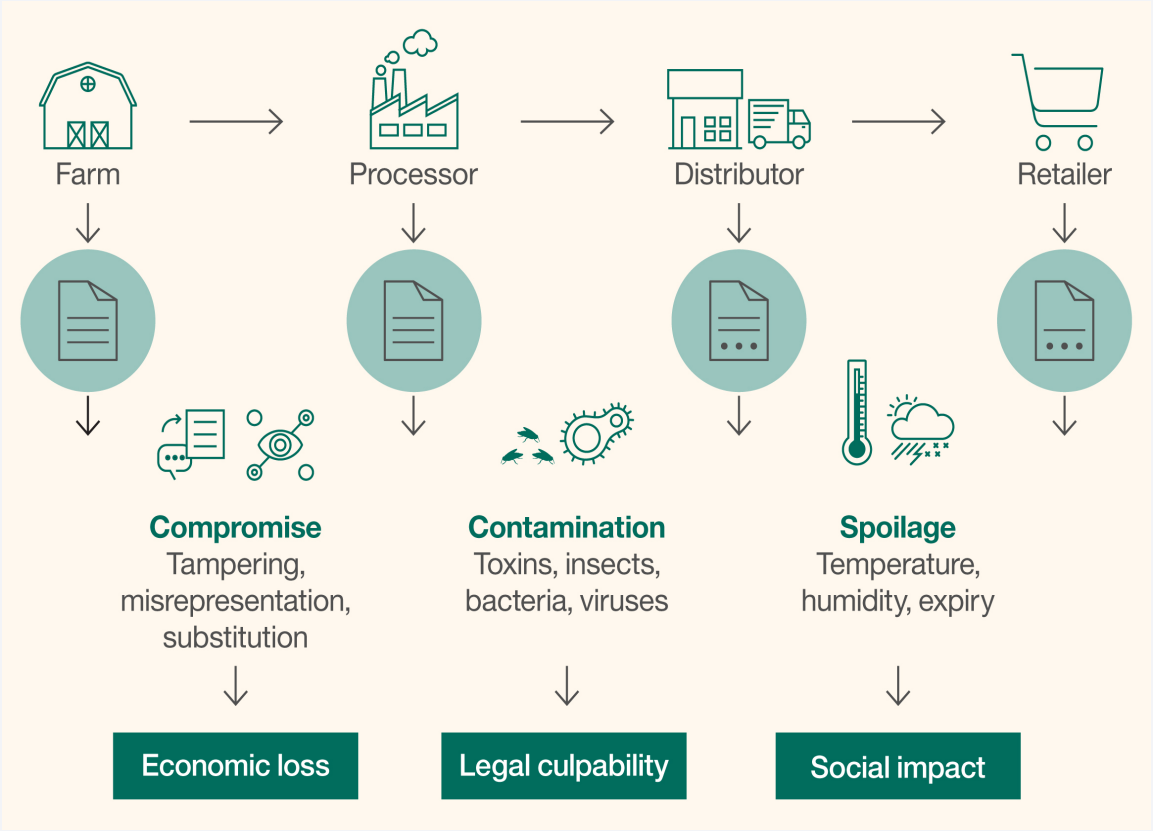
- Traceability of food from “farm to fork”

How?

- Blockchain holds history of food items processed through entire supply chain

Benefits

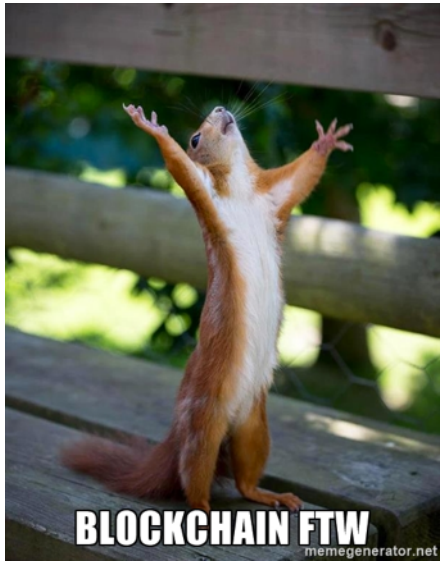
1. Increased trust – multiplied by each participant in food supply chain
2. Pinpoint source of compromised food, reducing the unnecessarily broad recall
3. Improved co-ordination in food supply chain



Summary

Blockchain …

- is a shared, replicated, permissioned ledger technology
- can open up business networks by taking out cost, improving efficiencies and increase accessibility
- addresses an exciting and topical set of business challenges, which cross every industry



Learn, discuss & build!

Gerhard Dinhof, gerhard.dinhof@at.ibm.com / gerhard.dinhof@iot-austria.at, @gdinhof
“Blockchainers Vienna” Meetup – sektor5, August 14th 2017

Reach out to me for questions or discussing / sharing your ideas – I love to hear them and support!

Gerhard Dinhof
IBM / Technikum Wien / Hyperledger Vienna Meetup Co-Founder / IoT Austria Mentor

Web: https://dinhof.com
Mail: gerhard.dinhof@at.ibm.com / gerhard.dinhof@iot-austria.at / gerhard@dinhof.eu
Twitter: @gdinhof

Interesting Projects to follow

Industry Use Cases: https://www.hyperledger.org/industries

IBM Blockchain Use Cases: https://www.ibm.com/blockchain/

Hyperledger Industries: http://hyperledger.org/industries

Everledger: https://www.everledger.io

Ujo: https://ujomusic.com

DECENT: https://decent.ch

Follow My Vote: https://followmyvote.com/

IPFS / Keybase: https://keybase.io

Recommended wallets:

- https://jaxx.io
- https://electrum.org
- https://trezor.io / https://www.ledgerwallet.com/

Handpicked Resources

Blockchain General:

Blockchain for Dummies: https://public.dhe.ibm.com/common/ssi/ecm/xi/en/xim12354usen/XIM12354USEN.PDF

WeUseCoins: https://www.weusecoins.com

Mastering Bitcoin: https://github.com/bitcoinbook/bitcoinbook

Julian Hosp: https://www.julianhosp.com

Development:

IBM Blockchain for Developers Course: https://developer.ibm.com/courses/all-courses/blockchain-for-developers/

Fabric Docs: https://hyperledger-fabric.readthedocs.io/en/latest/

Hyperledger Composer: https://github.com/hyperledger/composer

Handpicked Resources

Advanced:

Hyperledger Architecture: http://hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

Ethereum Mining Algorithm:
- proof-of-work: https://github.com/ethereum/wiki/wiki/Ethash
- proof-of-stake: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

Bitcoin hashing Algorithm (proof-of-work): https://en.bitcoin.it/wiki/Block_hashing_algorithm

Blockchain Consensus Protocols in the Wild: https://arxiv.org/abs/1707.01873