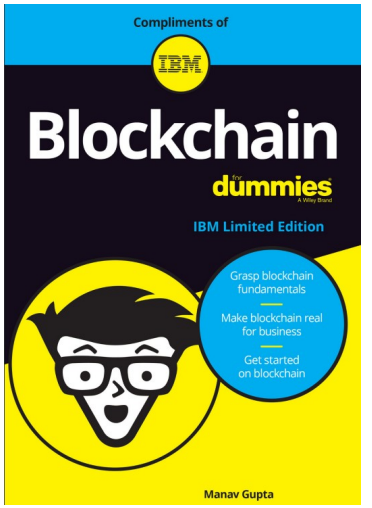
Blockchain – Beyond the Cryptocurrency Slot Machine

Paul Newton

Agenda

- Control of Business Truth using Computer Science Artifacts
- Blockchain Fundamentals & Terminology
- Permissionless vs. Permissioned
- Performance & Reality
- Use Cases
- Blockchain Jobs



Truth

- Who and What Controls the Truth
- How is the Truth Controlled

An accepted single source of **truth** has **risk** associated with keepers of the single source

Today's **business data** and **agreements** are subject to **Regulation, Compliance, Risk, Fraud, Legal Action** to help maintain truth

Control of Business Truth using Computer Science Artifacts

- Byzantine Fault Tolerance (BFT)
- Merkle (hash) Tree, etc.

Blockchain are **immutable** records for archives using classic computer science algorithms.

Crypto-currency Blockchains are **'Permissionless'**
Participant identities are anonymous
Transactions are public knowledge
Consesus/Agreement by “Proof of Work”, “mining”.

Industry Blockchains are **“Permissioned”**
Participant identities are known
Transactions are private between authorized participants
Industrial Encryption/Selective Endorsement

Block is a collection of transactions with complex hash

Transaction has a **size**

Transaction has a **nonce**

- Part of the data that is hashed while finding the block hash

Block (package of transactions) has a header with a **nonce**

- Limit on number of transactions in a block based on total size
- Block hash includes hash of all the transactions in the block
- Block hash (aka solution)

Block header fields:

- https://en.bitcoin.it/wiki/Block_hashing_algorithm

Blockchain Fundamentals & Terminology

Smart Contract – agreed upon defined rules and penalties

Transaction – message sent from one account to another

Packages – collection of transactions (aka 'blocks')

Blockchain – packages linked in specific order

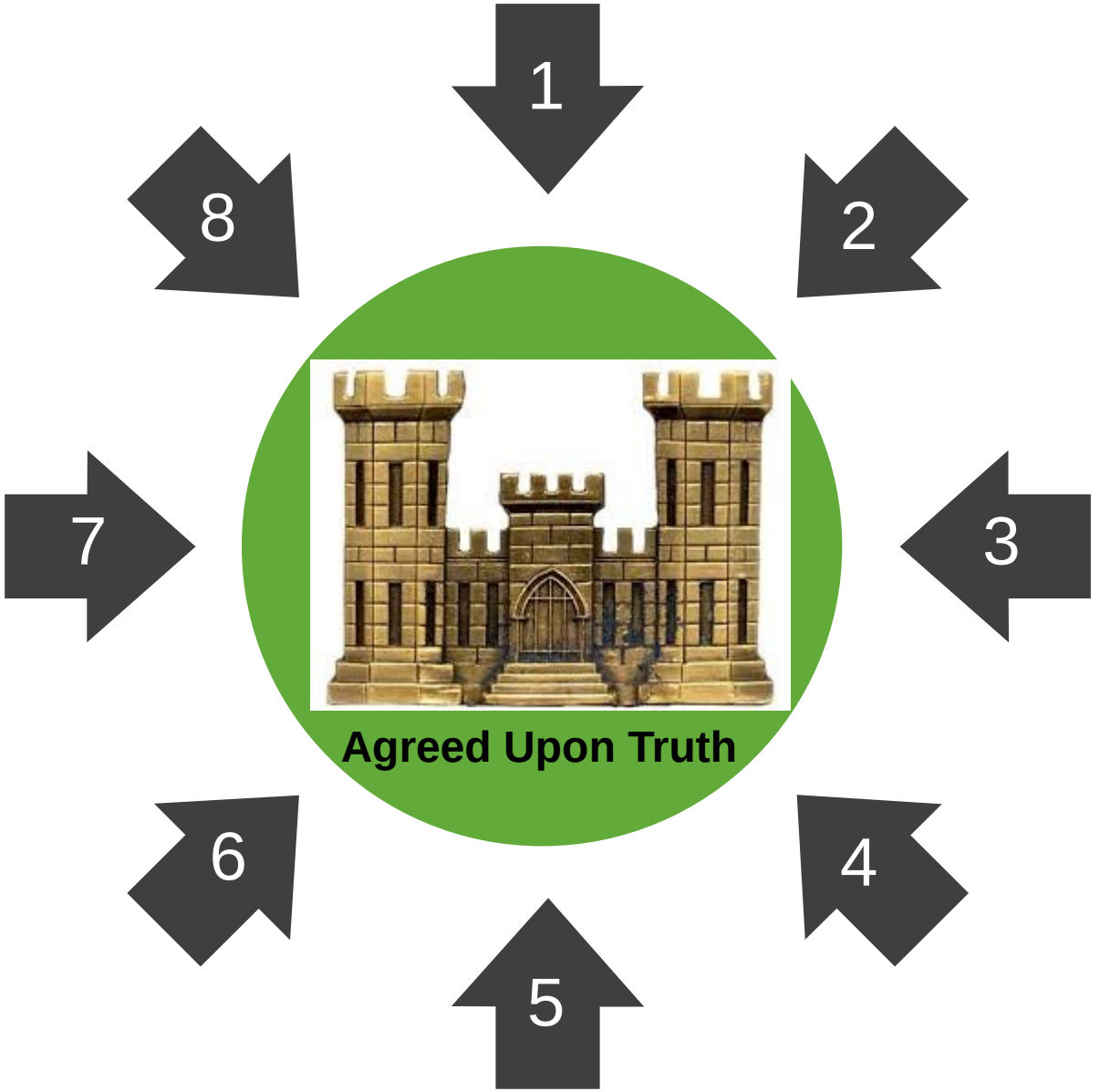
Wallet – transaction request

1) Transaction broadcast
2) Transaction validation
3) Validated transactions stored into a 'block' and sealed with lock
4) **Others** validate lock on the block is correct
6) Accepted into blockchain

Permissionless

Cryptocurrency Blockchains are Permissionless

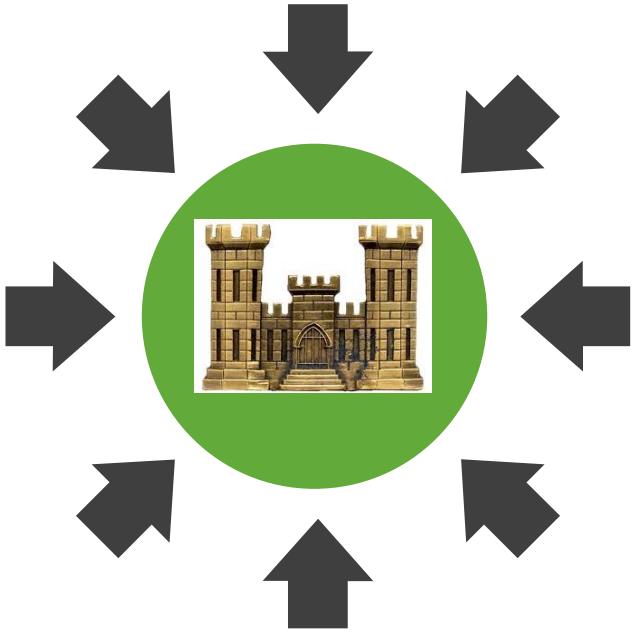
Consensus Algorithm – Proof of Work



Byzantine General's Problem

Crypto-currency Mining

General public participation in collective agreement (consensus)

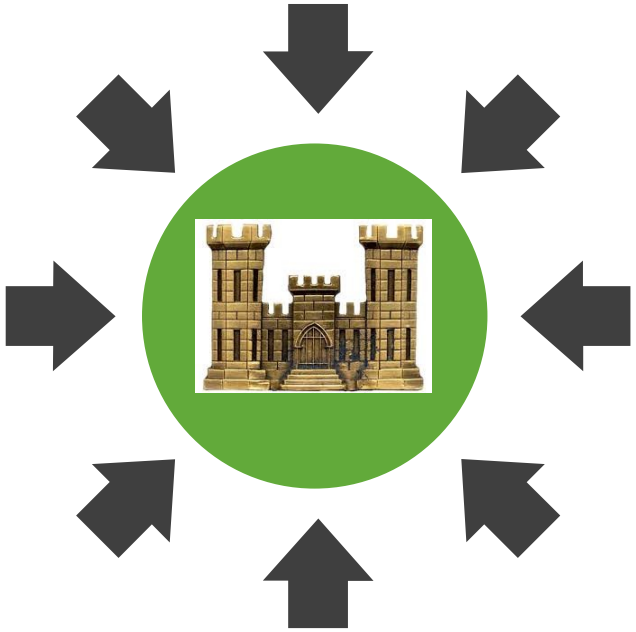


November 17, 2017

https://hackernoon.com

Cryptominers Earn $125,000 Every 10 Minutes

Crypto-currency mining



February 9, 2018

http://www.bbc.com/news/world-europe-43003740

Crypto-currencies like Bitcoin do not rely on centralised computer servers. People who provide computer processing power to the crypto-currency system, to enable transactions to take place, can get **rewards in Bitcoins**.

Russian security officers have arrested several **scientists** working at a top-secret Russian nuclear warhead facility for allegedly **mining crypto-currencies.**

The suspects had tried to use one of Russia's **most powerful supercomputers to mine Bitcoins**, media reports say.

The supercomputer was not supposed to be connected to the internet - to prevent intrusion - and once the scientists attempted to do so, the nuclear centre's security department was alerted.

Permissioned

Industrial Blockchains are Permissioned

Industry Blockchain Fundamentals

Transferring assets is the heart of blockchain

People, Process, and Paper transformation to blockchain Participants, Transactions, and Assets

Blockchain for crypto currency is very different from the underlying blockchain used for industry

Transformation	**Industry**	**Bitcoin,etc.**
People/Participants	Identity	Anonymity
Process/Transactions	Selective Endorsement	Proof of Work
Paper/Assets	Any Asset	Crypto-currency

What is the same is the trusted shared ledger of immutable records

Core requirements of business blockchain

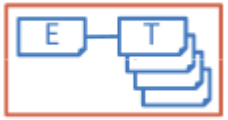
- Shared ledger
- Smart contract
- Privacy services
- Trust

- Consensus
- Provenance
- Immutability
- Finality

Blockchain attributes that engender trust

Reduce the cost of doing business while improving **Trust** and **Transparency**

Blockchain Components

Ledger		contains the current world state of the ledger and a Blockchain of transaction invocations
Smart Contract		encapsulates business network transactions in code. transaction invocations result in gets and sets of ledger state
Consensus Network		a collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger
Membership		manages identity and transaction certificates, as well as other aspects of permissioned access
Events		creates notifications of significant operations on the Blockchain (e.g. a new block), as well as notifications related to smart contracts. Does not include event distribution.
Systems Management		provides the ability to create, change and monitor Blockchain components
Wallet		securely manages a user's security credentials
Systems Integration		responsible for integrating Blockchain bi-directionally with external systems. Not part of Blockchain, but used with it.

Blockchain Performance & Reality

SOR transactional systems on IBM Z use transactional managers such as IMS*, CICS* and DB2*. Transactional managers process billions of transactions a day at millisecond speed with high volume, high throughput and high qualities of service

Blockchains today don’t provide millisecond response times, and a single blockchain network won’t support billions of transactions a day

A blockchain transaction will keep all parties on blockchain informed and will provide a record for all parties

Blockchain is good to optimize business processes that currently take days or weeks

Transaction manager API's are being built to interface with blockchain, then timestamps can be used to synchronize record truth

Infancy of Blockchain Performance

http://blog.deloitte.com.au/blockchain-performance-sucks-not-problem/

“However, Blockchain’s performance is determined by network performance, as it is the network that limits the number of transactions in a block (block size) and the time between blocks (dwell time).

Networks don’t obey Moore’s law nor will their throughput increase exponentially. Bitcoin has also reached its current performance limits at around 1/10,000th of VISA’s transaction volume.

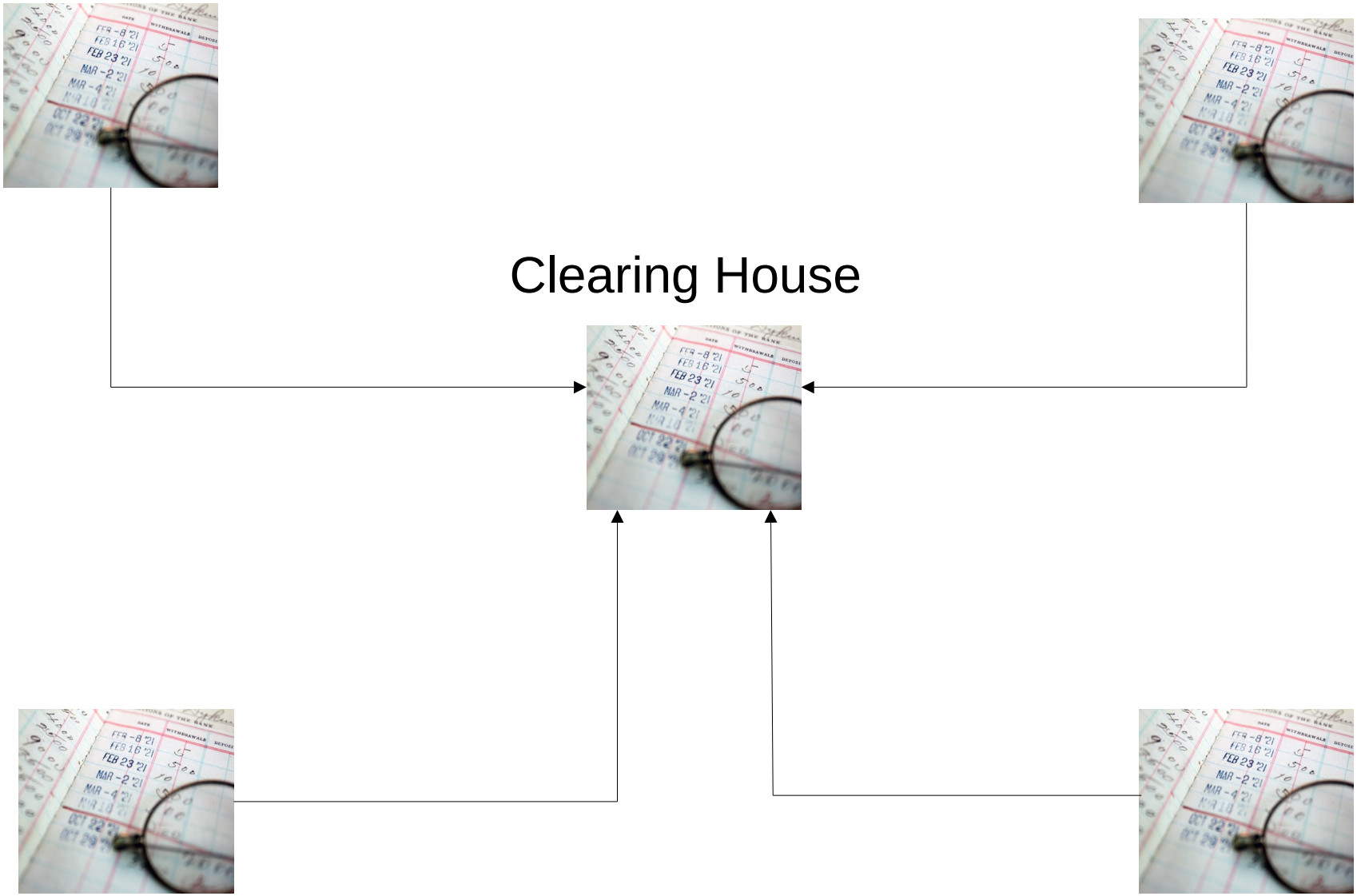
Reaching VISA’s current volume involves creating a gigabyte-sized block every minute, which is clearly unattainable.”

Blockchain Fundamentals

A **ledger** is the **permanent summary**
for **recording transactions**

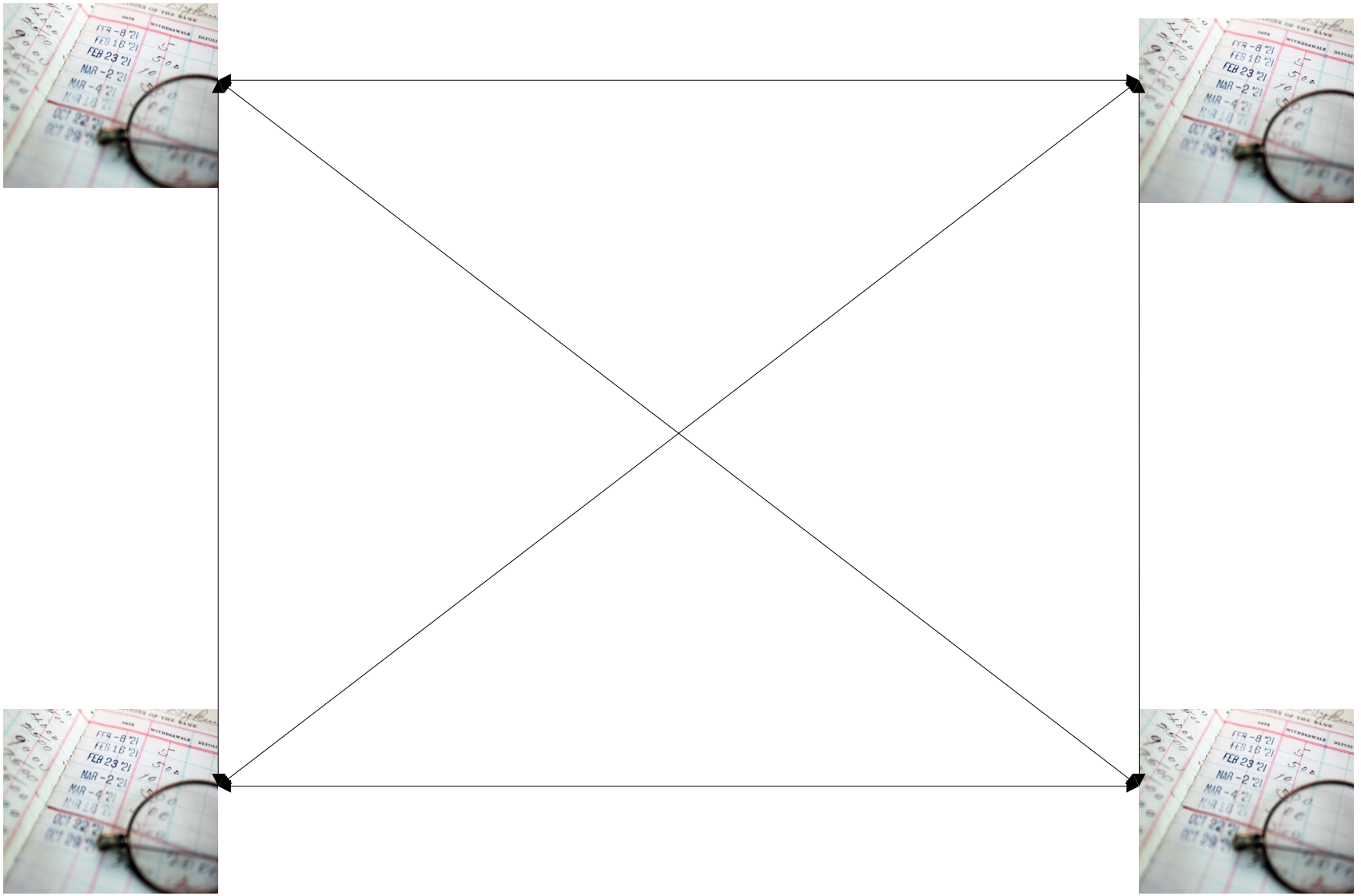
Blockchain Fundamentals

Doing Business Today

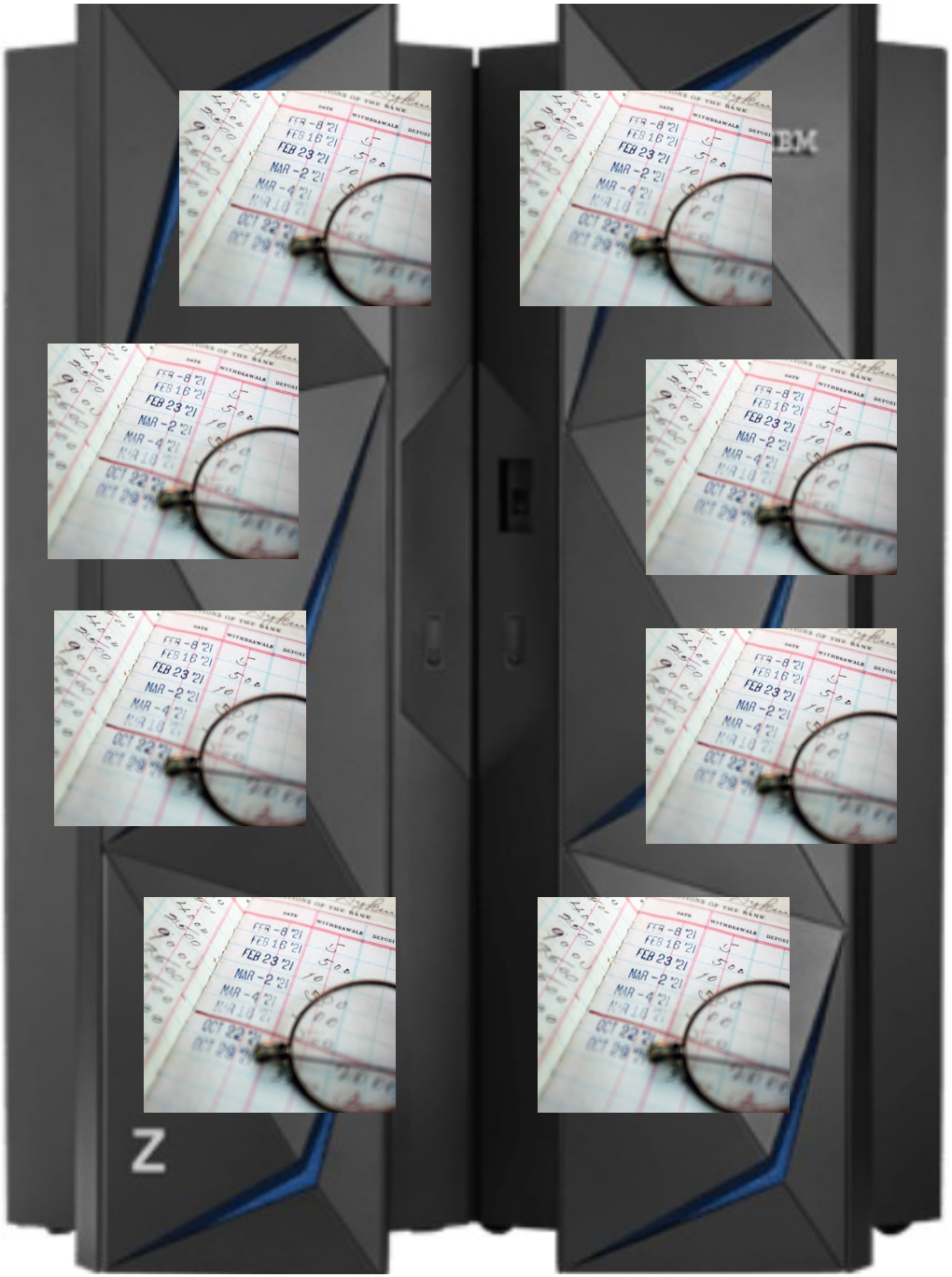


Blockchain Fundamentals

Future is Shared Ledgers



IBM Blockchain as a Service



Blockchain Performance & Platform Selection

IBM Z Family includes:

1) hardware accelerators for hashing
2) encryption and elliptic curve digital signatures used to sign blockchain transactions

Blockchain can be run in a VM next to an existing IBM Z business process, such as DB2, CICS, IMS and the Transaction Processing Facility.

IBM Z HiperSockets accelerated network communication provides 7x more throughput and 82 percent faster response time to speed communications.

A user can run multiple blockchain peers on IBM Z server as separate VMs, LPARs or Docker containers.

Blockchain Use Cases

Blockchain Beyond the Financial Institutions

Walmart

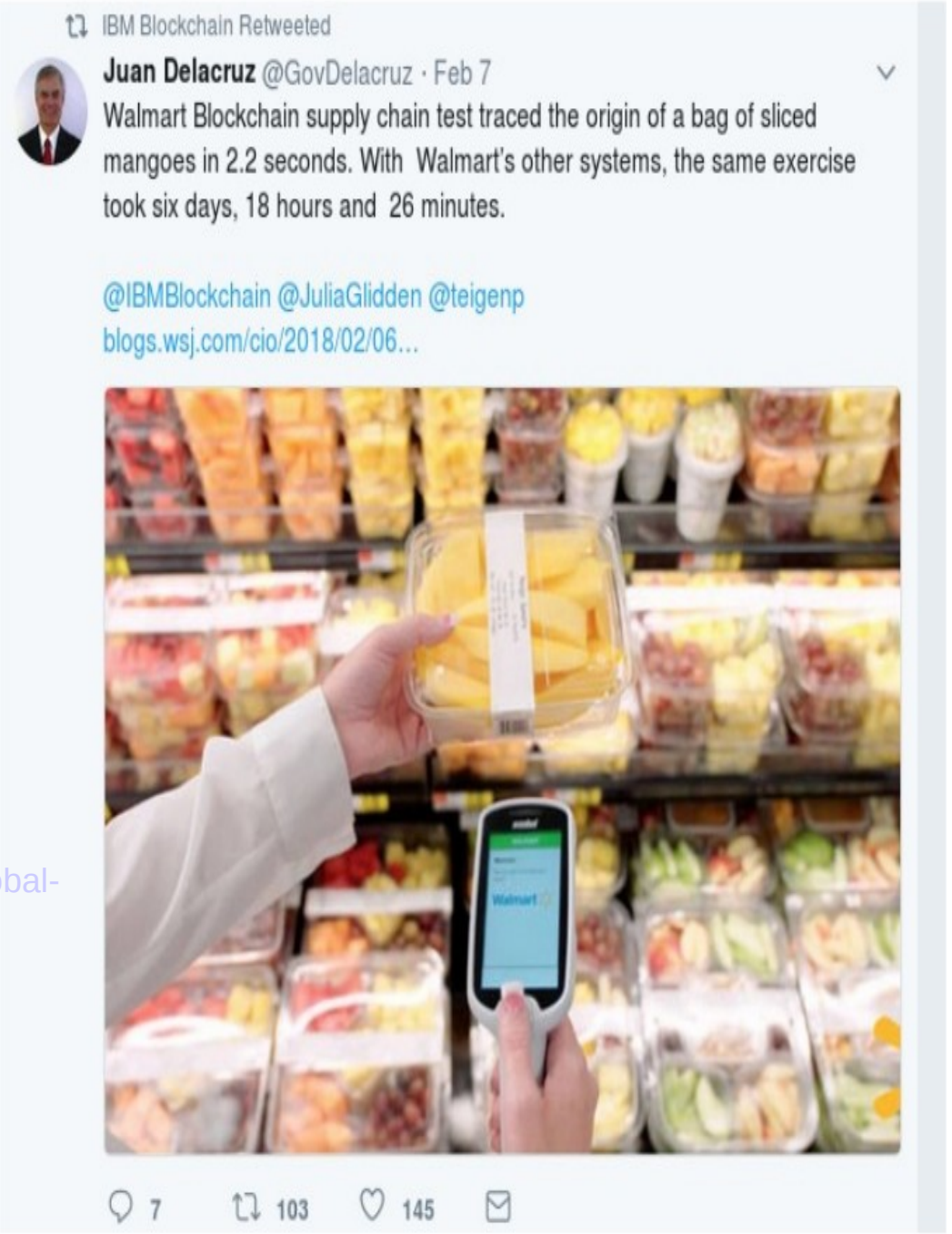
Wal-Mart started tracking two products using blockchain: a packaged produce item in the U.S., and pork in China. While only two items were included, the test involved thousands of packages shipped to multiple stores.

If Wal-Mart adopts the blockchain to track food worldwide, it could become of the largest deployments of the technology to date.

Fast Forward by approximately 1 year
Tweet from February 7, 2018
Observe the likes and retweets

Maersk – Digitizing Global Trade

https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/



7 Best Blockchain Careers & Jobs for the Future

Blockchain technologies and cryptocurrencies are on the upswing

1. Blockchain Intern
2. Blockchain Project Manager
3. Blockchain Developer
4. Blockchain Quality Engineer
5. Blockchain Legal Consultant or Attorney
6. Blockchain Designer
7. Blockchain Engineer

Building a blockchain for business with the Hyperledger Project

https://www.youtube.com/watch?v=EKa5Gh9whgU

Technical Details supporting the above video

https://github.com/hyperledger/fabric/blob/master/proposals/r1/Next-Consensus-Architecture-Proposal.md

Want to build a personal Hyperledger Environment?
How do I get started?
Forward 24:41 into following video

https://www.youtube.com/watch?v=kMktpqo0FH8

Supporting Detail

https://github.com/hyperledger/fabric/blob/master/docs/protocol-spec.md

https://github.com/hyperledger/fabric/blob/v0.6/docs/protocol-spec.md#fabric

https://github.com/hyperledger/fabric/blob/master/docs/Setup/Chaincode-setup.md