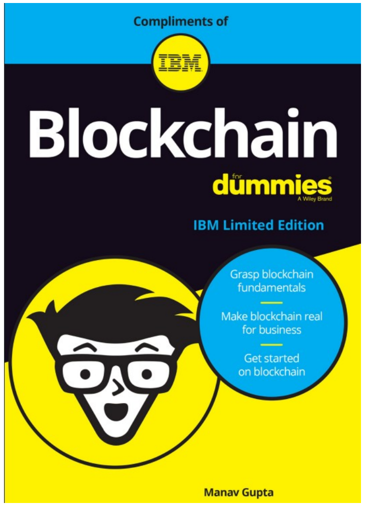
Blockchain – Beyond the Crypto-currency Slot Machine

Paul Newton
February 21, 2018

Agenda

- Control of Truth
- Control of Business Truth
- Business Truth use of Computer Science Artifacts
- Crypto-currency is a 'Permissionless' Blockchain
- Blockchain Fundamentals & Terminology
- Performance & Reality
- Blockchain and the Future


Compliments of
IBM
Blockchain
for dummies
A Wiley Brand
IBM Limited Edition
Grasp blockchain fundamentals
Make blockchain real for business
Get started on blockchain
Manav Gupta

Truth

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

In one classical formulation, truth is defined as the **good of logic**, where logic is treated as **a normative science**, that is, an inquiry into a good or a value that seeks knowledge of it and the means to achieve it

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

Computer Science Artifacts

- Byzantine Fault Tolerance (BFT)
- Merkle (hash) Tree

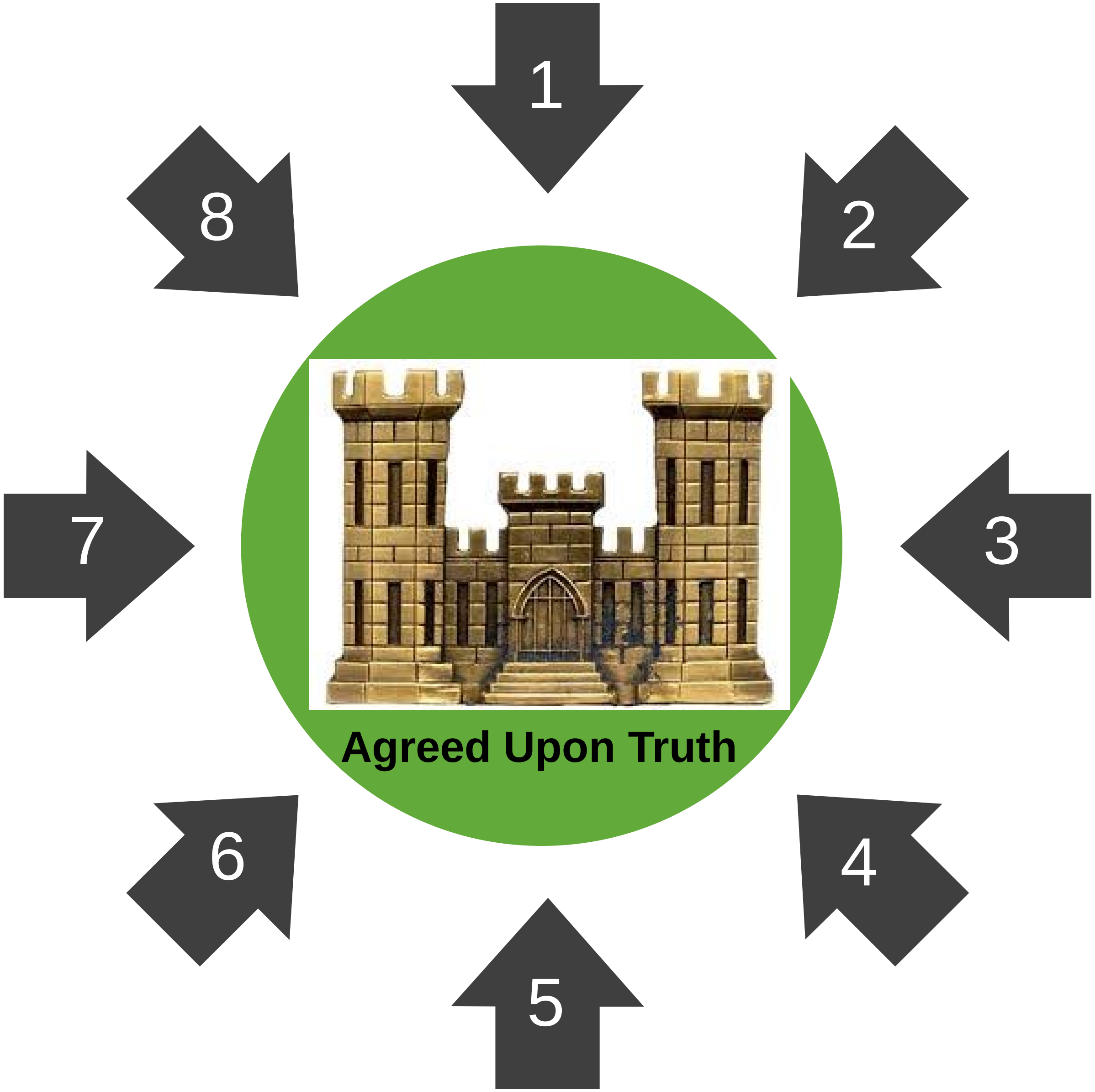
Blockchain offers an **immutable** record for archives using the above classic computer science artifacts

Crypto-currencies are **'Permissionless'** where the general public participates in collective agreement (consensus)

Truth & Data Management

- System of Record (SOR)
- Master Data Management (MDM)
- Source of Truth (SOT)
- Chart of Accounts (COA)

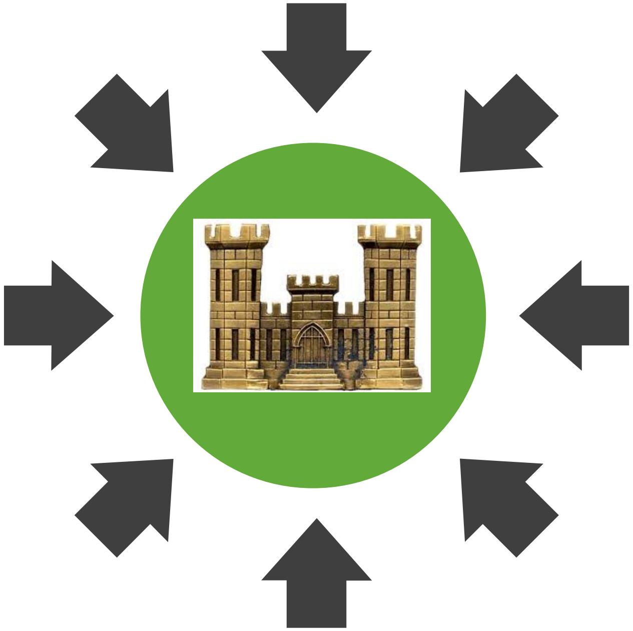
Consensus Algorithm – Proof of Work



Byzantine General's Problem

Crypto-currency Mining

General public participation in collective agreement (consensus)

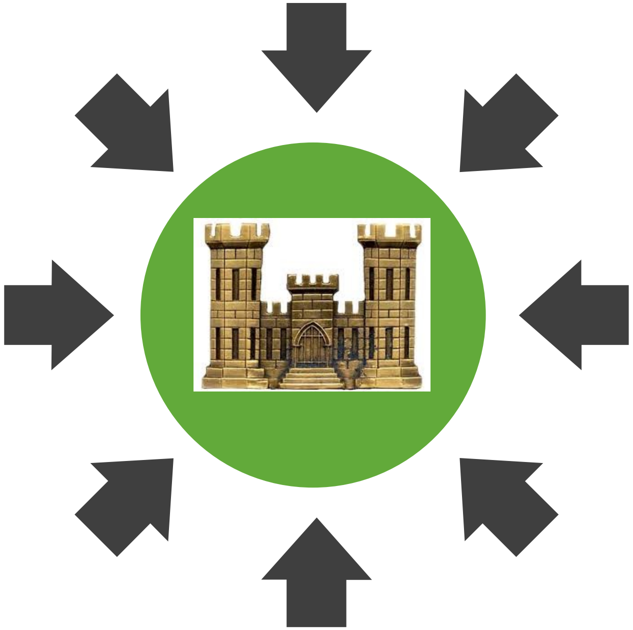


November 17, 2017

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.**

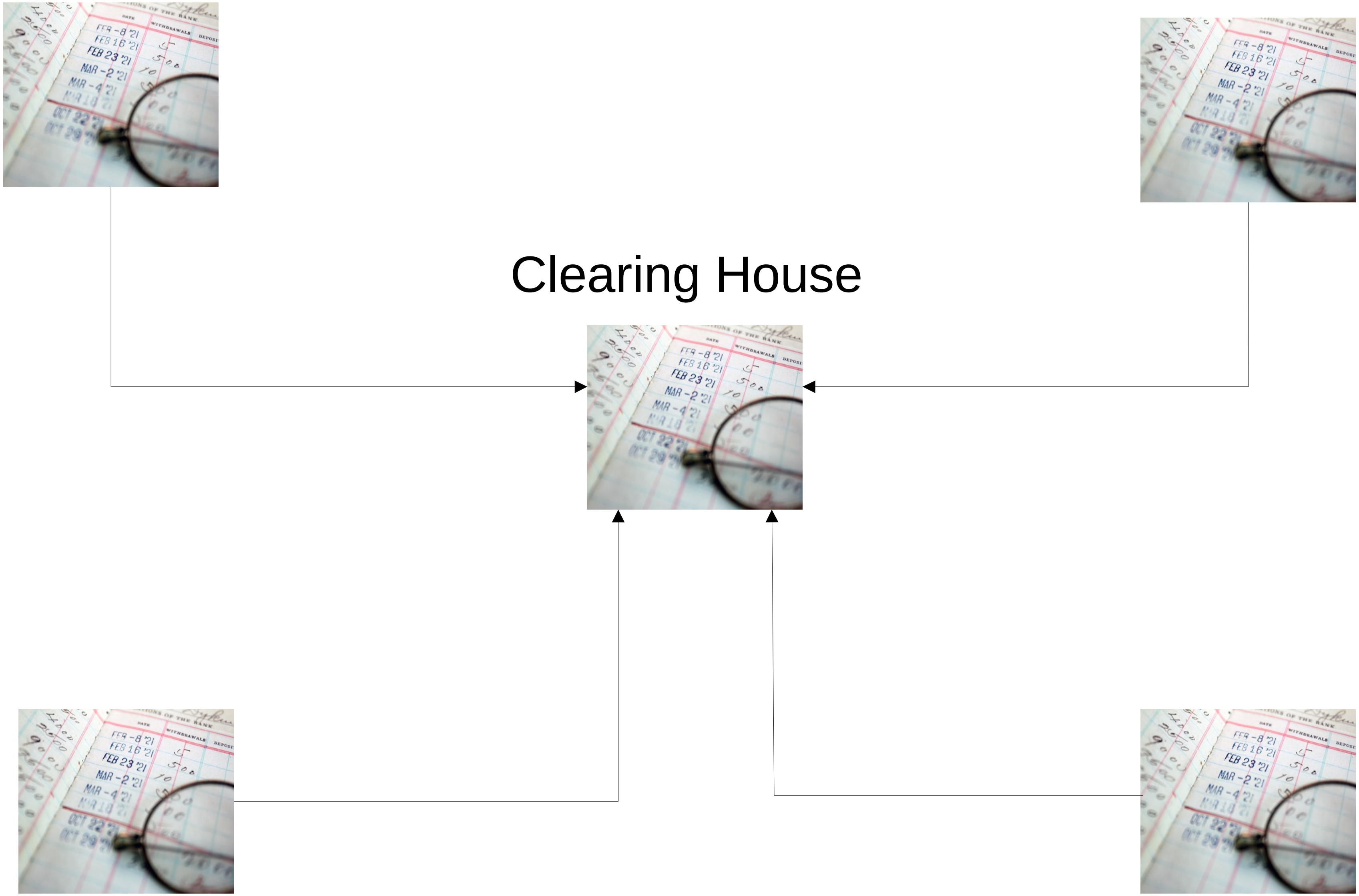
The suspects had tried to use one of Russia's **most powerful supercomputers to mine Bitcoins**, media reports say.

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.

Blockchain Fundamentals

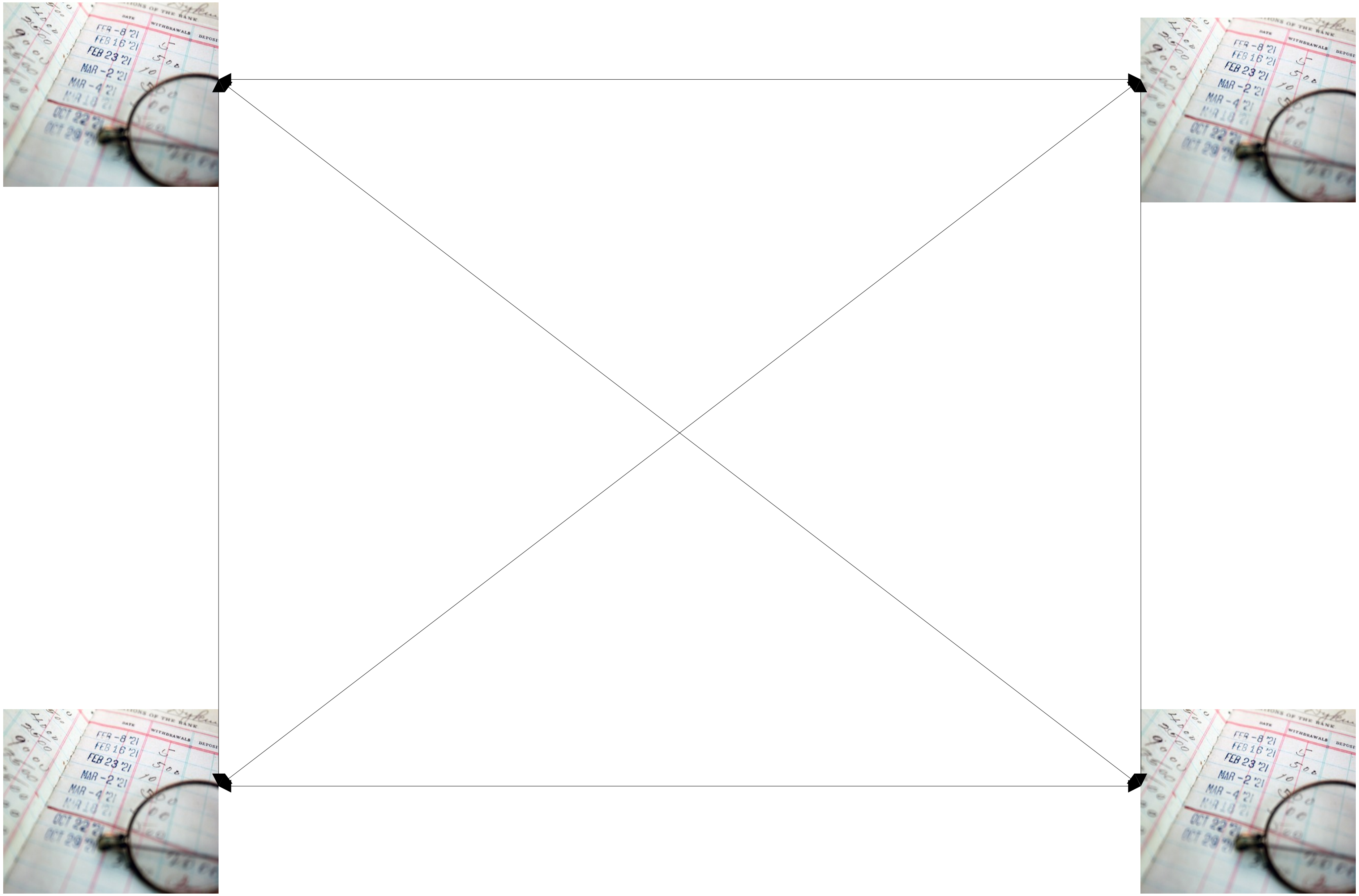
A **ledger** is the **permanent summary** for **recording transactions**

Doing Business Today



Clearing House

Future is Shared Ledgers



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

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)

Nonce has 2 meanings
1) Proof of work nonce - mining
2) Account nonce – transaction counter

Block header fields:
- https://en.bitcoin.it/wiki/Block_hashing_algorithm

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.”

Infancy of Blockchain Performance

https://wiki.hyperledger.org/groups/pswg/performance-and-scale-wg

“At this point in time the Hyperledger community feels it is inappropriate to discuss or disclose performance and scalability numbers for the Hyperledger projects.”

There are multiple reasons for this and the main concerns include no formal definitions of the various metrics and how to measure them, etc.

“PSWG is open to all and we encourage you to join our efforts to help ensure that we are proposing a fair and equitable manner to define the performance and scalability of the projects”

Blockchain Performance & Platform Selection

IBM Z Family includes:

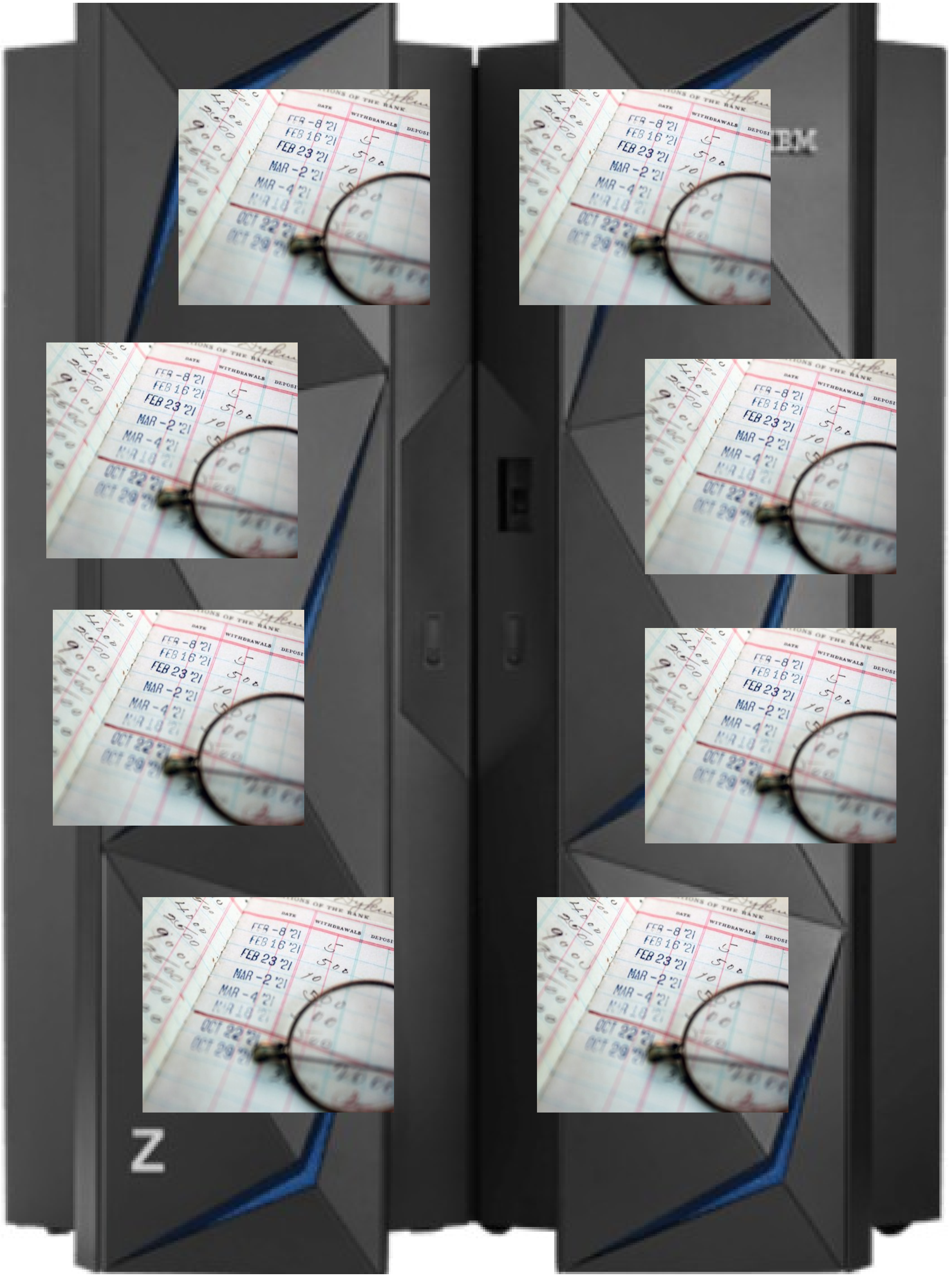
1) hardware accelerators for hashing
2) encryption and elliptic curve digital signatures used to sign blockchain transactions

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.

IBM Blockchain as a Service



Change is

- Hard at the beginning
- Messy in the middle
- Potentially gorgeous in the end

Anyone who claims to know exactly how this will play out as these systems grow and evolve is selling their own book rather than providing insight.

The real answer is that a variety of tools are being experimented with and built up as we speak, and it will come down to using the right tool for the job for a given use case. There is no silver bullet.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

SWIFT

DTCC
The Depository Trust &
Clearing Corporation

PayPal

AMERICAN EXPRESS

VISA

MasterCard

Yellen said that blockchain technology “could have very significant implications for the payments system” and that the Fed wants “to foster innovation”.

December 2016

“DTCC is excited about the potential of blockchain and distributed ledger technology to modernize the post-trade ecosystem,” Palatnick said. “The key to fully leveraging the technology lies in fostering greater collaboration across the industry and with supervisors globally. We believe there are many ‘white spaces’ where distributed ledgers can help increase processing efficiencies and reduce risks and costs.

April 2016

Swift CEO Gottfried Leibbrandt told an audience of 8,000 people at Sibos that his company was looking at blockchain as a way to further enhance the GPI.

September 2016

PayPal believes that blockchains, while holding interesting potential, particularly in the world of finance, are still in their early days. We have not yet seen use cases in the financial space that are highly differentiated and particularly compelling, but we remain engaged with the broader ecosystem and are interested in how blockchain may result in demonstrable benefits for financial services.

Visa has announced new details about a forthcoming business-to-business payments service developed in partnership with blockchain startup Chain.

"We believe that there is a role of blockchain in the future of commerce. This future needs to be developed in partnership with banks, merchants and industry participants,"

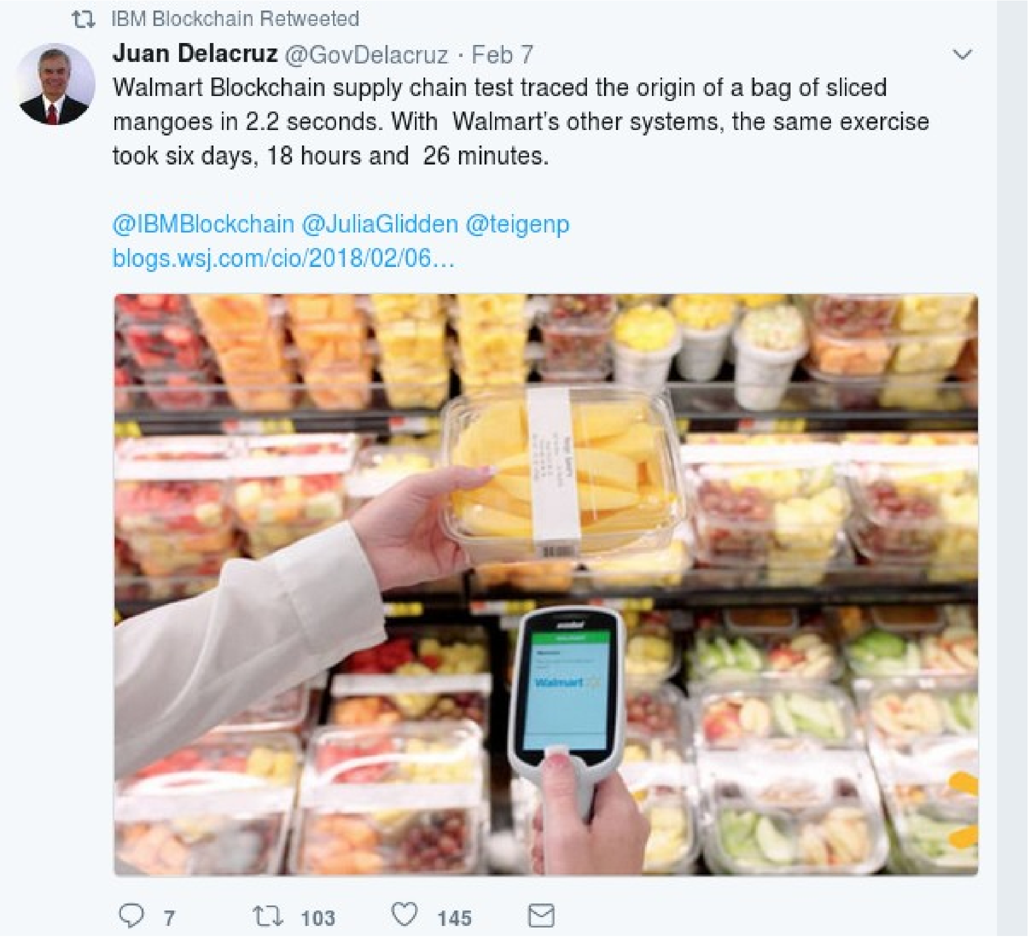
"As we watch the digital currency industry develop, we have seen that blockchain technology and the distributed ledger can play an important role in shaping the future,”

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.



IBM Blockchain Retweeted

Juan Delacruz @GovDelacruz · Feb 7

Walmart Blockchain supply chain test traced the origin of a bag of sliced mangoes in 2.2 seconds. With Walmart's other systems, the same exercise took six days, 18 hours and 26 minutes.

@IBMBlockchain @JuliaGlidden @teigenp
blogs.wsj.com/cio/2018/02/06...

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.

It is easy to imagine a future where a permissioned blockchain with multi-factor authentication mechanisms (biometric+) would maintain records for:

- Government Institutions
    - Birth and Death Certificates
    - Education Credentials
    - Driver License
    - Passport
    - Taxes
    - Social Security, Disability, Unemployment
    - Medicare/Medicaid
    - Votes
    - Patents
- Health Care Providers and Insurance Carriers
    - Health Information, Statistics, etc.
- Telecommunications Industry
    - Digital Voice and Message History
- Transportation Industry
    - Personal Travel and Merchandise Distribution
- Financial Institutions
    - Savings, Loans, Deposits, Withdrawals, Securities, Trades

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