RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: PDAC-T08

BLOCKCHAIN IS THE NEW BLACK. WHAT ABOUT ENTERPRISE SECURITY?

MARTA PIEKARSKA

DIRECTOR OF ECOSYSTEM, HYPERLEDGER
THE LINUX FOUNDATION

DAVE HUSEBY

SECURITY MAVEN, HYPERLEDGER
THE LINUX FOUNDATION

RSAConference2018

#RSAC

ORANGE IS THE NEW BLACK

SETTING THE STAGE FOR BLOCKCHAIN DISCUSSION

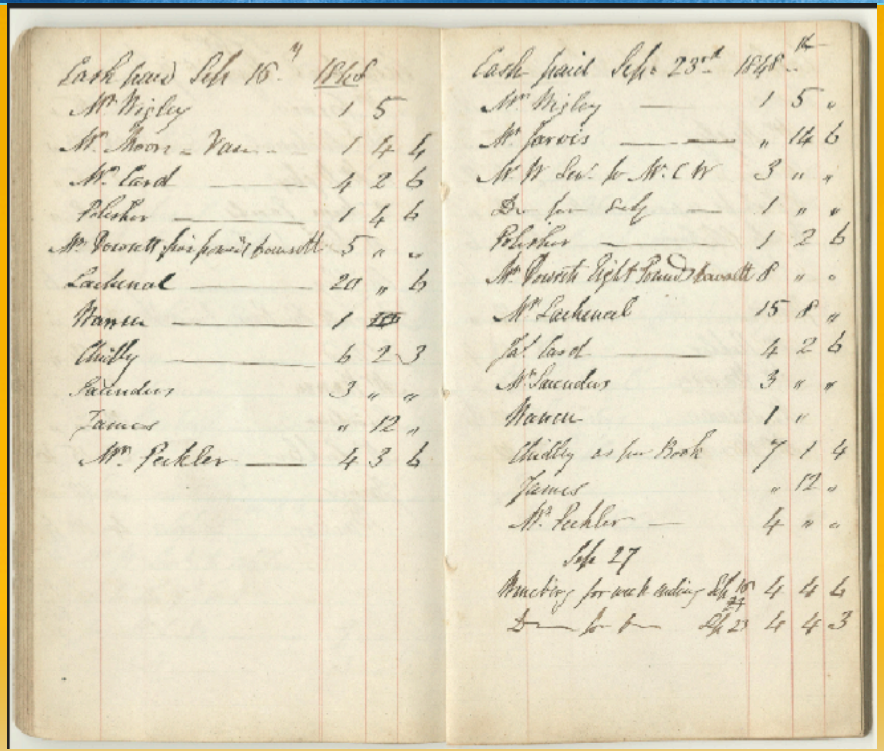
It’s all about money, money, money

THE FIRST LONG-DISTANCE TRADE OCCURRED BETWEEN MESOPOTAMIA AND INDUS VALLEY IN PAKISTAN ~3000 B.C

How do you agree on assets balance?

HOW TO TRACK THE VALUE OF EXCHANGED GOODS?

Traditional ledgers



Cash paid Sept 16th 1848

Mr Wigley	1	5	
Mr Moor - Van	1	4	4
Mr Card	4	2	6
Fletcher	1	4	6
Mr Prowett for paid Bonnett	5	"	"
Lackenal	20	"	6
Warren	1	[illegible]	
Chubby	6	2	3
Saunders	3	"	"
James	"	12	"
Mr Peckler	4	3	6

Cash paid Sept 23rd 1848

Mr Wigley	1	5	"
Mr Jarvis	"	14	6
Mr H Sen for Mr CW	3	"	"
Do for Lady	1	"	"
Fletcher	1	2	6
Mr Prowett Eight Pound Bonnett	8	"	"
Mr Lackenal	15	8	"
Jas Card	4	2	6
Mr Saunders	3	"	"
Warren	1	"	
Chubby as for Book	7	1	4
James	"	12	"
Mr Peckler	4	"	"
Sept 27			
Printing for week ending Sept 16	4	4	6
Do do do Sept 23	4	4	3

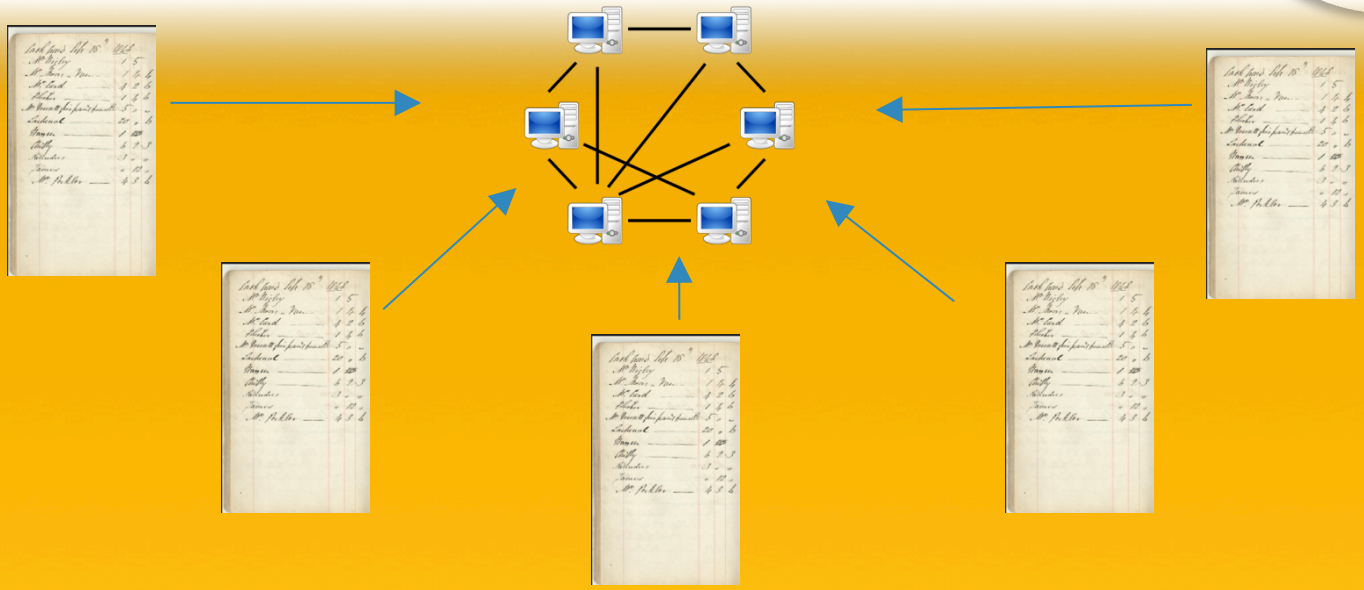
Digital World

IN THE DIGITAL WORLD THERE ARE MANY COPIES THAT MAY CONTAIN DIFFERENT VERSIONS

THE CHALLENGE: WHICH DO YOU TRUST AS A SINGLE SOURCE OF TRUTH?

Internet Connected Reality

Potential of Peer to Peer Network



NOW WE CAN KEEP OUR LEDGERS IN SYNC

(PROVIDED WE CAN AGREE)

GREEN FIELDS OF BLOCKCHAIN POTENTIAL

Facets of distributed, shared ledgers

Network nodes both **generate their own data** and **verify data** generated by others	Contain historic record of verified transactions and **easily auditable**	**Distributed Consensus** eliminates costly and inefficient reconciliation processes
No central repository – each node stores identical copies of the ledger	**Resilient** due to network power and cryptographic integrity	Large economic **disincentive for malicious** actors

Everyone wants their own DLT

BY 2025, 10% OF GLOBAL GDP WILL BE ASSETS TRACKED AND TRADED USING BLOCKCHAIN-BASED DISTRIBUTED LEDGERS

Report by WEF 2017

Google these words

Consensus:

PoW, PoS, POET, RaFT, BFT, PBFT

Crypto/Security:

PKI, HASH, SHA-256, zk-SNARK, HE, ECC, EXDSA, SGX

Ledger Concepts:

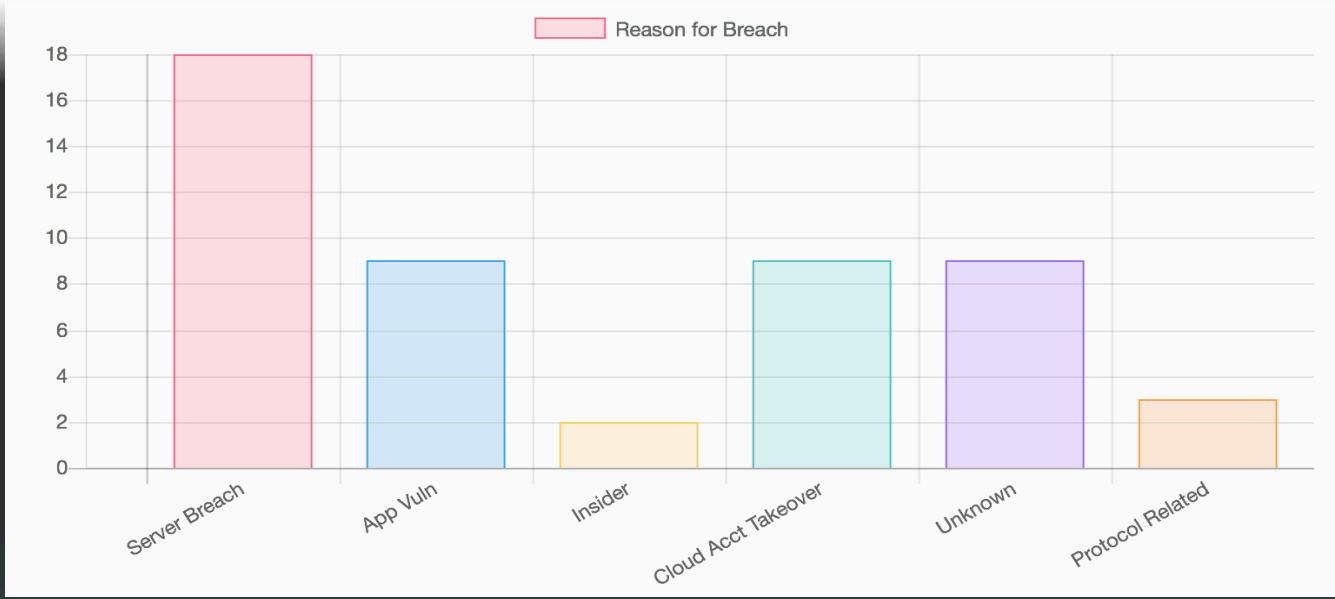
Mining, Blocks, Forks, Parents, Uncles, Merkle Trees

Platform Concepts

Nodes, Oracles, Notaries, Wallet, Smart Contracts

DARK WATERS OF SECURITY

Have you heard about Bitcoin Graveyard?



GRAVEYARD CONTAINS ANALYSIS OF 51 PUBLICLY AVAILABLE ATTACKS

Take a look at Coincheck Hack

Japan's Coincheck to regulators over cryptocurrency he

- Japanese cryptocurrency exchange Coinch million of digital money last month, is expe with regulators on the hacking.
- Coincheck said on Friday it would allow customers to restart yen withdrawals on Tuesday, saying it has confirmed the integrity of its system s
- Still, the exchange said it would keep restrictions on cryptocurr withdrawals until it could guarantee the secure resumption of it

Published 8:32 PM ET Mon, 12 Feb 2018

REUTERS

Coincheck users are suing to get their money off the hacked cryptocurrency exchange

Posted yesterday by Taylor Hatmaker (@tayhatmaker)

The timeline of events tells the story, but there's been far more at play in the wake of the massive hack.

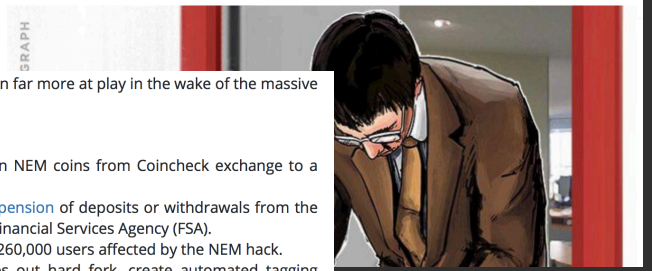
Timeline:

- Friday Jan. 26 - 03:00 - hackers transfer 523 mln NEM coins from Coincheck exchange to a single address.
- Friday Jan.26 - 05:25 - Coincheck announces suspension of deposits or withdrawals from the exchange, report theft to the police and Japan's Financial Services Agency (FSA).
- Saturday Jan. 27 - Coincheck promises to refund 260,000 users affected by the NEM hack.
- Saturday Jan. 27- NEM development team rules out hard fork, create automated tagging system to identify and flag all stolen NEM coins in circulation.
- Tuesday Jan. 30 - NEM Foundation vice president Jeff McDonald announces that hackers are moving stolen NEM coins to various addresses 100 NEM at a time - while confirming no coins had been sold at exchanges.
- Friday Feb. 2 - FSA visits Coincheck's offices for a site inspection following the hack.
- Friday Feb. 2 - FSA order Coincheck to submit a report on the incident and a systems improvement proposal by Feb. 13.
- Friday Feb. 9 - Coincheck announces some users will be able to make Japanese Yen withdrawals for the first time since transaction freeze on Feb. 13.
- Monday Feb. 12 - 10 traders announce plans to file a lawsuit against Coincheck to recover stolen funds.

By Gareth Jenkinson 14 HOURS AG

Coincheck Delivers Report to Japan's FSA

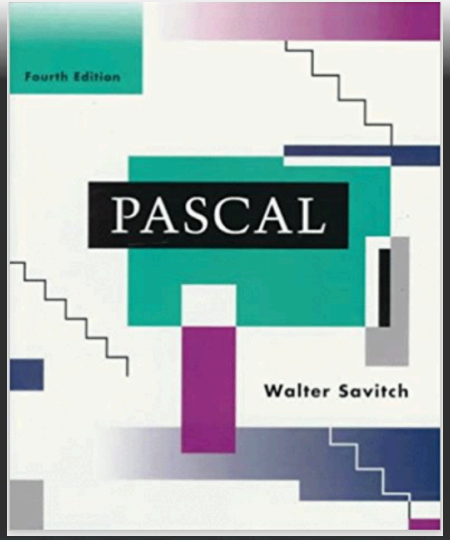
11890 Total views 176 Total shares



What does it teach us?

- Basic security matters
- Users matter even more
- What happens to security of Blockchain-backed solutions?
- The same techniques apply as in old world

It's about the whole solution



**IN THEORY THERE IS NO DIFFERENCE BETWEEN THEORY AND PRACTICE.
IN PRACTICE, THERE IS.**

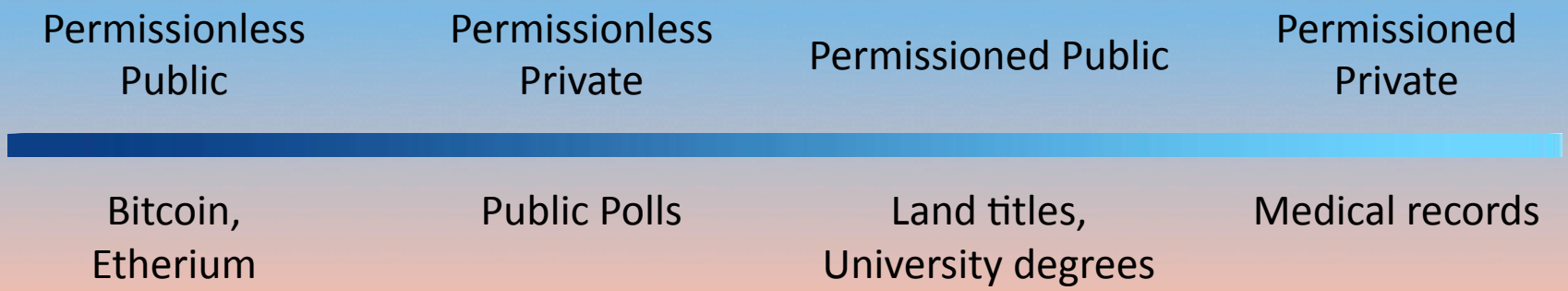
Walter Savitch

Moving from old to new

BASING WALLETS ON CHAUM'S KEY PAIRS MAKES PRIVATE KEYS HIGH VALUE TARGETS

SPECTRUM OF SOLUTIONS

Spectrum of Blockchains



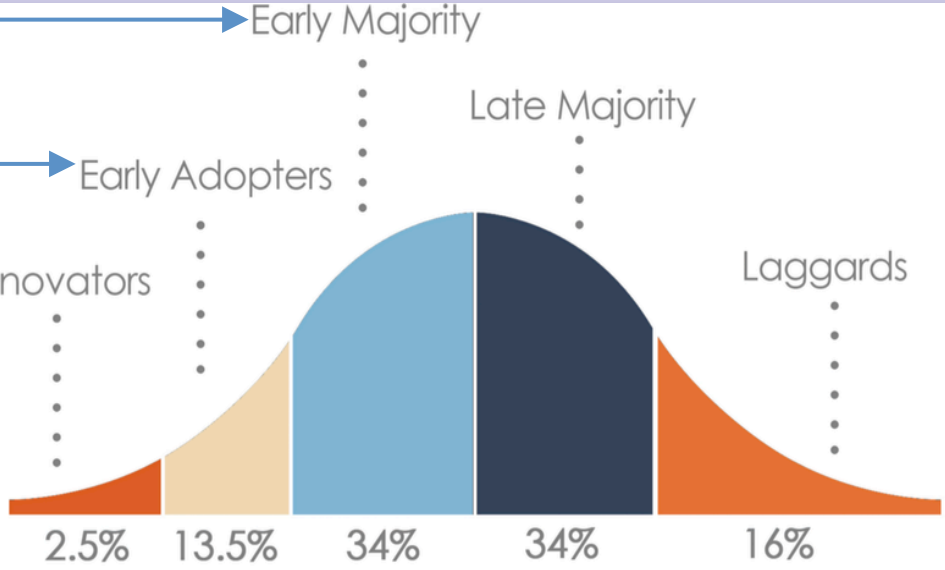
Permissioned vs. Permissionless: Who can write to a Blockchain (i.e., accessibility)
Public vs. Private: Who can read from a Blockchain (i.e., visibility)

Blockchain Industries Curve

Logistics, Insurance, Governments

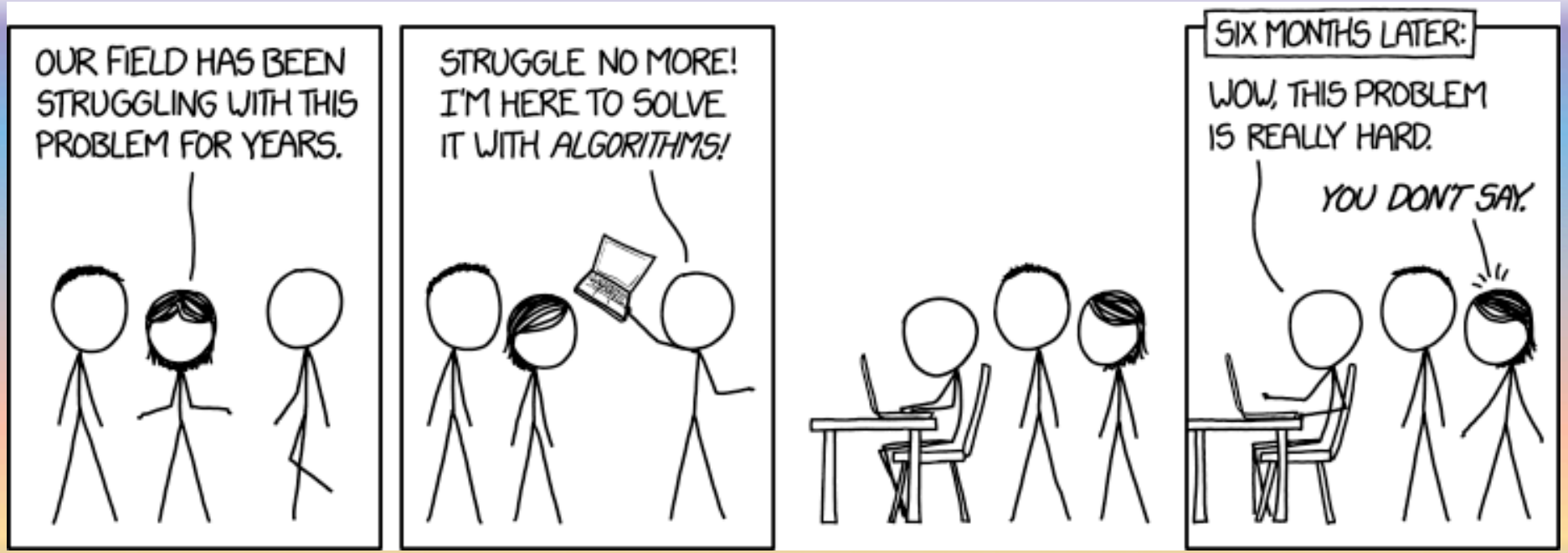
Healthcare, Supply Chain

Fintech



Diffusion of Innovations Curve, by Everett Rogers

Not all problems can be solved with Blockchain



GREY ZONE OF PROBLEMS

When Frenemies try to be Friends

Enterprises are not designed to collaborate

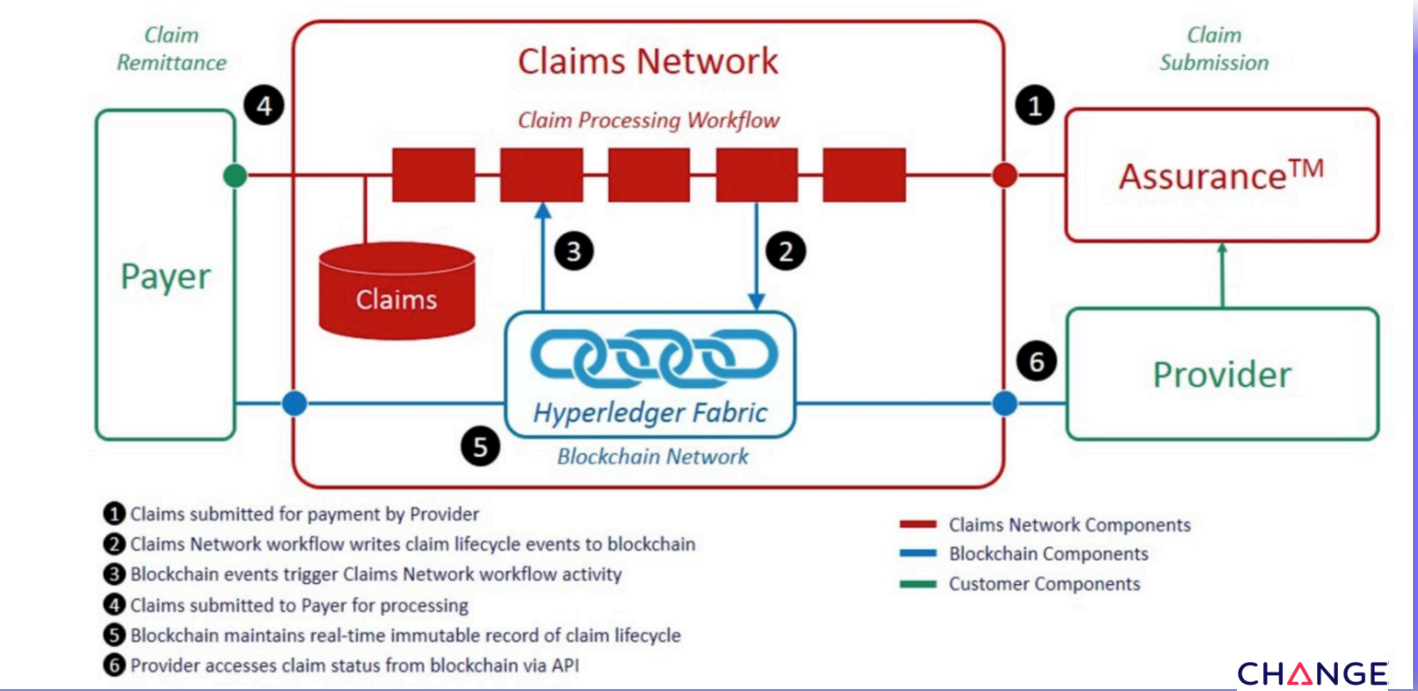
- How do you protect IP?
- Can Open Source help?
- Why join Blockchain consortia?
- Which technology to choose?

The importance of being Earnest

- Responsible disclosure in decentralized and anonymous environment?
- It is still a Network! DDoS is a Dirty Drag.
- Smart Contracts are only as smart as their authors.
- We already know most of it, just need to be more cautious

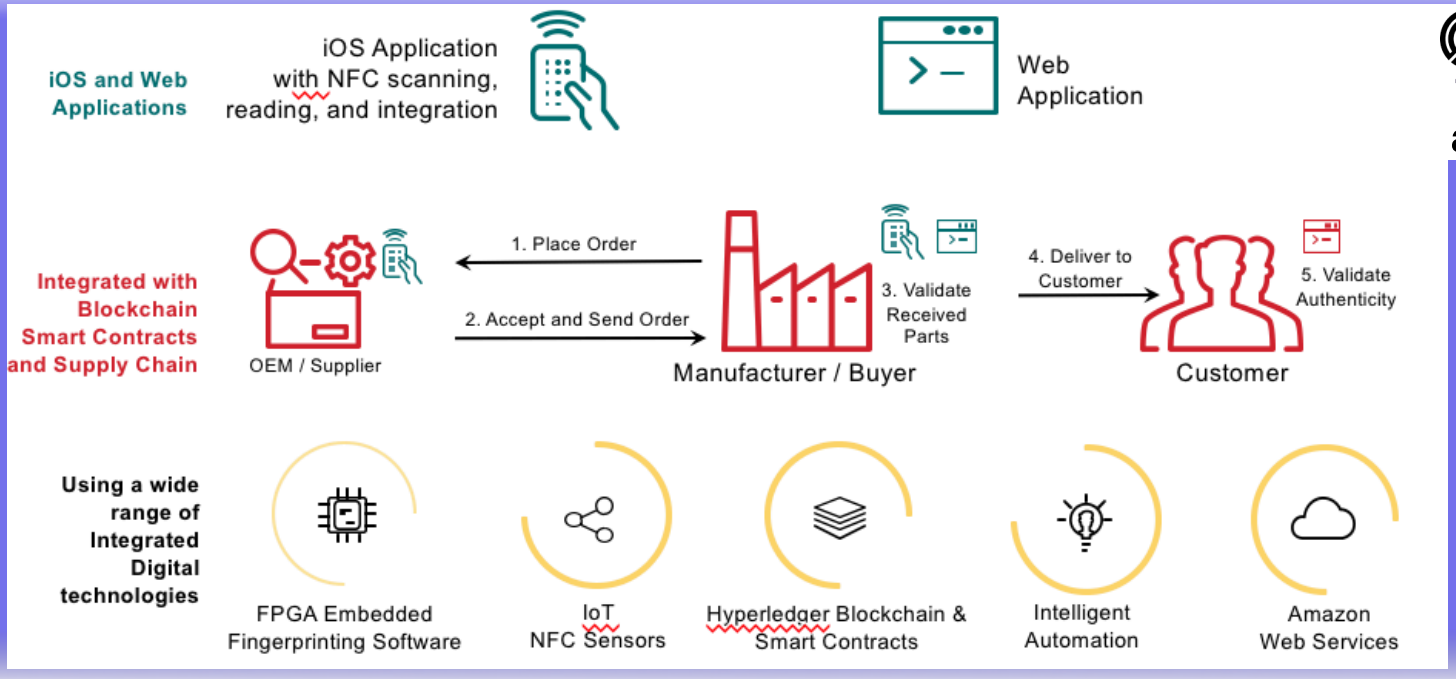
WHAT COLOR IS THE SKY IN YOUR WORLD?

Exemplary Deployment: Claims Transparency



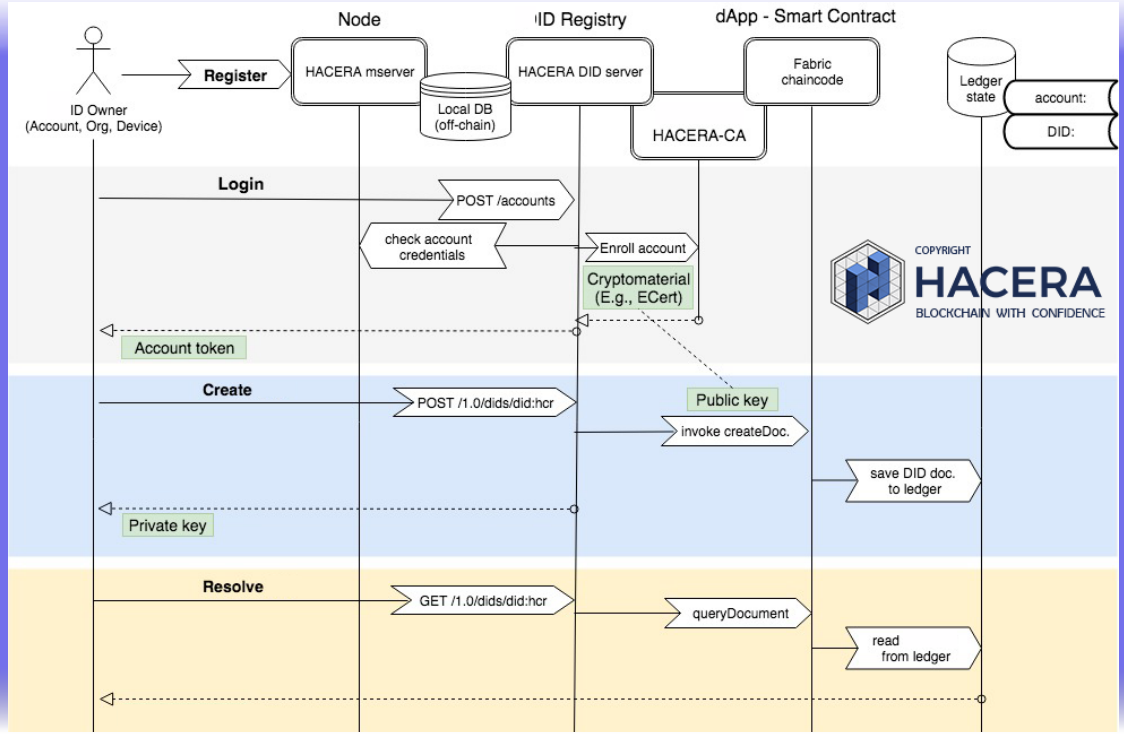
CHANGE HEALTHCARE

Exemplary Deployment: Secure Supply Chain



CHRONICLED
THALES
accenture

Exemplary Deployment: Posture Validation



You've come, you've seen, now Vici!

- **General Remark:** Blockchain is just a tool. Design your solutions well, please.
- **Action Item 1:** Old security measures apply. In addition to new ones. **REVISIT YOUR SECURITY MODELS AND ARCHITECTURES.**
- **Action Item 2**: Ease of use might be the most important of your challenges. **DESIGN SYSTEMS WITH USABILITY IN MIND.**
- **Action Item 3:** Collaboration matters. Seriously. **RETHINK WHOM YOU SHOULD BE COLLABORATING WITH AND START DOING IT.**

Recommended reading

- Massive online open-souce course: “**Blockchain for Business**”
- Publications: www.hyperledger.org/resources
- Comparison of Hyperledger Frameworks
- Collection of interesting use cases for Blockchain technologies
- On Bitcoin: https://bitcoin.org/en/faq
- Just subscribe: MIT chainletter

RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: PDAC-T08

QUESTIONS?

MARTA PIEKARSKA

marta@linuxfoundation.org

DAVE HUSEBY

Dhuseby@linuxfoundation.org