Blockchain is the New Black

What about enterprise security?

Dave Huseby, Security Maven, Hyperledger, *The Linux Foundation*
Marta Piekarska, Director of Ecosystem, Hyperledger, *The Linux Foundation*

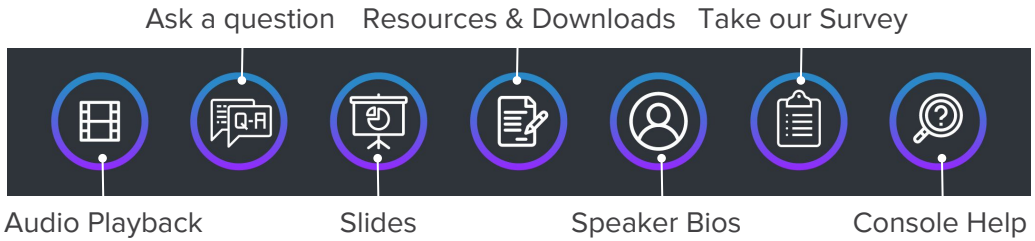
HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Housekeeping

Recording
Session is being recording and replay link will be emailed tomorrow

Widgets
All the widgets on your console are moveable and re-sizable so you can adjust your layout

Slide Download
Slides are already available as a PDF in the Resources & Downloads widget



Marta Piekarska

Directory of Ecosystem, Hyperledger, *The Linux Foundation*

PhD in User Informed Design of Privacy Tools

10 years of experience in technology companies, including Apple, Yahoo & Deutsche Telekom

4 years in Blockchain: Blockstream & Hyperledger

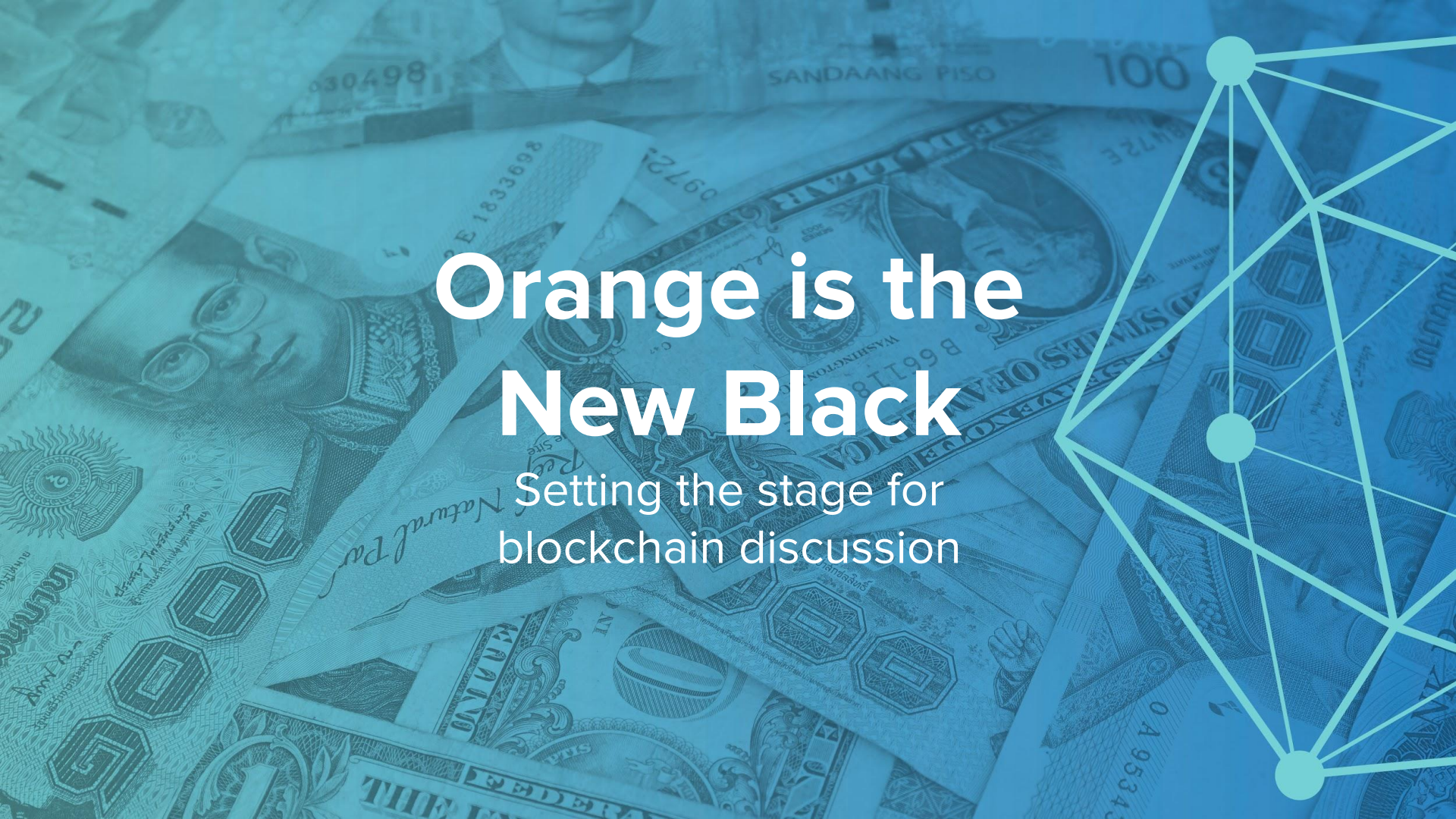
Dave Huseby

Security Maven, Hyperledger, *The Linux Foundation*

Security Maven

Open source developer for 25 years

Focused on software security and engineering best practices for the last decade



Orange is the New Black

Setting the stage for blockchain discussion

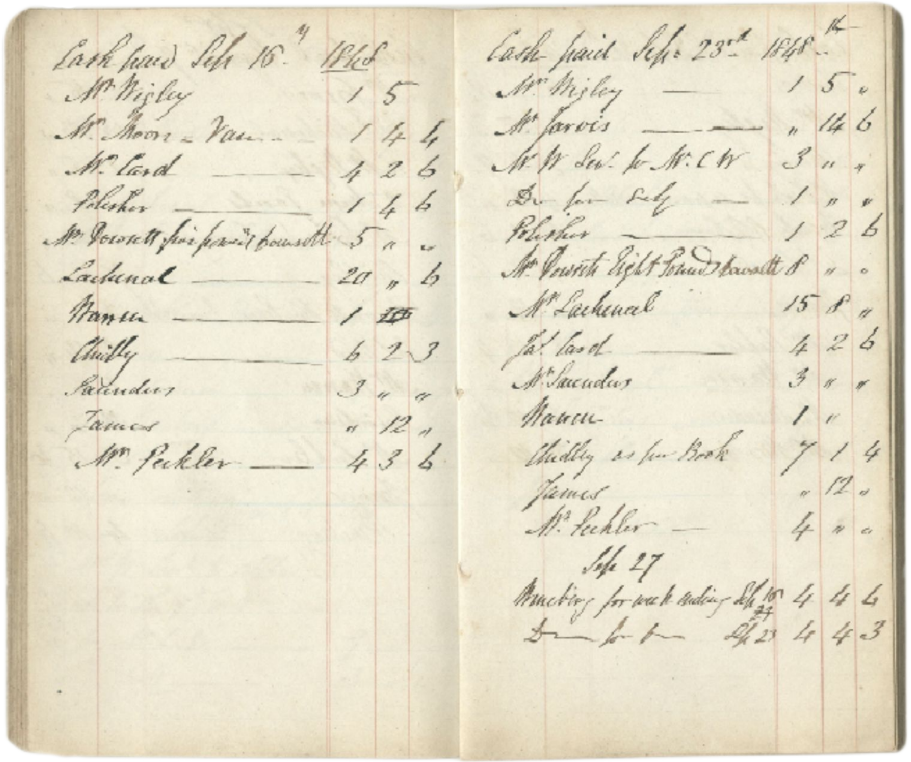
It’s all about money, money, money

The first long-distance trade occurred between Mesopotamia and indus valley in pakistan ~3000 b.C

How Do You Agree on Assets Balance?

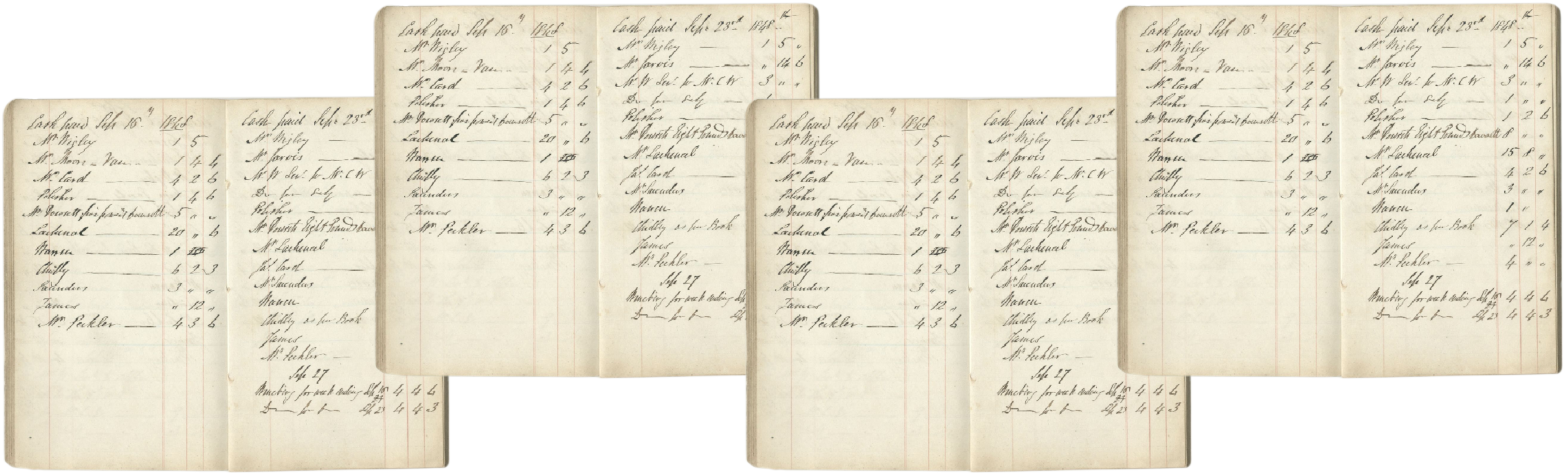
How to track the value of exchanged goods?

Traditional Ledgers



Digital World

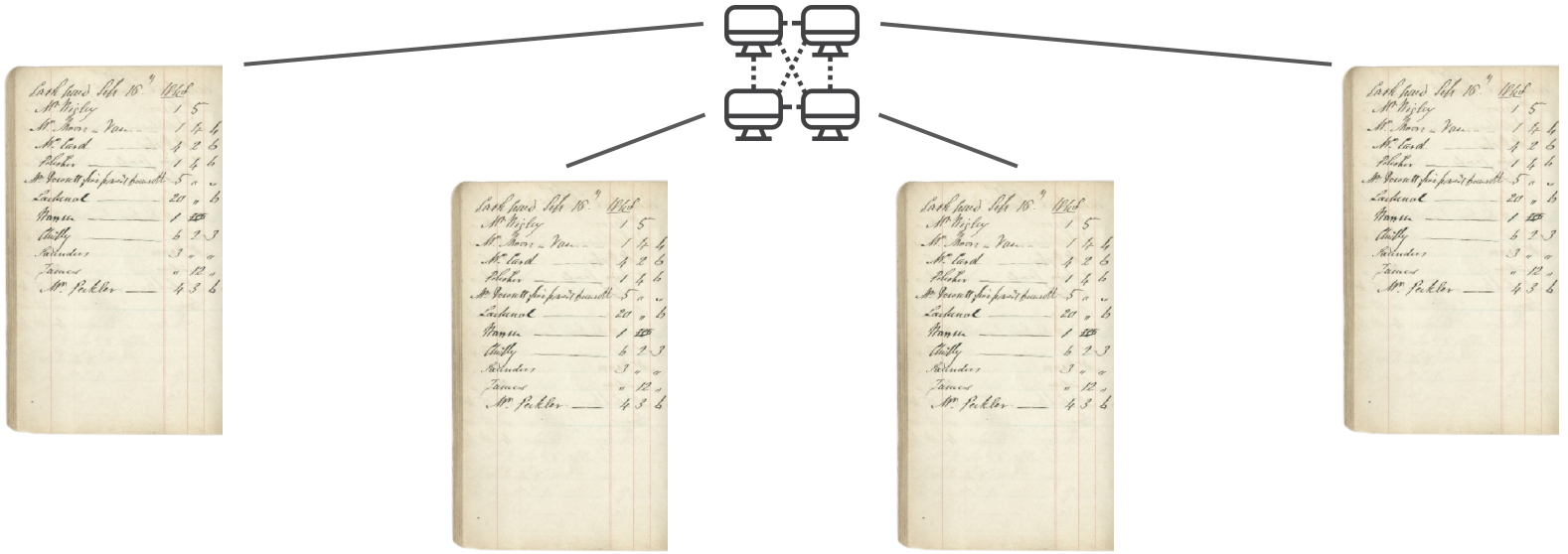
In the digital world there are many copies that may contain different versions. The challenge: which do you trust as a single source of truth?




LET ME INTRODUCE YOU
Internet Connected
Reality
TO THE INTERNET

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

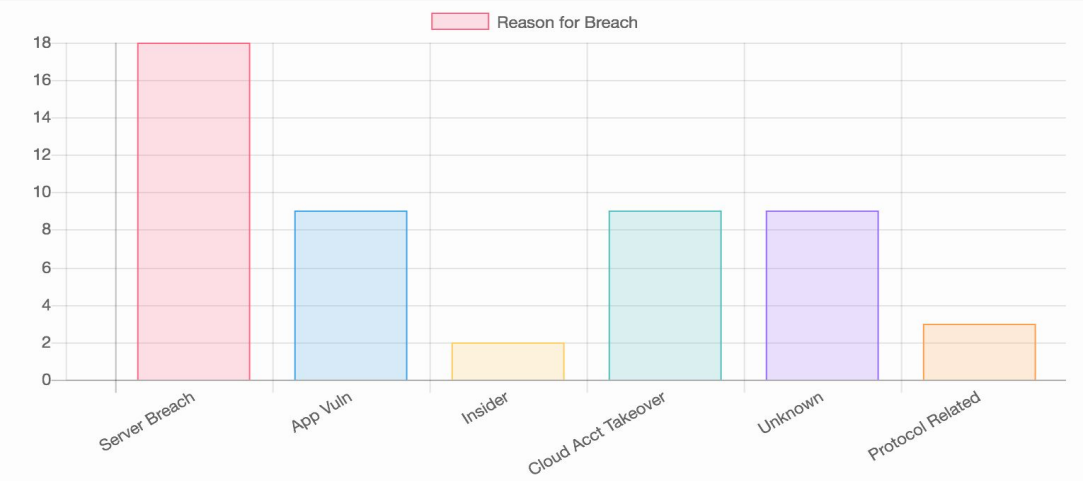
Platform Concepts

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 set to report to regulators over $530 million cryptocurrency heist

- Japanese cryptocurrency exchange Coincheck, stung by the theft of $530 million of digital money last month, is expected on Tuesday to file a report with regulators
- Coincheck said
on Tuesday, sayi
- Still, the exchan
withdrawals unt

Published 8:32 PM ET Mo

REUTERS

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.

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

Posted yesterday by Taylor Hatmaker (@tayhatmaker)

Next St

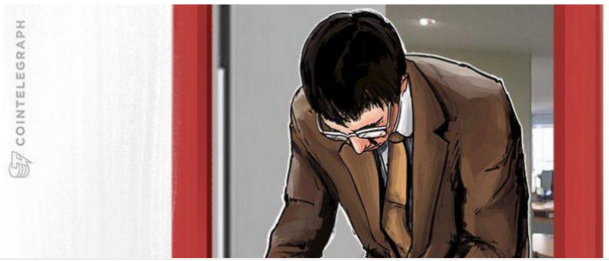
ADVERTISEMENT

By Gareth Jenkinson

14 HOURS AG

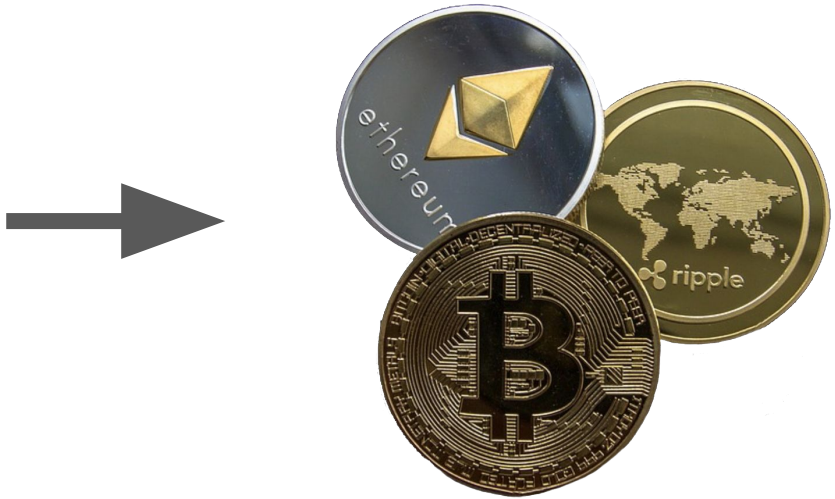
Coincheck Delivers Report to Japan's FSA

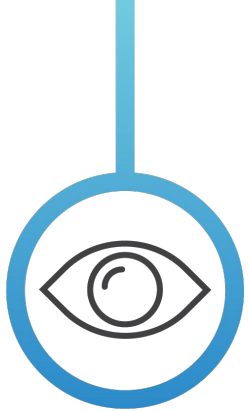
11890 Total views **176** Total shares



Moving from old to new

Basing wallets on chaum's key pairs makes private keys high value targets

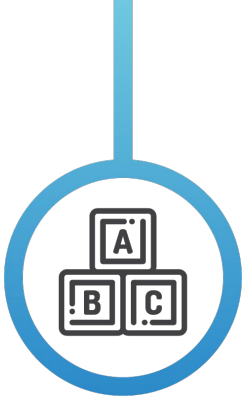




It’s About the Whole Solution

In theory there is no difference
between theory and practice.
In practice, there is.

- Walter Savitch



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


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)

Permissionless Public

Permissionless Private

Permissioned Public

Permissioned Private

Bitcoin, Ethereum

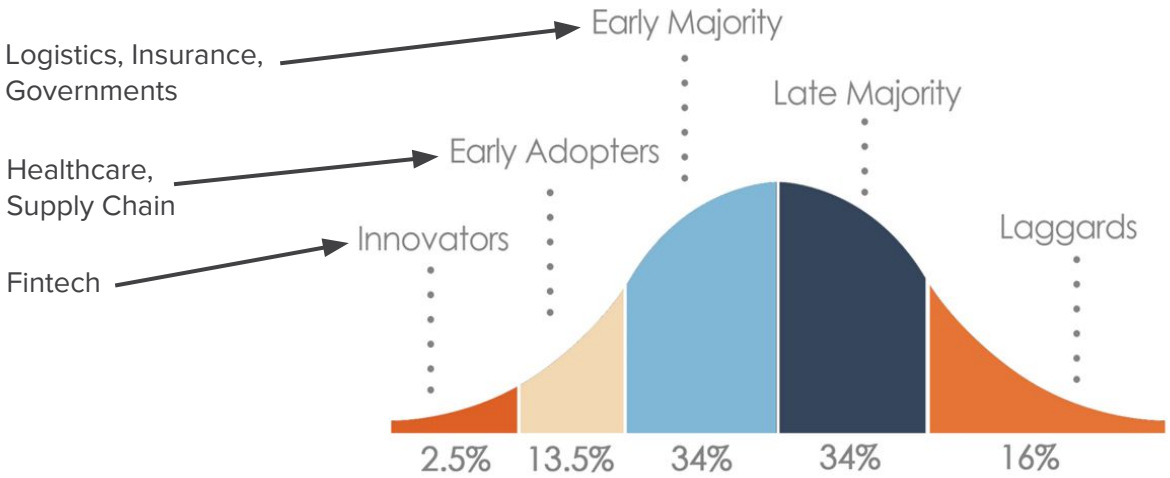
Public Polls

Land titles, University degrees

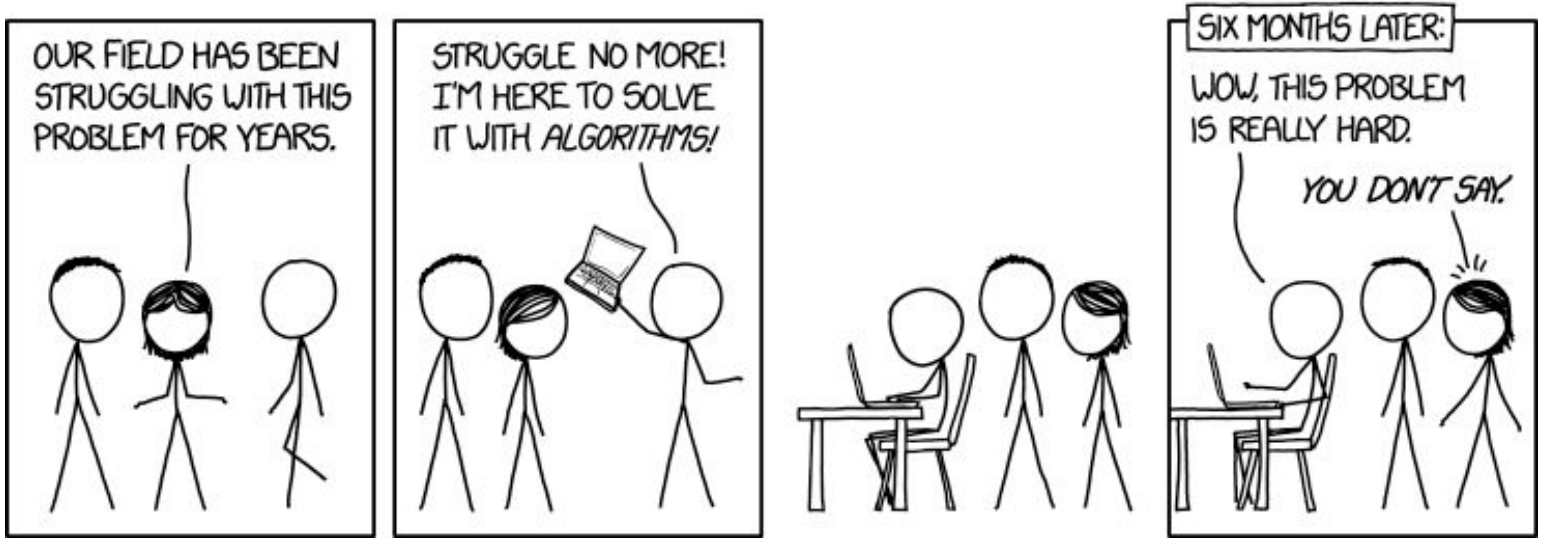
Medical records

Blockchain Industries Curve

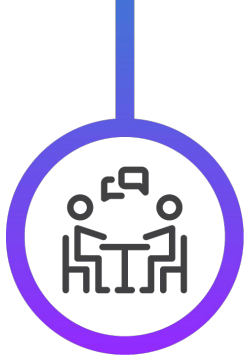
Diffusion of Innovations Curve, by Everett Rogers



Not all problems can be solved with Blockchain




Grey Zone of
Problems



When Frenemies try to be Friends

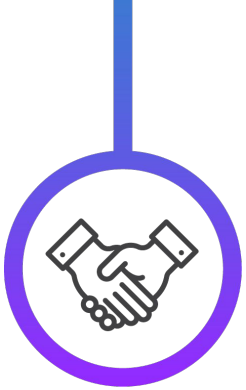
Enterprises are not designed to collaborate

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?

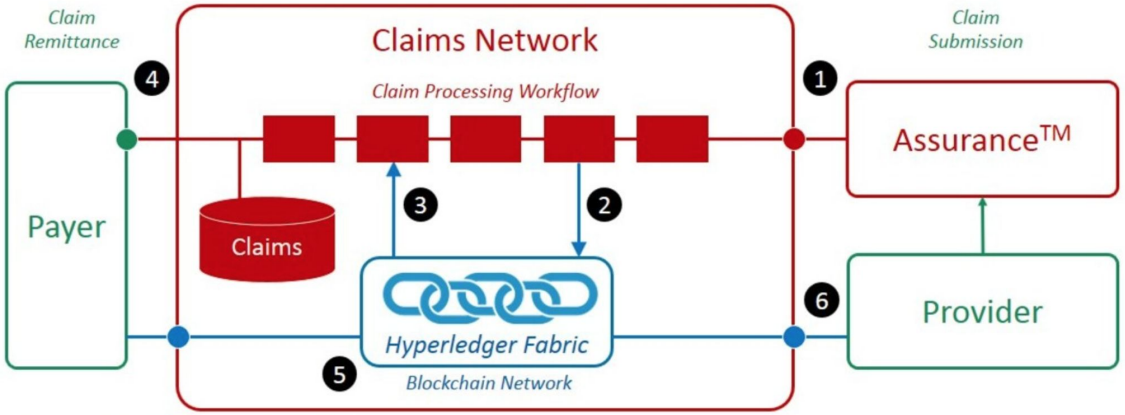
It is still a Network! DDoS is a Dirty Drag.

Smart Contracts are only as smart as their authors.

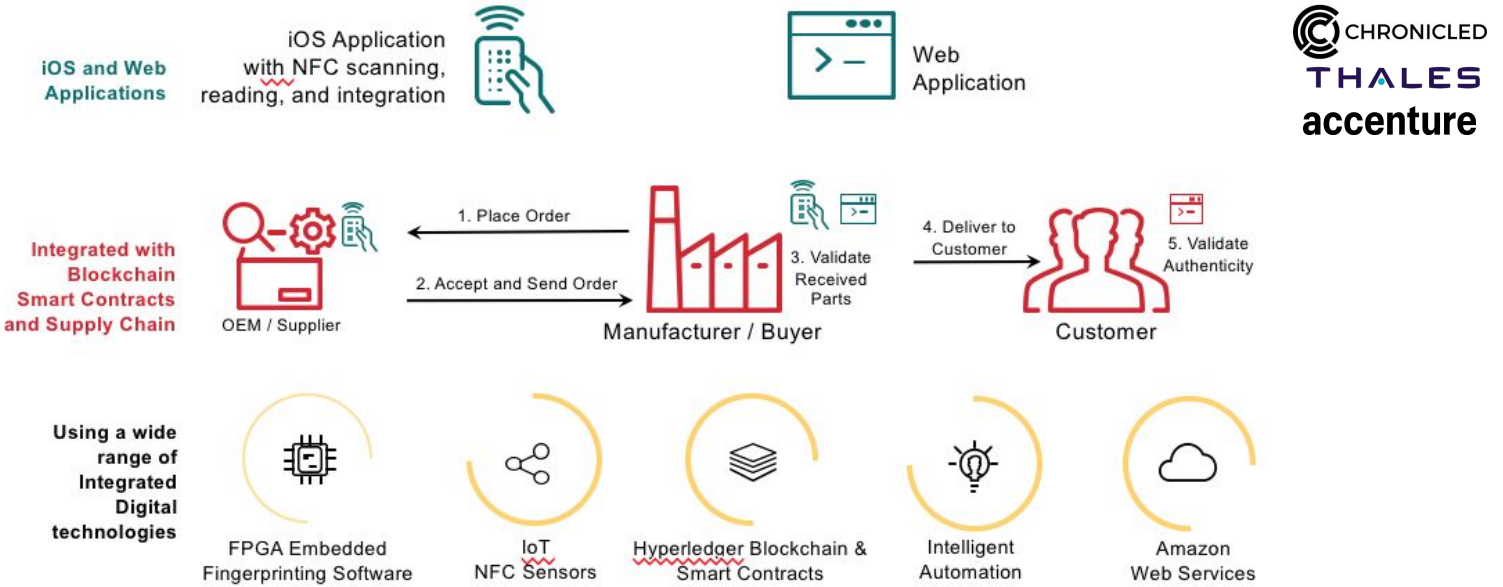
We already know most of it, just need to be more cautious

What Color is the Sky in Your World?

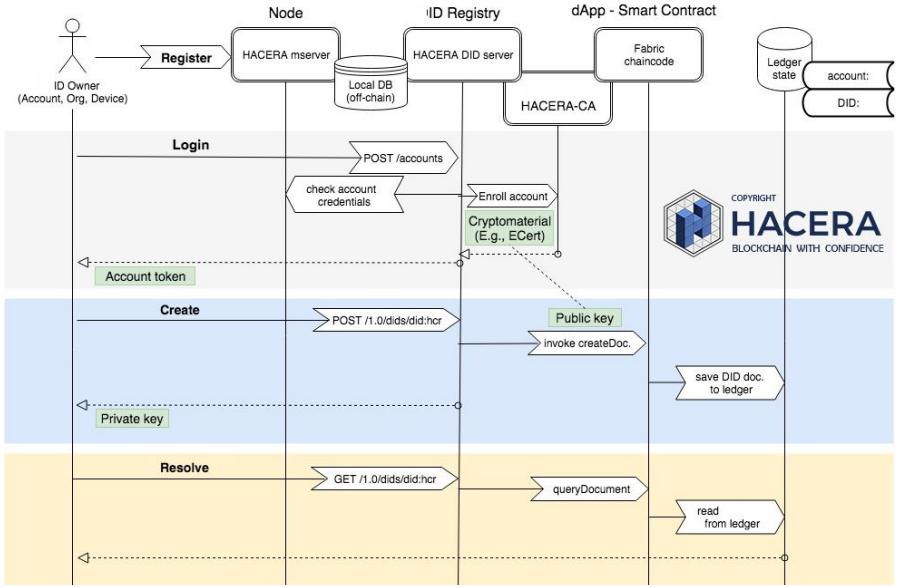
Exemplary Deployment: Claims Transparency



Exemplary Deployment: Secure Supply Chain



Exemplary Deployment: Posture Validation




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

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.**

You can help!

Report a Security Bug

security@hyperledger.org

We Have a Bug Bounty—Use It!

hackerone.com/hyperledger

Join a Working Group

wiki.hyperledger.org

Watch the Webinar Replay: Get Involved!

hyperledger.org/webinars/get-involved

Recommended Reading

Massive online
open-souce course
"Blockchain for Business"

Publications
hyperledger.org/resources

Comparison of
Hyperledger Frameworks

Collection of interesting
use cases for Blockchain technologies

On Bitcoin
bitcoin.org/en/faq

Just subscribe
MIT chainletter

Questions?

Marta Piekarska
Director of Ecosystem, Hyperledger
marta@linuxfoundation.org

Dave Huseby
Security Maven, Hyperledger
dhuseby@linuxfoundation.org