Assurance of Trust: Blockchain and AI

Ashish Kundu
ACM Distinguished Speaker, ACM Distinguished Member

Keynote
Records Knowledge Conference, Sacramento
May 23, 2019

Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

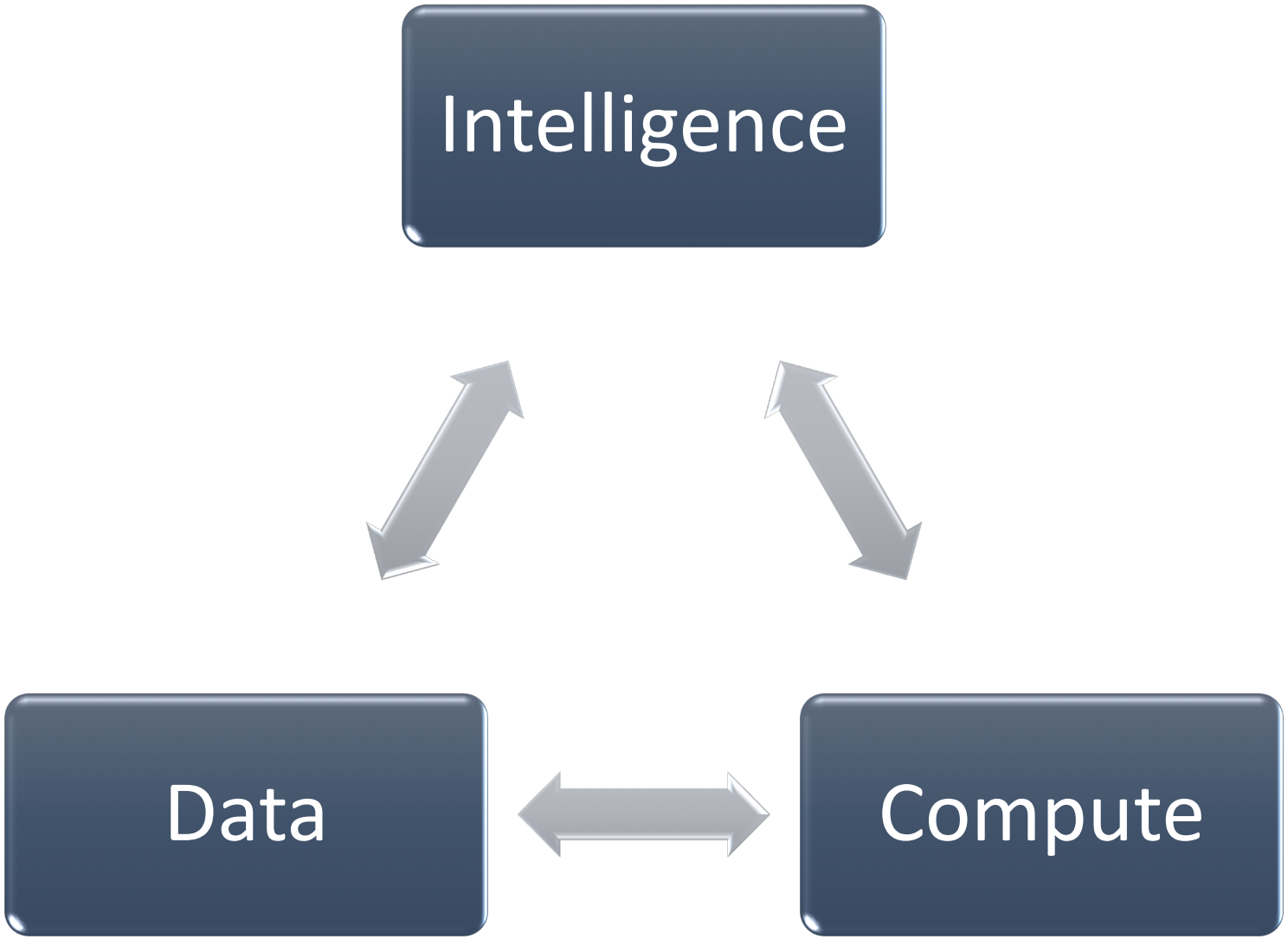
Ken Thompson
Turing Award Lecture, 1984

What is trust

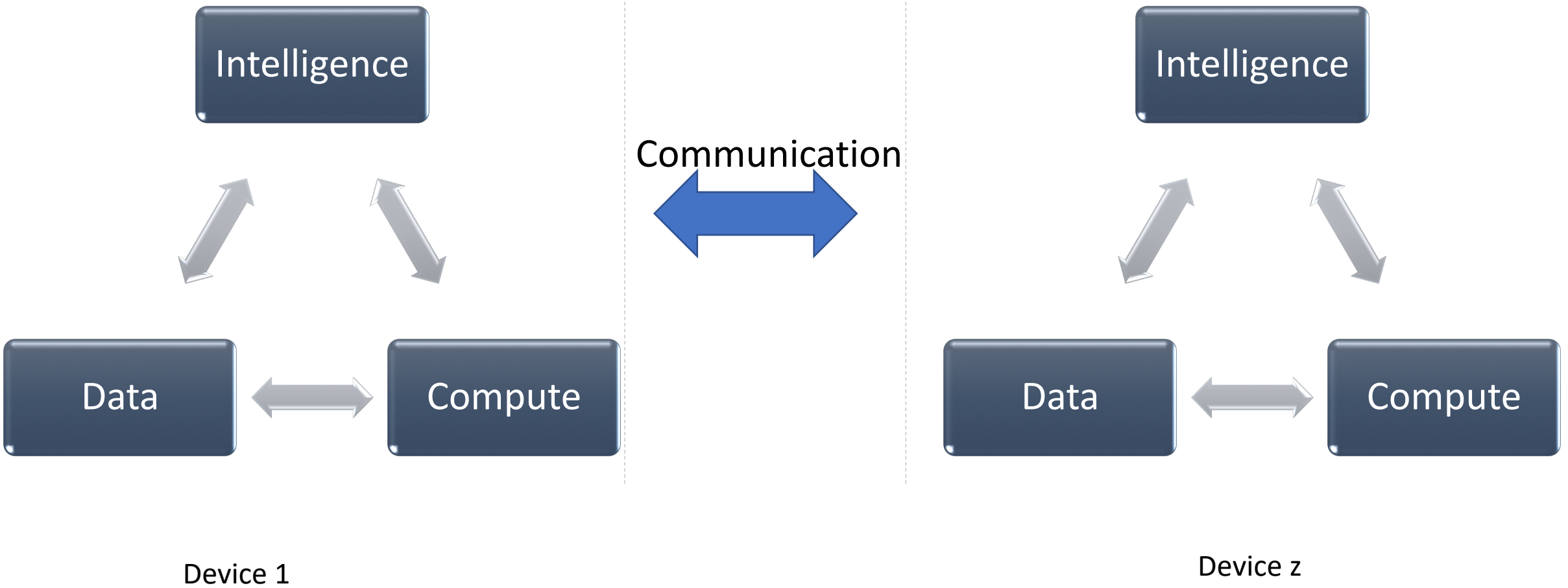
trust is seen as **qualified reliance on received information…**

https://en.wikipedia.org/wiki/Trusted_system

Why do we need trust



Why do we need trust



Trends on Data

Qubits

Graphs

Trees

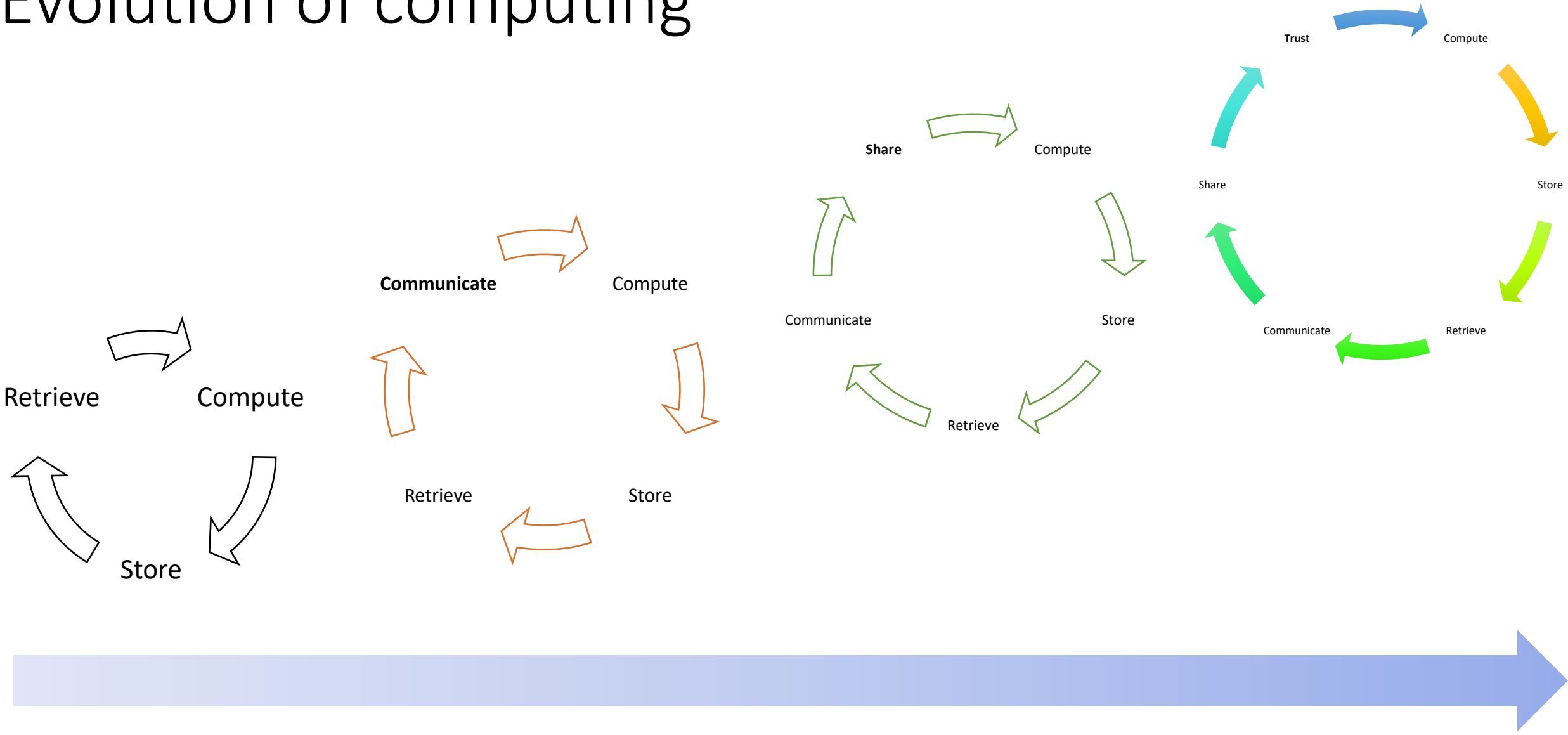
Tables Objects

Arrays

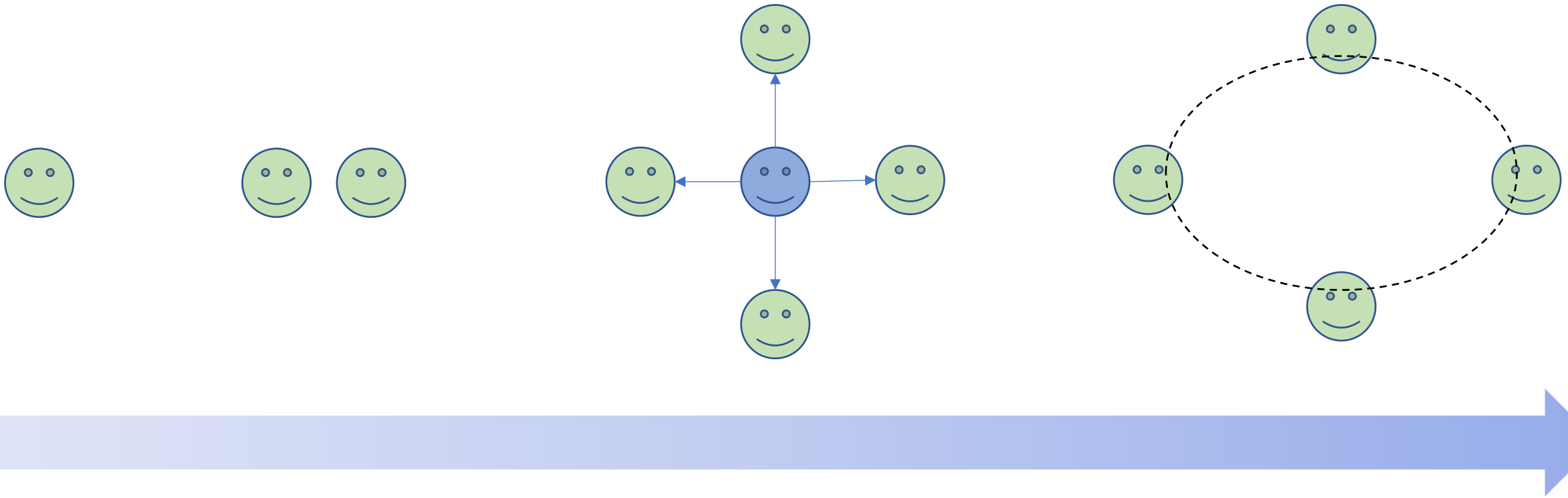
Bytes, words

Analog 0 1

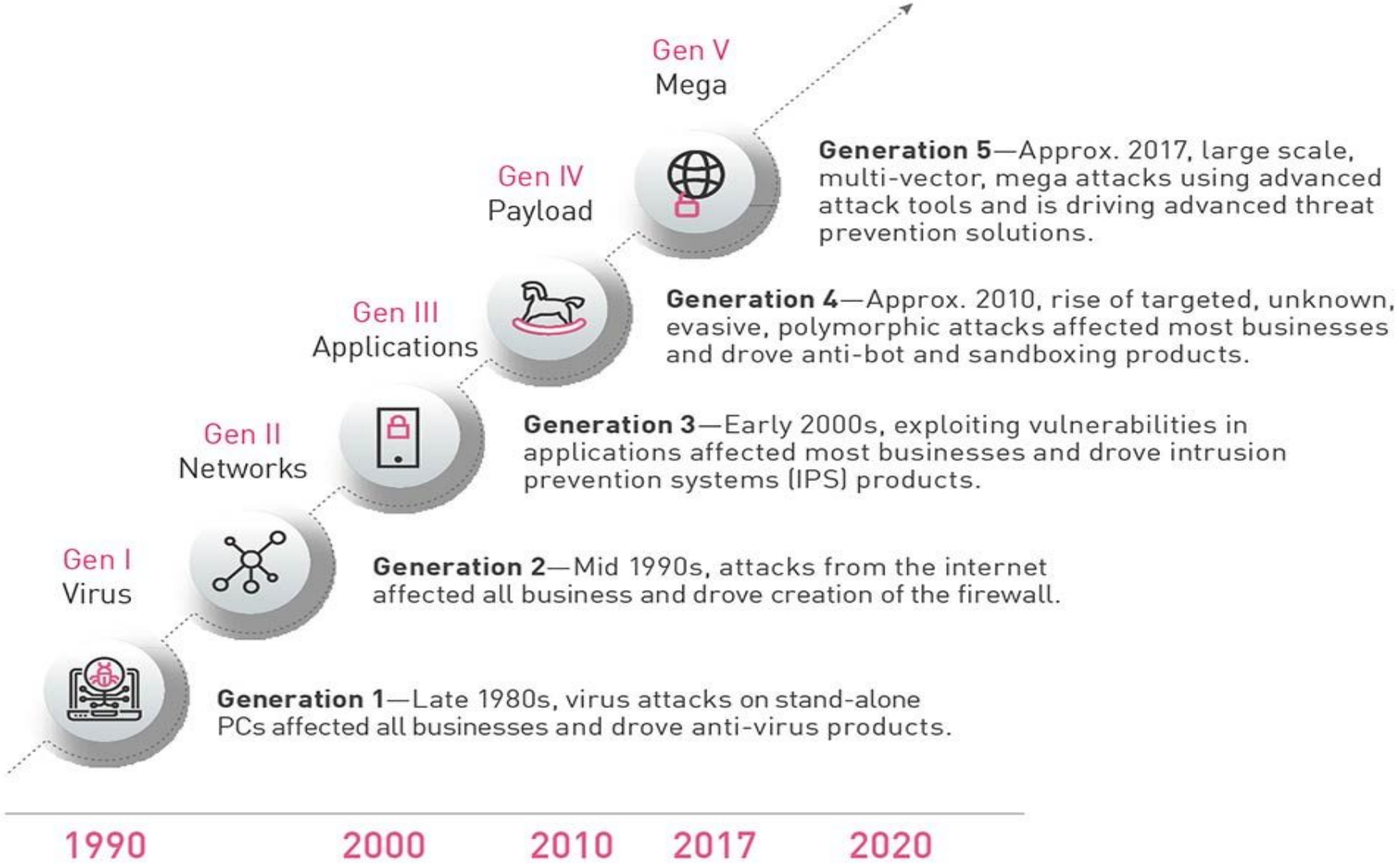
Evolution of computing



Trend towards de-centralized trust

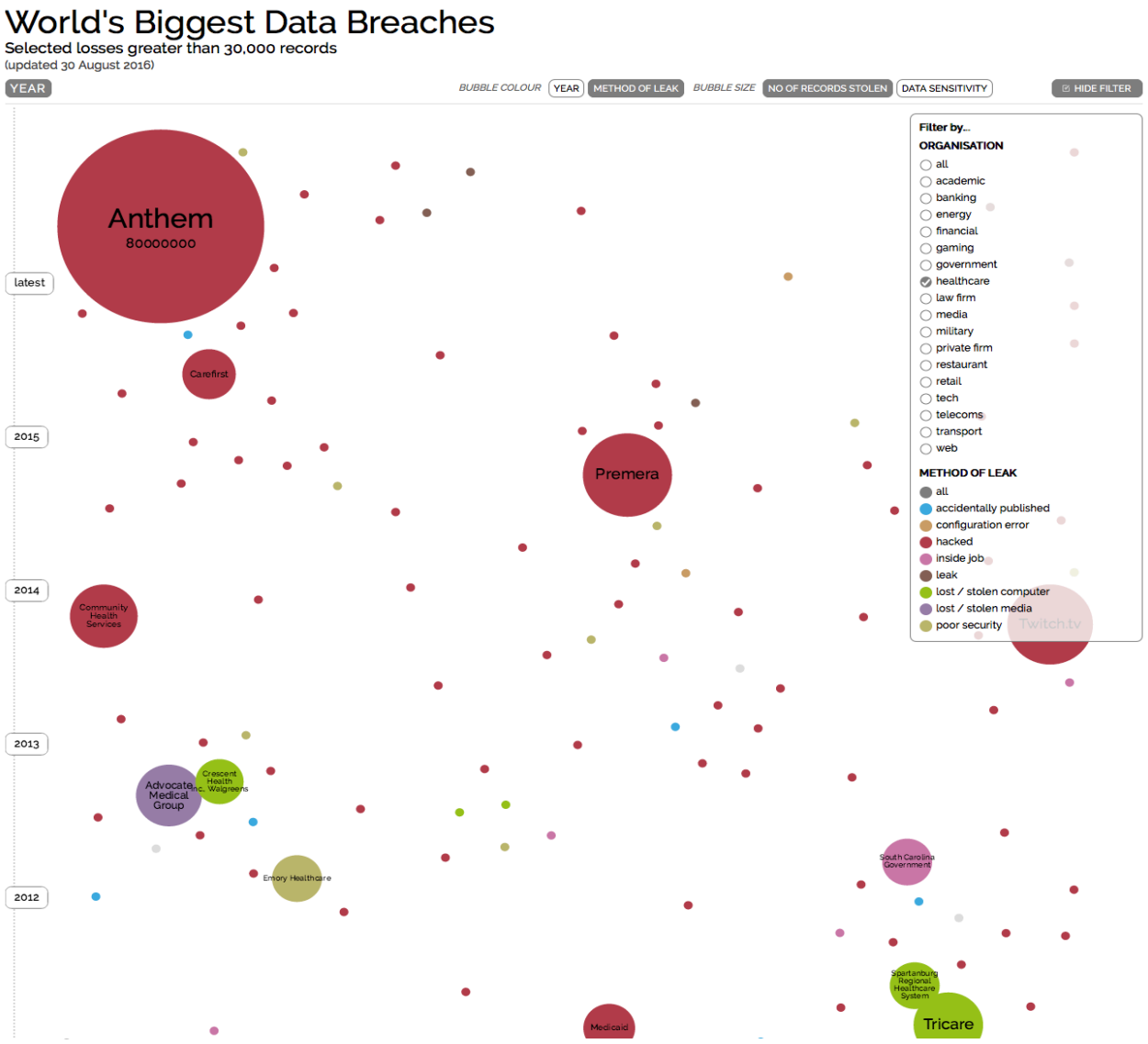


Why trust



Source - https://www.checkpoint.com/gen-v-cyber-security/

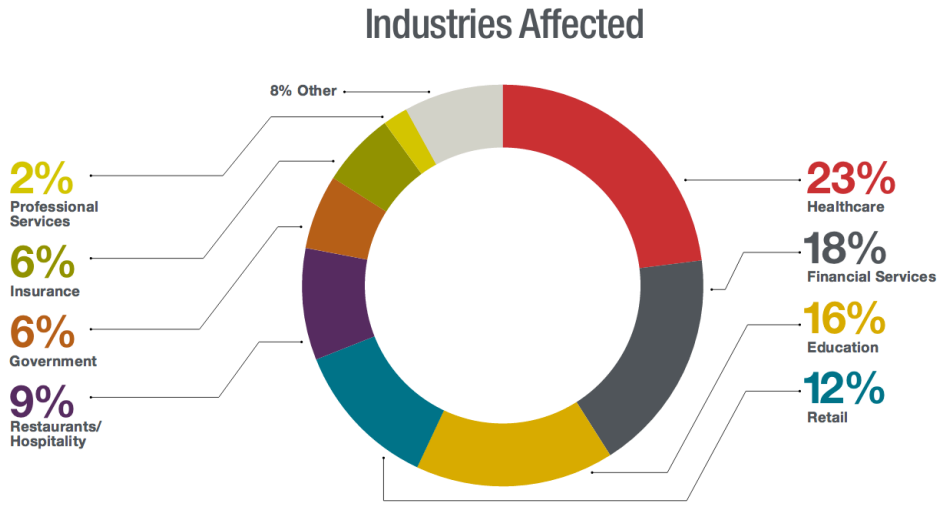
Where are we?



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Table 2: Severity of Breach Patterns, Top 5 Country Targets	Compromised Records Per 100 People	Compromised Records Per 100 Internet Users
Germany	68	79
Greece	81	140
Netherlands	23	24
Norway	80	83
United Kingdom	220	245

http://www.statewatch.org/news/2014/oct/data-breaches-in-europe.pdf



https://iapp.org/media/images/resource_center/BakerHostetler%202016%20Data%20Security%20Incident%20Response%20Report.pdf

Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

Ken Thompson
Turing Award Lecture, 1984

Trusting Trust (+ AI)

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

Perhaps it is more important to trust the people ***and the AI/ML systems*** *who wrote the software.*

Countering Trusting Trust

Counter the “trusting trust trojan attack” using diverse double-compiling (DDC), …

David Wheeler, 2010
https://dwheeler.com/trusting-trust/wheelerd-trust.pdf

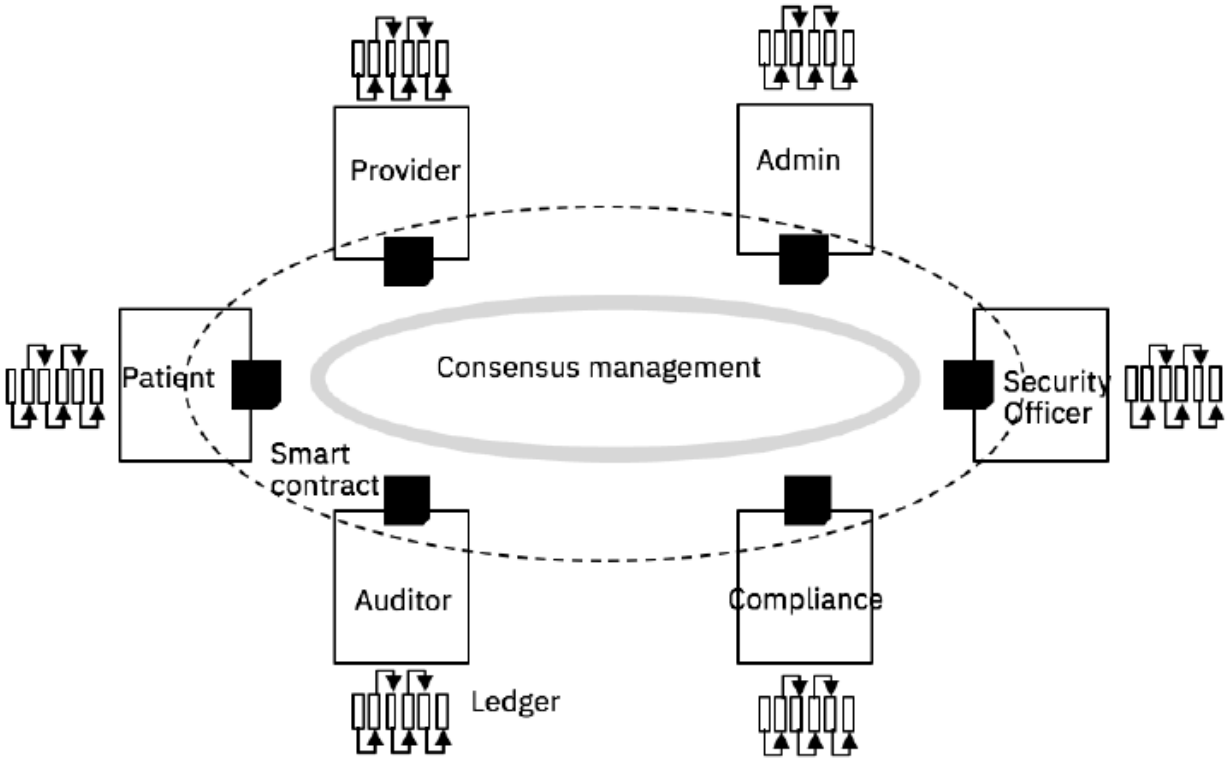
Countering Trusting Trust (+ de-centralized)

Counter the “trusting trust trojan attack” using diverse double-compiling (DDC), …

de-centralized trust among multiple compilers

Blockchain

What is a blockchain



- De-centralized Peers (untrusted)
- Consensus
- Smart contracts
- Immutable ledger for chained/hashed data items

Bitcoin & Virtual Currencies

how computers shall be compensated for their work!

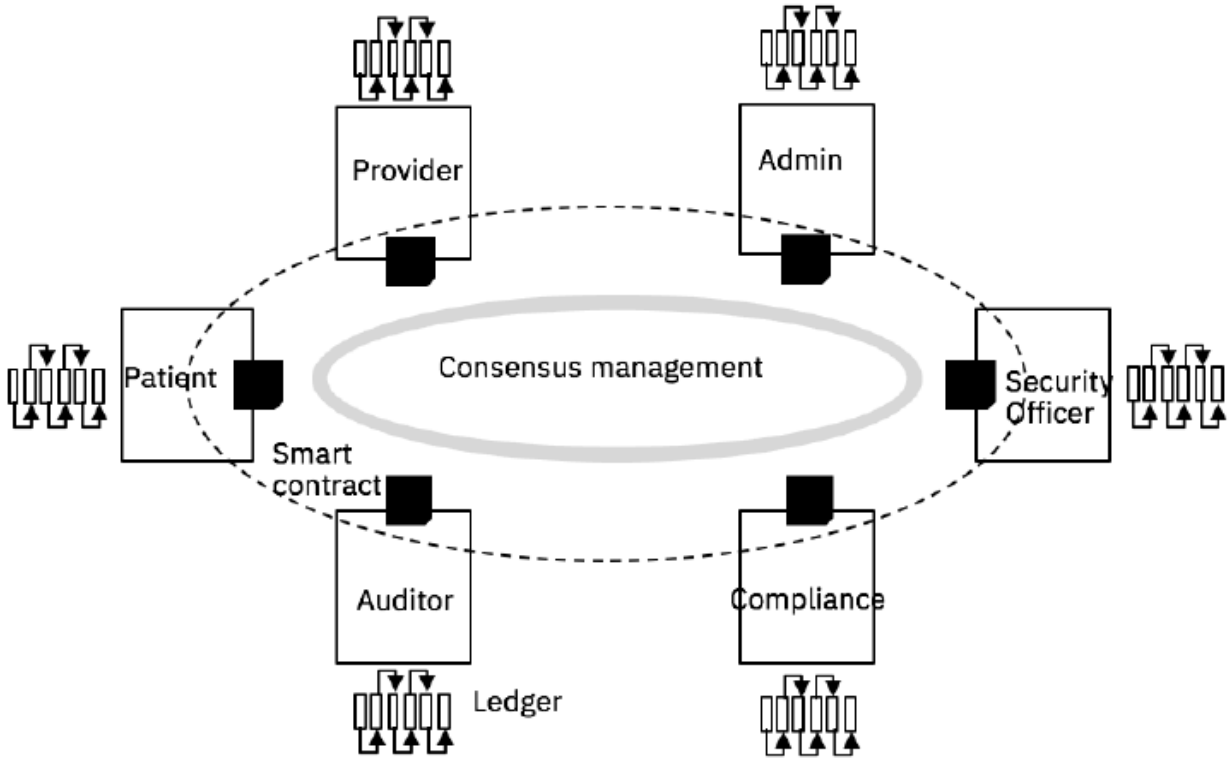
~~Cryptocurrency~~ Virtual/Digital Currency

- Not all bitcoin-type currency need to rely on “crypto”
- Any hard-to-compute/process, but easy to verify can act as PoW
- MIT Digital currency
  - https://dci.mit.edu/
- Ethereum Ether
  - Memory-hard

Blockchain platforms

how de-centralized trust is enabled in computing

Blockchain-based support for trust management



- Consensus management enables managing trust
- Each stakeholder has a smart contract that implements policies
- Smart contracts verify the state of security of data and the systems

Summary of Features of top 5 Blockchain Platforms for Enterprises

	Ethereum	Hyperledger Fabric	R3 Corda	Ripple	Quorum
Industry-focus	Cross-industry	Cross-industry	Financial Services	Financial Services	Cross-industry
Governance	Ethereum developers	Linux Foundation	R3 Consortium	Ripple Labs	Ethereum developers & JP Morgan Chase
Ledger type	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned
Cryptocurrency	Ether (ETH)	None	None	Ripple (XRP)	None
% providers with experience[1]	93%	93%	60%	33%	27%
% share of engagements[2]	52%	12%	13%	4%	10%
Coin Market Cap[3]	$91.5 B (18%)	Not applicable	Not Applicable	$43.9 B (9%)	Not Applicable
Consensus algorithm	Proof of Work (PoW)	Pluggable framework	Pluggable framework	Probabilistic voting	Majority voting
Smart contract functionality	Yes	Yes	Yes	No	Yes

1. *Based on responses from 15 leading blockchain service providers*
2. *Based on a random sample of set of 50 enterprise blockchain engagements across multiple industries*
3. *Coinmarketcap.com as of Feb 20, 2018, 6:20 PM UTC*

Source: HfS Research, 2018

HfS

Some of the industry applications

Banking & Financial Markets

Bring trust, simplicity & enhanced customer experience to financial services.

Insurance

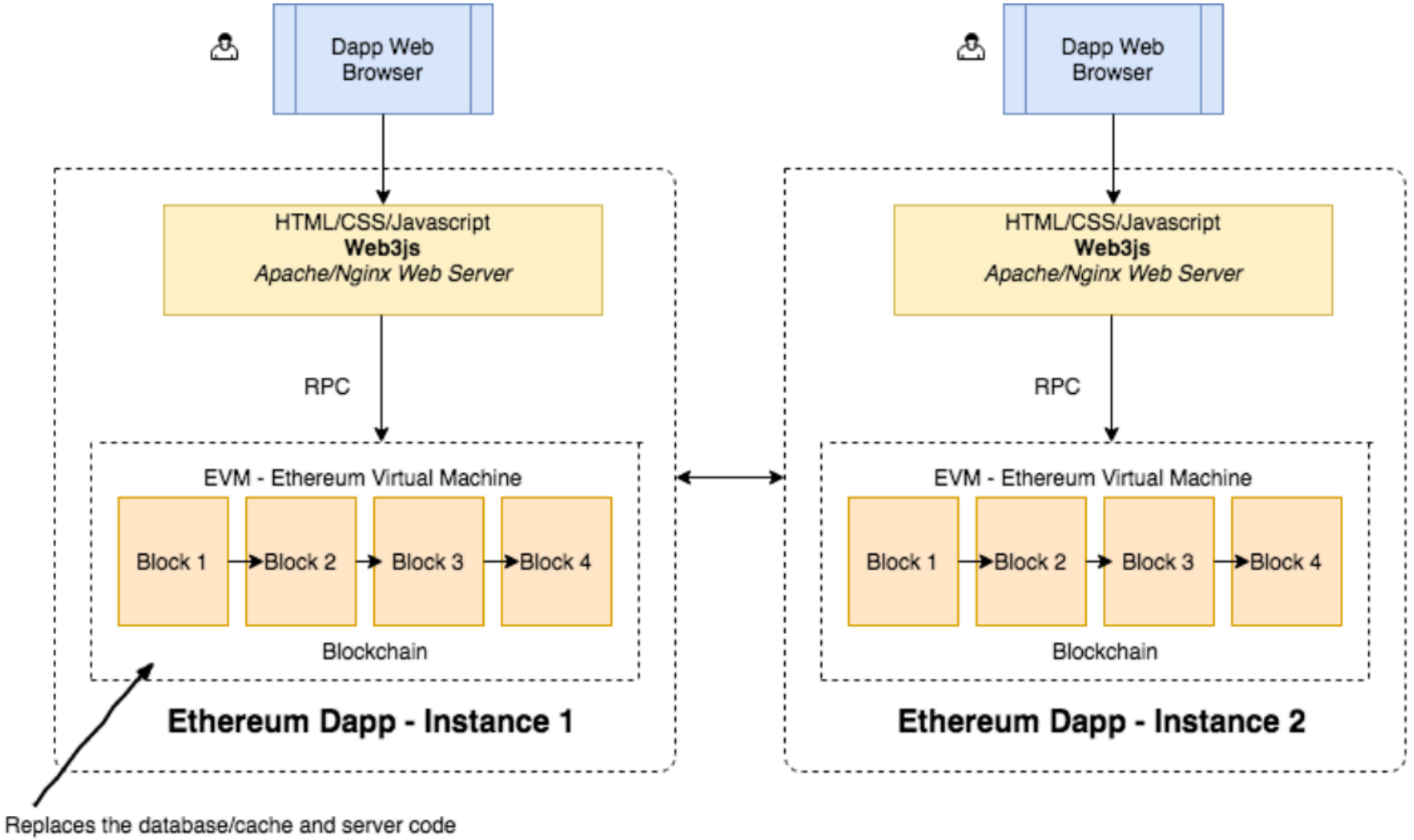
Revolutionize the trust that powers insurance with an immutable foundation of transparency and shared purpose.

Retail & Consumer Goods

Harness blockchain to reinvent the product authenticity, operational excellence and consumer experience.

https://www.ibm.com/blockchain/industries

Ethereum



https://www.zastrin.com/courses/ethereum-primer/lessons/1-5

Bitcoin Vulnerabilities

https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures

Common Vulnerabilities and Exposures

CVE	Announced	Affects	Severity	Attack is...	Flaw	Net
Pre-BIP protocol changes	n/a	All Bitcoin clients	Netsplit[1]	Implicit[2]	Various hardforks and softforks	100%
CVE-2010-5137	2010-07-28	wxBitcoin and bitcoind	DoS[3]	Easy	OP_LSHIFT crash	100%
CVE-2010-5141	2010-07-28	wxBitcoin and bitcoind	Theft[4]	Easy	OP_RETURN could be used to spend any output.	100%
CVE-2010-5138	2010-07-29	wxBitcoin and bitcoind	DoS[3]	Easy	Unlimited SigOp DoS	100%
CVE-2010-5139	2010-08-15	wxBitcoin and bitcoind	Inflation[5]	Easy	Combined output overflow	100%
CVE-2010-5140	2010-09-29	wxBitcoin and bitcoind	DoS[3]	Easy	Never confirming transactions	100%
CVE-2011-4447	2011-11-11	wxBitcoin and bitcoind	Exposure[6]	Hard	Wallet non-encryption	100%
CVE-2012-1909	2012-03-07	Bitcoin protocol and all clients	Netsplit[1]	Very hard	Transaction overwriting	100%
CVE-2012-1910	2012-03-17	bitcoind & Bitcoin-Qt for Windows	Unknown[7]	Hard	MingW non-multithreading	100%
BIP 0016	2012-04-01	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softfork: P2SH	100%
CVE-2012-2459	2012-05-14	bitcoind and Bitcoin-Qt	Netsplit[1]	Easy	Block hash collision (via merkle root)	100%
CVE-2012-3789	2012-06-20	bitcoind and Bitcoin-Qt	DoS[3]	Easy	(Lack of) orphan txn resource limits	100%
CVE-2012-4682		bitcoind and Bitcoin-Qt	DoS[3]			100%
CVE-2012-4683	2012-08-23	bitcoind and Bitcoin-Qt	DoS[3]	Easy	Targeted DoS by CPU exhaustion using alerts	100%
CVE-2012-4684	2012-08-24	bitcoind and Bitcoin-Qt	DoS[3]	Easy	Network-wide DoS using malleable signatures in alerts	100%

Conclusions

- De-centralized trust – easy to achieve but hard to maintain
- Security risks and threat model
- Privacy and confidentiality challenges

About ACM

- ACM, the Association for Computing Machinery (www.acm.org), is the premier global community of computing professionals and students with nearly 100,000 members in more than 170 countries interacting with more than 2 million computing professionals worldwide.

- OUR MISSION: We help computing professionals to be their best and most creative. We connect them to their peers, to what the latest developments, and inspire them to advance the profession and make a positive impact on society.

- OUR VISION: We see a world where computing helps solve tomorrow's problems – where we use our knowledge and skills to advance the computing profession and make a positive social impact throughout the world.

The Distinguished Speakers Program is made possible by

Association for Computing Machinery

Advancing Computing as a Science & Profession

For additional information, please visit http://dsp.acm.org/

Thanks and Questions!