Paths toward Semantic Blockchains

David Hyland-Wood

PEGASYS

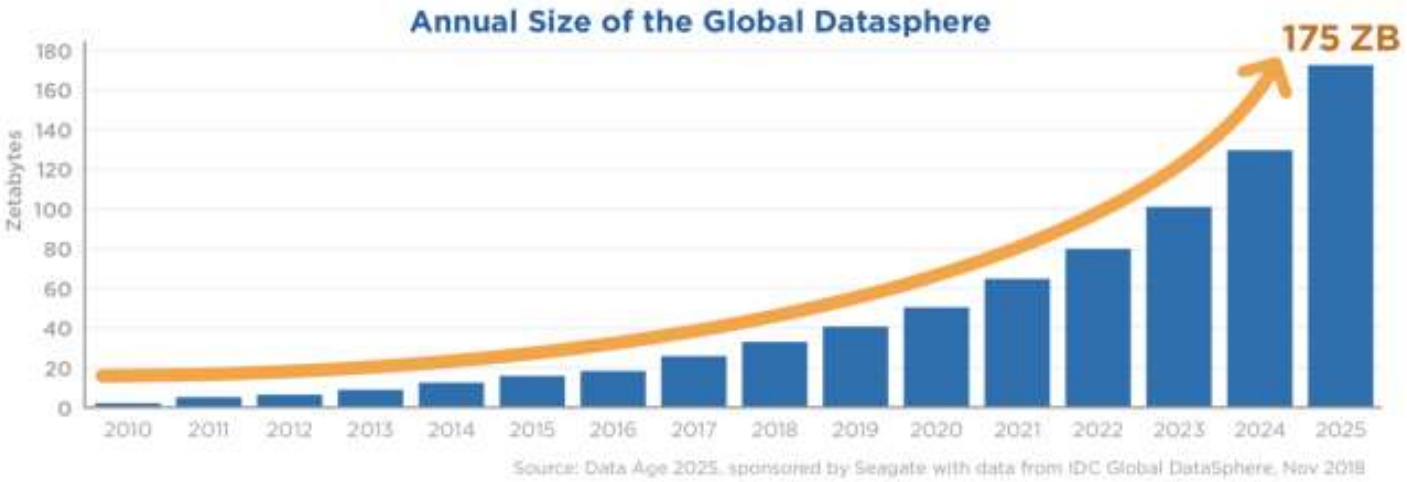
BlockSW 2019
Blockchain enabled Semantic Web Workshop
October 27, 2019

http://w3id.org/people/prototypo/talks/BlockSW2019

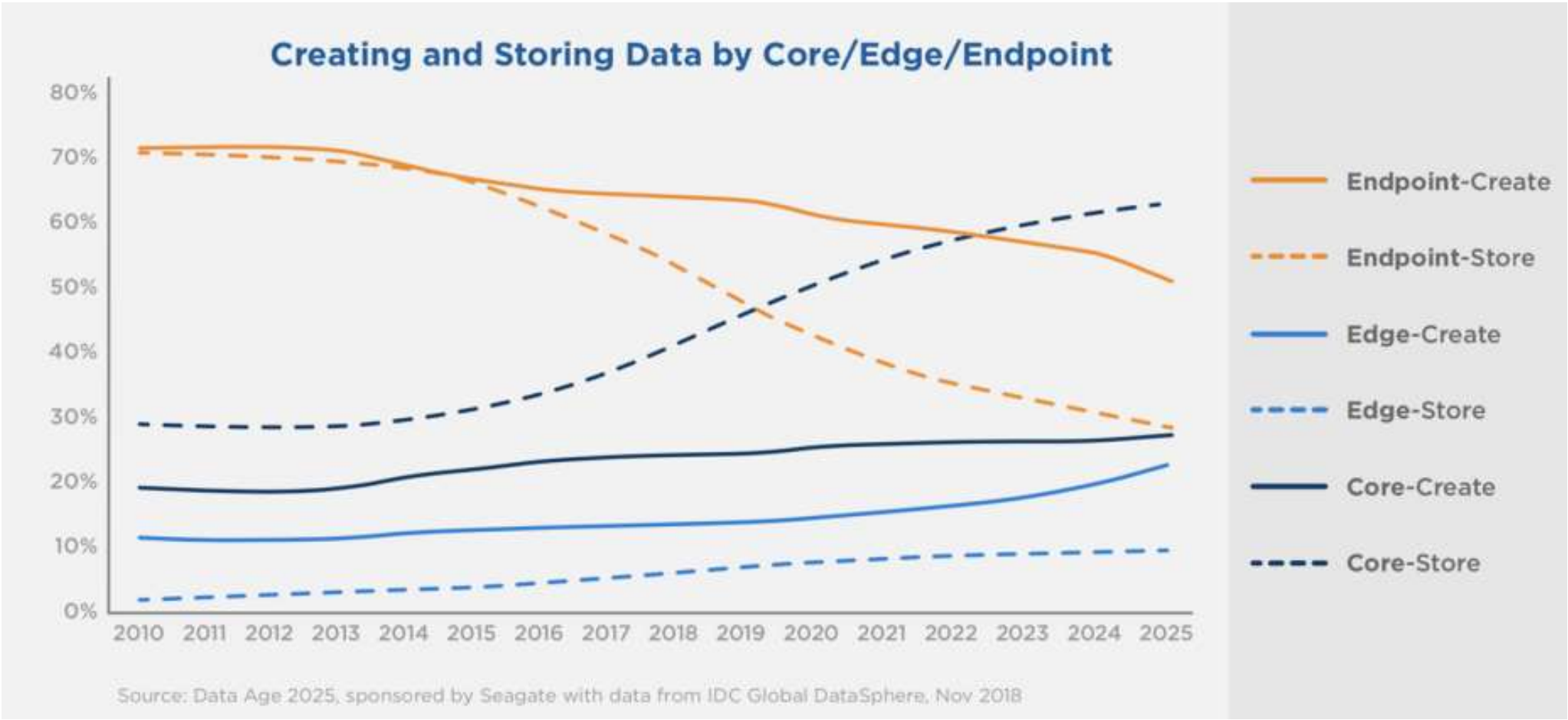
Abstract

A number of approaches have been suggested to enhance blockchains with concepts from Semantic Web research.

This talk will provide a brief overview of steps taken to date, and discuss **possible paths** toward standardisation and implementation of semantic blockchains.



In 2025 IDC predicts that **49%** of the world's stored data will reside in public cloud environments


Creating and Storing Data by Core/Edge/Endpoint
80%
70%
60%
50%
40%
30%
20%
10%
0%
2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025
Endpoint-Create
Endpoint-Store
Edge-Create
Edge-Store
Core-Create
Core-Store
Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere, Nov 2018


Twitter / dbasch: Many com
Twitter, Inc. [US] https://twitter.com/dbasch/status/269868078152691714?uid=16824747&iid=a8a8c6b7-5a76-437a-b355-9226dd00ba26&nid=12+49+20...
Home
Connect
Discover
Me
Search
Diego Basch
@dbasch
Follow
Many companies think they have a "big data" problem when they really have a big "data problem."
Reply
Retweeted
Favorited
306
RETWEETS
63
FAVORITES
1:22 PM - 17 Nov 12 from San Francisco, CA · Embed this Tweet
Reply to @dbasch

Forbes

24,559 views | Oct 10, 2019, 05:34pm

Why Knowledge Bases Are The Next Big Thing

Kurt Cagle Contributor
COGNITIVE WORLD Contributor Group ⓘ
Futurist, Technologist, Information Architect, Blogger

Forbes

24,559 views | Oct 10, 2019, 05:34pm

Why Knowledge Bases Are The Next Big Thing

Kurt Cagle Contributor
COGNITIVE WORLD Contributor Group ⓘ
Futurist, Technologist, Information Architect, Blogger

33B USD per annum in 2023
12% CAGR

Forbes

24,559 views | Oct 10, 2019, 05:34pm

Why Knowledge Bases Are The Next Big Thing

Kurt Cagle Contributor
COGNITIVE WORLD Contributor Group ⓘ
Futurist, Technologist, Information Architect, Blogger

33B USD per annum in 2023
12% CAGR

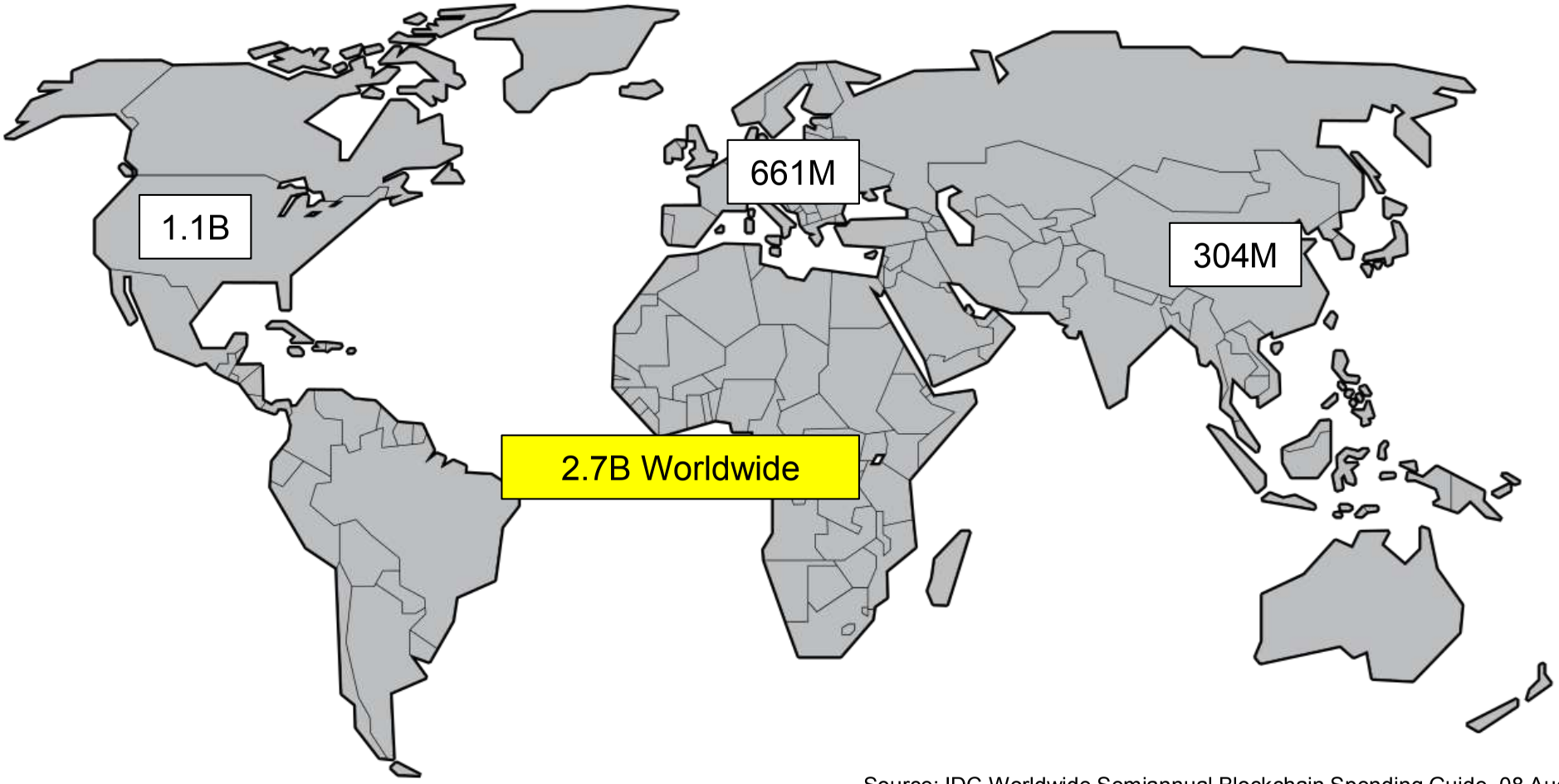
MarketWatch

PRESS RELEASE

Knowledge Management Software Market 2019 Global Size, Trends, Competitors Strategy, Regional Study and Industry Growth by Forecast to 2023

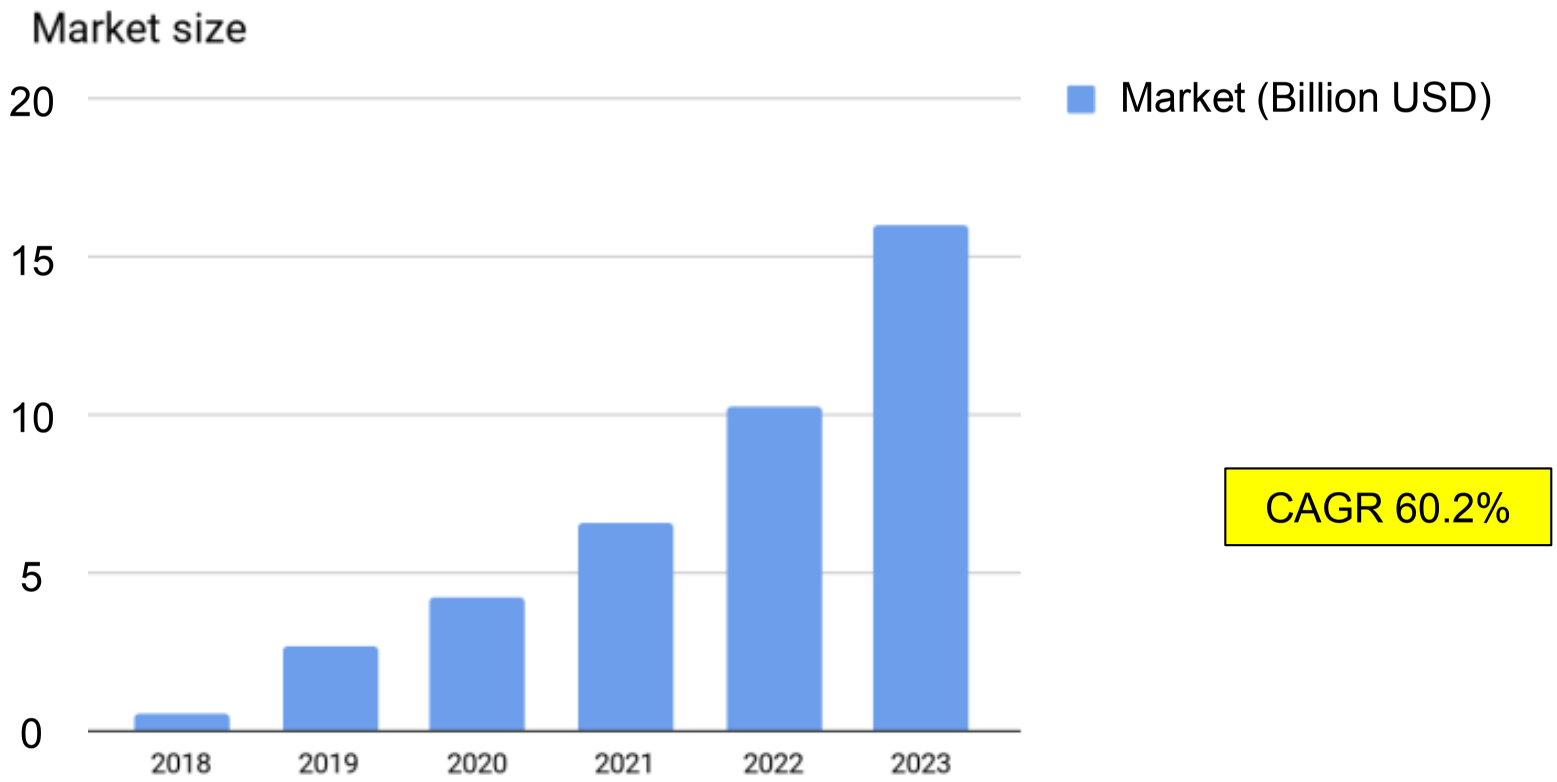
Published: Feb 4, 2019 5:24 a.m. ET

Blockchain Software & Services Market 2019 (USD)



Source: IDC Worldwide Semiannual Blockchain Spending Guide, 08 Aug 2019

Blockchain Software & Services Market (USD)



Source: IDC Worldwide Semiannual Blockchain Spending Guide, 08 Aug 2019

Bitcoin

Bitcoin Cash

Ethereum

Ripple

Litecoin

Dash

NEO

NEM

BitConnect

Monero

Ethereum Classic

IOTA

Qtum

OmiseGO

Cardano

Zcash

Lisk

EOS

Tether

Stellar Lumens

Hshare

Waves

Stratis

Komodo

Ark

Bytecoin

Steem

Ardor

Augur

Decred

PIVX

TenX

Binance Coin

Populous

Golem

Vertcoin

BitShares

MaidSafeCoin

BitcoinDark

Gas

TRON

MonaCoin

Basic Attention Token

Dogecoin

Kyber Network

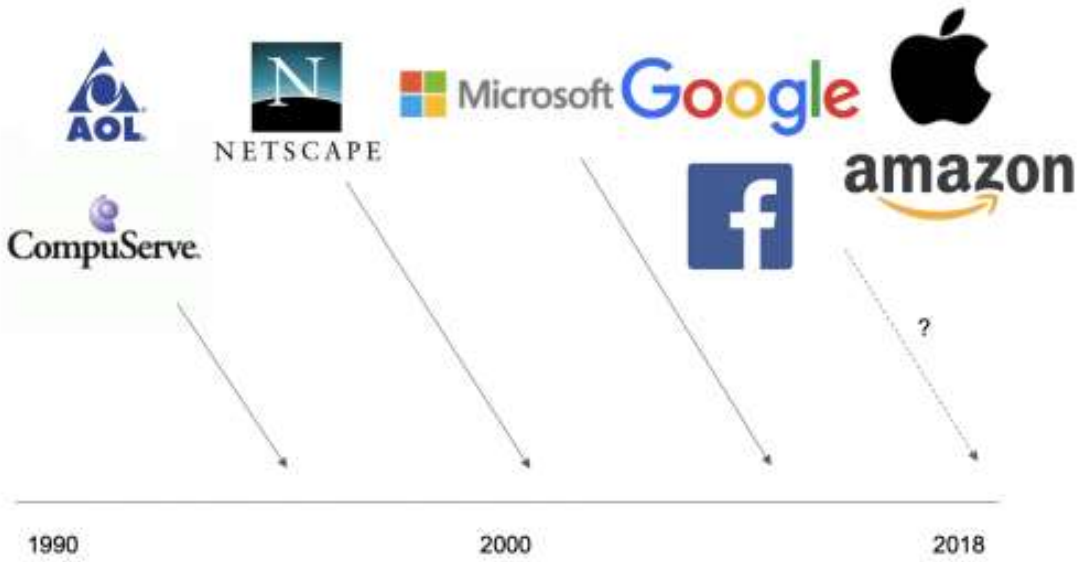
Verge

Factom

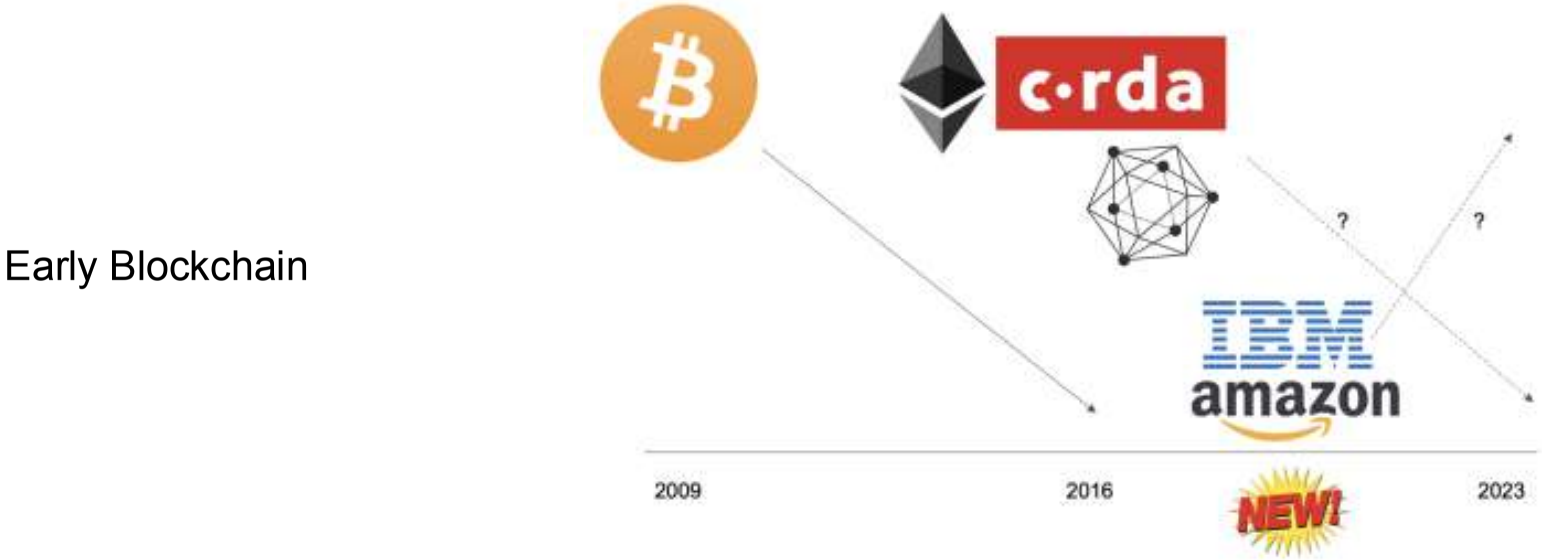
DigixDAO

Walton

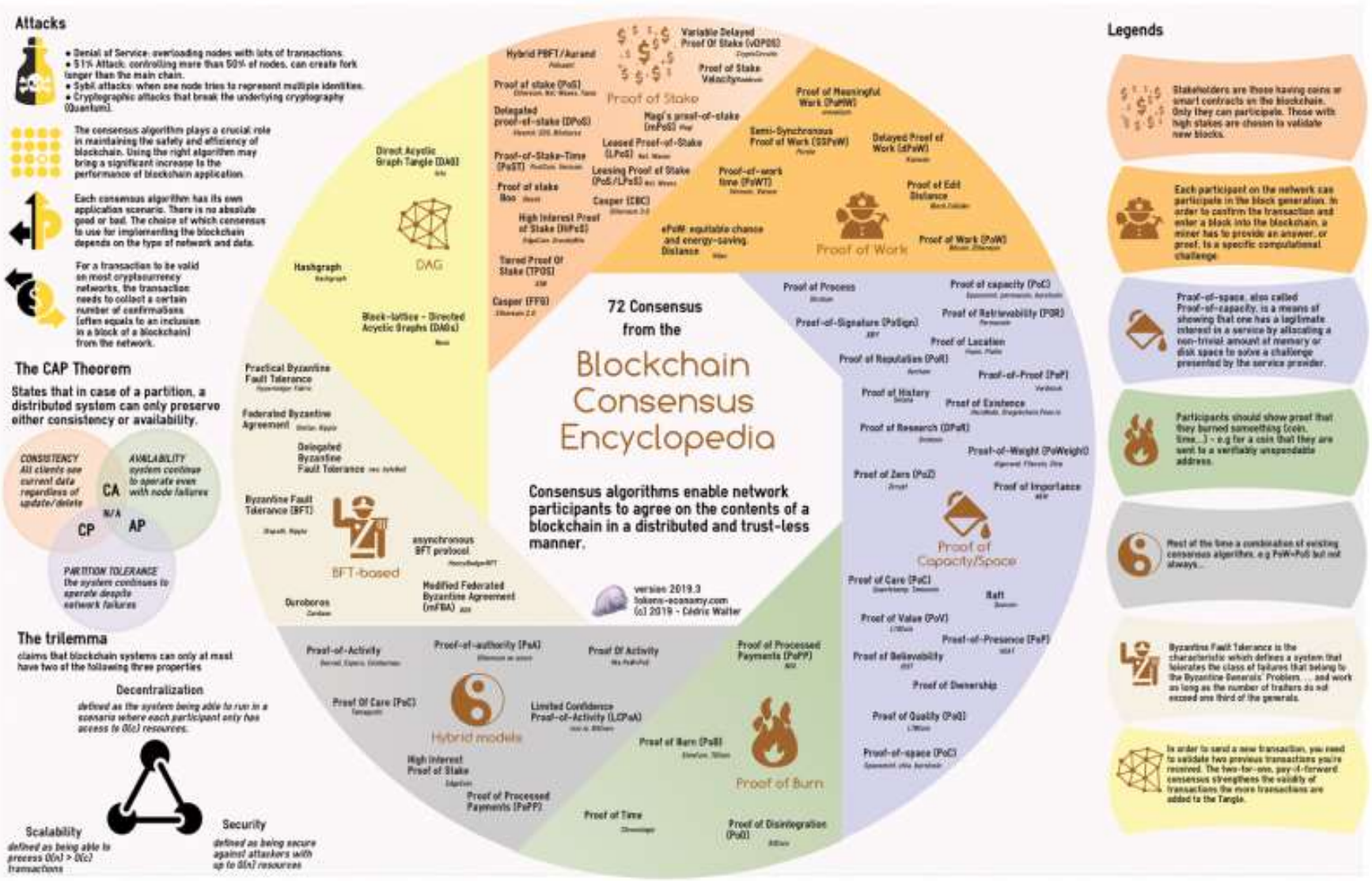
SALT

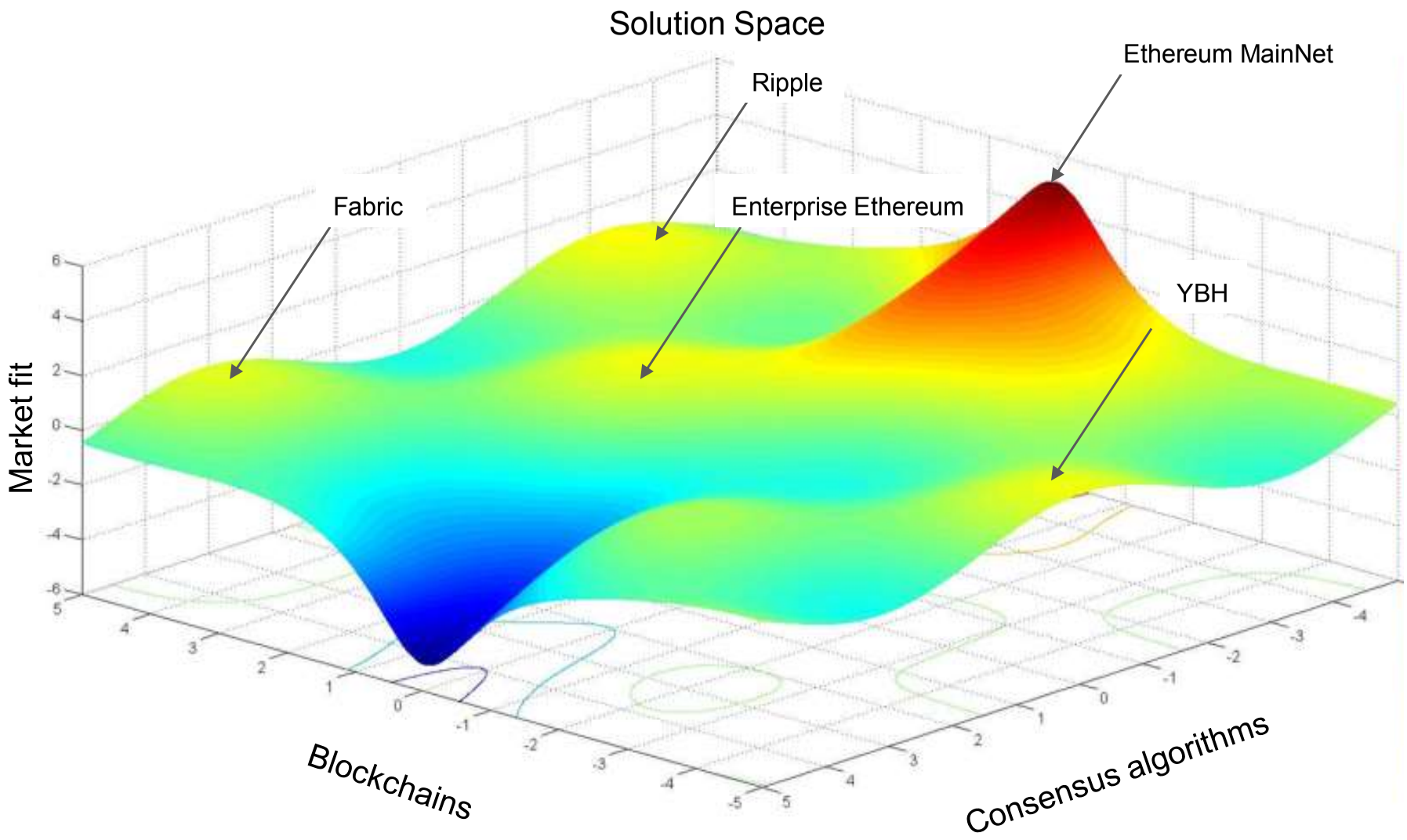


Early Web



Early Blockchain


Attacks
• Denial of Service: overloading nodes with lots of transactions.
• 51% Attack: controlling more than 50% of nodes, can create fork longer than the main chain.
• Sybil attacks: when one node tries to represent multiple identities.
• Cryptographic attacks that break the underlying cryptography (Quantum).
The consensus algorithm plays a crucial role in maintaining the safety and efficiency of blockchain. Using the right algorithm may bring a significant increase to the performance of blockchain application.
Each consensus algorithm has its own application scenario. There is no absolute good or bad. The choice of which consensus to use for implementing the blockchain depends on the type of network and data.
For a transaction to be valid on most cryptocurrency networks, the transaction needs to collect a certain number of confirmations (often equals to an inclusion in a block of a blockchain) from the network.
The CAP Theorem
States that in case of a partition, a distributed system can only preserve either consistency or availability.
CONSISTENCY
All clients see current data regardless of update/delete
AVAILABILITY
system continue to operate even with node failures
CA
N/A
CP
AP
PARTITION TOLERANCE
the system continues to operate despite network failures
The trilemma
claims that blockchain systems can only at most have two of the following three properties
Decentralization
defined as the system being able to run in a scenario where each participant only has access to O(c) resources.
Scalability
defined as being able to process O(n) > O(c) transactions
Security
defined as being secure against attackers with up to O(n) resources
72 Consensus from the
Blockchain Consensus Encyclopedia
Consensus algorithms enable network participants to agree on the contents of a blockchain in a distributed and trust-less manner.
version 2019.3
tokens-economy.com
(c) 2019 - Cédric Walter
Proof of Stake
Variable Delayed Proof Of Stake (vDPOS)
Hybrid PBFT/Aurand
Proof of Stake Velocity
Proof of stake (PoS)
Delegated proof-of-stake (DPoS)
Mapl's proof-of-stake (mPoS)
Leased Proof-of-Stake (LPoS)
Proof-of-Stake-Time (PoST)
Leasing Proof of Stake (PoS/LPoS)
Proof of stake Boo
Casper (CBC)
High Interest Proof of Stake (HiPoS)
ePoW: equitable chance and energy-saving Distance
Tarred Proof Of Stake (TPOS)
Casper (FFG)
Proof of Work
Proof of Meaningful Work (PoMW)
Semi-Synchronous Proof of Work (SSPoW)
Delayed Proof of Work (dPoW)
Proof-of-work time (PoWT)
Proof of Edit Distance
Proof of Work (PoW)
DAG
Direct Acyclic Graph Tangle (DAG)
Hashgraph
Block-lattice - Directed Acyclic Graphs (DAGs)
BFT-based
Practical Byzantine Fault Tolerance
Federated Byzantine Agreement
Delegated Byzantine Fault Tolerance
Byzantine Fault Tolerance (BFT)
asynchronous BFT protocol
Modified Federated Byzantine Agreement (mFBA)
Ouroboros
Proof of Capacity/Space
Proof of Process
Proof of capacity (PoC)
Proof-of-Signature (PoSign)
Proof of Retrievability (PoR)
Proof of Location
Proof of Reputation (PoR)
Proof-of-Proof (PoP)
Proof of History
Proof of Existence
Proof of Research (DPoR)
Proof-of-Weight (PoWeight)
Proof of Zero (PoZ)
Proof of Importance
Proof of Care (PoC)
Raft
Proof of Value (PoV)
Proof-of-Presence (PoP)
Proof of Believability
Proof of Ownership
Proof of Quality (PoQ)
Proof-of-space (PoC)
Hybrid models
Proof-of-Activity
Proof-of-authority (PoA)
Proof Of Activity
Proof Of Care (PoC)
Limited Confidence Proof-of-Activity (LCPoA)
High Interest Proof of Stake
Proof of Processed Payments (PoPP)
Proof of Time
Proof of Processed Payments (PoPP)
Proof of Burn
Proof of Burn (PoB)
Proof of Disintegration (PoD)
Legends
Stakeholders are those having coins or smart contracts on the blockchain. Only they can participate. Those with high stakes are chosen to validate new blocks.
Each participant on the network can participate in the block generation. In order to confirm the transaction and enter a block into the blockchain, a miner has to provide an answer, or proof, to a specific computational challenge
Proof-of-space, also called Proof-of-capacity, is a means of showing that one has a legitimate interest in a service by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.
Participants should show proof that they burned something (coin, time,...) - e.g for a coin that they are sent to a verifiably unspendable address.
Most of the time a combination of existing consensus algorithm. e.g PoW+PoS but not always...
Byzantine Fault Tolerance is the characteristic which defines a system that tolerates the class of failures that belong to the Byzantine Generals' Problem. ... and work as long as the number of traitors do not exceed one third of the generals.
In order to send a new transaction, you need to validate two previous transactions you're received. The two-for-one, pay-it-forward consensus strengthens the validity of transactions the more transactions are added to the Tangle.


Solution Space
Ethereum MainNet
Ripple
Fabric
Enterprise Ethereum
YBH
Market fit
Blockchains
Consensus algorithms

On Certainty

- Transaction certainty
  - certainty about whether and under what circumstances agreement has taken place between participants.
- Semantic certainty
  - certainty that the meaning is the same for all participants

After von Wendland 2018

1st LDDL

- “A web of blockchains”
- Indexing blockchains for query
- Adding metadata to transactions

2nd LDDL

- EthOn
- Flowchain
- Temporal streaming of graph data
- Semantic Descriptors for Smart Contracts

3rd LDDL

- Architectures for interoperability
- GraphChain, a native RDF blockchain
- Proof of Trust
- A cryptocurrency to incentivise peer review

1st LDDL

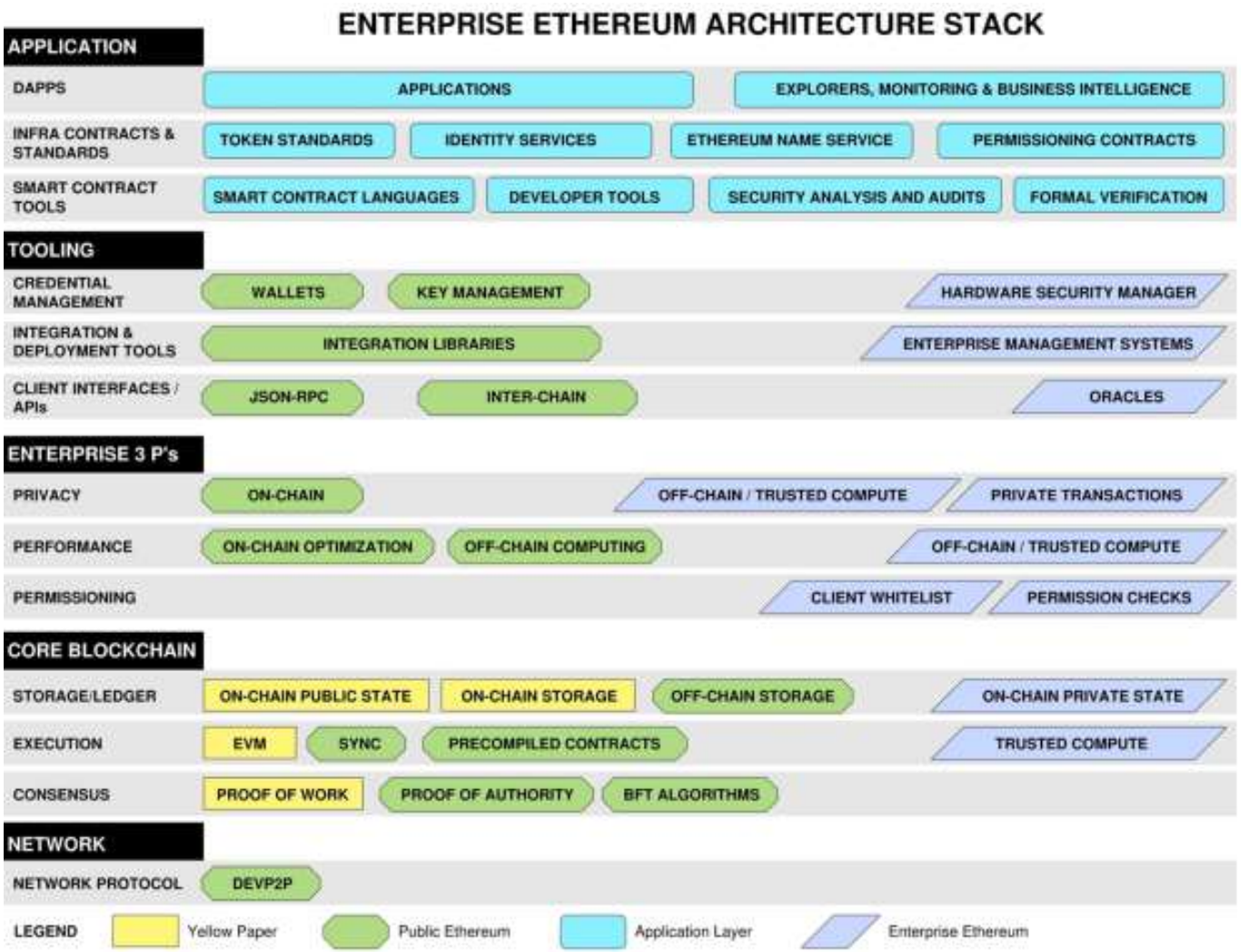
- **“A web of blockchains”**
- Indexing blockchains for query
- **Adding metadata to transactions**

2nd LDDL

- EthOn
- Flowchain
- Temporal streaming of graph data
- **Semantic Descriptors** for Smart Contracts

3rd LDDL

- Architectures for **interoperability**
- GraphChain, a native RDF blockchain
- Proof of Trust
- A cryptocurrency to incentivise peer review



Adding metadata to transactions

EthOn

"Pinning" state of digital resources

A web of blockchains

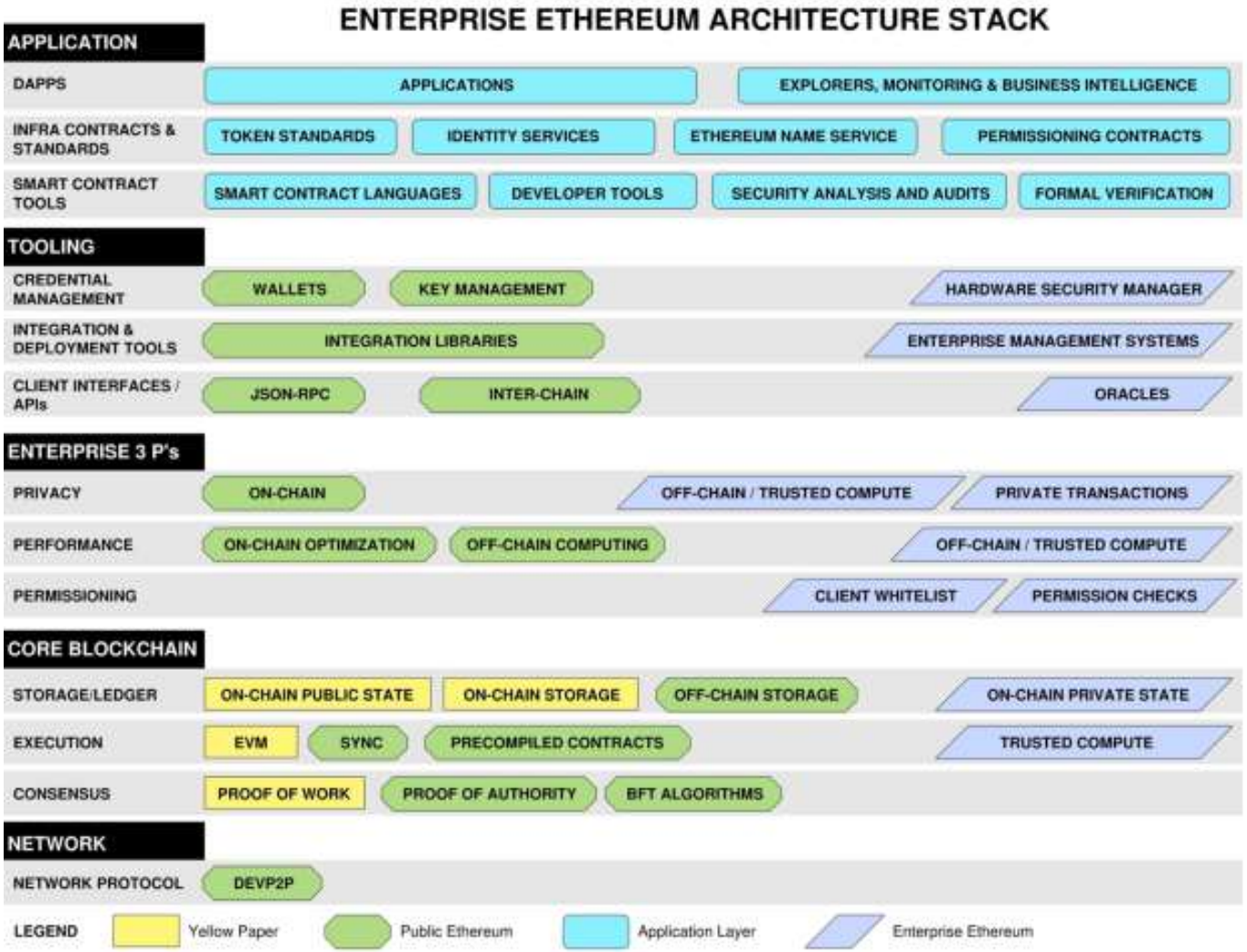
Architectures for interoperability

Semantic descriptors for smart contracts

Indexing for query

New blockchain

New consensus protocol



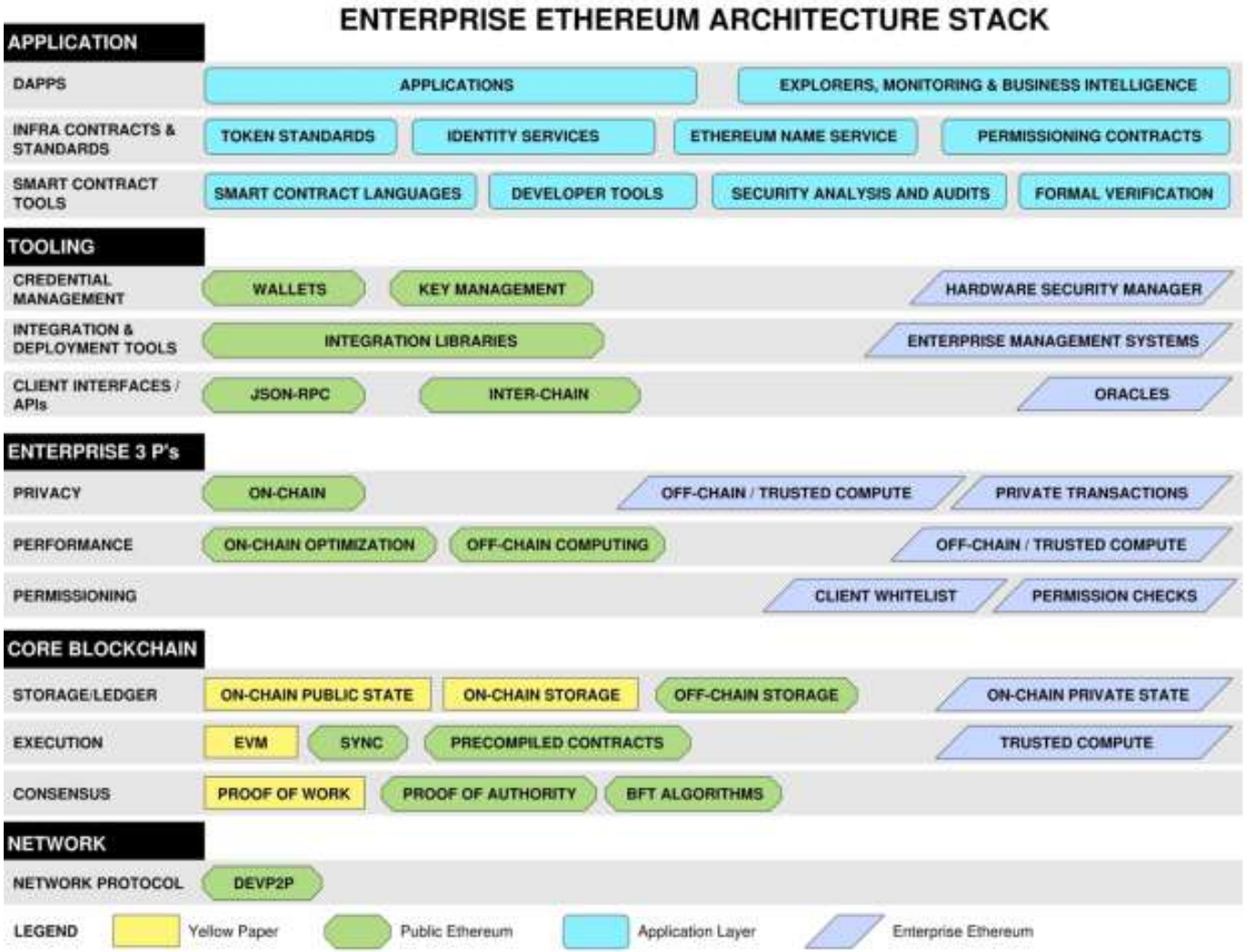
All Yellow Paper, Public Ethereum, and Application Layer components may be extended for Enterprise Ethereum as required.

Metadata additions

Interoperability

Semantic search

Distributed computing research



Metadata additions

Interoperability

Semantic search

Distributed computing research

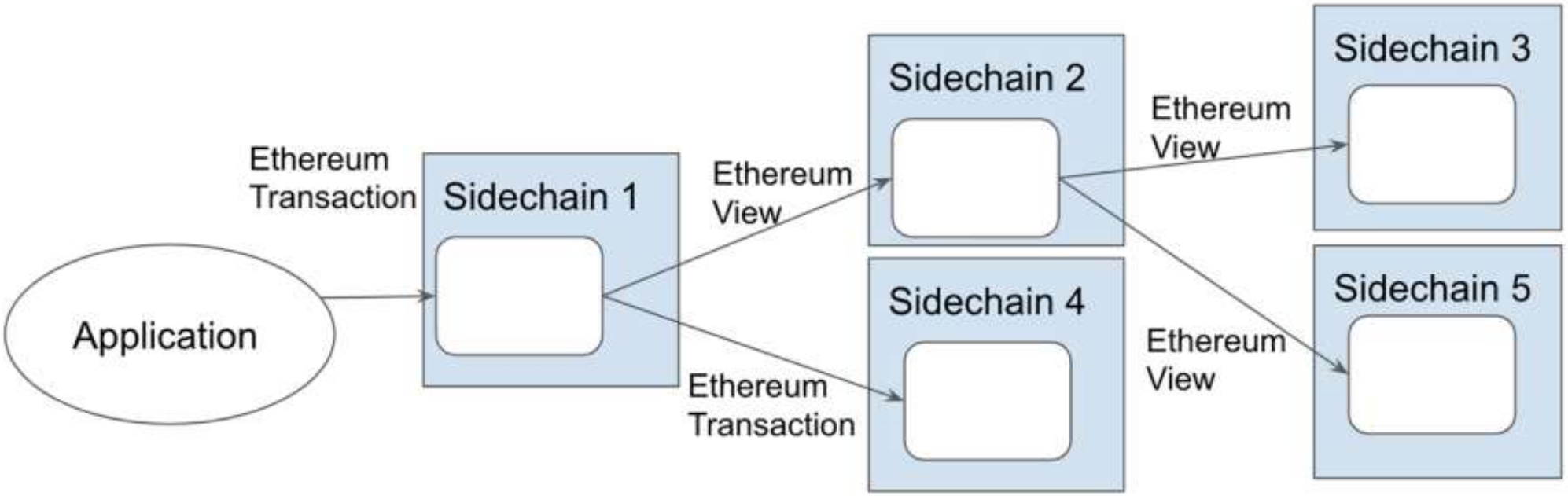
The Web Ledger Protocol

Interledger

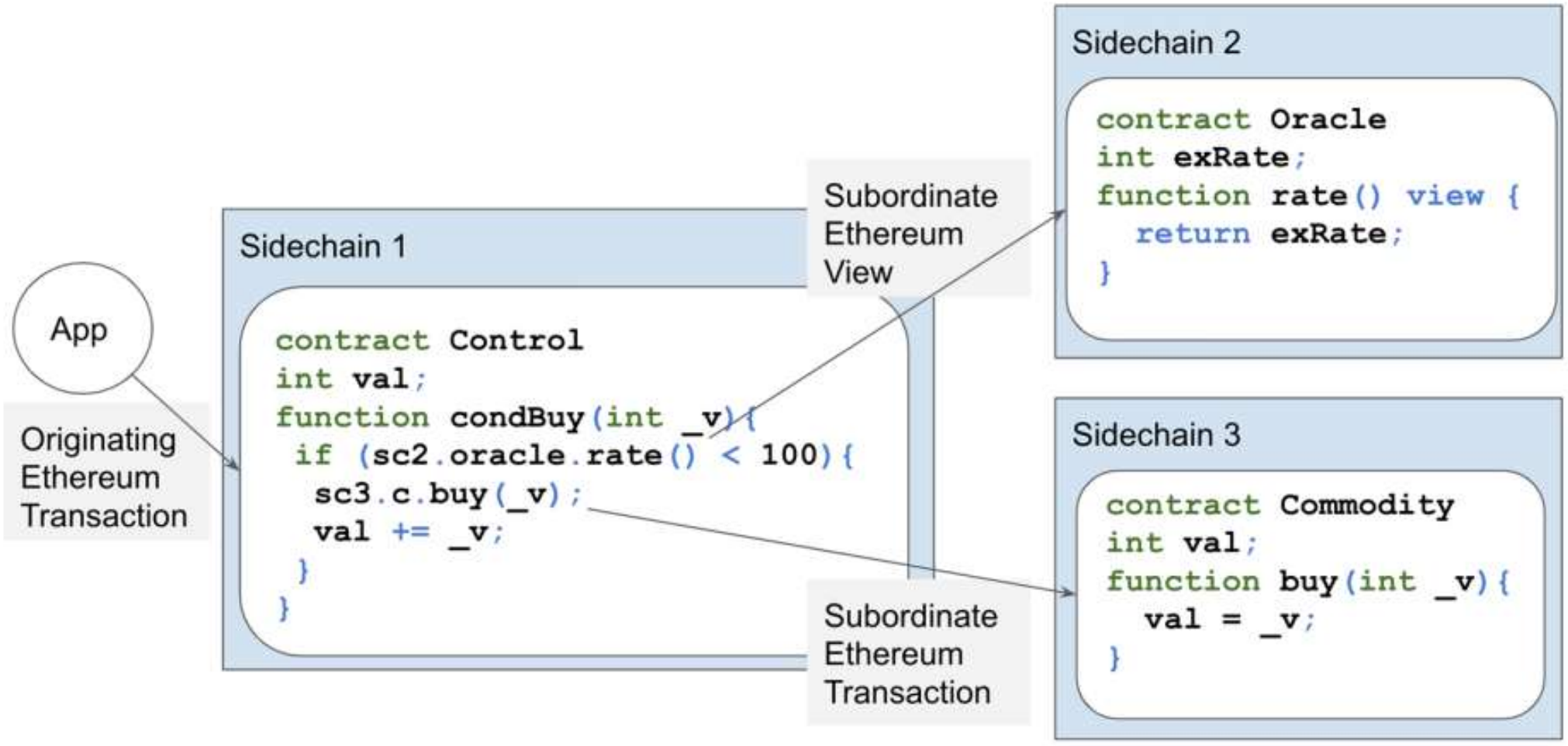
ENTERPRISE
ETHEREUM
ALLIANCE

Atomic Crosschain Transactions for Ethereum Private Sidechains

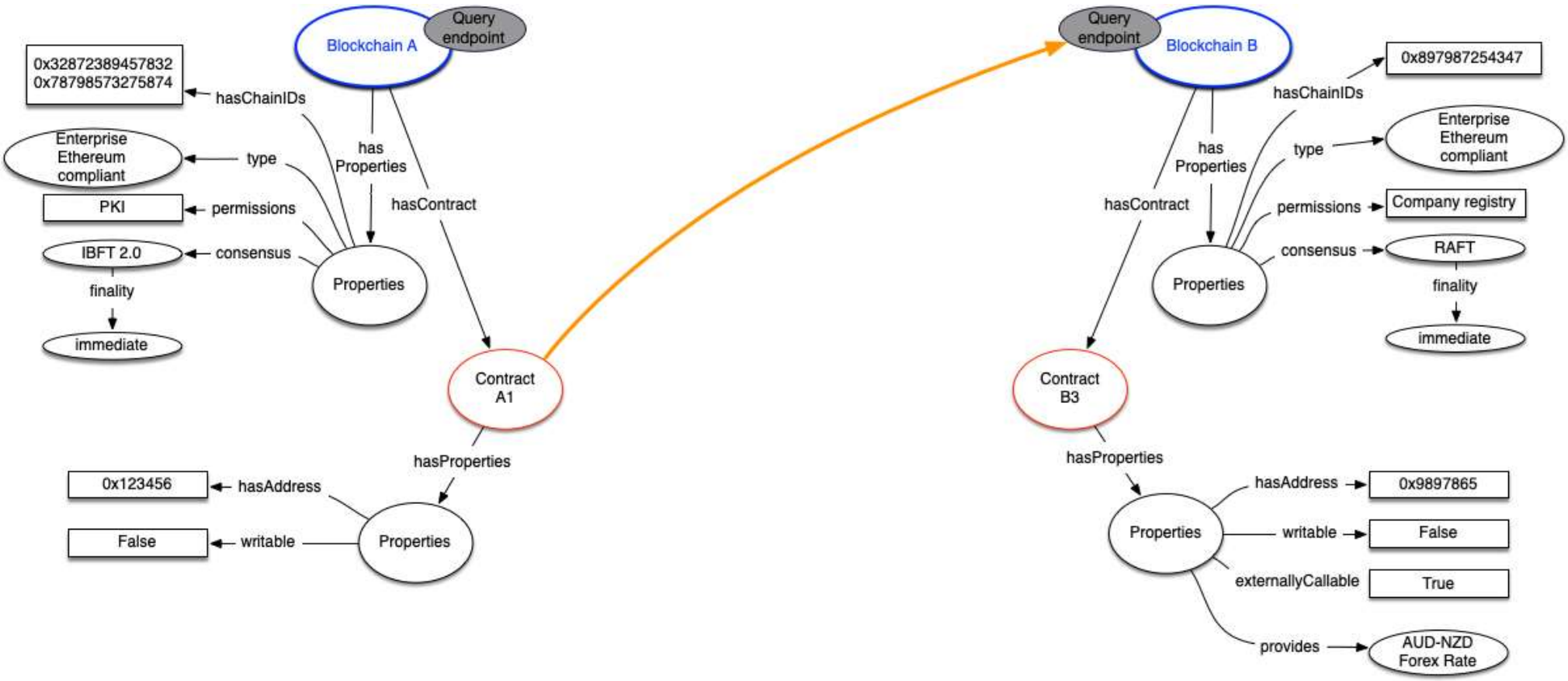
Crosschain contract transactions

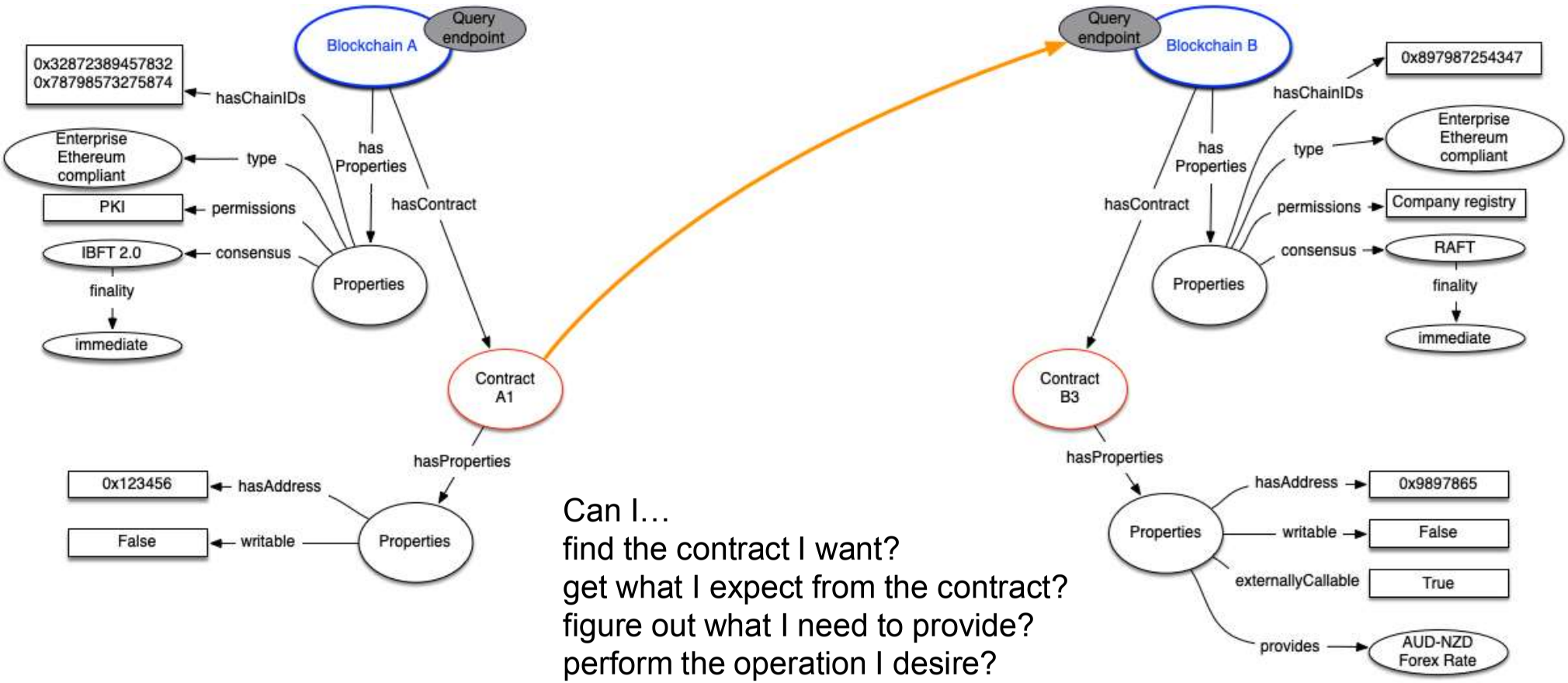


Peter Robinson, David Hyland-Wood, Roberto Saltini, Sandra Johnson, John Brainard. Atomic Crosschain Transactions for Ethereum Private Sidechains, ArXiv preprint, arXiv:1904.12079v2, 3 May 2019, v2.



Peter Robinson, David Hyland-Wood, Roberto Saltini, Sandra Johnson, John Brainard. Atomic Crosschain Transactions for Ethereum Private Sidechains, ArXiv preprint, arXiv:1904.12079v2, 3 May 2019, v2.


Blockchain A
Query endpoint
0x32872389457832
0x78798573275874
hasChainIDs
Enterprise Ethereum compliant
type
PKI
permissions
IBFT 2.0
consensus
finality
immediate
has Properties
Properties
hasContract
Contract A1
hasProperties
0x123456
hasAddress
False
writable
Properties
Blockchain B
Query endpoint
0x897987254347
hasChainIDs
Enterprise Ethereum compliant
type
has Properties
hasContract
permissions
Company registry
consensus
RAFT
Properties
finality
immediate
Contract B3
hasProperties
Properties
hasAddress
0x9897865
writable
False
externallyCallable
True
provides
AUD-NZD Forex Rate



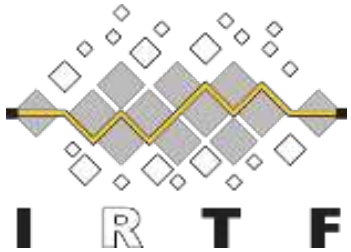
Can I…
find the contract I want?
get what I expect from the contract?
figure out what I need to provide?
perform the operation I desire?
etc.

(David) Wheeler's Law

All problems in computer science can be solved by another level of indirection

(David) Wheeler's Law

All problems in computer science can be solved by another level of indirection, but that will usually create another problem.

Producing standards	 
Talking a lot	
Talking a bit	 

References and Credits

- Marcelle von Wendland. “Semantic Blockchain - A Review of Sematic Blockcghain and Distributed Ledger Technology Approaches (DLT)” (sic). ResearchGate preprint, April 2018, https://www.researchgate.net/publication/324706165, DOI: 10.13140/RG.2.2.33005.90088 (sic)
- Blockchain Consensus Encyclopedia graphic by Nick Youngson, CC BY-SA 3.0, https://tokens-economy.gitbook.io/consensus/
- Cryptocurrency logos courtesy of Designmodo, https://designmodo.com/wp-content/uploads/2018/01/6-Top-100-cryptocurrency-icons.jpg
- W3C Semantic Web icons, W3C Document License, http://www.w3.org/2001/sw/
- Simple world map by Wikimedia user Tom-b, public domain, https://en.wikipedia.org/wiki/File:Simple_world_map.svg
- Interledger Protocol, https://interledger.org/
- Manu Sporny and Dave Longley. The Web Ledger Protocol 1.0, W3C Draft Community Group Report, 18 June 2019, https://w3c.github.io/web-ledger/
- Peter Robinson, David Hyland-Wood, Roberto Saltini, Sandra Johnson, John Brainard. Atomic Crosschain Transactions for Ethereum Private Sidechains, ArXiv preprint, arXiv:1904.12079v2, 3 May 2019, v2.
- EEA Architecture Stack, https://entethalliance.org/wp-content/uploads/2019/10/arc-stack-pdf.pdf
- Standards body logos © their respective owners.

Paths toward Semantic Blockchains

David Hyland-Wood

PEGASYS

BlockSW 2019
Blockchain enabled Semantic Web Workshop
October 27, 2019

http://w3id.org/people/prototypo/talks/BlockSW2019