Distributed Ledger Technologies Ecosystem Mapping

In development of a tool for (i) assessing relevance of DLTs to address UNFCCC needs & for (ii) identifying innovative applications

Research Conducted by Marc Johnson
& Patrick Medenou

July-August 2018

Distributed Ledger Technologies

“Distributed Ledger Technology is 'a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions'...essentially an asset database that can be shared across a network of multiple sites, geographies or institutions.”

➔ Matthew Hancock, UK Government Chief Scientific Adviser

Distributed Ledger Technology is a combination of existing technologies & schools of thought at the crossroads of:

- Computer Networking & Data Transmission
- Game Theory
- Cryptography
- Mechanism Design
- Economic & Monetary Theory

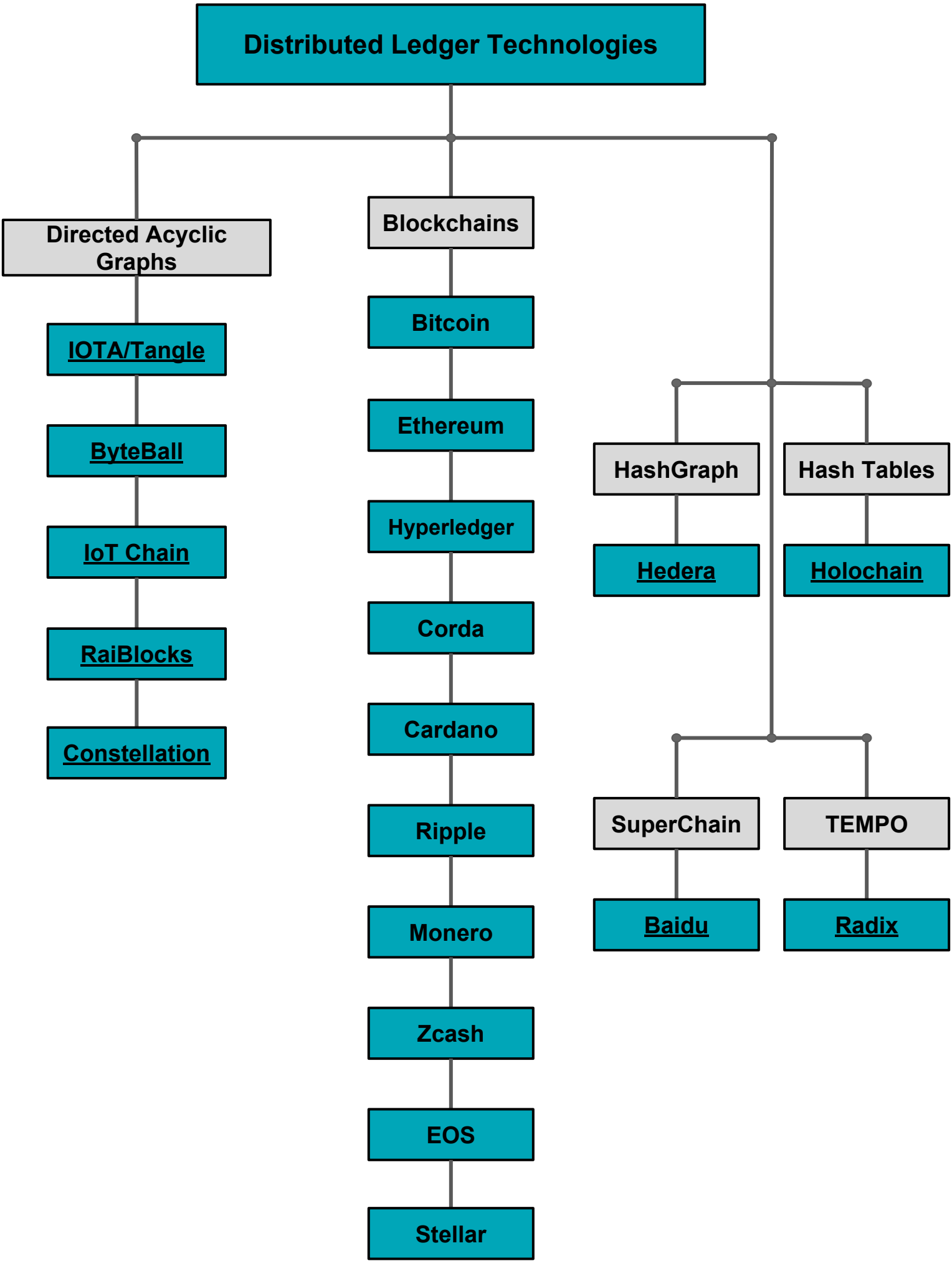
The core Features of DLTs include:

- Append-Only Sequential Data Structure
- Cryptographically Secured
- Distributed
- Cannot be Easily Altered Retroactively
- ‘Trust Machine’

There are multiple different forms of Distributed Ledger Technologies, such as:

- Blockchains
- Alternative Directed Acyclic Graphs
- Hash Graphs
- Distributed Hash Tables

DLT is a form of record keeping, secured by cryptography, and maintained by a network of computers.


Distributed Ledger Technologies
Directed Acyclic Graphs
IOTA/Tangle
ByteBall
IoT Chain
RaiBlocks
Constellation
Blockchains
Bitcoin
Ethereum
Hyperledger
Corda
Cardano
Ripple
Monero
Zcash
EOS
Stellar
HashGraph
Hedera
Hash Tables
Holochain
SuperChain
Baidu
TEMPO
Radix

Blockchain

A blockchain is a specific type of Distributed Ledger Technology. By definition, it is a distributed database of transactions whose complete history can be accessed and maintained by each member of the network. Features Include:

- Append-Only Sequential Data Structure
- Cryptographically Secured
- Distributed
- Cannot be Easily Altered Retroactively
- Blocks of Transactions

Due to these unique features, it can be said that a blockchain is a form of record keeping, secured by cryptography, and maintained by a network of computers. Essentially, a blockchain is a way of structuring data by forming and linking blocks of cryptographically signed and time-stamped transaction data.

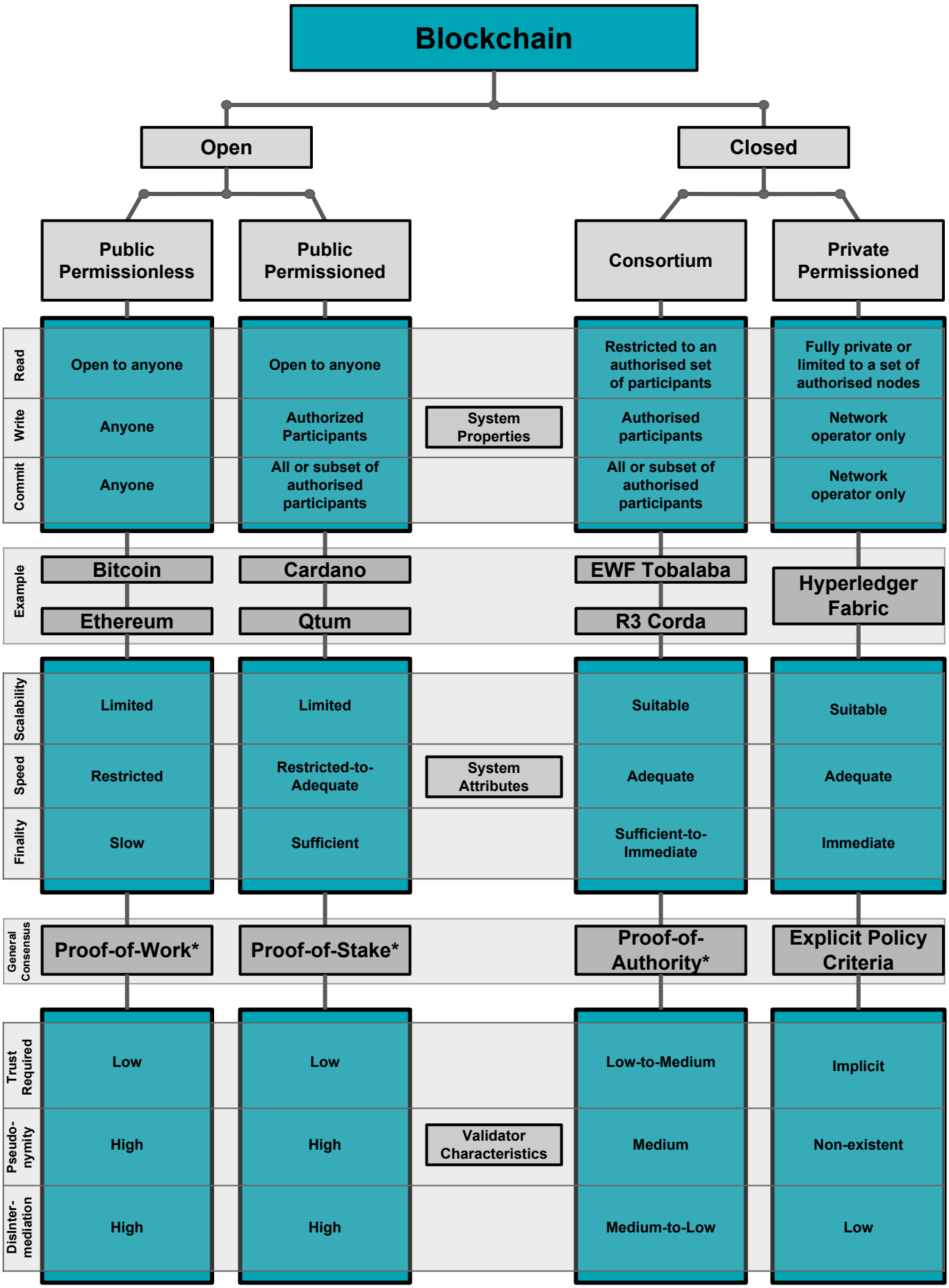
- Each block typically contains a cryptographic hash of the previous block, a timestamp, and transaction data which is inherently resistant to modification of the data.

- Some utilize '***Smart Contracts***', which refers to transactional terms and conditions embedded in computer code which allow automatic execution of the relevant transaction once precise conformity with those terms and conditions has been established.

- '***Mining***' a *cryptocurrency* means doing complex mathematical calculations to verify each transaction on the ledger. By doing so, the miner gets a financial reward in the form of the cryptocurrency in question, and in the amount agreed upon by the consensus protocol.

Since the technologies inception in 2008, blockchain has evolved in many directions. There are four main categories that blockchains can be split into. Open (Public), Closed (Private), Permissionless, and Permissioned. Each one of these categories describes the level of 'trust' required by parties involved in transactions.

As an example, Bitcoin is a 'permissionless' blockchain, meaning that anyone can read the data and become part of the network, or act as a transaction validator. Permissionless blockchains like Bitcoin represent the most decentralised form of blockchains, but blockchains can also be useful for a more limited set of actors. 'Permissioned' blockchains restrict access in some way, for instance only to a certain set of registered participants or validators. A prime example of this is the Energy Web Foundations Tobalaba network.



*Generalization. Not employed by all blockchains of this type.

Directed Acyclic Graphs

Directed Acyclic Graphs (DAGs) are a complex data architecture that are a completely different data structure from Blockchains, where transactions are not sequentially ordered, per say, but transactions do flow in same direction. In DAGs, transactions are linked to multiple previous transactions, and in order for a new transaction to be verified, the individual trying to submit a transaction must verify a number of previous transactions.

DAGs usually employ the heaviest-chain consensus mechanism, confirming a new deal through transaction weight and partial consensus among nodes, which binds proof of work with each deal efficiently. In theory, this form of consensus not only solves the current problem of centralization of Bitcoin's mining but also greatly improves the whole distributed networks throughput capacity, thereby lowering, or eliminating, the transaction costs.

With the rapid growth of IoT (Internet of Things), the demand for micropayments is expected to increase exponentially. Blockchain consensus mechanisms and smart contract architectures currently cannot scale to a level that is required for consumer grade IoT applications to function efficiently.

Directed Acyclic Graphs provide solutions to these problems in the following ways:

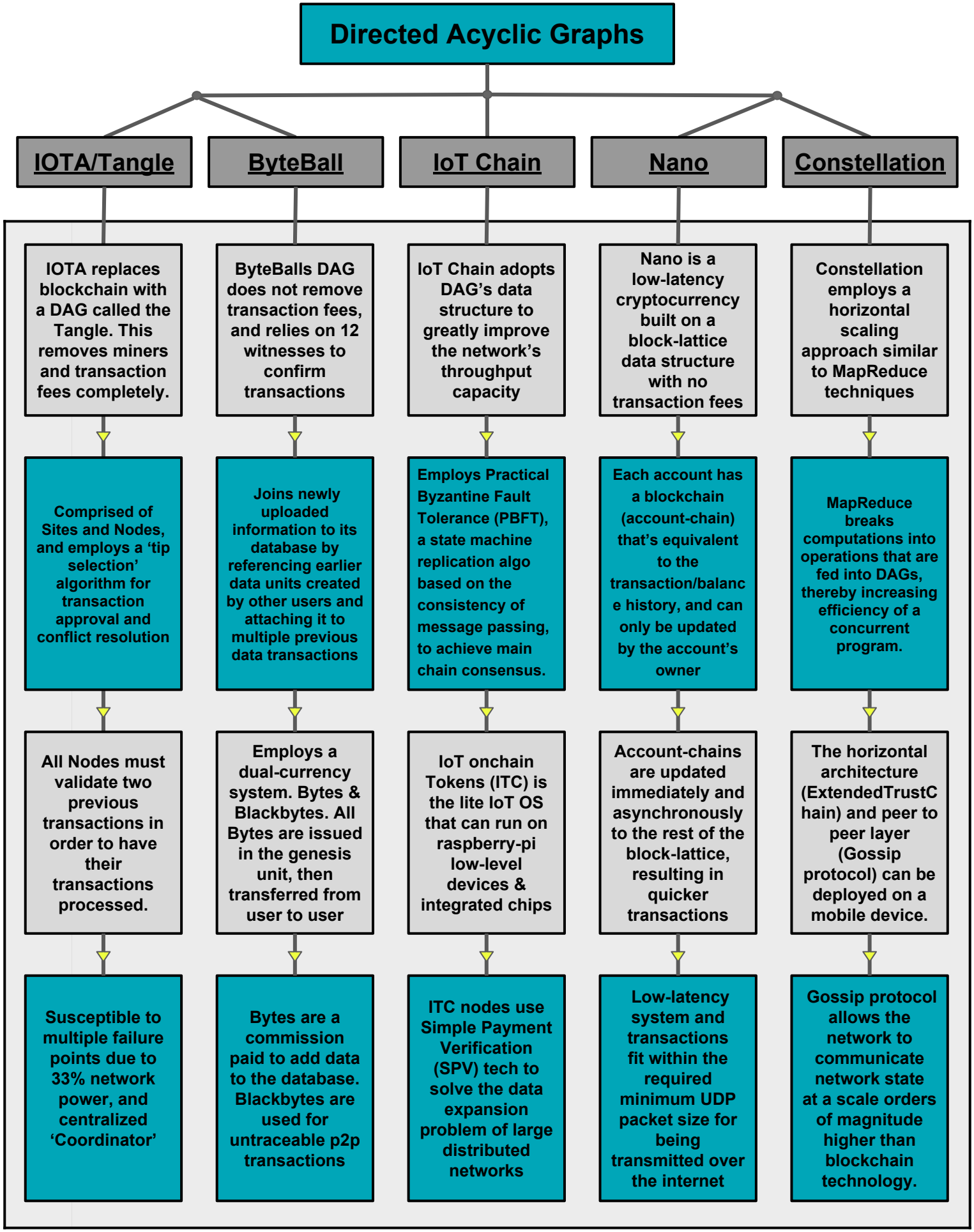
- **Instant Confirmation**: DAG technology allows a transaction to get confirmation from peers almost instantaneously because the system doesn't rely on miners to verify transactions.

- **Transaction Finality**: DAG systems theoretically allow definite transaction completion alerts. This is unlike Bitcoin where the number of confirmations can be used to calculate only the probability that the transaction completed.

- **Lower Energy Burden**: DAGs theoretically require significantly less energy to keep their networks working and secure than proof of work cryptocurrencies.

Many DAGs utilize a structure that employs little or no transaction fees, however, they are susceptible to multiple points of failure due to lower threshold to gain outstanding share of network power (33%).

Although widely scrutinized, and ripe with problems, there is great hope that DAGs will become the basic data structure for the next generation of blockchains.


Directed Acyclic Graphs
IOTA/Tangle
ByteBall
IoT Chain
Nano
Constellation
Core Features
IOTA replaces blockchain with a DAG called the Tangle. This removes miners and transaction fees completely.
ByteBalls DAG does not remove transaction fees, and relies on 12 witnesses to confirm transactions
IoT Chain adopts DAG's data structure to greatly improve the network's throughput capacity
Nano is a low-latency cryptocurrency built on a block-lattice data structure with no transaction fees
Constellation employs a horizontal scaling approach similar to MapReduce techniques
Comprised of Sites and Nodes, and employs a 'tip selection' algorithm for transaction approval and conflict resolution
Joins newly uploaded information to its database by referencing earlier data units created by other users and attaching it to multiple previous data transactions
Employs Practical Byzantine Fault Tolerance (PBFT), a state machine replication algo based on the consistency of message passing, to achieve main chain consensus.
Each account has a blockchain (account-chain) that's equivalent to the transaction/balance history, and can only be updated by the account's owner
MapReduce breaks computations into operations that are fed into DAGs, thereby increasing efficiency of a concurrent program.
All Nodes must validate two previous transactions in order to have their transactions processed.
Employs a dual-currency system. Bytes & Blackbytes. All Bytes are issued in the genesis unit, then transferred from user to user
IoT onchain Tokens (ITC) is the lite IoT OS that can run on raspberry-pi low-level devices & integrated chips
Account-chains are updated immediately and asynchronously to the rest of the block-lattice, resulting in quicker transactions
The horizontal architecture (ExtendedTrustChain) and peer to peer layer (Gossip protocol) can be deployed on a mobile device.
Susceptible to multiple failure points due to 33% network power, and centralized 'Coordinator'
Bytes are a commission paid to add data to the database. Blackbytes are used for untraceable p2p transactions
ITC nodes use Simple Payment Verification (SPV) tech to solve the data expansion problem of large distributed networks
Low-latency system and transactions fit within the required minimum UDP packet size for being transmitted over the internet
Gossip protocol allows the network to communicate network state at a scale orders of magnitude higher than blockchain technology.

Smart Contracts

Smart Contracts are a set of computer protocols intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. The aim of smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting.

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman. Smart contracts work on the If-Then premise, and afford the user a number of benefits, including:

- **Autonomy**: You're the one making the agreement; there's no need to rely on a broker, lawyer or other intermediaries to confirm. Incidentally, this also knocks out the danger of manipulation by a third party, since execution is managed automatically by the network, rather than by one or more, possibly biased, individuals who may err.

- **Trust**: Your documents are encrypted on a shared ledger. There's no way that someone can say they lost it.

- **Backup**: Imagine if your bank lost your savings account. On the blockchain, each and every one of your friends has your back. Your documents are duplicated many times over.

- **Safety**: Cryptography, the encryption of websites, keeps documents safe. This limits hacking, as it would take a significant amount of time & resources to infiltrate.

- **Speed**: Smart contracts use software code to automate tasks, thereby time on a range of business processes that you'd ordinarily have to perform manually.

- **Savings**: Smart contracts disintermediate processes, save you money in the process.

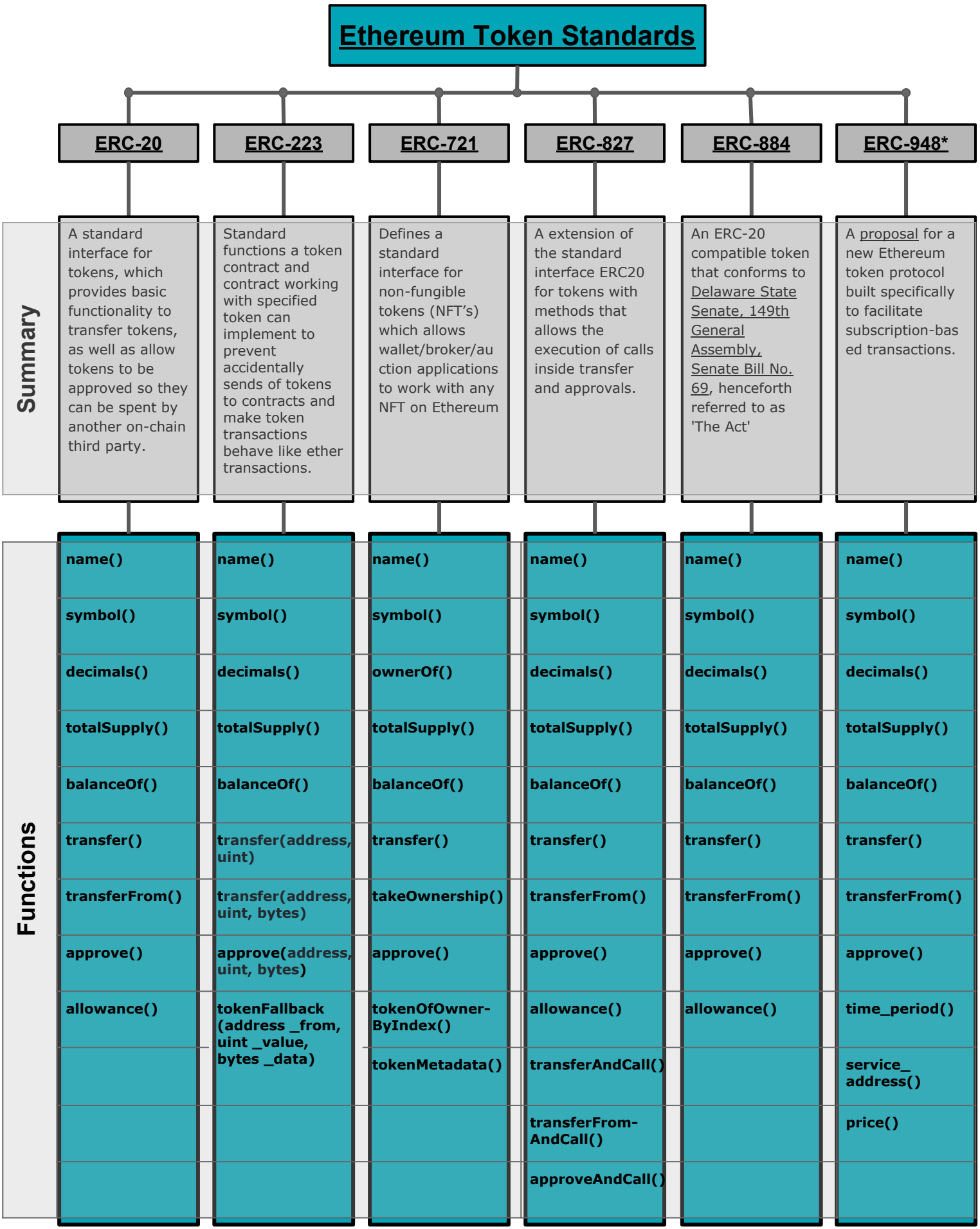
- **Accuracy**: Automated contracts are not only faster and cheaper but also avoid the errors that may arise from manually filling out forms.

"The potential for [smart contracts] to alter aspects of society is of significant magnitude. This is something that would provide a technical basis for all sorts of social changes, and I find that exciting."

- Ethereum CTO, Gavin Wood

Although many DLT platforms claim to have smart contract functionality, the Ethereum ecosystem is the obvious leader in the space, as can be seen from their ever-expanding Ethereum Improvement Proposal ERC repository. With more than 100 Improvement Proposals and Token Standards, Ethereum has the most robust smart contract standards library.

Ethereum Token Standards



*Proposal for a subscription-based token

Zero-Knowledge Proofs

Zero-knowledge proofs are a method by which one party (the prover) can prove to another party (the verifier) that she knows a value x, without conveying any information apart from the fact that she knows the value x.

ZK Proofs let you validate the truth of something without revealing how you know that truth. To qualify as zero-knowledge,protocols embedded programmatically in digital systems must satisfy three requirements:

1. **Completeness**: If the statement is true, an honest verifier will be convinced by an honest prover.
2. **Soundness**: If the statement is false, no cheating prover can convince an honest verifier that it is true.
3. **Zero-knowledge**: If the statement is true, no cheating verifier learns anything other than the fact that the statement is true.

For Ethereum specifically, the issues of data privacy and confidentiality were addressed in its Byzantium upgrade via the zero-knowledge protocol in zkSnarks. As explained by Ethereum's Christian Reitwiessner: SNARKs are short for *succinct non-interactive arguments of knowledge* …The individual parts of the acronym have the following meaning:

1. **Succinct**: The sizes of the messages are very small in comparison to the length of the actual computation.

2. **Non-interactive**: There is no or only little interaction. For zkSNARKs, there is usually a setup phase and after that a single message from the prover to the verifier. Additionally, SNARKs often have the so-called "public verifier" property, meaning anyone can verify without interacting anew, which is important for blockchains.

3. **ARguments**: The verifier is only protected against computationally limited provers. Provers with enough computational power can create arguments about wrong statements (note that with enough computational power, any public-key encryption can be broken). This is also called "computational soundness" as opposed to "perfect soundness."

4. **of Knowledge**: It is not possible for the prover to construct a proof/argument without knowing a certain so-called witness (for example the address she wants to spend from, the preimage of a hash function, or the path to a certain node).

In essence, Zk Proofs allow parties to exchange information while provably revealing no information beyond the single bit of information corresponding to 'this statement is true'. The identity and amount being spent can remain hidden, and problems such as "front-running" can be avoided. ZK protocols provide the ability to transfer assets across a distributed, peer-to-peer blockchain network with secrecy.

Complementary Technologies

“Ultimately it will be the combination of artificial intelligence, IoT and blockchain that will prove most interesting across industries and in myriad possible IoT applications”

➔ Dan Bieler, Forrester Research

IoT & Remote Sensors:

It is widely accepted that distributed systems must play a role in how devices communicate directly between each other. A distributed ledger, and more specifically blockchain architectures, are designed to act as the basis for applications that involve transactions and interactions.

Distributed Ledgers can act as the foundational data layer on which device audit trails are created, not just to record how the devices interact, but also potentially in which state they are and how they are ‘handled’ throughout a connected value-chain.

The inherent features of transparency and immutability, coupled with the enhanced feature of automating complex business logic through the utilization of smart contracts, provides the proper ingredients to improve compliance and cost-efficiency of IoT devices.

> *“Blockchain technology promises to be the missing link enabling peer-to-peer contractual behavior without any third party to “certify” the IoT transaction. It answers the challenge of scalability, single point of failure, time stamping, record, privacy, trust and reliability in a very consistent way.”*
>
> ➔ Nicolas Windpassinger, Digitize or Die

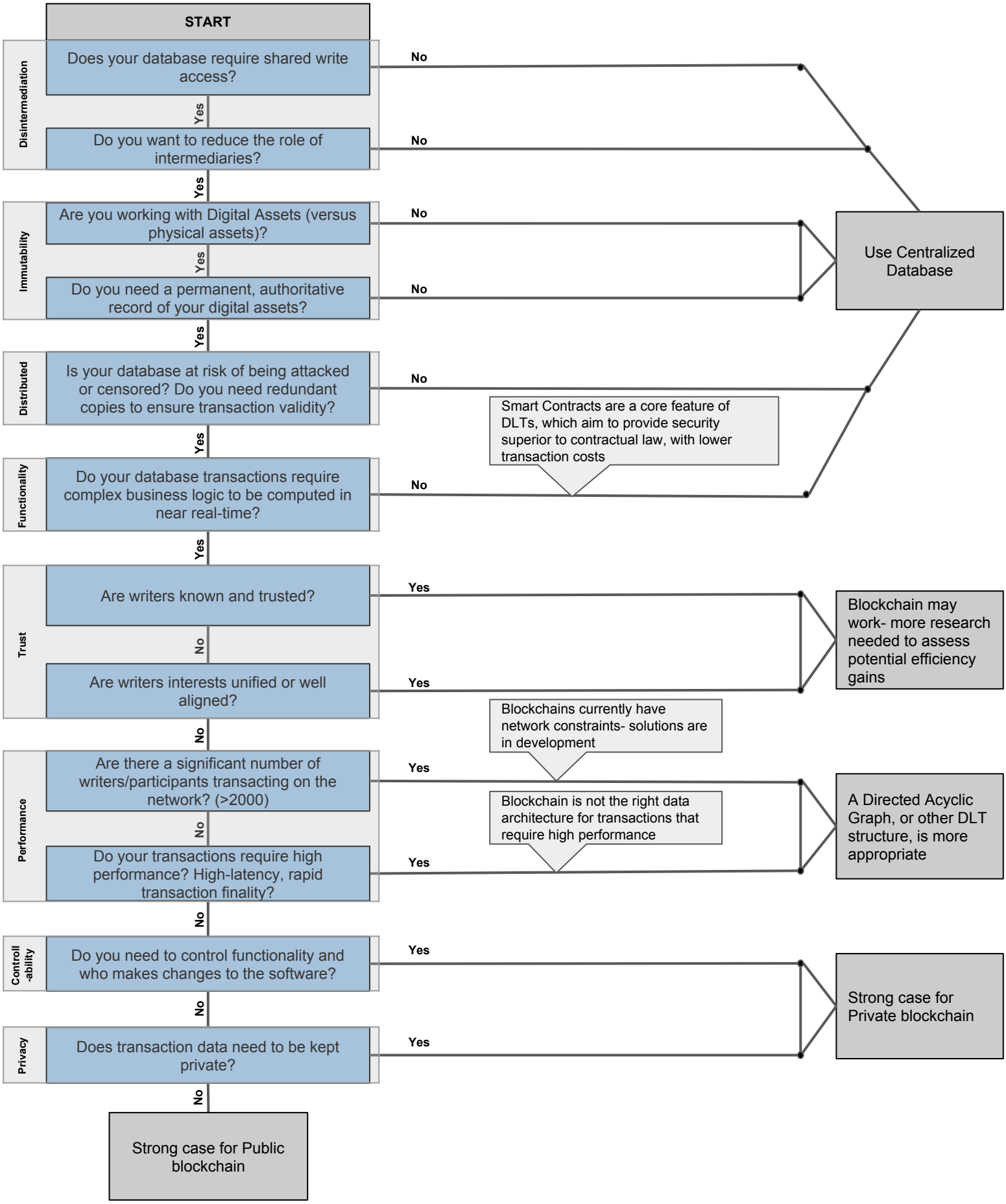
Machine Learning & Artificial Intelligence:

Artificial Intelligence and blockchain are the two major technologies that are catalyzing the pace of innovation and upending traditional business models in every industry.

Utilizing machine learning techniques, for unearthing indiscernible data trends, in combination with blockchain-based marketplaces, for ensuring data veracity & privacy, can create a "maximally longitudinal" view of an individual's online presence & preferences, and the multi-sided marketplace network effects from users, data providers, and data scientists can create self-reinforcing incentization systems.

> “Machine learning models trained on data from blockchain-based marketplaces have the potential to create the world’s most powerful artificial intelligences.”
>
> ➔ Fred Ehrsam, Co-founder Coinbase

Decision Tree to Assess the Appropriate Data Structure



References:

1. bitcoin.org/bitcoin.pdf
2. www.ethereum.org/foundation
3. www.hyperledger.org/
4. www.r3.com/
5. cardanodocs.com/introduction/
6. ripple.com/
7. getmonero.org/
8. z.cash/
9. eos.io/
10. energyweb.org/blockchain/
11. www.iota.org/
12. byteball.org/
13. iotchain.io/
14. raiblocks.net/
15. constellationlabs.io/
16. www.hederahashgraph.com/
17. holochain.org/
18. www.radixdlt.com/
19. www.ptdlgroup.org/
20. www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf
21. jjablog.com/tag/blockchain
22. www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#5cb23c180bc9
23. www.coinbureau.com/education/directed-acyclic-graphs-dags/
24. www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2223/RAND_RR2223.pdf
25. medium.com/basecs/spinning-around-in-cycles-with-directed-acyclic-graphs-a233496d4688
26. github.com/holochain/holochain-proto
27. steemit.com/steemit/@spiritualmax/blockchain-vs-hashgraph-vs-tangle-epic-tech-battles-of-history
28. www.mangoresearch.co/blockchain-vs-distributed-ledger-technology-dlt/
29. twitter.com/antgrasso/status/951363097188552704
30. blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/
31. workflowy.com/s/HjlY.oGzJASjh93
32. https://en.wikipedia.org/wiki/Directed_acyclic_graph
33. https://dispatchlabs.io/technology/
34. https://www.youtube.com/watch?v=LtWUJtnQbKs
35. https://www.daglabs.com/
36. https://www.reddit.com/r/Iota/comments/7jike6/negative_sides_of_iota_discussion/
37. https://www.reddit.com/r/ethereum/comments/72mf83/the_flaws_of_iota/
38. https://news.ycombinator.com/item?id=15944112
39. https://news.ycombinator.com/item?id=16457120
40. https://www.researchgate.net/publication/5761225_Lifestyle_variables_and_the_risk_of_myocardial_infarction_in_the_General_Practice_Research_Database/figures?lo=1
41. https://users.ics.aalto.fi/ntatti/papers/malmi15dag.pdf
42. https://www.quora.com/How-are-directed-acyclic-graphs-different-from-trees
43. https://www.researchgate.net/post/How_do_you_measure_the_difference_between_DAGs
44. https://arxiv.org/abs/1709.01007
45. https://medium.com/@hamzasurti/advanced-data-structures-part-1-directed-acyclic-graph-dag-c1d1145b5e5a
46. https://qtum.org/en
47. http://tangle.glumb.de/
48. https://tanglemonitor.com/
49. https://medium.com/@jj1385jeff850527/iota-tangle-introductory-overview-of-white-paper-for-beginners-df9b14882b64
50. https://medium.com/@ywh.eric/iot-chain-this-is-just-the-beginning-e4f12933c01
51. https://github.com/Constellation-Labs/Whitepaper
52. https://blockgeeks.com/guides/smart-contracts/

References Continued:

53. https://en.wikipedia.org/wiki/Smart_contract
54. https://openzeppelin.org/api/docs/open-zeppelin.html
55. https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/
56. https://z.cash/technology/zksnarks.html
57. https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof
58. https://en.wikipedia.org/wiki/Zero-knowledge_proof
59. https://medium.com/iot-chain/iot-chain-frequently-asked-questions-371fa7cdf445
60. https://media.consensys.net/subscription-services-on-the-blockchain-erc-948-6ef64b083a36
61. https://blog.chronobank.io/ethereum-token-standards-19fbcc54fe27
62. https://theethereum.wiki/w/index.php/Main_Page
63. https://eips.ethereum.org/EIPS/eip-20
64. https://github.com/ethereum/EIPs/issues/223
65. https://github.com/ethereum/EIPs/issues/827
66. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-884.md
67. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-927.md
68. https://github.com/ethereum/EIPs/issues/948
69. https://eips.ethereum.org/all
70. https://hackernoon.com/5-erc-standards-every-ethereum-developer-should-know-about-c1ea79d3483e
71. https://medium.freecodecamp.org/lets-talk-about-the-ethereum-token-standards-you-need-to-know-8af9fcb7e54b
72. https://medium.com/crypto-currently/the-anatomy-of-erc721-e9db77abfc24
73. https://en.wikipedia.org/wiki/ERC20
74. https://medium.com/wepower/erc-standards-to-move-ethereum-forward-erc-20-erc-223-erc-721-e1712456449d
75. https://github.com/ConsenSysLabs/ethereum-developer-tools-list
76. https://consensys.github.io/smart-contract-best-practices/
77. https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff
78. https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1
79. https://venturebeat.com/2017/12/16/what-zero-knowledge-proofs-will-do-for-blockchain/
80. https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/
81. https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1
82. https://medium.com/@bsuichies/why-blockchain-must-die-in-2016-e992774c03b4
83. https://www.cointelligence.com/content/when-do-you-need-blockchain/
84. https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain
85. https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business
86. https://www.i-scoop.eu/blockchain-distributed-ledger-technology/blockchain-iot/
87. https://www.forbes.com/sites/forbestechcouncil/2018/07/18/is-blockchain-the-way-to-save-iot/#661405555a74
88. https://www.coindesk.com/blockchain-for-iot-a-big-idea-meets-hard-design-questions/
89. https://www.forrester.com/report/Disentangle+Hype+From+Reality+Blockchains+Potential+For+IoT+Solutions/-/E-RES135966
90. http://nicolaswindpassinger.com/about-the-book/?utm_source=iscoop
91. https://medium.com/@FEhrsam/blockchain-based-machine-learning-marketplaces-cb2d4dae2c17
92. https://truebit.io/
93. https://medium.com/@Francesco_AI/the-convergence-of-ai-and-blockchain-whats-the-deal-60c618e3accc
94. http://mattturck.com/ai-blockchain/
95. https://www.forbes.com/sites/bernardmarr/2018/03/02/artificial-intelligence-and-blockchain-3-major-benefits-of-combining-these-two-mega-trends/#30cfeb224b44
96. https://hackernoon.com/how-to-actually-combine-ai-and-blockchain-in-one-platform-ef937e919ec2
97. https://algorithmia.com/research/ml-models-on-blockchain
98. https://numer.ai/learn
99. http://www.usv.com/blog/fat-protocols
100. https://media.consensys.net/blockchain-vs-distributed-ledger-technologies-1e0289a87b16
101. https://medium.com/the-hague-pioneers/myth-busting-blockchain-1-75debc04becd
102. https://hackernoon.com/why-use-the-blockchain-instead-of-a-database-what-gives-tokens-value-263449681153