Blockchain Certification / Conformance

Fred Douglis, Angelos Stavrou

Need for IEEE Certification / Conformance for Blockchain

- **New Blockchain technologies are constantly being developed**
  - Hundreds of new Blockchain & Crypto Currency designs are in progress
  - How are existing technologies ”fit” in the existing design space?
  - What are the trade-offs between different Blockchain technologies?
  - Are there any Soft or Hard Limitations?
- **New Application Areas emerge – ambiguity persists**
  - **Is Blockchain a good fit for MY Use Case or Application?**
  - Can we adopt existing technologies or do we need new designs?
  - What are the costs involved and return-on-investment for Blockchain adoption?
  - Is there Interoperability and Governance between Blockchain Technologies?

Need for IEEE Certification / Conformance for Blockchain

- **New Blockchain technologies are constantly being developed**
  - Hundreds of new Blockchain & Crypto Currency designs are in progress
  - How are existing technologies ”fit” in the existing design space?
  - What are the trade-offs between different Blockchain technologies?

Lack of Conformance and Design Space Clarity is Inhibiting Blockchain Adoption and Future Advances

  - **Is Blockchain a good fit for this application?**
  - Can we adopt existing technologies or do we need new designs?
  - What are the costs involved and return-on-investment for Blockchain adoption?
  - Is there Interoperability and Governance between Blockchain Technologies?

Need for IEEE Certification / Conformance for Blockchain

- **Existing Blockchain technologies are very Heterogeneous**[1]
  - More than 1910 cryptocurrencies that depend on multiple technology variations (https://coinmarketcap.com)
  - Hyperledger, Ethereum, EOS, Bitcoin, Ripple, EoS are **just a few of the Blockchain technologies**
  - **Many different Vendors and Capabilities**
    - Hard to understand Limitations & Differentiators
    - Persistent confusion among Engineers and Decision makers

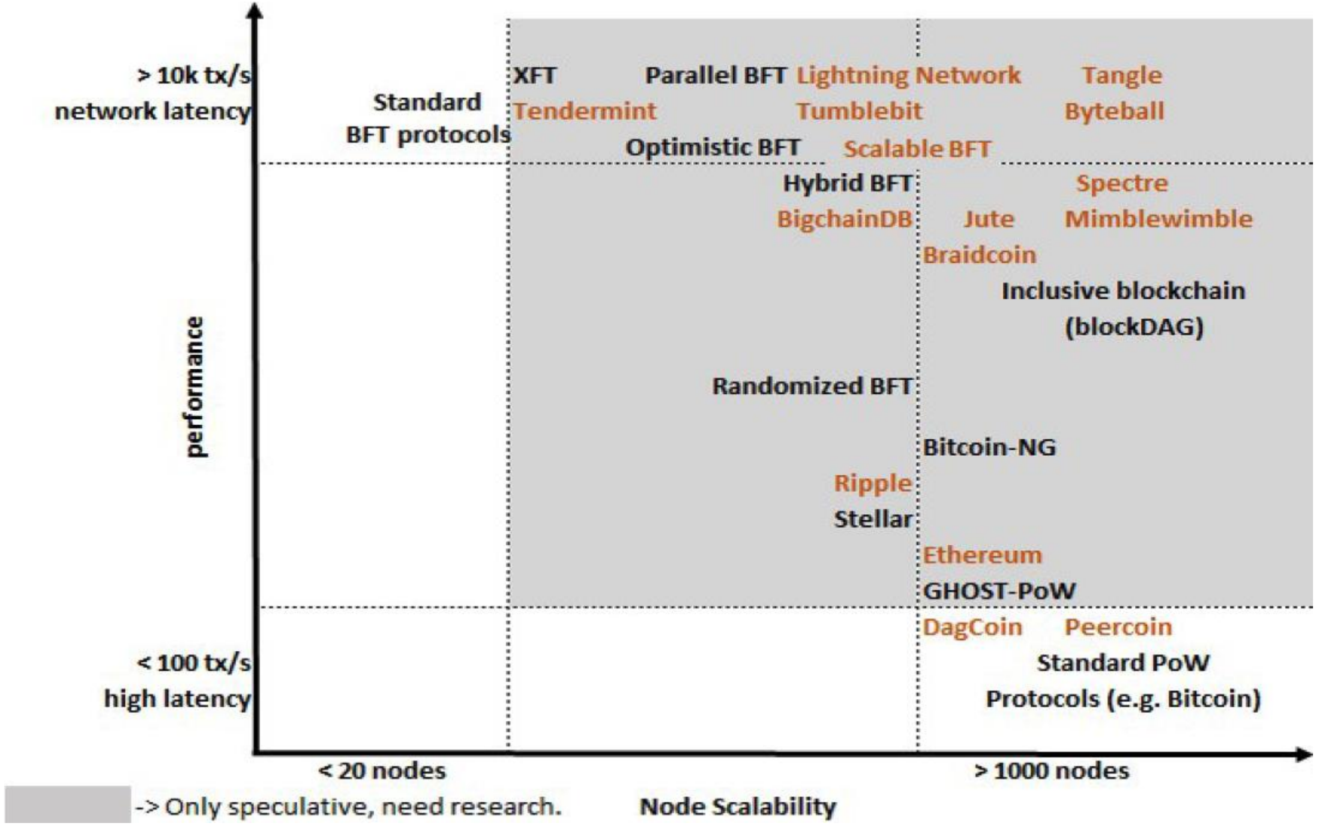
Some Blockchain Characteristics

Blockchain Concepts

Operation	Centralized	Decentralized	Distributed
Governance/ Business Model	Centrally Controlled	Community Controlled	Autonomous
Stability/Resilience	Unstable	Bounded Stability	Stable
Scalability	Large Throughput/ Small Number of Nodes	Small Throughput/Medium Number of Nodes	Infinite
Speed of Enterprise Development	Fast	Medium	Very Slow
Architecture Evolution/Diversity	Permissioned/Private	Hybrid	Permissionless/Public
Tokenization	No	Possibly	Yes
Trust Control	High Traditional/Low Algorithmic	Medium Traditional/ Medium Algorithmic	Low Traditional/High Algorithmic

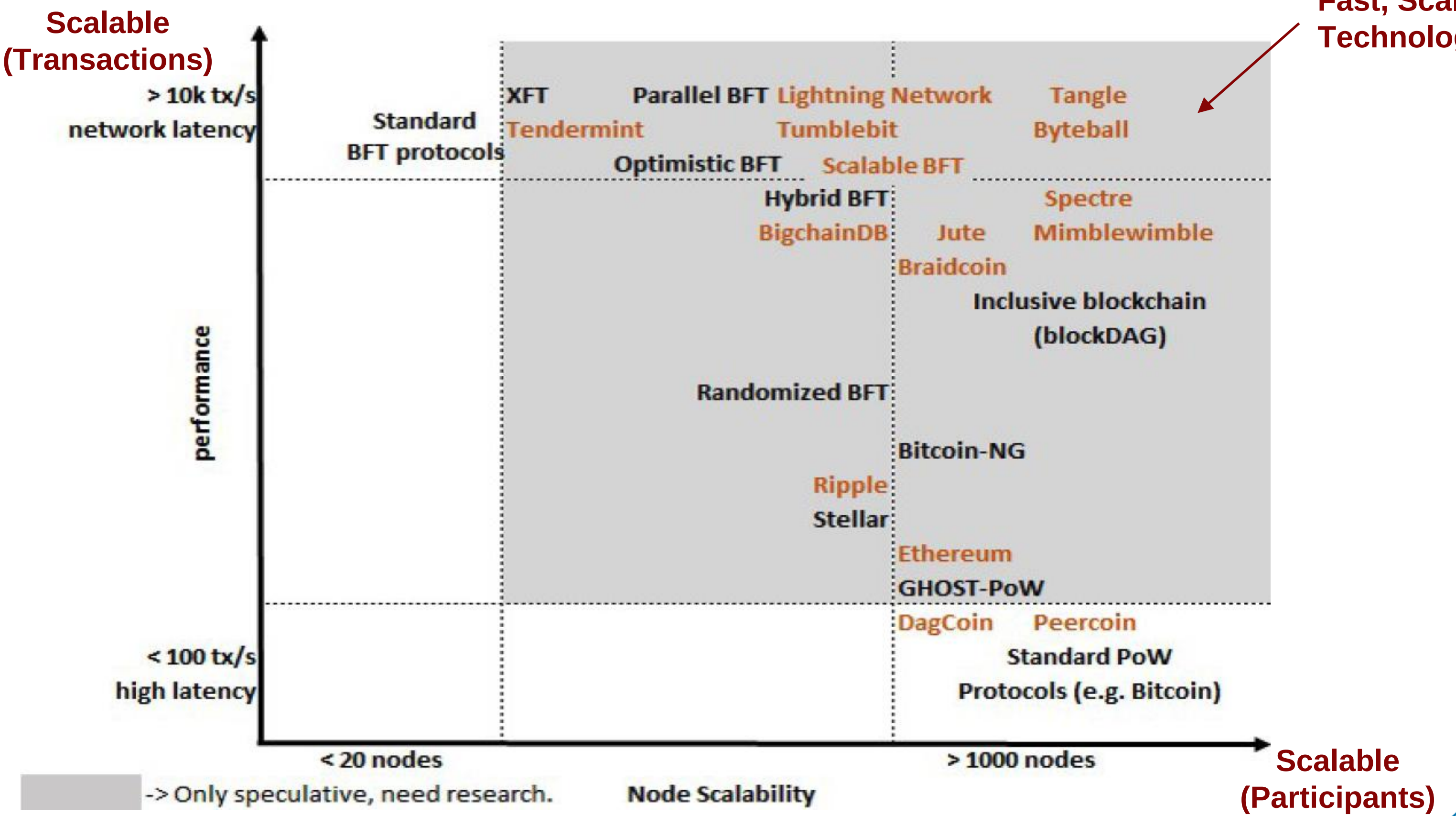
ID: 352362

Some Blockchain Differentiators



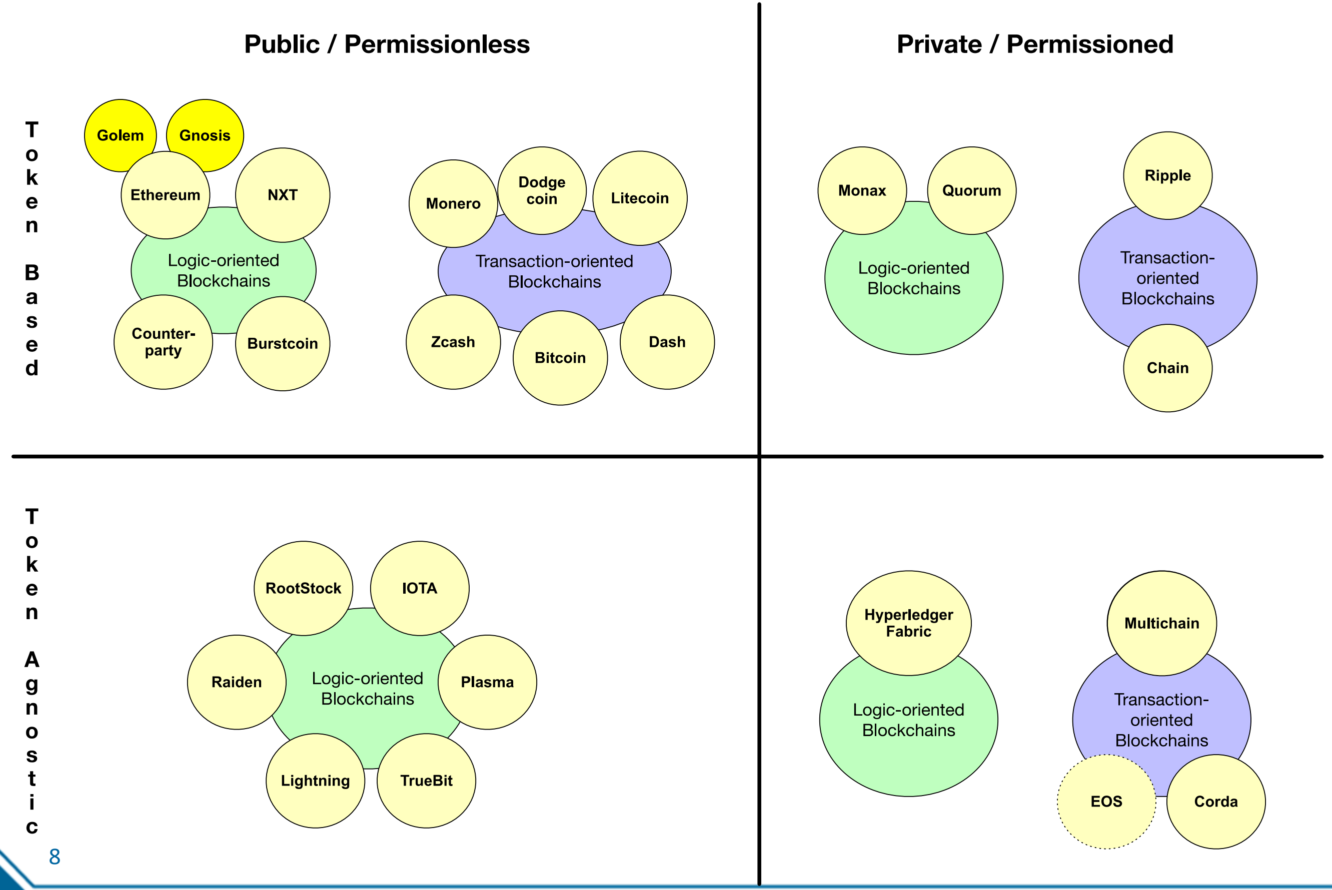
K. Yeow et al.: Decentralized Consensus for Edge-Centric IoT: Review, Taxonomy, and Research Issues

Some Blockchain Differentiators



K. Yeow et al.: Decentralized Consensus for Edge-Centric IoT: Review, Taxonomy, and Research Issues

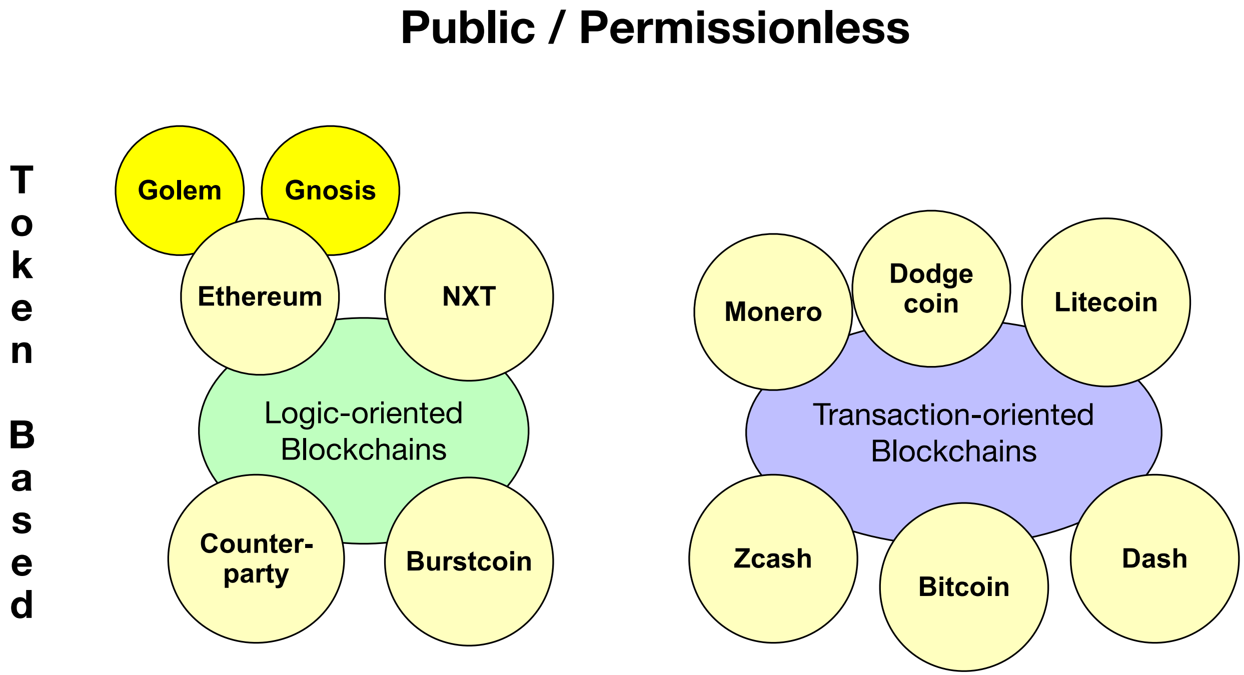
Some Blockchain Differentiators



Access Control & Governance

- Public or Private, Permissioned or Permissionless,
- Identity Management, Support for Entity and Transactional ACLs

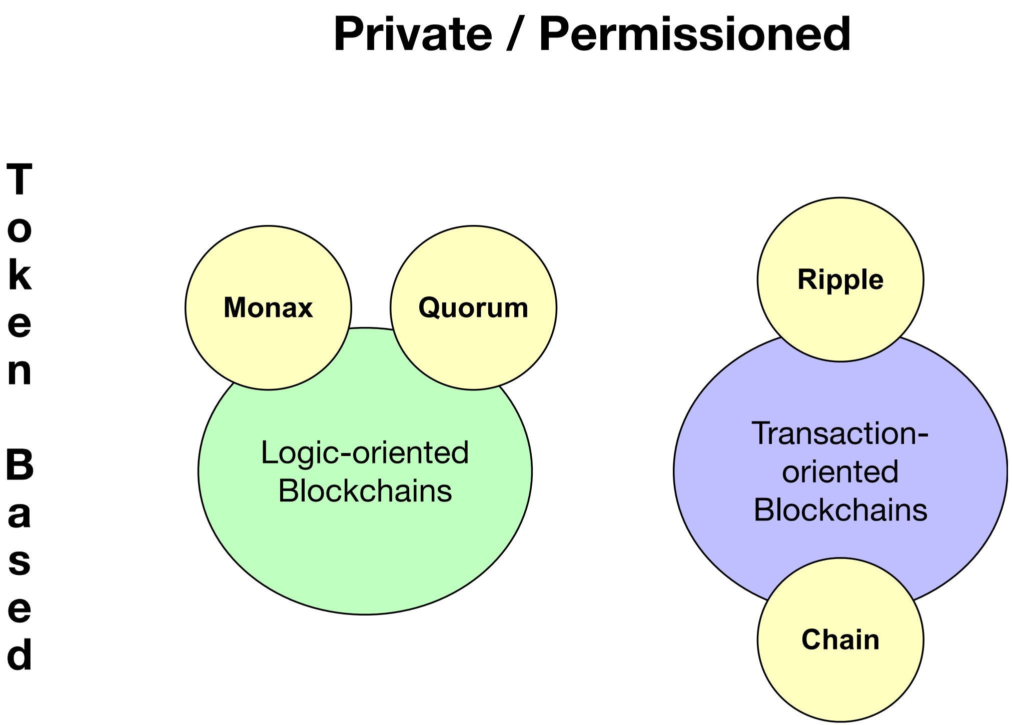
Some Blockchain Differentiators



Access Control & Governance

- Public or Private, Permissioned or Permissionless,
- Identity Management, Support for Entity and Transactional ACLs

Some Blockchain Differentiators



Access Control & Governance

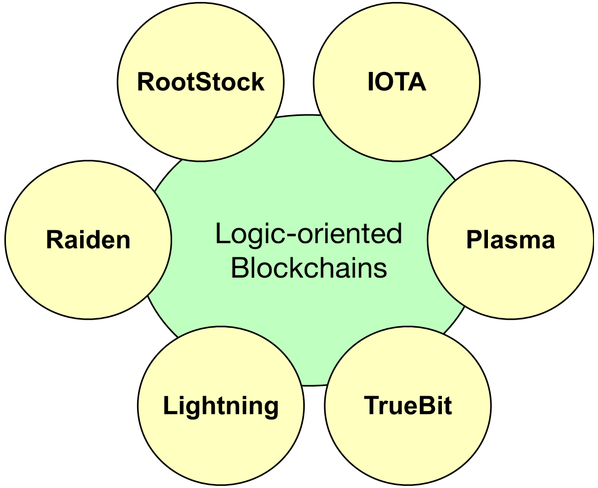
- Public or Private, Permissioned or Permissionless,
- Identity Management, Support for Entity and Transactional ACLs

Some Blockchain Differentiators

Public / Permissionless

T
o
k
e
n

A
g
n
o
s
t
i
c



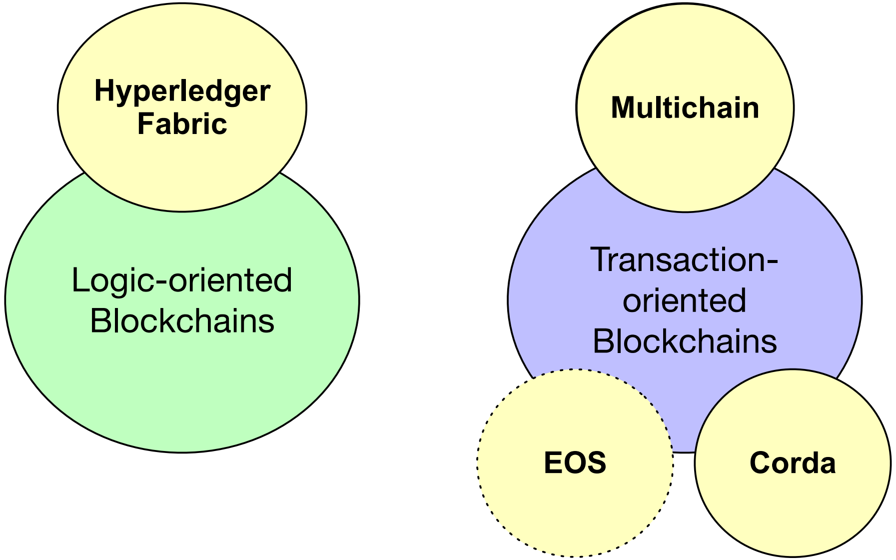
Access Control & Governance

- Public or Private, Permissioned or Permissionless,
- Identity Management, Support for Entity and Transactional ACLs

Some Blockchain Differentiators

Private / Permissioned

Token Agnostic



Access Control & Governance

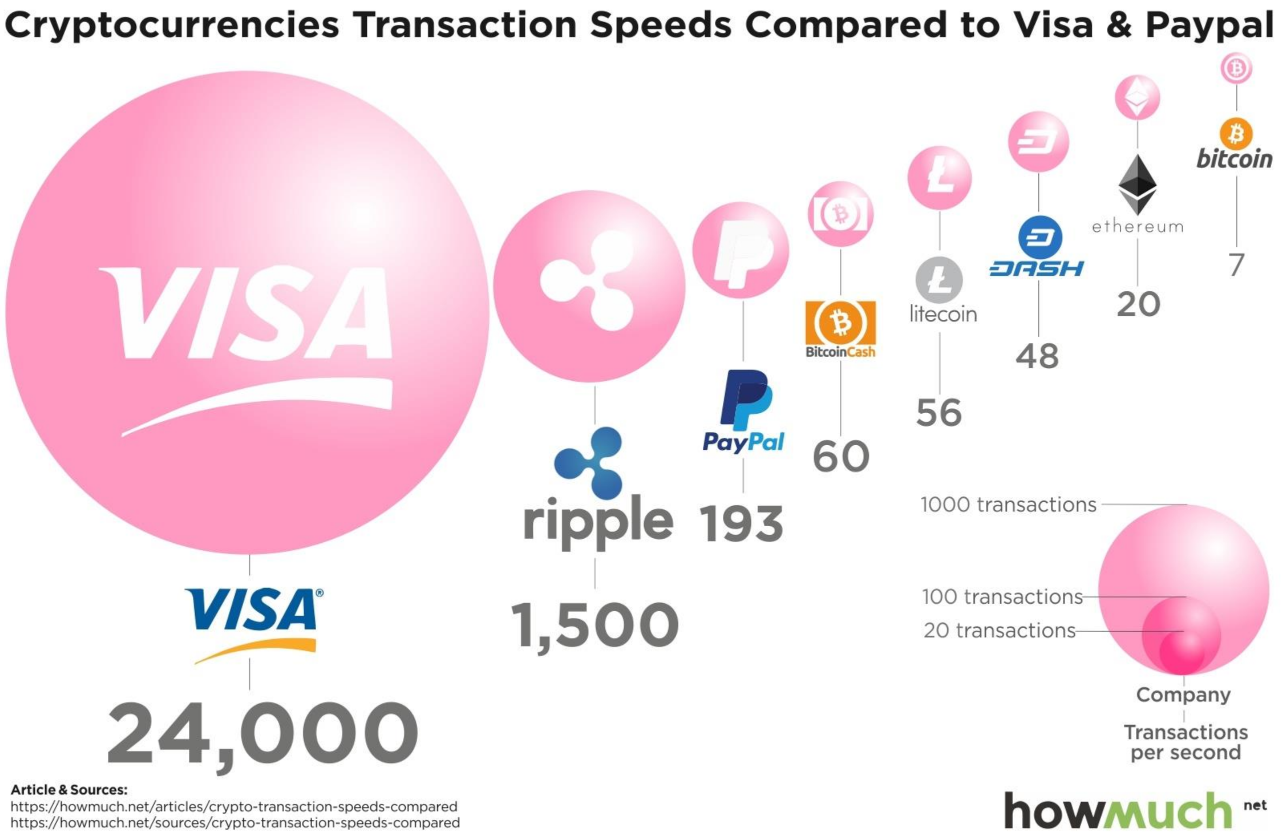
- Public or Private, Permissioned or Permissionless,
- Identity Management, Support for Entity and Transactional ACLs

Transactional Capabilities: Transactions Per Second (TPS), Scalability, Storage, Smart Contracts, tokenization, native assets, asset supply management

Protocol Comparison

	Bitcoin's blockchain	Ethereum	Stellar	Ripple
Average Transaction Confirmation Time	1 hour	15 minutes	3 to 5 seconds	3 to 5 seconds
Average Transaction Fees	$0.61 per transaction	$0.02 per transaction	$0.01 will pay for 300,000 transactions	$0.01 will pay for 3 transactions
Transactions Per Second	3 transactions per second	7 transactions per second	1000 transactions per second	1000 transactions per second
Consensus Mechanism	Proof of Work	Proof of Work	Stellar Consensus Protocol (SCP)	Ripple Consensus Algorithm
Validator control	Decentalized	Decentalized	Decentalized	Centralized
Governance	Non-profit	Non-profit	Non-profit	For profit

Transactional Capabilities: Transactions Per Second (TPS), Scalability, Storage, Smart Contracts, tokenization, native assets, asset supply management



Need for IEEE Certification / Conformance for Blockchain

➢ Blockchain Primary Differentiating Factors (cont)

- Software Architecture: Centralized, De-centralized, Modular (Polylithic) vs Monolithic, Open Source, Closed Source
- System Requirements: Server & Node Capabilities in terms of storage, CPU, networking and limits to scalability
- Data Encryption: Support for strong Cryptographic Primitives, Configuration of additional layers of security
- Data Privacy/Data Revocation: Support for Anonymity (Zero Knowledge) and Data Revocation or Masking
- Other secondary factors depending on the Blockchain design goals

Five Factors in Determining a Good Business Case With DLTs

Source: Aite Group

Throughput	Latency	Node scalability	Security	Cost
Volume of transactions the DLT is able to process (tps)	How long the DLT takes to confirm and commit each transaction	How many nodes the DLT supports without compromising performance	How resilient the DLT system is to various security threats	How much it costs to build and run a DLT system
• Bitcoin protocol has an extremely low throughput of 7 tps	• Bitcoin protocol takes 10 minutes on average to validate transactions	• Bitcoin protocol is the most scalable DLT in number of validation nodes	•The security aspects are fundamentally impacted by the consensus algorithms	•Running cost: Cost per confirmed transactions (CPCT)
• Many DLTs have made significant progress on throughput, ranging from 500 tps to 5,000 tps	• Private DLTs running on a consensus algorithm without mining can provide subsecond latency levels	•Private DLTs provide sufficient client-node scalability but with limited validation-node scalability	-Client onboarding -Digital signatures -Network attacks -Data privacy -Governance control -Legal enforcement	•Building cost: capital investment in hardware and equipment, software development and licensing, and IT staffing

Need for IEEE Certification / Conformance for Blockchain

- **IEEE Certification & Conformance Goals**
  - Create a framework for algorithmic and performance evaluation for Blockchain technologies that is open and can be easily validated
  - Select the N Blockchain technologies that best represent the design space
  - Enumerate the Factors to be assessed for the selected technologies
  - Identify the theoretical limitations for these factors and technologies selected
  - Validate the implementation performance of the technologies against different use scenarios

Need for IEEE Certification / Conformance for Blockchain

- **IEEE Certification & Conformance Goals (Cont)**
  - Present the findings to the IEEE community at large
  - Enable the IEEE community to enrich the framework and extend it to
    - Additional Blockchain Technologies
    - Factors and Configuration parameters
  - **Mature the Conformance Process to an IEEE Technology Certificate**
    - Provide a seamless transition from Conformance to Certification
  - **Transition the Certification Process to IEEE Standards**

IEEE

Conclusions & Call for Participation

We are at the forefront:

- Conformance Process is important for Blockchain maturity & adoption
- We are looking for participants in IEEE community at large
- Create a consortium/council of companies to support the effort
- **Build the IEEE Standards to enable Blockchain adoption**

You can contact us at: blockchain@ieee.org

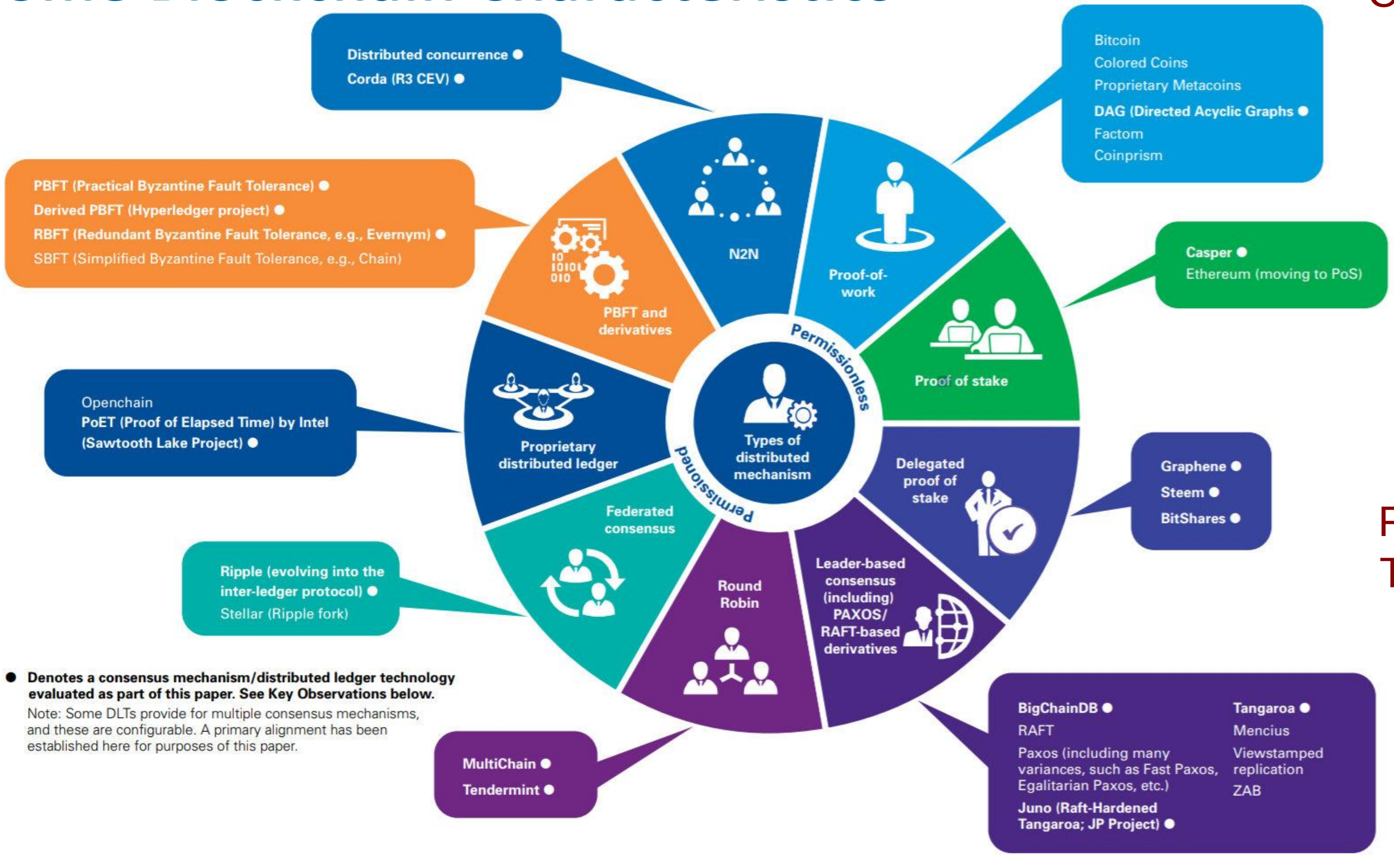
Backup Slides

IEEE Conformity Assessment Program (ICAP)

- What is IEEE Conformity Assessment?
  - Conformity Assessment is the process or processes that are used to demonstrate that a product or service meets specified requirements (set forth in Standards, Test Plans, etc.)
- Conformity Assessment Benefits
  - Provides manufacturers a proven method of demonstrating compliance to the requirements
  - Empowers the end-user to make better purchasing decisions
  - Benefits the supplier as products can quickly gain market acceptance
  - Increases the likelihood of a stable technology in the market with robust products
- Conformity Assessment Activities Include:
  - Conformance, Commissioning, Interoperability, Inspection, Accreditation
  - Test Suite Specification development
  - "Catch-all" term to address range of test-related activities

IEEE Conformity Assessment Program (ICAP) Completes the IEEE-SA Business/Standards Lifecycle

Some Blockchain Characteristics



Consensus Type:

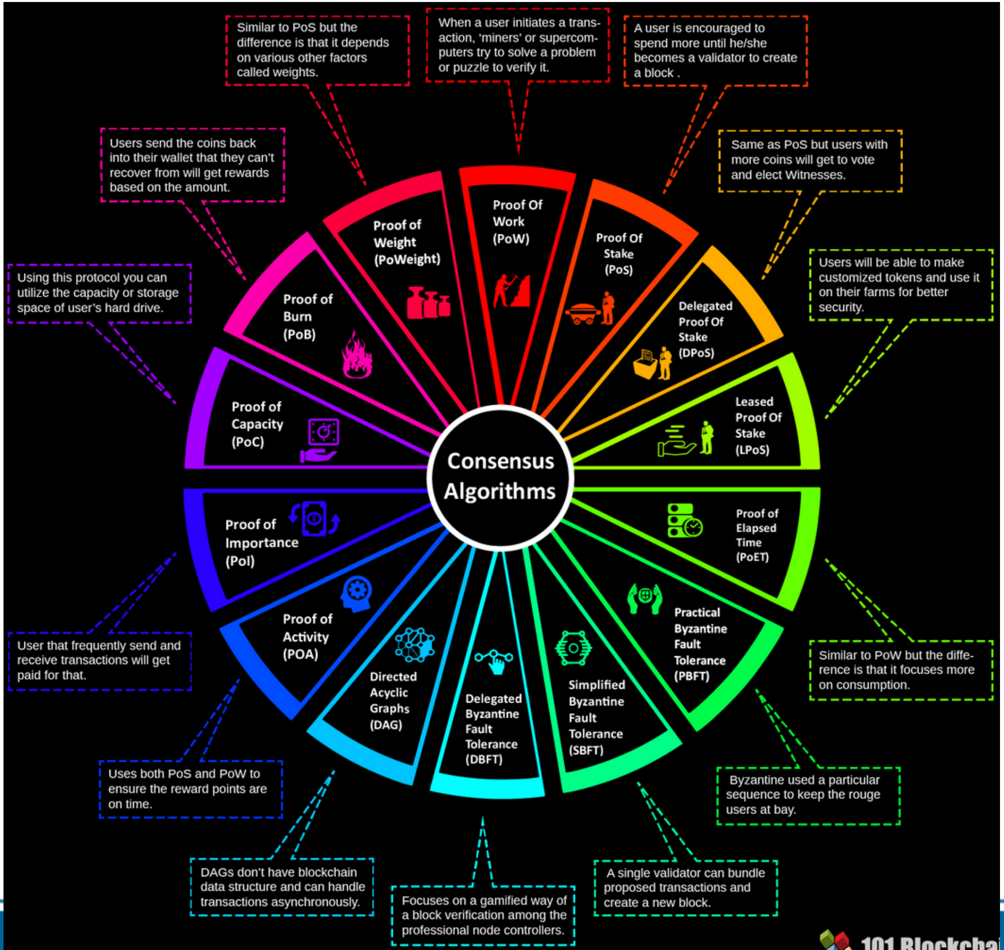
Proof-of-Work,
Proof-of-Stake
Proof-of-Authority
Proof-of-Capacity
Proof-of-Space
Proof-of-Storage
Proof-of-Burn
Proof of Elapsed Time
Hybrid

Failure Tolerance/Attack Tolerance:

Byzantine Fault Tolerance
Synchronous
Asynchronous
Hybrid, Non-Deterministic
Deterministic

https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

Some Blockchain Characteristics



https://101blockchains.com

Consensus Type:

- Proof-of-Work,
- Proof-of-Stake
- Proof-of-Authority
- Proof-of-Capacity
- Proof-of-Space
- Proof-of-Storage
- Proof-of-Burn
- Proof of Elapsed Time
- Hybrid

Failure Tolerance/Attack Tolerance:

- Byzantine Fault Tolerance
- Synchronous
- Asynchronous
- Hybrid, Non-Deterministic
- Deterministic