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?
Existing Blockchain technologies are very Heterogeneous

- More than 1910 cryptocurrencies that depend on multiple technology variations ([https://coinmarketcap.com](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

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

© 2018 Gartner, Inc.
Some Blockchain Differentiators

![Blockchain Differentiators Diagram]

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

- Scalable (Transactions)
- Fast, Scalable Technologies
- Scalable (Participants)
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

- Access Control & Governance
  - Public or Private, Permissioned or Permissionless,
  - Identity Management, Support for Entity and Transactional ACLs
Some Blockchain Differentiators

Private / Permissioned

Access Control & Governance
- Public or Private, Permissioned or Permissionless,
- Identity Management, Support for Entity and Transactional ACLs
Some Blockchain Differentiators

Public / Permissionless

Access Control & Governance
- Public or Private, Permissioned or Permissionless,
- Identity Management, Support for Entity and Transactional ACLs
Some Blockchain Differentiators

Private / Permissioned

Access Control & Governance
- Public or Private, Permissioned or Permissionless,
- Identity Management, Support for Entity and Transactional ACLs

Token Agnostic

Hyperledger Fabric
Logic-oriented Blockchains

Multichain
Transaction-oriented Blockchains

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

## Protocol Comparison

<table>
<thead>
<tr>
<th></th>
<th>Bitcoin’s blockchain</th>
<th>Ethereum</th>
<th>Stellar</th>
<th>Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average Transaction Confirmation Time</strong></td>
<td>1 hour</td>
<td>15 minutes</td>
<td>3 to 5 seconds</td>
<td>3 to 5 seconds</td>
</tr>
<tr>
<td><strong>Average Transaction Fees</strong></td>
<td>$0.61 per transaction</td>
<td>$0.02 per transaction</td>
<td>$0.01 will pay for 300,000 transactions</td>
<td>$0.01 will pay for 3 transactions</td>
</tr>
<tr>
<td><strong>Transactions Per Second</strong></td>
<td>3 transactions per second</td>
<td>7 transactions per second</td>
<td>1000 transactions per second</td>
<td>1000 transactions per second</td>
</tr>
<tr>
<td><strong>Consensus Mechanism</strong></td>
<td>Proof of Work</td>
<td>Proof of Work</td>
<td>Stellar Consensus Protocol (SCP)</td>
<td>Ripple Consensus Algorithm</td>
</tr>
<tr>
<td><strong>Validator Control</strong></td>
<td>Decentralized</td>
<td>Decentralized</td>
<td>Decentralized</td>
<td>Centralized</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>Non-profit</td>
<td>Non-profit</td>
<td>Non-profit</td>
<td>For profit</td>
</tr>
</tbody>
</table>

March 2018
Transactional Capabilities: Transactions Per Second (TPS), Scalability, Storage, Smart Contracts, tokenization, native assets, asset supply management

Cryptocurrencies Transaction Speeds Compared to Visa & Paypal

- Visa: 24,000 transactions per second
- Ripple: 1,500 transactions per second
- Others: 100, 56, 48, 20, 7 transactions per second

Article & Sources: https://howmuch.net/articles/crypto-transaction-speeds-compared
https://howmuch.net/sources/crypto-transaction-speeds-compared
Blockchain Primary Differentiating Factors (cont)

- **Software Architecture:** Centralized, De-centralized, Modular (Polythic) 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**

Need for IEEE Certification / Conformance for Blockchain
## Five Factors in Determining a Good Business Case With DLTs

**Source: Aite Group**

<table>
<thead>
<tr>
<th>Throughput</th>
<th>Latency</th>
<th>Node Scalability</th>
<th>Security</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Graph" /></td>
<td><img src="image" alt="Clock" /></td>
<td><img src="image" alt="People" /></td>
<td><img src="image" alt="Warning" /></td>
<td><img src="image" alt="Currency" /></td>
</tr>
</tbody>
</table>

**Throughput**
- Volume of transactions the DLT is able to process (tps)
  - Bitcoin protocol has an extremely low throughput of 7 tps
  - Many DLTs have made significant progress on throughput, ranging from 500 tps to 5,000 tps

**Latency**
- How long the DLT takes to confirm and commit each transaction
  - Bitcoin protocol takes 10 minutes on average to validate transactions
  - Private DLTs running on a consensus algorithm without mining can provide subsecond latency levels

**Node Scalability**
- How many nodes the DLT supports without compromising performance
  - Bitcoin protocol is the most scalable DLT in number of validation nodes
  - Private DLTs provide sufficient client-node scalability but with limited validation-node scalability

**Security**
- How resilient the DLT system is to various security threats
  - The security aspects are fundamentally impacted by the consensus algorithms
    - Client onboarding
    - Digital signatures
    - Network attacks
    - Data privacy
    - Governance control
    - Legal enforcement

**Cost**
- How much it costs to build and run a DLT system
  - Running cost: Cost per confirmed transactions (CPCT)
  - 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
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
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://101blockchains.com