DLT Development Platforms Comparison

Dr Jean-Marc Seigneur
April 2019
• Director of the Certificate of Advanced Studies in blockchain development at University of Geneva (12 European credits, ECTS)
  • https://www.cas-blockchain-certification.com

• President of Reputaction
  • Patent-pending hardened crypto wallet for KYC-AML-enforced Bitcoin/tokens transactions, even offline

• Google Award of Excellent Research in Academia in 2016
Non-financial use-cases of blockchains
Directed Acyclic Graph (DAG)

• Blockchains are only a subset of Distributed Ledger Technologies (DLT).
• Another type of DLT are solutions relying on DAG rather than blockchain: IOTA, Hashgraph…
Decentralized Applications (dApp) Requirements

- Different DLT platforms have different advantages and disadvantages for dApp development and production:
  - Peer-reviewed
  - Transaction per seconds (TPS)
  - Attack-resistance
  - Turing completeness
  - Safety or liveness
  - Final or probabilistic
  - Permissioned or permissionless
  - Programmability
  - Popularity
  - Sustainability
  - Interoperability
  - Privacy and legal aspects

- However, the first requirement to check is to know whether a DLT is needed or not!
How to decide if you need a DLT?

<table>
<thead>
<tr>
<th>[Wüst and Gervais]</th>
<th>Permissionless Blockchain</th>
<th>Permissioned Blockchain</th>
<th>Central Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>Low</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Latency</td>
<td>Slow</td>
<td>Medium</td>
<td>Fast</td>
</tr>
<tr>
<td>Number of readers</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Number of writers</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Number of untrusted writers</td>
<td>High</td>
<td>Low</td>
<td>0</td>
</tr>
<tr>
<td>Consensus mechanism</td>
<td>Mainly PoW, some PoS</td>
<td>BFT protocols (e.g. PBFT [5])</td>
<td>None</td>
</tr>
<tr>
<td>Centrally managed</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

[Birch]
US DHS DLT Decision Flow Chart
<table>
<thead>
<tr>
<th>Foundation</th>
<th>Partners</th>
<th>Code</th>
<th>Consensus</th>
<th>Transaction Speed (without layer 2)</th>
<th>Attack Resistance</th>
<th>Current Decentralization</th>
<th>Team Size</th>
<th>Token Generation</th>
<th>Legal Aspects</th>
<th>Current Growth Potential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>Switzerland</td>
<td>World</td>
<td>Difficult (Solidity)</td>
<td>PoW, try PoS</td>
<td>25</td>
<td>Yes if PoW, no if PoS</td>
<td>Good</td>
<td>Large</td>
<td>Proven</td>
<td>No KYC</td>
</tr>
<tr>
<td>Hashgraph (Hedera)</td>
<td>USA</td>
<td>Swirlds</td>
<td>Medium (Java, Solidity)</td>
<td>Gossip of gossip</td>
<td>100 000</td>
<td>Yes if permission-based, No if permissionless</td>
<td>Tied to Swirlds</td>
<td>Medium</td>
<td>Not a current objective</td>
<td>KYC + AML + SAFT regulated</td>
</tr>
<tr>
<td>NEO</td>
<td>China</td>
<td>China / OnChain</td>
<td>Easy (C#, Java...)</td>
<td>dBFT</td>
<td>To be confirmed</td>
<td>Tied to China / OnChain</td>
<td>Medium</td>
<td>Proven</td>
<td>No KYC</td>
<td>Medium</td>
</tr>
<tr>
<td>ICON</td>
<td>Switzerland</td>
<td>South Korea / LoopChain</td>
<td>Easy (Python)</td>
<td>LFT</td>
<td>Better than Ethereum</td>
<td>To be confirmed</td>
<td>Tied to South Korea / LoopChain</td>
<td>Medium</td>
<td>To be confirmed</td>
<td>KYC &amp; AML</td>
</tr>
<tr>
<td>Cardano</td>
<td>Switzerland</td>
<td>Japan</td>
<td>Difficult (Haskell)</td>
<td>PoS (Ouroboros, formally proven)</td>
<td>To be confirmed</td>
<td>Formally proven</td>
<td>Medium</td>
<td>Medium</td>
<td>Not yet ready</td>
<td>KYC</td>
</tr>
<tr>
<td>Tezos</td>
<td>Switzerland</td>
<td>US/France ...</td>
<td>Difficult (Michelson)</td>
<td>DPoS (staking, governance)</td>
<td>40</td>
<td>Formal verification friendly</td>
<td>Good</td>
<td>Medium</td>
<td>Not a current objective</td>
<td>KYC &amp; AML</td>
</tr>
</tbody>
</table>
Programmability

• The following questions may be asked when selecting a DLT:
  • Does the DLT uses a well-known programming level with high-level bug and security checks?
  • Does the DLT provides an Integrated Development Environment (IDE)?
  • How big is the developers community?
  • Are all the DLT components open-source?
  • Are there any restricting patents?
  • How does the governance work?
  • Does the DLT use peer-reviewed cryptography?
  • How many other projects/dApp have successfully used the DLT?
  • How many projects/dApps built with the DLT have been successfully attacked due to bugs or security holes?
  • Does the DLT have a testnet separated from the mainnet?
    • Is it easy to use the testnet?
  • Does the DLT have a detailed blocks/transactions explorer?
  • Does the DLT provide an open-source wallet?
  • Is it possible to create privatenets for testing purposes?
  • Does the DLT have an emulator?
  • Does the DLT have an active open-source repository?
    • Including a test suite (unit tests…)?
    • Including active bugs treatments?
    • Including detailed documentation, at least in English?
    • Including tested templates, e.g., ICO smart contracts or tokens generation templates (ERC20, NEP-5…)?
Thanks for your attention!

Jean-Marc.Seigneur@reputaction.com

https://www.reputaction.com