Blockchain Solutions for Sustainable Development

Wulf A. Kaal
Overview

• Core Problems
• Blockchain’s Promise
• Blockchain Challenges
• Possible Solution
provenance and trackability throughout the supply chain to assure goods are ethically sourced and followed sustainability protocols.
Making tomorrow a better place

**Better Business**
- Investing in safety, health and talent
- Creating customer trust
- Developing supply chains

**Better Environment**
- Tackling climate change
- Conserving resources
- Protecting the environment

**Better Communities**
- Building community relationships
- Inspiring young people
- Supporting employment
The most unequal regions in the world

GINI index measure of inequality

Source: GINI Index (World Bank estimate)
A CRISIS OF LEGITIMACY
Old: Industrial Age Power Generation
Ethical Trade
Human Rights
Our rights holders’ issues which we can directly or indirectly influence through our policy and activity have been linked to the relevant global sustainable development goals.
Blockchain’s Promise

• Criminals can be called out via blockchain technology
• Monopolies will die out – ability to clone a company than anybody who has rent seeking behaviour. Smart contracts, Competition becomes frictionless without rent seeking behavior. Suffering that happens because of monopolies are inhibited. Decentralized systems are far more efficient.

• Anonymity allows power from politics to be pulled
• All monopolistic tendencies (materials, spaces, politics) to stop competition cannot work with the decentralized nature of blockchain. Space does not matter, material is gone because you can find it anywhere on the planet.
• Cannot control people with regulations. Cannot politically pull the lever
The Economics of Collaboration

VALUE CREATION

Self-Organization

Traditional Hierarchy

CRITICAL RESOURCES

Physical Financial

Networked Intelligence

Distributed Value Creation

Business Webs

Extended Enterprise

Industrial Age Corporation
ENDING THE REMITTANCE RIP-OFF
Everledger: Tracing Ownership and Certifying Provenance of Diamonds

PROTECTION.
We are a fraud detection system, overlaying big data from closed sources like insurers and law enforcement.
blockchain is the new supply chain
NEW: Distributed micro-grids powered by blockchain
Join The Mobile Voting Revolution

Votem® is a revolutionary mobile voting platform designed to securely cast votes in elections across the globe.

Your first name

Your last name

Your email address
Could Government Really Be an Early Adopter?

Figure 1

*First to finish: Respondents' expectations of when they will have blockchains in production and at scale*

Blockchain adoption in government (Source: IBM)
Almost half of enterprise DLT start-ups are based in North America (Figure 10), followed by Europe (28%) and Asia-Pacific (19%). While Western countries are currently dominating DLT development, Asia-Pacific is catching up. In terms of individual countries, a total of 24 countries have a DLT start-up, with the US leading, followed by the UK and China.

There is also a growing number of more established companies and corporations that have begun offering a variety of DLT-based services and managing platforms. Indeed, the large number of technology firms, consultancies, banks, insurers, payment companies, and other firms that have made some type of foray into DLT has become difficult to track. A recent report found that 39% of surveyed companies (and 55% of large corporations with more than 20,000 employees) are either in the process of or considering deploying DLT-based networks and applications.

The total number of employees working at enterprise DLT start-ups is at least 1,761. We estimate the actual number of staff working at enterprise DLT start-ups is likely well over 2,000. When including established corporations, the total number of people working full-time on enterprise DLT is considerably higher than 2,000. Publicly available figures for some large technology and consulting firms reveal that some companies have teams of more than 800 people working exclusively on DLT (e.g., Deloitte). We therefore estimate the combined enterprise DLT employment level for start-ups and established companies to be in the range of several thousand.

The DLT ecosystem has witnessed the entrance of established corporations in recent years.
58% of OPSIs plan to actively trial DLT applications this year, compared to only 25% of central banks.
Table 7: Legal risks and an unclear regulatory environment are key inhibitors to broader DLT adoption

<table>
<thead>
<tr>
<th>CHALLENGES TO BROAD DLT ADOPTION</th>
<th>WEIGHTED AVERAGE</th>
<th>INFRASTRUCTURE PROVIDERS</th>
<th>APPLICATION DEVELOPERS</th>
<th>OPERATORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal risks/regulatory framework</td>
<td>1.97</td>
<td>2.25</td>
<td>1.60</td>
<td>1.64</td>
</tr>
<tr>
<td>Confidentiality issues</td>
<td>2.09</td>
<td>2.05</td>
<td>2.20</td>
<td>2.10</td>
</tr>
<tr>
<td>Reluctance to change established business processes</td>
<td>2.17</td>
<td>2.47</td>
<td>2.00</td>
<td>1.73</td>
</tr>
<tr>
<td>Immature technology</td>
<td>2.28</td>
<td>1.85</td>
<td>3.20</td>
<td>2.64</td>
</tr>
<tr>
<td>Difficulty of building business network</td>
<td>2.44</td>
<td>2.45</td>
<td>2.20</td>
<td>2.55</td>
</tr>
<tr>
<td>Potential issues with data protection laws</td>
<td>2.60</td>
<td>2.85</td>
<td>2.80</td>
<td>2.00</td>
</tr>
<tr>
<td>Scalability/performance concerns</td>
<td>2.81</td>
<td>2.70</td>
<td>2.80</td>
<td>3.00</td>
</tr>
<tr>
<td>Reluctance to give up some control</td>
<td>2.88</td>
<td>3.05</td>
<td>2.60</td>
<td>2.70</td>
</tr>
<tr>
<td>Security concerns</td>
<td>2.91</td>
<td>2.95</td>
<td>2.80</td>
<td>2.89</td>
</tr>
<tr>
<td>Unknown costs/benefits</td>
<td>3.08</td>
<td>3.14</td>
<td>3.60</td>
<td>2.70</td>
</tr>
<tr>
<td>Lack of suitable use/business case</td>
<td>4.00</td>
<td>4.10</td>
<td>4.00</td>
<td>3.82</td>
</tr>
</tbody>
</table>

Note: The lower the score, the more important the challenge is considered (1: very significant challenge; 5: no challenge at all).
Blockchain’s Promise?
Blockchains Challenges

- Developer Support
- End-user Support
- Throughput
- Latency
- Usability
- Versioning, hard forks, multiple chains
- Size and bandwidth
- Privacy
- Wasted Resources
- Authenticaion
- Security
- 51% attack
- Data Malleability
- Security incidents
- Security
- Malleability
Fragmentation: The Need For a Network of Value

• Need to connect different ledgers together for the blockchain to deliver true value
• Aggregating the various parts of the blockchain and all value is authenticated.
• IoT and web services
• AI - becomes the basic engine.
• Yet this is where tension occurs.
• For true value to become a reality, require buy-in from all parties, otherwise fragmented chains.

• **How to obtain buy-in from all parties to overcome fragmentation?**
Trust Vs Trustlessness

• Blockchain is trustless by design, to deliver a new type of trust.

• A new type of trust that we are not familiar with, nor are traditional institutions built upon.

• There is no point using blockchain in the same frame of mind of our existing economy and system.

• How can we create true societal believe in the interconnected blockchains?
Centralization Vs. Decentralization

• Blockchain by design decentralizes power.
• Yet there’s tension in that if we want to make sure blockchain is used for good
• Who defines “good”?
• Need for a central authority to provide the guiding rules and principles?
• Throughout history centralized authority has decided the “GOOD”
• Decentralized blockchain technology offers a new option to define Good
• **How can we create a decentralized anonymous and autonomous consensus mechanism that helps define “GOOD”**
Humanising the Blockchain

• Ease of relating the blockchain to binary engagements, transactions etc.

• Humans are complex not binary

• How can the blockchain encapsulate the human condition / complexity / preferences?
Possible “Tech Integrated” Solution

Semada Platform

Blockchain infrastructure for measuring domain specific reputation

Flexible, Secure, Transparent, Governance
Reputation Verification Platform

Blockchain reduces need for trusting intermediaries.
But blockchain elements also need **reputation** rating in order to be trusted.

- Difficult to assess trust in **smart contracts**
  - who will read every single line of code to check for backdoors and hacks?

- Difficult to assess trust in **entities** using the smart contracts
  - prevent against bad actors

- How can smart contracts evolve without a core **legal infrastructure**?
  - how can we build a crypto legal system that can be trusted?

- How can we use **crypto economic incentives** to reward trustful parties and punish bad actors?

- How can we create a reputation system that is **secure** against Sybil and tyranny of majority attacks?

- How can we trust data coming from **oracles**?
Semada’s Proof of Stake Protocol - Comparison

Wulf Kaal

February, 2018

Overview

SPoS has elements of DPoS and chain-based PoS, as time slots are regular, and block producers are chosen randomly based on stake holdings. SPoS also has BFT-style PoS elements since all blocks are evaluated through Semada’s validation pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>SPoS</th>
<th>dPoS</th>
<th>dBFT POS</th>
<th>PoS</th>
<th>PoS</th>
<th>PoW</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Decentralized</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Large number of nodes</td>
<td>9/10</td>
<td>6/10</td>
<td>6/10</td>
<td>7/10</td>
<td>7/10</td>
<td>7/10</td>
</tr>
<tr>
<td>● Anyone can become a node?</td>
<td>+ Open membership allows any pseudonymous user with proper skills + inflationary token encourages active participation and discourages rent sitting, inhibiting cartels + prevents economy of scale centralization that comes from computing resources (Bitcoin and Ethereum) or campaigning ability (EOS) + on-chain governance; +Can regenerate from 1 node</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Nodes are not concentrated</td>
<td>- delegate election protocol favors corruption of delegates (e.g., through loss of anonymity) - Sybil delegates likely by economy of scale of campaigning skill</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Censorship resistant</td>
<td>- delegates similar to EOS - 66% network connectivity and participation required to guarantee liveness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Governance</td>
<td>+on chain governance first version of Ouroboros deployed with the Byron release; - only IOHK-controlled nodes participating in consensus; Community participation via delegated staking will begin with the Shelley release (2018)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● ICO process</td>
<td>- details not finalized; ad hoc solutions - concentrated rewards leads to cartels</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Regeneration</td>
<td>- mining pools arise from economy of scale of computing resources; - lack of transparent governance process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>SPoS Semada</td>
<td>dPoS EOS</td>
<td>dBFT POS NEO</td>
<td>PoS Cardano</td>
<td>PoS Casper</td>
<td>PoW BTC/ETH</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>2) Scalability</strong></td>
<td>8/10 TBD + Evolutionary structure quickly drives/adapts to maximal efficiency; swift adoption of optimal protocols, balancing speed and security in response to market needs</td>
<td>9/10 + Delegation enables higher computational efficiency than PoW EOS: with optim. &lt;=50k TPS Steemit: 1.2 mil T/Day</td>
<td>9/10 + ditto - 66% network connectivity required With optim. &lt;=10k TPS</td>
<td>7/10 Expectation of high transaction throughput via use of Recursive Internetwork Architecture (RINA) technology, partitioning transactions to different sets of elected leaders – same likely for sharding</td>
<td>TBD ETH &lt;=15TPS</td>
<td>5/10 - no SC Hash Mining &lt;=3.3 - 7 TPS - Storage - Bandwidth -CPU/Memory</td>
</tr>
<tr>
<td><strong>3) Language</strong></td>
<td>TBD</td>
<td>8/10 + uses web assembly (Microsoft, Google, Apple); Ethereum will move to it + very fast + C, C++, Rust, Solidity in progress - not a safe language</td>
<td>8/10 + Python, Java, C#, F#</td>
<td>7/10 + Haskell functional language CBD safety - poor Haskell adoption world wide + IELT supports smart contracts written in any programming language that has a formal semantics in K, e.g. Simon</td>
<td>8/10 + Solidity (~C, JavaScript), Serpent &amp;Viper (~Python), LLL (~Lisp), Mutan (~Go), Rust</td>
<td>5/10 Satoshi=C++, distributed binary data; limited functionality</td>
</tr>
<tr>
<td>Parameter</td>
<td>SPoS Semada</td>
<td>dPoS EOS</td>
<td>dBFT POS NEO</td>
<td>PoS Cardano</td>
<td>PoS Casper</td>
<td>PoW BTC/ETH</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>4) Security*</td>
<td>9/10 + reward structure incentivizes honest block production, policing; continual protocol development fairly rewarded; flexibility allows pivots to increase security at expense of speed</td>
<td>7/10 - Centralization concerns; anonymity; perverse delegates incentive; Sybil delegates; Tyranny of the majority; stake grinding; $P + \varepsilon$ attack; censorship transaction fees make spam and DoS attacks expensive to carry out; without them smart contracts and blockchains are vulnerable to these kinds of attacks</td>
<td>7/10 - Similar delegate concerns to EOS - 66% network connectivity/ liveness required</td>
<td>8/10 + structure of economic rewards increase safety, check on block production via transaction endorsing – assumptions of partially synchronous network with honest majority and upper limit on how long honest nodes can be offline +KEVM constructs designed with security as priority</td>
<td>TBD - ad hoc solutions; under development</td>
<td>9/10 +hash mining; openness - Long-term centralization concerns; censorship</td>
</tr>
<tr>
<td>*SPoS paper, Chapter 6 for definitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5) Governance | 8/10 + On-chain governance properly incentivized, designed to create and maintain consensus within and between DAOS as they evolve, gives DAOS the opportunity to properly reward users for their contribution | 5/10 Famous developers (+ short term/ - long term) | 5/10 Famous developers/ whales | 7/10 + On-chain protocol changes. Assumes fair “rule of law” system lowers likelihood of forking over simple protocol changes; plans for on-chain treasury for long-term protocol improvement and with machine testable specifications | 6/10 Famous developers/ whales; + historical evidence of open culture | 5/10 Famous developers/ whales |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>SPoS Semada</th>
<th>dPoS EOS</th>
<th>dBFT POS NEO</th>
<th>PoS Cardano</th>
<th>PoS Casper</th>
<th>PoW BTC/ETH</th>
</tr>
</thead>
<tbody>
<tr>
<td>6) Corresponding Market</td>
<td>Reputation Systems, DAOs, IoT, Gig-Economy</td>
<td>Large enterprises / Apps that need high performance</td>
<td>Government ties Large enterprises</td>
<td>DAOs, large enterprises</td>
<td>DAOs, Smart Contracting sensitive to decentralization</td>
<td>Store of Value</td>
</tr>
</tbody>
</table>
Thank You
Join the Conversation!

wulf@wulfkaal.com
Wulf Kaal
@wulfkaal
medium.com/@wulfkaal
Facebook.com/wulf.kaal
wulfkaal.com
wulfkaal