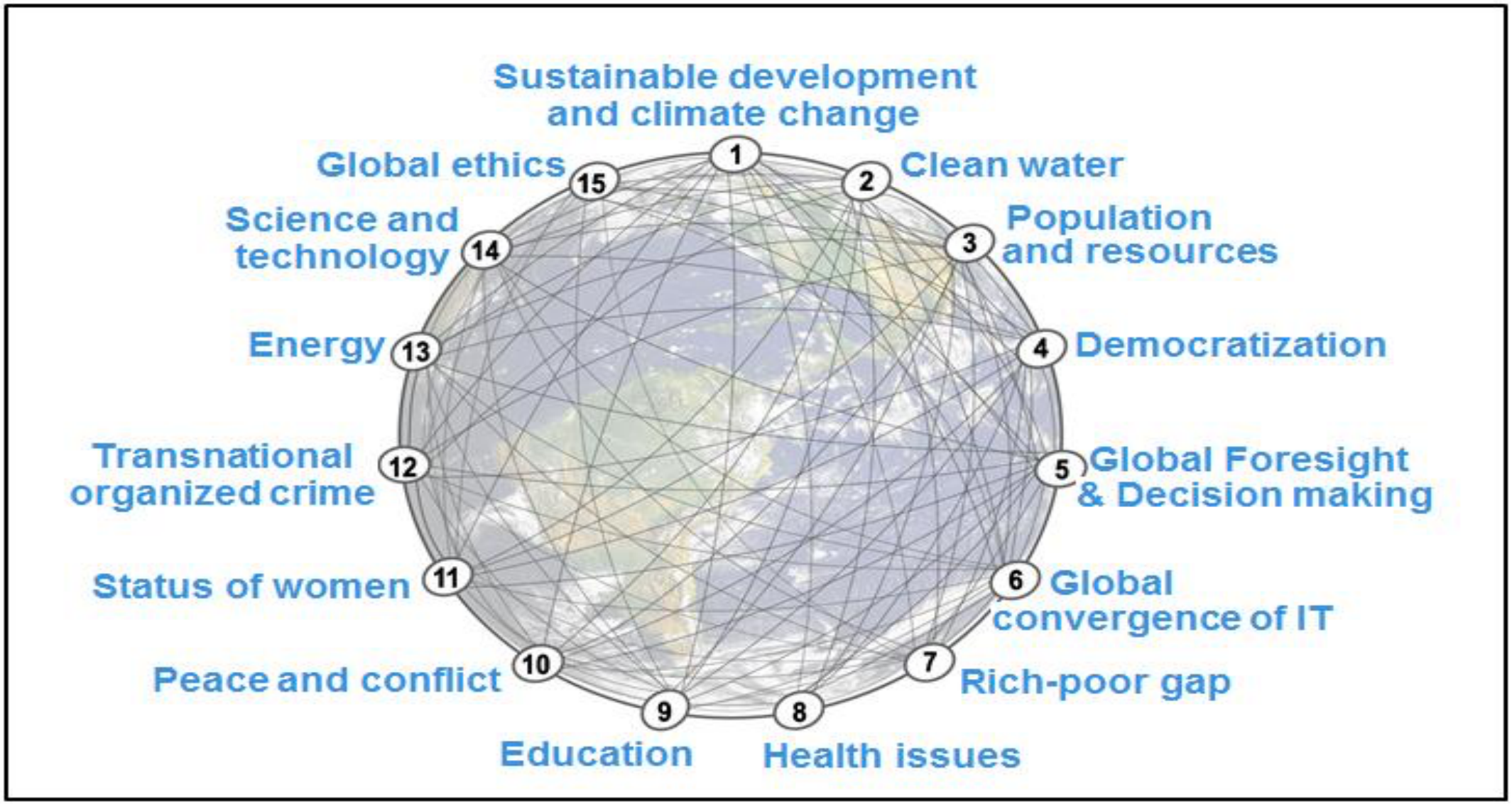
Blockchain Solutions for Sustainable Development

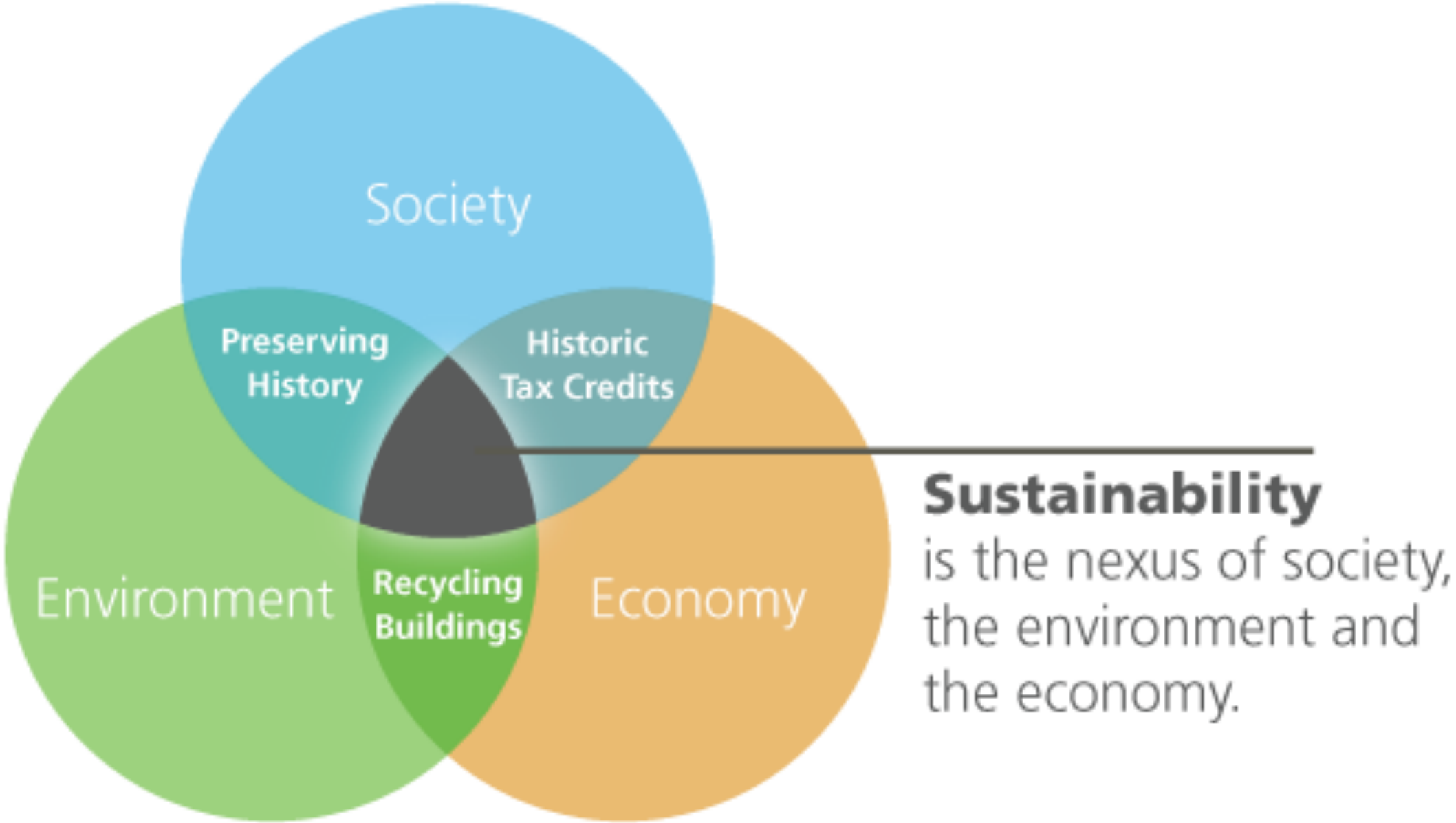
Wulf A. Kaal

Overview

- Core Problems
- Blockchain’s Promise
- Blockchain Challenges
- Possible Solution

Core Problems



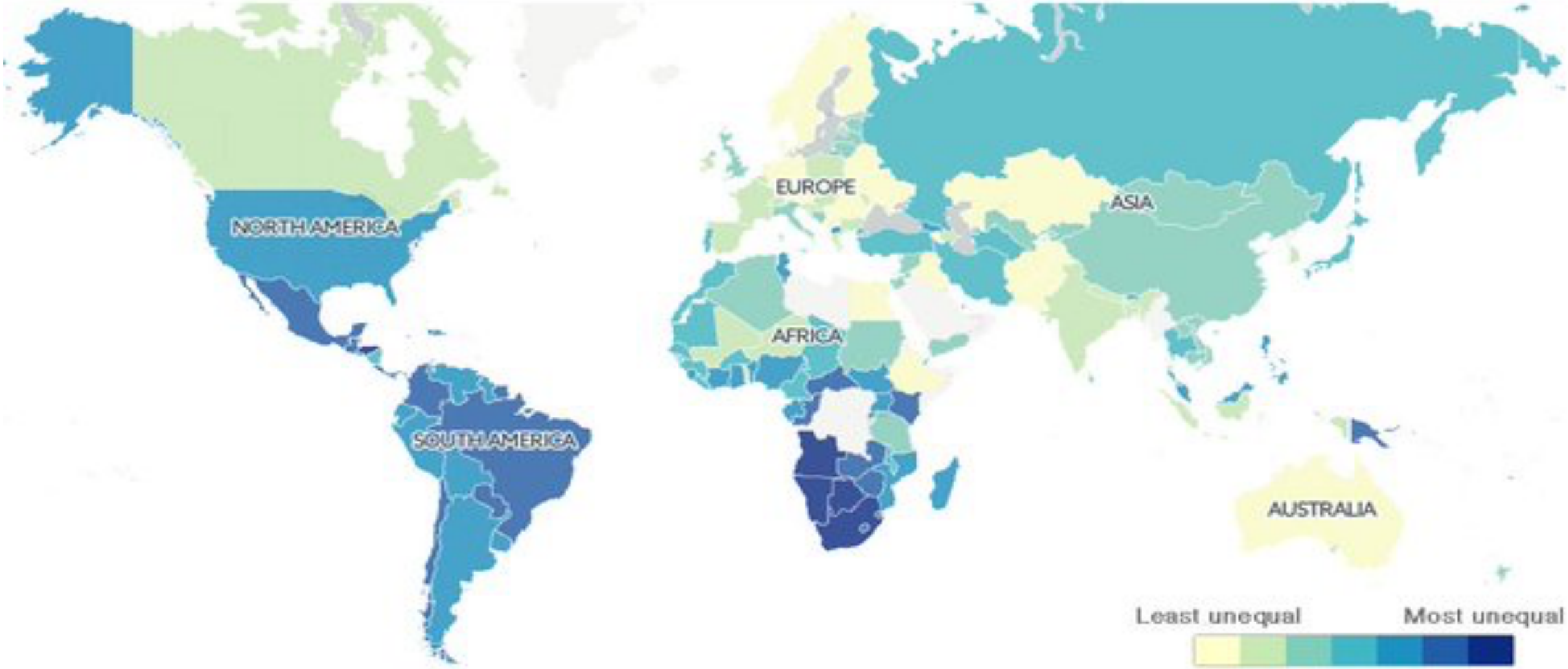


provenance and trackability throughout the supply chain to assure goods are ethically sourced and followed sustainability protocols.


BETTER BUSINESS
Investing in safety, health and talent
Creating customer trust
Developing supply chains
BETTER ENVIRONMENT
Tackling climate change
Conserving resources
Protecting the environment
Making tomorrow a better place
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)

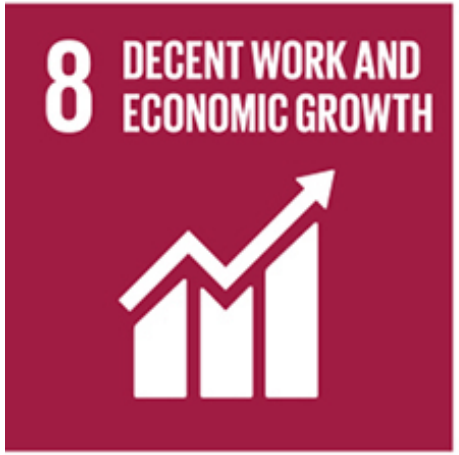

REFORMS
CORRUPTION


ton Post
Los Anacles Ti
The New York Times
Ring terror
amNEWYORK
THAT'S RICH!
Vote Leave
#TakeControl
A CRISIS OF LEGITIMACY

Old: Industrial Age Power Generation


FAIR TRADE
FAIR TRADE
FAIR TRADE

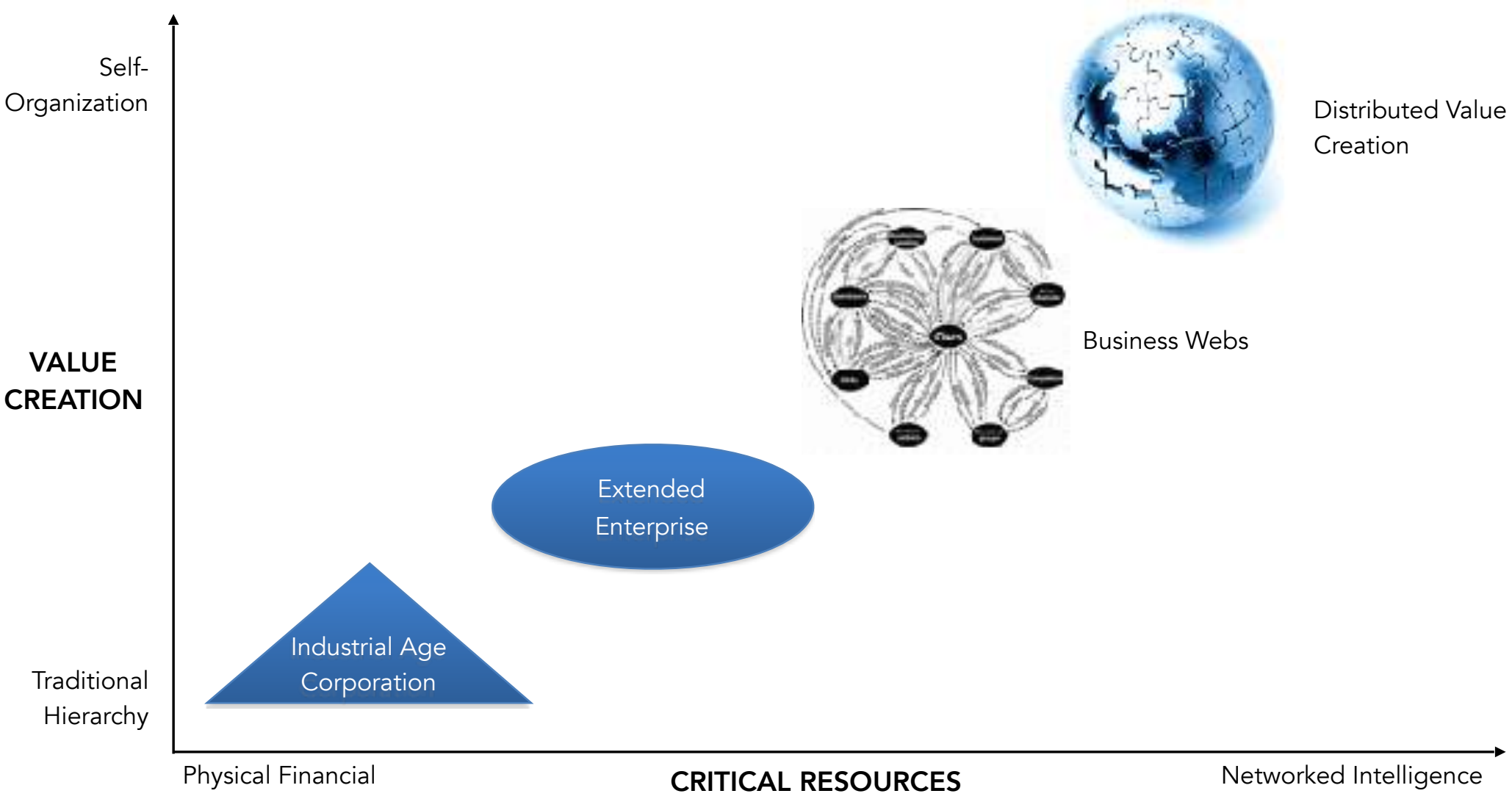
Human Rights



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.

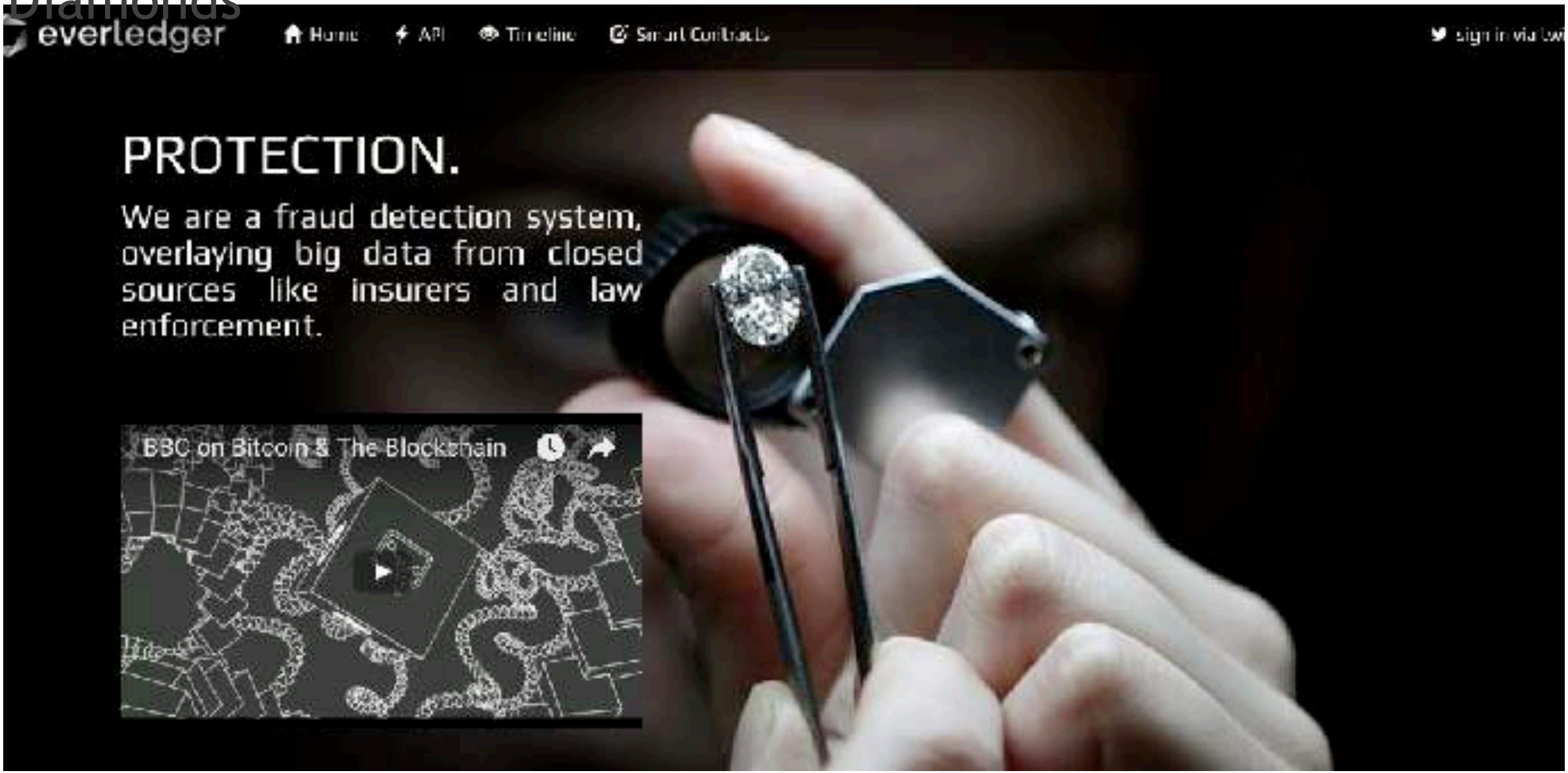
Blockchain’s Promise

The Economics of Collaboration




money transfer
WESTERN UNION
pengeoverføring
can i feel welcome here?
ja!
money transfer
WESTERN UNION
pengeoverføring
yes!

Everledger: Tracing Ownership and Certifying Provenance of Diamonds



blockchain is the new supply chain

NEW: Distributed micro-grids powered by blockchain


IDENTITY

Votem

Home | Government Elections | Private Elections | Our Products | Resources | About Us

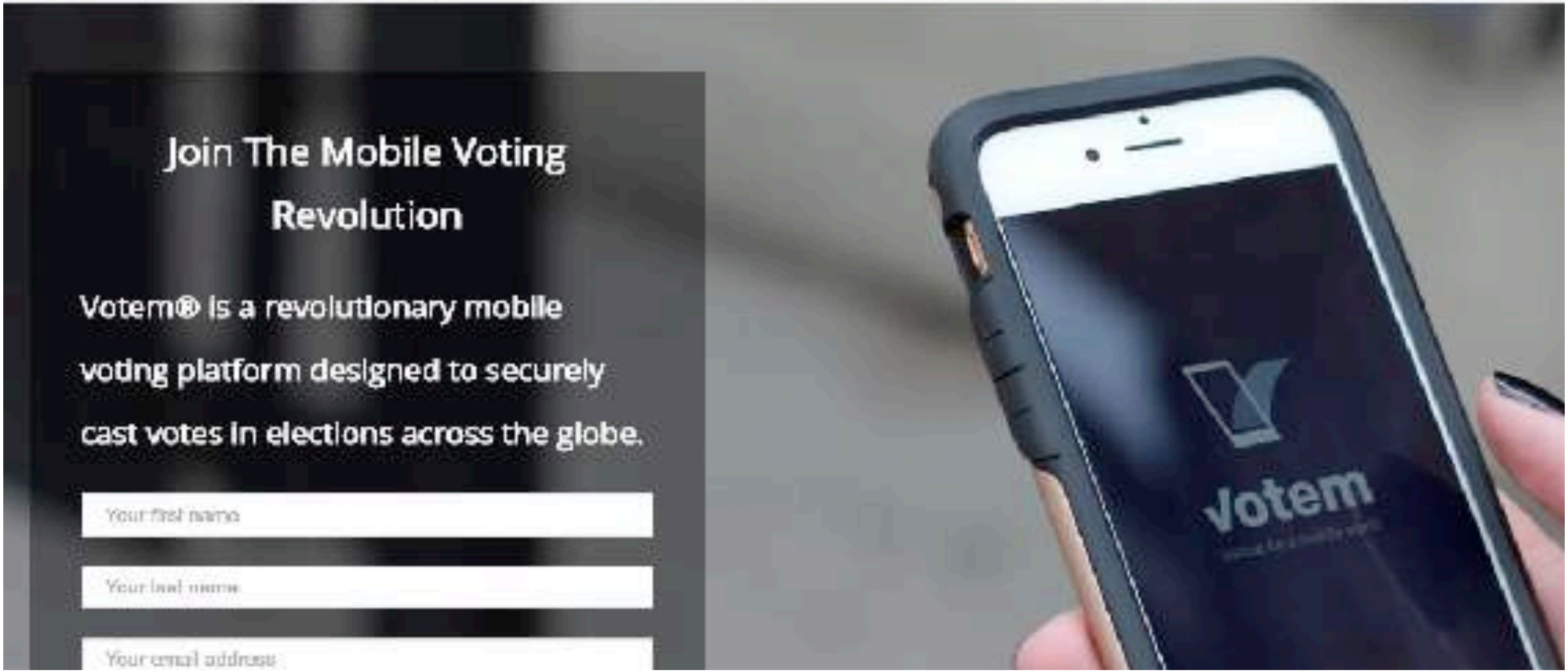
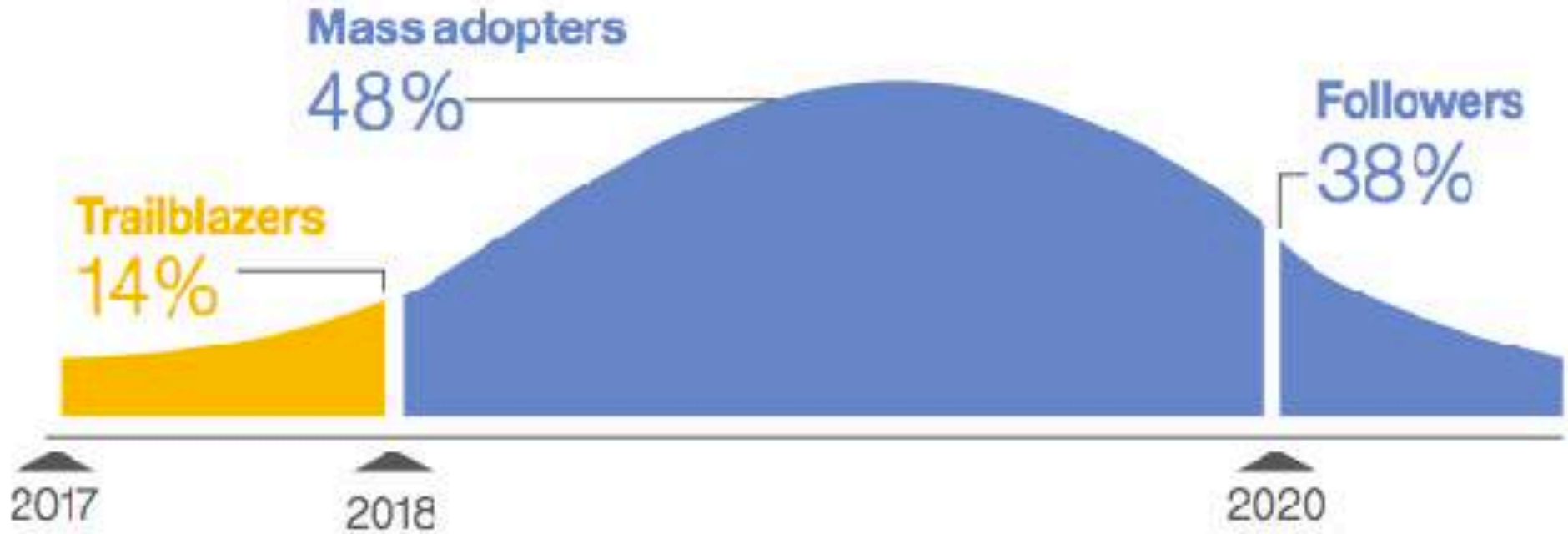


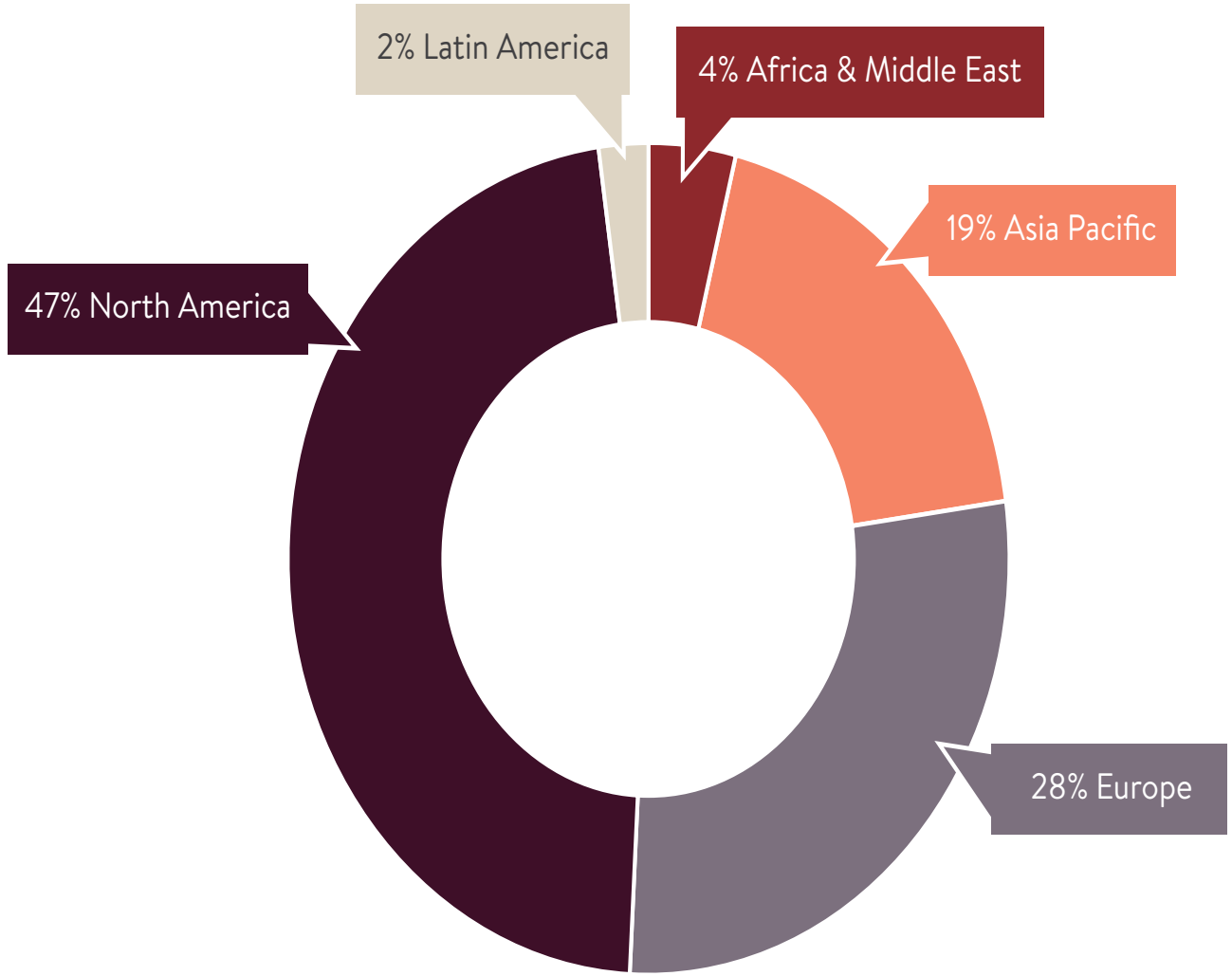
Figure 1

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



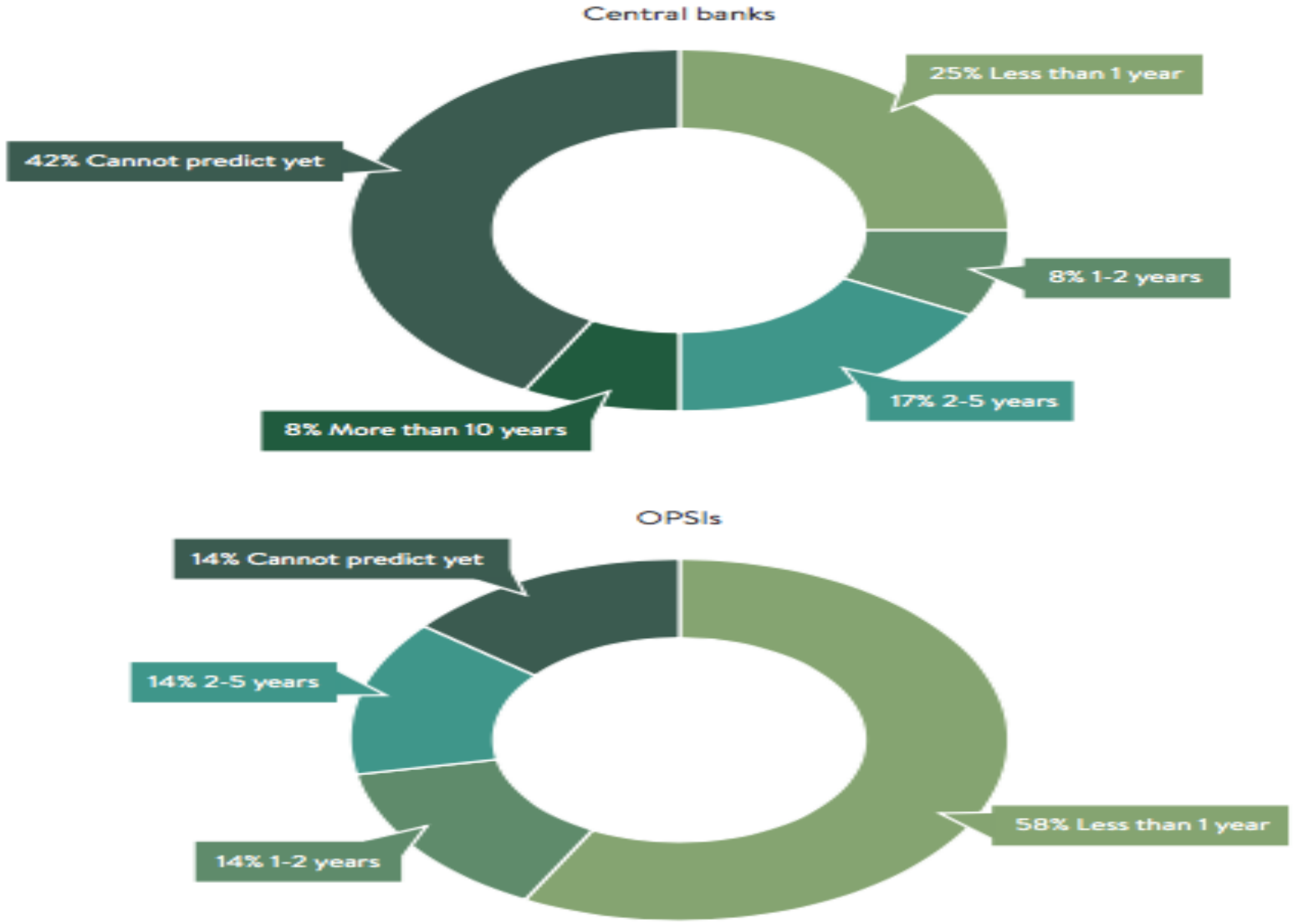
Blockchain adoption in government (Source: IBM)

Distribution of Blockchain Startups



Hileman, Garrick and Rauchs, Michel, 2017 Global Blockchain Benchmarking Study (September 22, 2017)

Expected time window of first DLT trials at their institution



58% of OPSIs plan to actively trial DLT applications this year, compared to only 25% of central banks

Hileman, Garrick and Rauchs, Michel, 2017 Global Blockchain Benchmarking Study (September 22, 2017

Table 7: Legal risks and an unclear regulatory environment are key inhibitors to broader DLT adoption

Lowest average score — Highest average score

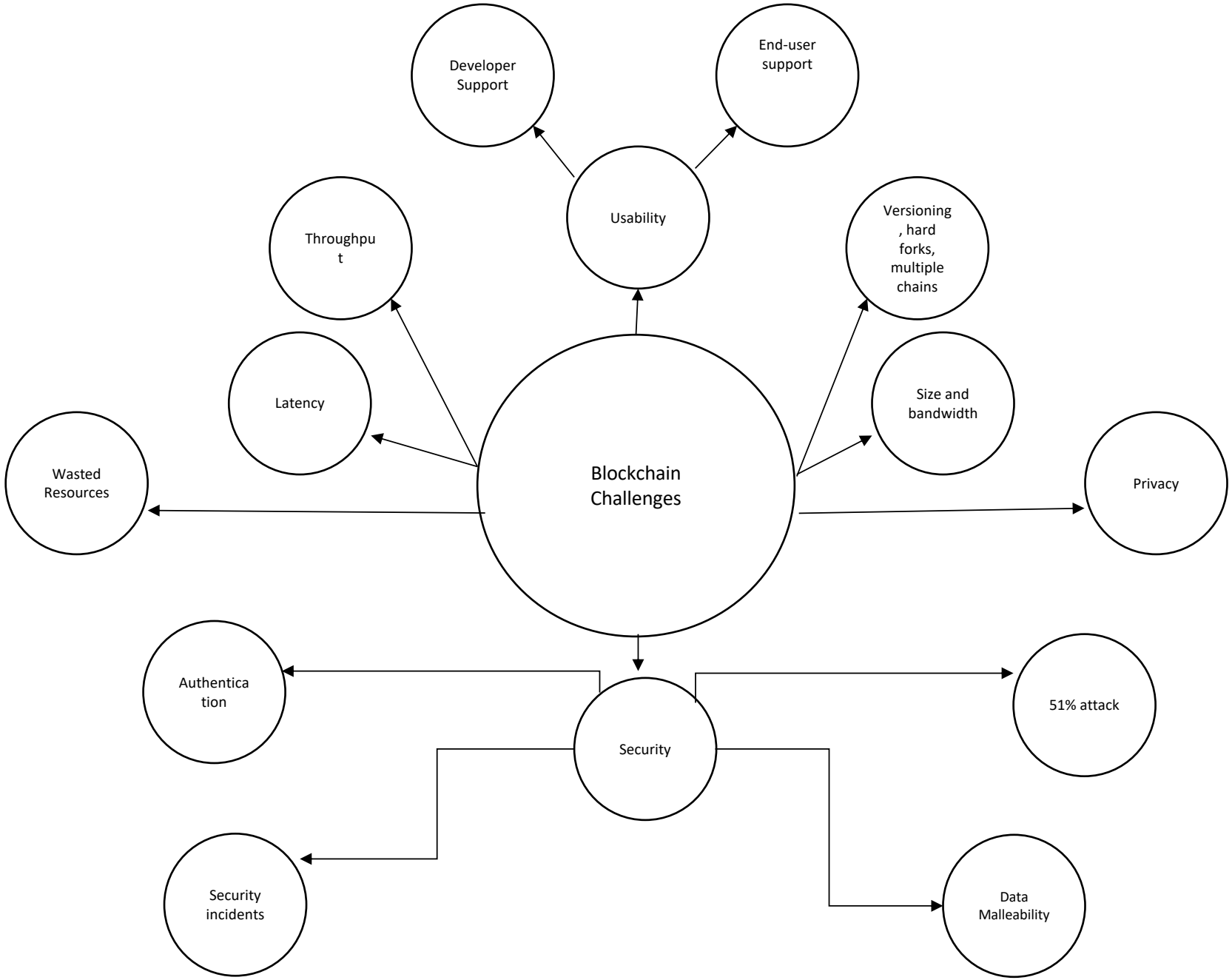
1: Strongly agree **2:** Somewhat agree **3:** Neither agree nor disagree **4:** Somewhat disagree **5:** Strongly disagree

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

Note: The lower the score, the more important the challenge is considered (1: very significant challenge; 5: no challenge at all).

Hileman, Garrick and Rauchs, Michel, 2017 Global Blockchain Benchmarking Study (September 22, 2017

Blockchain’s Promise ?


Developer Support
End-user support
Usability
Throughput
Versioning, hard forks, multiple chains
Latency
Size and bandwidth
Wasted Resources
Blockchain Challenges
Privacy
Authentication
Security
51% attack
Security incidents
Data 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

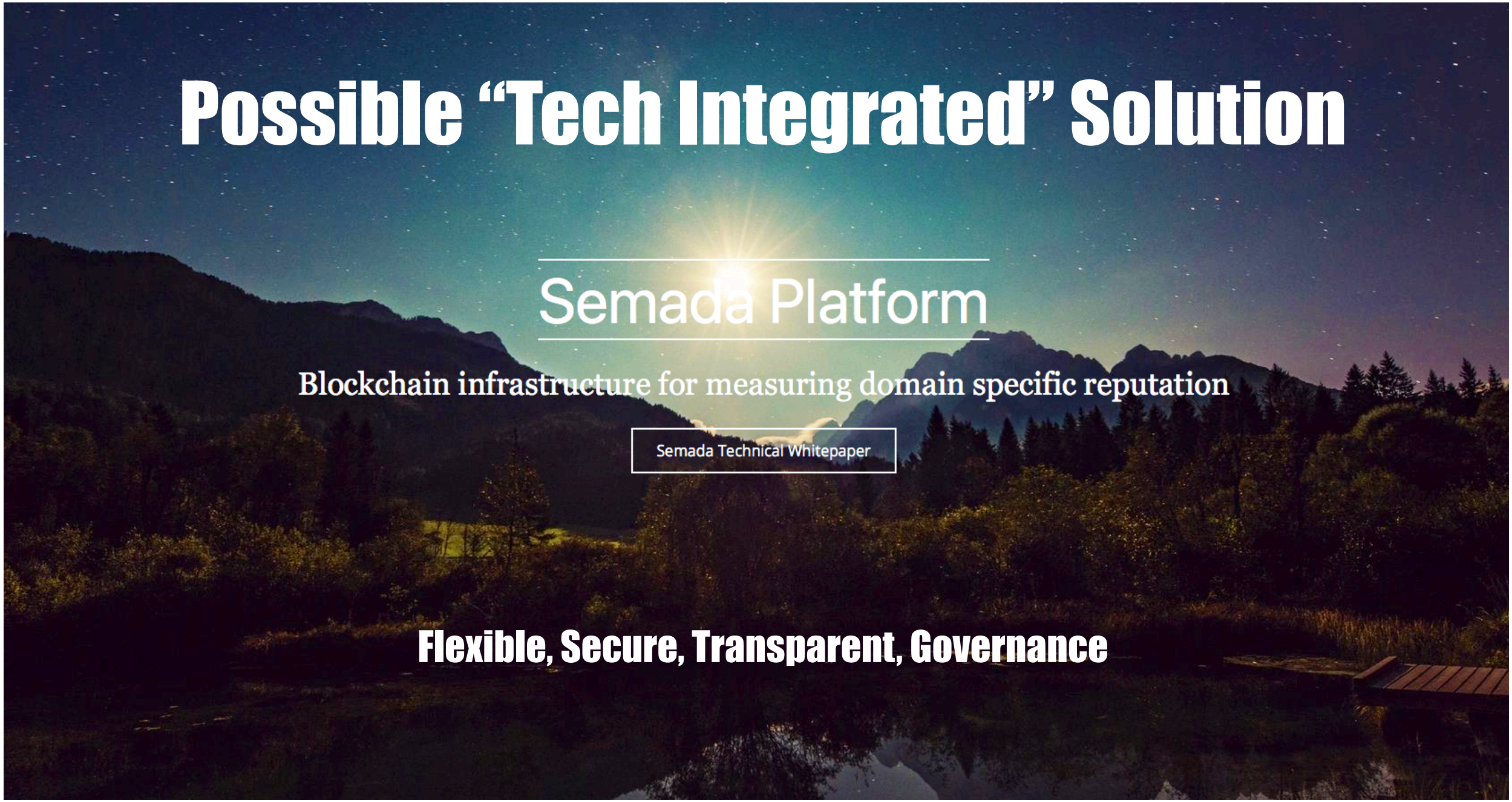
- Blockchain is trustless by design, to deliver a new type of trust.
- A new type of trust that we are not familiar with, nor are traditional institutions built upon.
- There is no point using blockchain in the same frame of mind of our existing economy and system.
- **How can we create true societal believe in the interconnected blockchains?**

Centralization Vs. Decentralization

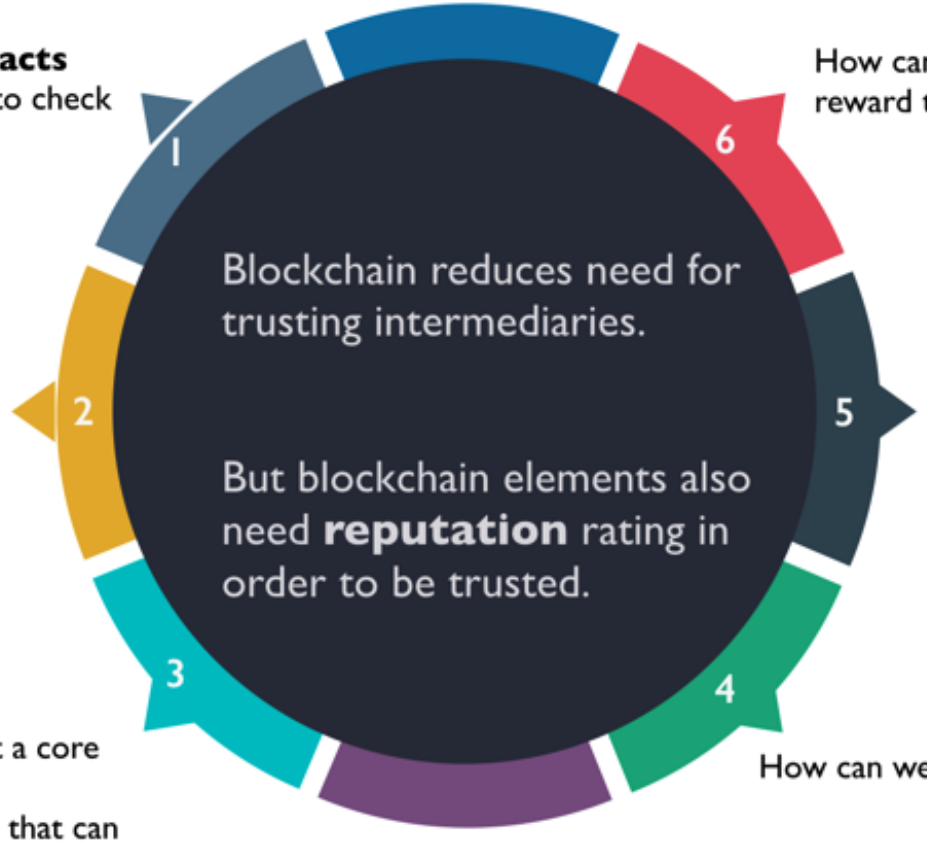
- Blockchain by design decentralizes power.
- Yet there's tension in that if we want to make sure blockchain is used for good
- Who defines "good" ?
- Need for a central authority to provide the guiding rules and principles ?
- Throughout history centralized authority has decided the "GOOD"
- Decentralized 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
Semada Technical Whitepaper
Flexible, Secure, Transparent, Governance

Reputation Verification Platform



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

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

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

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

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 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.

Parameter	SPoS Semada	dPoS EOS	dBFT POS NEO	PoS Cardano	PoS Casper	PoW BTC/ETH
1) Decentralized ● Large number of nodes ● Anyone can become a node? ● Nodes are not concentrated ● Censorship resistant ● Governance ● ICO process ● Regeneration	9/10 + 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	6/10 - delegate election protocol favors corruption of delegates (e.g., through loss of anonymity) - Sybil delegates likely by economy of scale of campaigning skill	6/10 - delegates similar to EOS - 66% network connectivity and participation required to guarantee liveness	7/10 +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)	7/10 - details not finalized; ad hoc solutions - concentrated rewards leads to cartels	7/10 - mining pools arise from economy of scale of computing resources; - lack of transparent governance process

Parameter	SPoS Semada	dPoS EOS	dBFT POS NEO	PoS Cardano	PoS Casper	PoW BTC/ETH
2) Scalability	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	9/10 + Delegation enables higher computational efficiency than PoW EOS: with optim. <=50k TPS Steemit: 1.2 mil T/Day	9/10 + ditto - 66% network connectivity required With optim. <=10k TPS	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	TBD ETH <=15TPS	5/10 - no SC Hash Mining <=3.3 - 7 TPS - Storage - Bandwidth -CPU/Memory
3) Language	TBD	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	8/10 + Python, Java, C#, F#	7/10 + Haskell functional language CBD safety - poor Haskell adoption world wide + IELE supports smart contracts written in any programming language that has a formal semantics in K, e.g. Simon	8/10 + Solidity (~C, JavaScript), Serpent &Viper (~Python), LLL (~Lisp), Mutan (~Go), Rust	5/10 Satoshi=C++, distributed binary data; limited functionality

Parameter	SPoS Semada	dPoS EOS	dBFT POS NEO	PoS Cardano	PoS Casper	PoW BTC/ETH
4) Security* *SPoS paper, Chapter 6 for definitions	9/10 + reward structure incentivizes honest block production, policing; continual protocol development fairly rewarded; flexibility allows pivots to increase security at expense of speed	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	7/10 - Similar delegate concerns to EOS - 66% network connectivity/ liveness required	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	TBD - ad hoc solutions; under development	9/10 +hash mining; openness - Long-term centralization concerns; censorship
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

Parameter	SPoS Semada	dPoS EOS	dBFT POS NEO	PoS Cardano	PoS Casper	PoW BTC/ETH
6) Corresponding Market	Reputation Systems, DAOs, IoT, Gig-Economy	Large enterprises / Apps that need high performance	Government ties Large enterprises	DAOs, large enterprises	DAOs, Smart Contracting sensitive to decentralization	Store of Value

Thank You

Join the Conversation!


wulf@wulfkaal.com


Wulf Kaal


Wulf Kaal


@wulfkaal


medium.com/@wulfkaal


Facebook.com/wulf.kaal


wulfkaal.com

wulfkaal