

Semada Research Institute

Reputation Protocol for the Internet of Trust

Conceptual Whitepaper

By

Craig Calcaterra, Wulf Kaal, Gopinath Sivalingam

Abstract

Internet-based platform businesses outcompete traditional brick and mortar business on nearly all measures of comparison. Similarly, distributed ledger technology (DLT) businesses depend on the internet and show a lot of promise in multiple business verticals. Yet, internet-based platform businesses and DLT businesses have not reached their full potential. Multiple studies, data, and anecdotal evidence suggest that one core factor that undermines their evolution is the worldwide decreasing trust in the internet and under-developed trust in decentralized technology solutions.

Semada and the Semada Research Institute (SRI) believe that a decentralized reputation protocol can reverse that trend to increase trust in the internet and increase decentralized technology adoption. We call this solution the Semada Internet of Trust - a network that uniquely captures real world information, context, and value in cryptographic transactions generating transparently validated consensus on truth. Through the creation of unconscious and conscious trust in decentralized networks adoption becomes a desirable outcome and increases.

Semada has a unique suite of protocols and a stable currency that combined enable commerce on the decentralized web. Semada's core architecture continually resolves the blockchain trilemma by combining - a) decentralization, b) scale, and c) security. Semada's version of proof-of-stake - a.k.a. the Anchor Protocol - is a unique consensus algorithm that enables block propagation through reputation staking and verification. Through its Sockpuppet Protocol, Semada is resilient to deceptive fake internet identities, so-called sockpuppet accounts, and 51% attacks. Through its Persona Protocol, Semada facilitates digital sovereignty, self sovereign identity, privacy, security and decentralized reputation. Trust enabling reputation can only be earned over time on the Semada network.

The Semada Internet of Trust creates a framework of trust through reputation and incentive optimization that enables market conditions for unprecedented business models and market capitalization while reducing adverse selection and moral hazards for transacting parties. The network will provide information symmetry while reducing transaction cost for market participants. Businesses will leverage the platform to achieve efficiencies across verticals.

Semada研究所

互联网信任协议

执行摘要

基于互联网平台的产业几乎在各项对比中都优于传统实体产业。同理，分布式账本技术（DLT）产业依托互联网技术，在多个业务垂直细分领域具有潜力。然而，互联网平台产业和DLT产业尚未充分发挥其潜能。多项研究，数据和轶闻证据表明，影响其发展的一个核心因素是全球互联网信任度下降，以及对分布式技术解决方案的信任不足。

Semada和Semada研究所（SRI）认为，分布式声誉网络可以扭转这种趋势，从而提升互联网信任，并提高分布式技术的应用。我们将此解决方案称为**Semada互联网信任体系**——一个将加密交易中的实时信息，背景和数值作为无可争议的真实信息源加以捕捉的网络体系。通过在分布网络中建立无意识和有意识的信任，从而达到理想的结果并提高应用。

Semada作为独特的区块链平台，与分布式网络极为契合。Semada的核心架构是通过结合a) 分布式，b) 规模化和c) 安全性，不断解决区块链的三难问题。Semada的权益证明（proof-of-stake）——即锚定协议（**the Anchor Protocol**）——一种独特的共识算法，通过声誉的建立和验证实现区块传播。通过其Sockpuppet协议，Semada可以抵御欺骗性虚假互联网身份，即所谓的“马甲”及51%的攻击。而Persona协议则有助于Semada在数字主权，自主身份，隐私，安全和分布式声誉等方面的推动。只有在Semada网络上才能实现建立在信任基础上的声誉逐渐增加。

Semada互联网信任体系通过声誉和激励优化的手段创建信任框架，为前所未有的商业模式和市场资本化提供市场条件，同时减少逆向选择和降低交易方的道德风险。该网络将提供信息对称性，同时降低市场参与者的交易成本。企业将利用该平台实现垂直领域的高效运作。

Table of Contents

Core Values	4
Problem	5
Internet-Based Platforms Proliferate	5
Trust Crises on the Internet	5
Internet-Based Platforms Use of Reputation Metrics	7
Internet of Trust	9
Semada Research Institute	9
Founding Principle	10
Reputation as True Decentralization	10
Motivation	10
Semada Research Network	11
Semada Platform	12
Protocols	13
Anchor Protocol	13
Selection Procedure for Block Producer in Semada Proof of Reputation	17
Validation Pool Block Verification	18
Block Production Salaries	18
Sockpuppet Protocol	21
Persona Protocol	22
Evolutionary Blockchain Governance Protocol	24
Core Semada DAOs	25
Anchor DAO	25
Network Improvement DAO	26
Stability DAO	26
Network Infrastructure for Decentralized Economies	26
DAO Infrastructure	27
Verification Platform	27
Reputation Economy	28
Decentralized Markets	30

‘a complete absence of trust would prevent us from even getting up in the morning’.

–Sociologist Niklas Luhmann¹

“A very large portion of "gig economy" startups are at the core basically just a dispute resolution system, a reputation system and a search engine.

If you're looking to build a decentralized version of one, maybe consider focusing on one component.” - Vitalik Buterin

Core Values

The Semada Team and the members of the Semada Research Institute share the following core beliefs:

- Freedom - means individual power and includes control of users’ personal info, individual security and privacy
- Equity - means distributed equitable allocation of power
- Collaboration for the common good - means improving power distribution by raising the power of the most individuals without harming the least powerful
- Efficiency - means the ratio of the useful work performed by a human, machine, or process to the total energy expended

Creating and maintaining secure and meaningful reputation motivates productive collaboration in a decentralized economy by focusing members' actions toward improving their DAOs for the promise of future currency rewards. The enduring nature of reputation linked to the blockchain promotes transparent and fair power distribution to those who contribute to the common good of a DAO and away from those who detract from this common good or cause harm to the least powerful.

The purpose of encryption technology on the blockchain is to safeguard individuals’ digital sovereignty and power over their personal privacy. Superficial identifiers such as physicality, sex, gender, race, culture, language, location, or group identification, which have traditionally disenfranchised minorities, are less relevant in DAOs with pseudonymous geographically distributed members. This encourages more opportunities in business and serves the goal of just distribution of power, creating an efficient and responsive meritocracy.

¹ Niklas Luhmann, Trust and Power, Chichester, John Wiley & Sons, 1979.

Problem

Internet-Based Platforms Proliferate

Internet-based platform businesses have been proliferating since the dot.com boom in the 2000s. With the increasing availability of big data, deep learning, machine learning, sensors and sensor data, as well as distributed ledger technology solutions, such technology-driven evolution of internet-based platform businesses can be expected to expand exponentially.

Since their inception, internet-based platform businesses have been disrupting centralized brick and mortar businesses. At least some evidence is provided by the disappearance of over half of the S&P 500 companies in the last 15 years. Competition from internet-based platform businesses is among the core factors that contributed to this trend.

Perhaps the dominant example that helps illustrate the prevalence of internet-based platform businesses is the comparison of a traditional brick-and-mortar business, such as Marriott, with a core internet-based platform business competitor, such as Airbnb. As of September 2016, Marriott is 90 years old with 1.1 million rooms listed in 110 countries, it has 127,500 employees and a valuation of \$17.8 bn, e.g. value per employee \$0.1m. By contrast, Airbnb is 9 years old as of September 2016, has 2 million listings in more than 191 countries, 4227 employees, a valuation of \$30bn, and a valuation per employee of \$7m. On all metrics of comparison, the internet-based platform business is dominating the brick-and-mortar business. While this is of course only one example of many others, it illustrates the core strengths of platform businesses and shows a trend in business development.

Internet-based platform services are so successful because their peer-to-peer capabilities make them compelling, efficient, and attractive in a fast-changing world. That is why people are so willing to place their trust in new businesses and brands.

But before they were widely adopted, trust issues that obviously exist in a peer-to-peer environment had to be solved. Why would consumers trust somebody you don't know or who is anonymous? Search algorithms, data analytics, and consensus protocols have helped digitize trust by minimizing bad experiences, maximizing great experiences, and avoiding unwanted issues (such as the double spending of cryptocurrencies). Yet, consumers continue to struggle with trust issues with these platforms. Digital trust may sound more attractive than institutionalized trust, but it still has its shortcomings. The most serious challenge for them are the trust crises on the internet.

Trust Crises on the Internet

Human lives are defined by who, what, when and how humans trust. While we tend to think of "trust" and "trusting" as a feeling or emotion, a better way to think of trust may be the particular types of decisions humans make. In essence, humans "trust" when we decide to take some kind

of risk. This trust can involve banal decisions such as what local supermarket to choose or which physician to select for a particular treatment. Trusting also involves a decision to expose ourselves to a danger of some kind. We decide to place our fate in another person or organization. As such, trust can be seen as the triumph of hope over fear. We overcome our natural aversion to risk in anticipation of a better future (a tasty meal, good health etc.). Every day, all of us make many different decisions to trust. Together, these choices define who we are and what matters to us.² But who, what, when and how we trust is changing.

The public trust in institutions and institutional governance, e.g. institutionalized trust, has been eroding for years. Scandals, corruption, slow procedures, human error, inefficient legacy systems, etc. increasingly destroy trust in the organizations and procedures of the modern world. As a result, we live in an age of diminishing trust in organizations and procedures. We are less and less willing to place our fate in the hands of incumbents and traditional ways of doing things.

To restore confidence in the “old world”, efforts have tended to focus on introducing and implementing more regulations, processes, and procedures. Yet, the traditional trust and cohesion mechanisms have reached their limits. Who and how we trust has already changed. The world of organizations (corporations, government, etc.), and procedures is being replaced by new forms of trust. Slow and expensive experiences have resulted in greater distrust in established institutions and their products and services.

This has driven the emergence of new and disruptive internet-based platform business models. Trust has become digitized and automated. We are much less trusting of organizations or procedures, but instead trust machines and algorithms.³ Yet, this digitized trust is experiencing its own crises which undermines the proliferation of value-enhancing internet-based platform businesses and DLT businesses.

The trust crises on the internet cannot be directly traced and have several origins and may in fact have a generational dimension.⁴ Because of the dominance of a few select broadband internet service providers, changes in the net neutrality rule, and concerted efforts at misinformation of the public via internet campaigns, the internet has become a network of vertically and horizontally integrated monopolies that create core deficiencies including: a) constrained knowledge exchange because of information silos, b) lack of competition impedes innovation (including at the protocol level), c) increased exposure to cyber and socially engineered attacks,

² Throughout human history, personal trust is first established within closed families and communities. Yet, in an industrialized and globalized world, trust is established by organizations (governments, businesses, schools, and other intermediaries) and procedures (rules, contracts, and hierarchies). Modern economy and society are built on the success of these more impersonal or institutionalized forms of trust.

³ <https://hackernoon.com/artificial-intelligence-is-more-than-just-a-technology-26d87774c011>

⁴ <http://www.pewresearch.org/fact-tank/2014/03/07/6-new-findings-about-millennials/> (“standing social science survey question, “Generally speaking, would you say that most people can be trusted or that you can’t be too careful in dealing with people,” just 19% of Millennials say most people can be trusted, compared with 31% of Gen Xers, 37% of Silents and 40% of Boomers.”)

d) diminished consumer protection and rights. These deficiencies in today's internet age consistently and progressively undermine trust on the web.

Human interaction with machines on the internet exacerbates the internet trust crises. Humans trust machines on the internet to store and process information and to transact with each other and with machines. Yet no centralized or decentralized authentication engine has typically verified the trust humans place in machines or otherwise enabled a trusting environment for internet-based transactions. Worse yet, today's internet is designed for hierarchical societal structures and with an underlying authoritative trust model. Many inefficiencies are associated with the traditional hierarchical trust model including serious cyber security vulnerabilities.

Several studies have provided evidence on the acceleration of trust issues on the internet around the globe.⁵ Trust issues in the United States can clearly be distinguished as exacerbated in international comparison.⁶

Cyber security attacks may be among the factors that help explain the decline in trust on the internet. Anecdotal evidence suggest that the cost of instigating cyber attacks have declined significantly. Cyber security attack can now be launched by unsophisticated parties at minimal cost with maximal potential for damage.⁷

By the year 2020 the majority of experts estimates that a total of 30 to 50 billion devices will connect to the internet.⁸ The prevailing opinion of these researchers suggests that the centralized version of the internet cannot scale to that level. This creates unprecedented cyber security issues.⁹ Decentralized authentication solutions for IoT devices are needed.

The Edelman report also suggests that trust is on the decline worldwide among multiple metrics. Fake news are contributing to this world wide trend.

Internet-Based Platforms Use of Reputation Metrics

Internet-based platforms use reputation metrics in an effort to improve their customer experience and their own business models. Those include Facebook's "like" mechanism as well as reputation rankings on Amazon, Uber, and Airbnb.

⁵ <https://pdfs.semanticscholar.org/036c/d160a736b6ba9ae6701565f3b93cb9f4ee1a.pdf>;
http://cms.edelman.com/sites/default/files/2018-02/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

⁶ http://cms.edelman.com/sites/default/files/2018-02/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

⁷ <http://fortune.com/2016/10/22/ddos-attack-hacker-profit/> (And despite the criminal reputation of Bitcoin, by far the largest method used to pay for DDoS-for-hire was Paypal.); <https://hacked.com/biggest-ddos-attack-2016-caused-angry-gamer/> (Angry gamer paid 7500\$ to bring down DynDNS service that cost 2.5 million dollars).

⁸ https://www.huffingtonpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_us_59a41fcee4b0a62d0987b0c6; <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>

⁹ <https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html>;
<https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx>

Several studies have demonstrated that existing reputation solutions for internet-based platform businesses are subjected to significant shortcomings.¹⁰ Resnick and Zeckhauser find that: “One of the earliest and best known internet reputation systems is run by eBay, which gathers comments from buyers and sellers about each other after each transaction. Examination of a large data set from 1999 reveals several interesting features of this system, which facilitates many millions of sales each month. First, despite incentives to free ride, feedback was provided more than half the time. Second, well beyond reasonable expectation, it was almost always positive. Third, reputation profiles were predictive of future performance. However, the net feedback scores that eBay displays encourages Pollyanna assessments of reputations, and is far from the best predictor available. Fourth, although sellers with better reputations were more likely to sell their items, they enjoyed no boost in price, at least for the two sets of items that we examined. Fifth, there was a high correlation.”¹¹

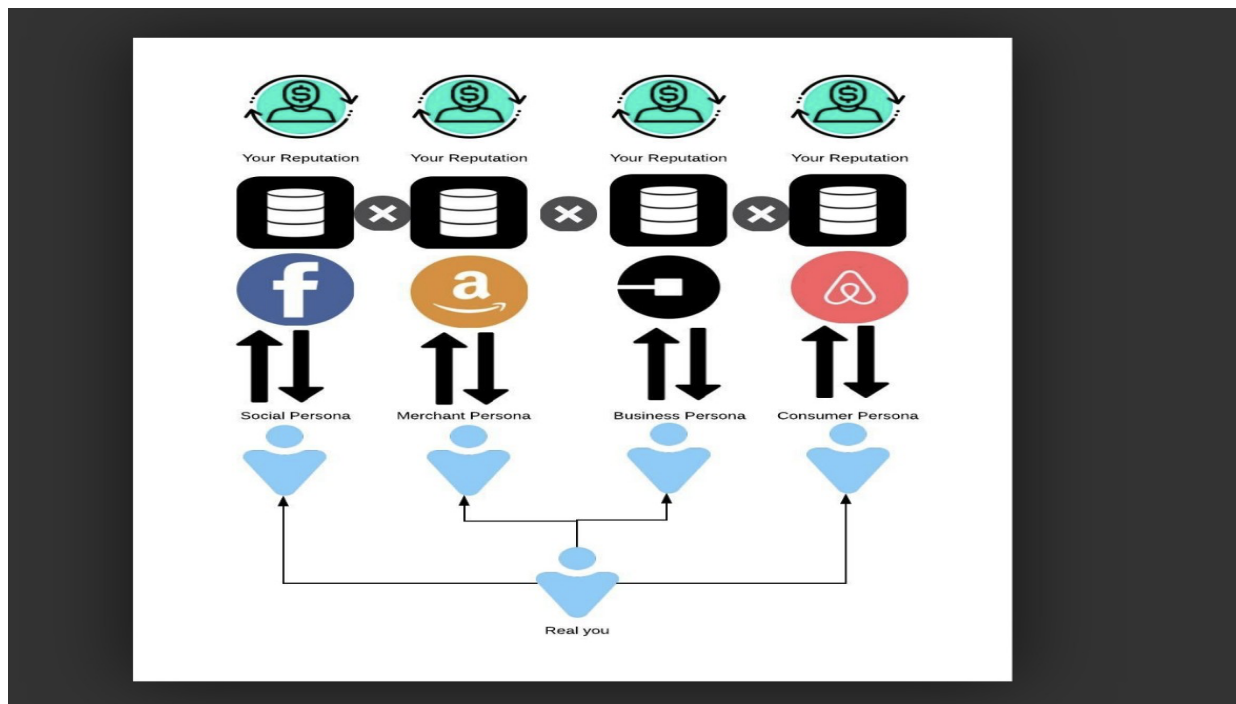


Figure 1: Internet-based platform’s use of reputation solutions.

The shortcomings of this use of reputation in internet-based platform businesses include the following:

¹⁰ <https://cseweb.ucsd.edu/groups/csag/html/teaching/cse225s04/Reading%20List/E-bay-Empirical-BodegaBay.pdf>

“The presumptive challenge to Internet-based feedback systems is to get buyers to provide feedback with reasonably high frequency, and to provide it honestly. Frequency is not a problem, presuming the feedback is unbiased. More than half of transactions receive feedback. However, the 0.3% negative feedback rate on transactions (.6% of those that provided feedback) and 0.3% neutral feedback numbers from eBay, our principal data source, are highly suspicious.”

¹¹ <https://cseweb.ucsd.edu/groups/csag/html/teaching/cse225s04/Reading%20List/E-bay-Empirical-BodegaBay.pdf>

- All centralized reputation scores can be sybil attacked, e.g. fake internet accounts (sockpuppets) or fictitious ratings disrupt true reputation scoring
- Users earned their reputation but do NOT own reputation - e.g. if Facebook and other internet-based platform businesses accidentally deleted user account, years of data would be removed and users have near zero ability to reclaim the data
- All financial and reputation scores are trapped in Silos. Such reputation data incompatibility undermines interoperability between platforms. There is also no way to aggregate user reputation in disparate platforms.
- Users cannot build reputation-based social capital - the platforms control the reputation and users cannot otherwise engage with the reputation built on such platforms.
- No Privacy: Employers have unfettered access and are checking people on social media and credit checks. No way to curtail for users
- No Reputation Data Autonomy for users
- No Reputation-Based Network Effect - lacking decentralized aggregation of reputation. Reputation currency created on the Platforms only benefits the respective platforms
- No Self-Sovereign Identity

Internet of Trust

While trust in old world organizations and procedures has been eroding for years, society is not convinced that distributed or decentralized peer-to-peer networks can deliver enhanced digitized trust. To truly enable a more distributed society, it is necessary to personalize and humanize digital trust.

Semada and the Semada Research Institute (SRI) believe that a decentralized reputation network can increase and humanize trust on the internet and in decentralized technology solutions. We call this solution the Semada Internet of Trust.

Core building blocks of the Semada Internet of Trust are Semada's protocols that enable a trust verification network.

Semada Research Institute

The Semada Research Institute (SRI) is a blockchain research laboratory that develops and promotes research built on the core reputation verification algorithm of the Semada Platform. Combining existing Semada protocols, such as Persona and Sockpuppet Protocols, among others, SRI's initiatives and research agenda is directed by the resolutions passed by the Semada Research Network (SRN). Together, SRI and SRN develop a research agenda to implement the Semada core as a truly decentralized reputation-based trust engine for the Internet of Trust in the distributed economy.

Founding Principle

A founding principle of the SRI is its recognition and affirmance of reputation-based networks as the inevitable and central methodology for any evolution of decentralized and centralized digital networks.

Reputation as True Decentralization

The transferability of stores of value entailed in cryptocurrencies creates core points of attack and undermines the very nature of decentralization. Because of the store of value entailed in cryptocurrencies (and really any currencies or store of value), exercise of power over such value inevitably leads to centralization due to economies of scale.

Reputation as a metric and store of value does not suffer the same consequences described above and does not lead to centralization because it must be earned, it can be lost, yet it cannot be turned into a fungible store of value that allows the exchange for goods etc. Hence, reputation does not naturally lead to centralization like currencies do.

Motivation

Does a need for a decentralized reputation-based research platform exist?

Conglomerates like Facebook, LinkedIn, Twitter, Uber, Airbnb, Yelp and other platforms have built platforms that capture reputation. Yet, nobody has created a truly Sybil-attack resistant reputation engine that cannot be corrupted, regardless of the economics at stake.

Smart contracts create new solutions and have multiple core benefits. The merciless mathematical logic of computerized code that makes up a smart contract is extremely valuable for **clarifying intent**, as well as making business transactions more **efficient** and **certain**.

Yet, smart contracting has several significant downsides:

- **Bugs:** Newly-coded programs, alas, always have the potential for bugs
- Human business interactions require a flexibility that is at odds with the **merciless mathematical logic of smart contracts**. Business interactions require:
 - Flexibility in **interpreting intent**
 - Ability to continue collaboration when **unanticipated eventualities** arise
 - Possibility that each party may **fulfill only a portion** of any intended collaboration

Business degenerates with smart contracting if left to its own devices:

The original vision for smart contracts is between businesses and clients following a “code is law” concept that self-executes and self-regulates, with often anonymous parties. This creates a zero-sum scenario where both parties are entirely incentivized to provide the minimum possible to fulfill the perfectly rigid self-executing contract. This type of business ultimately degenerates as people will spend extra effort to deliver the minimum acceptable products. In other words, both parties are bound by common sense to push the contract as far as possible in their own favor. The parties no longer create a harmonious long-term business relationship.

This effect changes if reputation of the counterparties is at stake. With the opportunity to create new valuable reputation tokens, members strive to act in ways which improve the platform for the long term instead of exploiting short-term arbitrage opportunities.

Semada Research Network

The development and evolution of Semada’s Internet of Trust requires a comprehensive research agenda. The Semada Research Institute (SRI) is a protocol research laboratory that develops and promotes research, architecture, and design built on the core reputation verification algorithm of the Semada Network. Combining existing Semada protocols, such as Persona and Sockpuppet Protocols, among others, SRI’s initiatives and research agendas are directed by the Semada Research Network (SRN), a decentralized autonomous organization (DAO) on the Semada Platform that originates and implements research proposals for the Semada Platform.

SRN is the research engine within the Semada platform. Its purpose is the identification of valuable new research ideas and protocol upgrades. SRN is a DAO on the Semada Platform and an expertise tag within Semada core.

Members of the SRN DAO develop and implement the research agenda for SRI by:

- 1) posting architecture expansion agendas or individual proposals, including via new use cases of Semada Core, and providing evidence of their research for protocol expansion, and
- 2) writing and posting code in Github or Bitbucket that is directly enhancing or further expanding the Semada Core architecture and/or its associated protocols, including its use cases and agenda.

SRN DAO Candidates:

Membership of the SRN DAO is contingent on being selected by the existing SRN DAO members. Candidates for SRN DAO membership only qualify if they posted valuable protocol upgrades that were upvoted by the existing members.

SRN DAO members get paid for their upvoted protocol contributions in both SEM Tokens and SRN Tokens. SEM tokens are fungible and traded on cryptocurrency exchanges. SRN Tokens are not fungible. SRN Tokens are the membership tokens that grant access to the SRN DAO. Only the SRN Tokens are used for voting on incoming protocol improvement proposals.

Semada Platform

Semada is building core protocol layers for the decentralized web. The core components of the platform are: a) core protocol stack to achieve consensus, repel network attacks and propagate transaction blocks, b) immutable decentralized memory ledger to store transaction blocks, c) network resource market/exchange to stake CPU, memory, bandwidth, etc. for rent seeking, d) programmable smart contract interface for transaction and resource manipulation.

The architecture is intended to solve the blockchain trilemma, combining scalability, security, and decentralization. The underlying protocols create inherent trust on the network based on a decentralized reputation system of trust scores. Semada is modular, has an advanced smart contracting platform and on-chain governance for swift protocol upgrades. Semada is resilient to Sybil attacks, tyranny of majority and 51% attacks. Through its universal trust protocol, Semada removes corruptible intermediaries and creates trusted paths to form an unprecedented trusted mesh as the foundation for the web 4.0.

Through cryptoeconomic incentives Semada adds network resources to process and propagate.

Semada is a decentralized platform that methodically builds trust for smart contracting parties and the smart contracting code itself. Semada properly rewards good-faith business behavior and smart contract development, providing an ideal evolutionary environment where business can continually improve and grow.

This evolutionary business environment is achieved by employing the basic strengths of blockchain technology: decentralization, an eternal record, and transparency. This allows Semada to create meaningful and secure SEM tokens which represent the reputation of members, with different types of tokens for every different type of expertise.

These foundational objects of secure and meaningful SEM tokens solve many basic problems in blockchain technology, such as giving the proper incentives for guaranteeing secure proof-of-stake consensus protocols for block production. This eliminates the unsustainable inefficiencies of proof-of-work based blockchains. Meaningful reputation tokens also naturally incentivize stable and productive on-chain governance for all protocol upgrades. With on-chain governance true DAOs are achieved for any type of business.

This general environment for creating DAOs provides the level playing field many independent companies require to negotiate and collaborate in developing the IoT. SEM tokens provide the membership identification layer for the IoT, where any device with the proper reputation can be

trusted to add or download information, and use smart contracts to automatically settle remuneration debts. The proper reputation is provided to a device if it is verified as being installed following the protocols specified by the particular DAO for the specific device.

Protocols

Anchor Protocol

Block propagation in the Semada platform is facilitated by staking reputation, not a fungible currency as in PoS. Accordingly, the consensus algorithm is called Semada Proof of Reputation (PoR). In the Semada network, this PoR protocol is called the Anchor Protocol because it is the first use of the underlying voting algorithm. Moreover, staking in the Anchor Protocol means anchoring your reputation to a block. In other words, Semada block producers anchor their reputation to a block, and if the block is invalid or cancelled out, their reputation depreciates.

How Semada uses reputation for block production and propagation.

Core comparison:



Consider a variation::

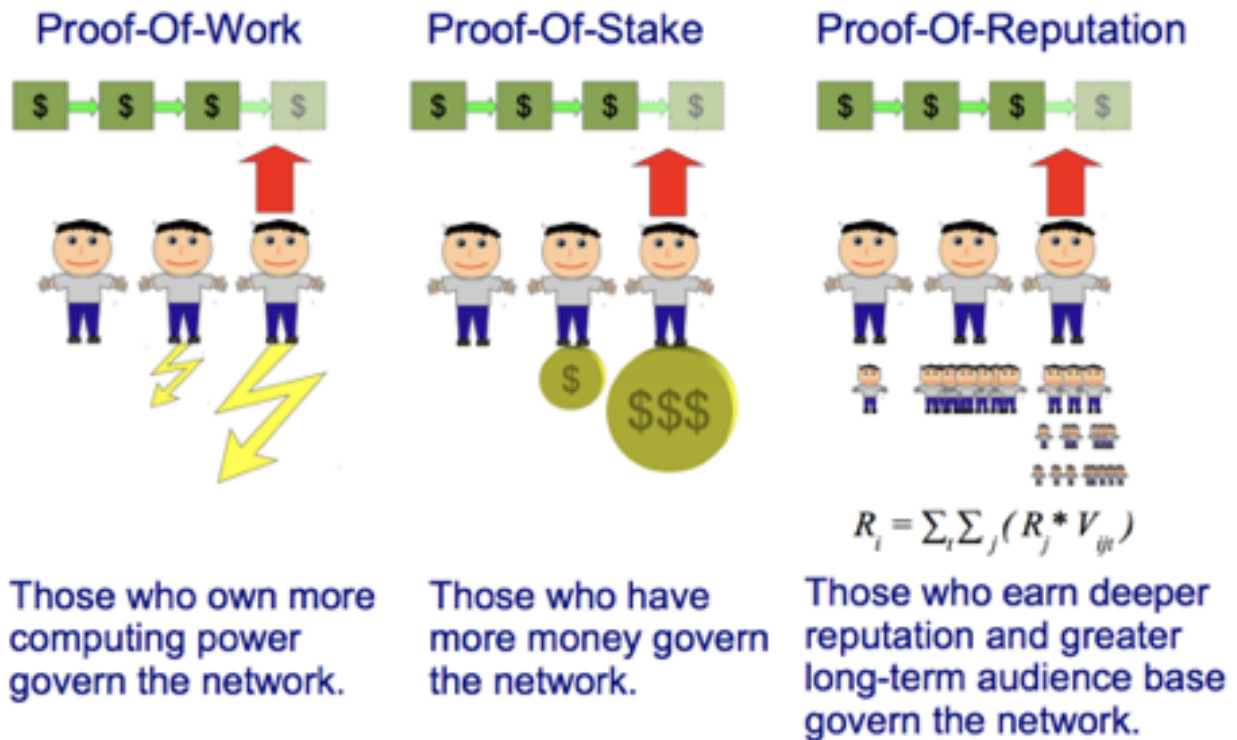


Figure 2: Figure 2 shows the core comparison of Proof of Work, Proof of Stake and Semada Proof of Reputation (otherwise known within the Semada infrastructure as the Anchor Protocol). While PoW necessitates slow and energy intensive hash mining, PoS enables some level of enhanced throughput through staking fungible currency that is used to qualify for block propagation. The fungibility of currency is the main point of attacks on PoS and leads inevitably to centralization. Unlike traditional PoS, PoR, e.g. Semada's Anchor Protocol, uses reputation scores as a non-fungible currency to qualify for block propagation. As such, the Anchor protocol (PoR) is attack resistant, fully decentralized, scalable and allows evolutionary protocol upgrades.

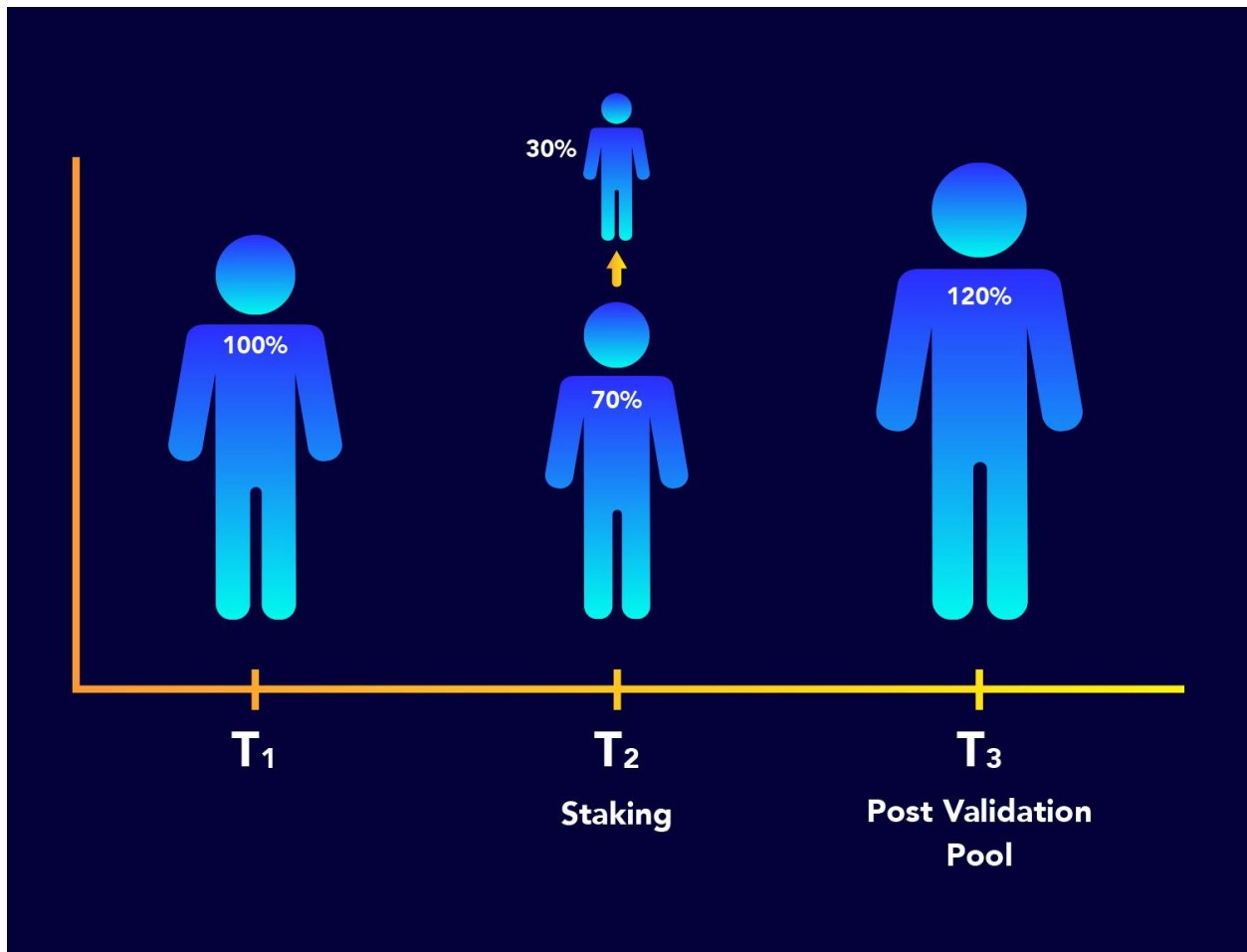


Figure 3: Figure e illustrates the staking mechanism in the Anchor Protocol and all Semada DAOs. In T₁, a DAO member has 100% of its DAO Reputation score at T₁. When staking at T₂, The DAO member takes part of her Persona, e.g. reputation score in that DAO, and stakes it either to qualify as a block producer or to participate in a validation pool. After the validation pool was decided in T₃, if the DAO member sided with the winners of the validation pool, her reputation was enhanced from 100% in T₁ to 120% in T₂. This process repeats itself as long as the DAO member actively participates on the Semada Platform by staking in her respective DAOs.

Anyone with any Anchor tokens has the potential to be a block producer. Semada Core (pseudo) randomly selects the block producers weighted by their holdings, meaning if you have more reputation, as evidenced by the Anchor holdings, you are more likely to be selected. This gives anyone on the planet, at any time, the opportunity to be a block producer.

Block production is scheduled ahead of time where a list of randomly selected block producers is selected weighted by their Anchortoken holdings in the specific DAO related to block production. When a block producer's time comes, they produce and publish the block, sending its reference and all fees included to Semada Core to open a validation pool (betting pool) where the other SEM Token holders can check the block is created according to protocol and vote accordingly. Consensus follows a slight variation on the GHOST protocol (greedy heaviest

observed subtree) that bitcoin and Ethereum use for proof of work, meaning the subtree with the greatest weight of SEM Token-backed votes is canonical. Then all fees collected from the block of transactions are distributed in the reputation-weighted salary.

So a successful block producer doesn't win the lottery with a great deal of fees if they are chosen, they win the lottery of half of a great deal of new reputation tokens if they are chosen while the rest of the members share the other half of newly minted reputation tokens for policing the block in the validation pool. This makes the whole system more stable (salary of fungible fees is regular and predictable as opposed to winning the lottery) and gives better incentives (e.g., there is less reason to join a mining pool, since all fungible fees are already shared in proper proportion, so it is more decentralized).

Active participation is encouraged because new reputation tokens are minted in every validation pool for every block. So block production is strongly encouraged (because a greater percentage of the new tokens are given to a successful producer) and policing is gently encouraged (you share in part of the new tokens with everyone who is active, which encourages activity but doesn't unstably slash non-participation (which can be innocent if the network is down, etc.)).

Producing bad blocks is slashed because the bad block producer will lose their availability stakes (the tokens the producer staked to be considered for the random selection of block producers) in the validation pool.

The computing resources are whatever it takes to make a block (no resources needed to hash mine). Currently making a block is very easy for a laptop or even a good cellphone to do.

Selection Procedure for Block Producer in Semada Proof of Reputation

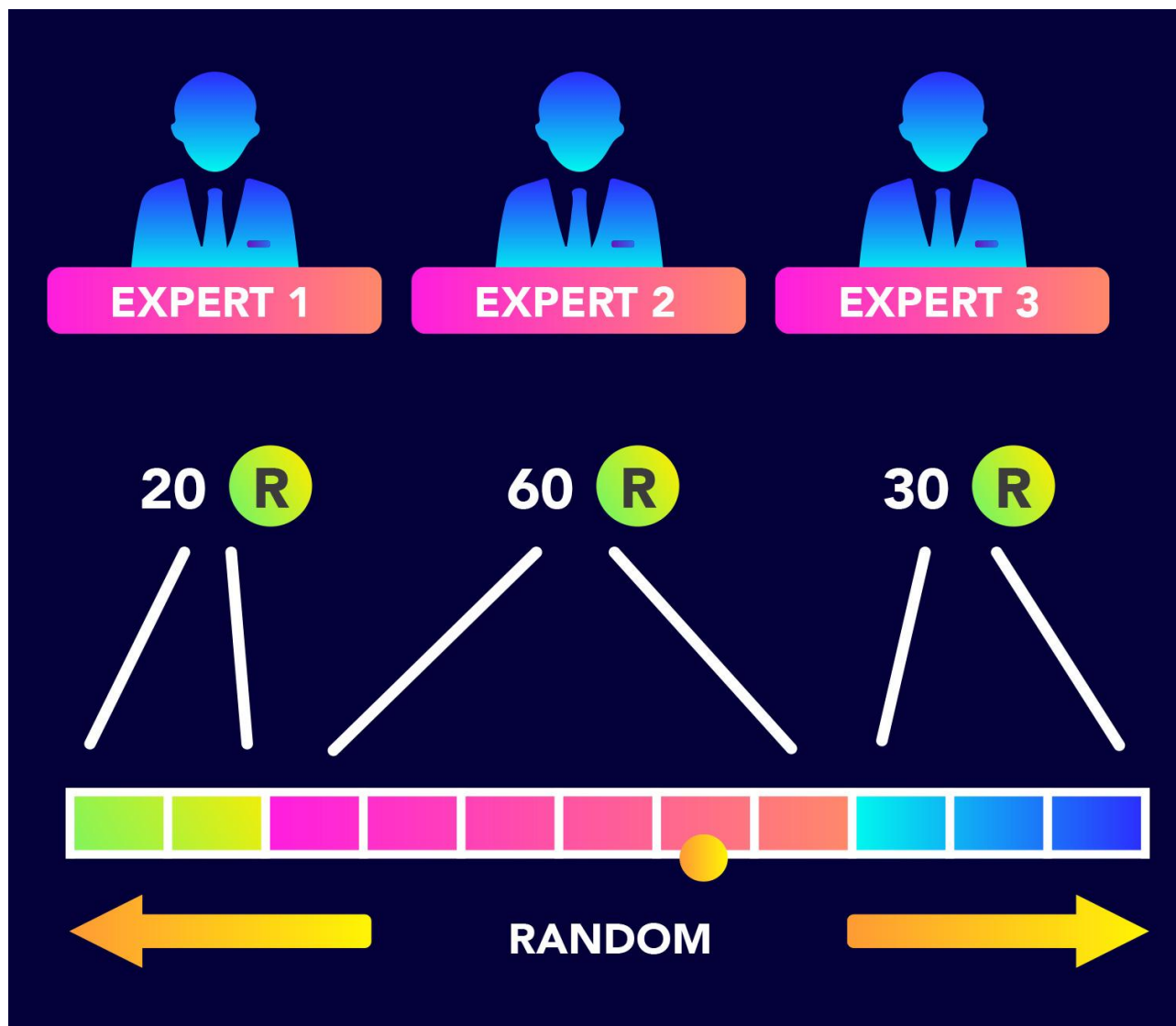


Figure 4: In the Semada Protocol, random selection of experts is decided by relative weight of reputation. Before a smart contract is engaged, experts have the opportunity to stake SEM tokens to signal their availability for work. These availability stakes will be added as the chosen experts' upvote bet on their evidence-of-work post. In this example, the yellow disk stops randomly along the bar, but is most likely to stop on the 2nd expert.

Validation Pool Block Verification

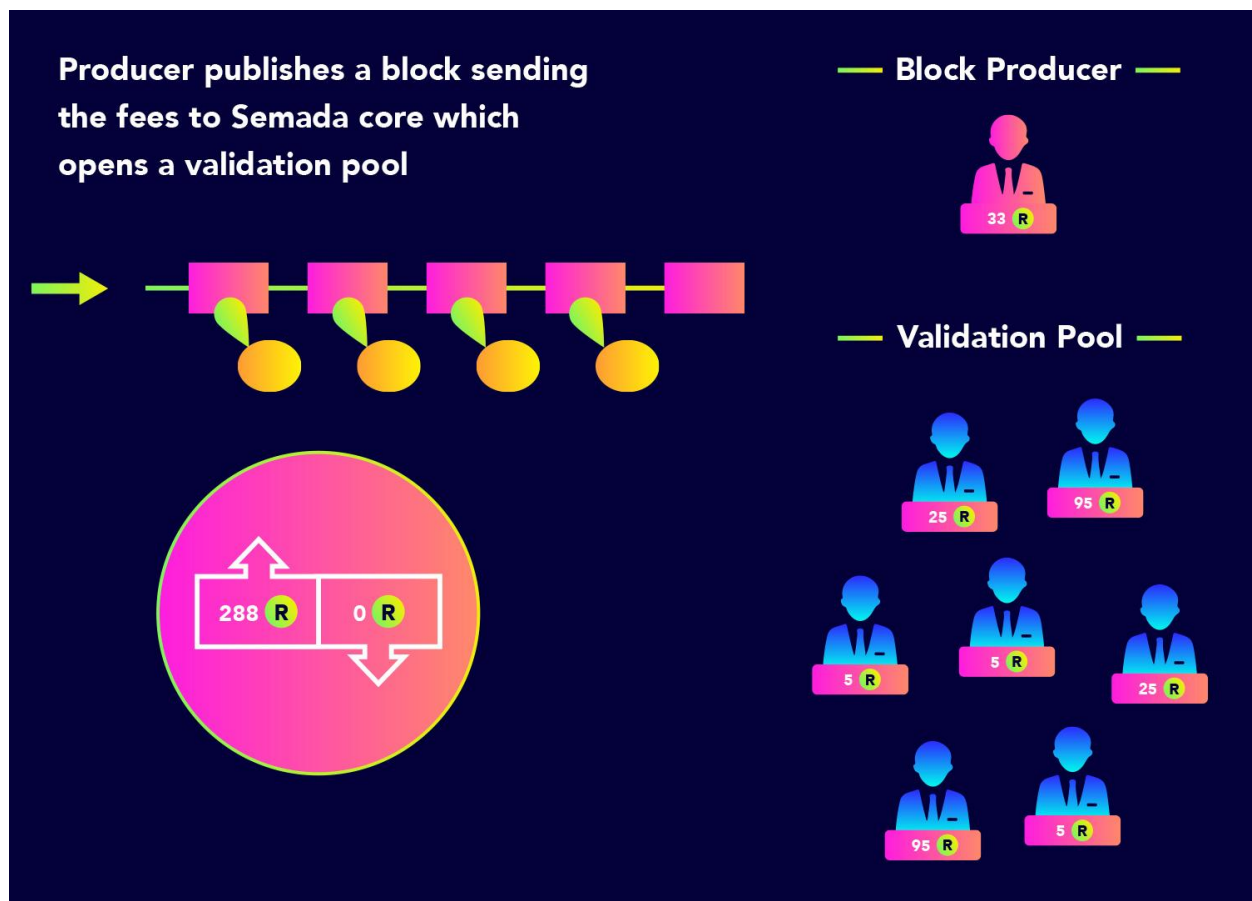


Figure 5: After the random selection of the Anchor token staked block producer as illustrated in Figure 4, the selected block producer collects all valid SEM-token gas-paying transactions in a block and publishes it. This proposed block is then sent to the Anchor tokenholder DAO validation pool. If the pool upvotes the block as valid, it is added to the Semada blockchain. The collected SEM token fees are distributed to all members of the DAO, as described below.

Block Production Salaries

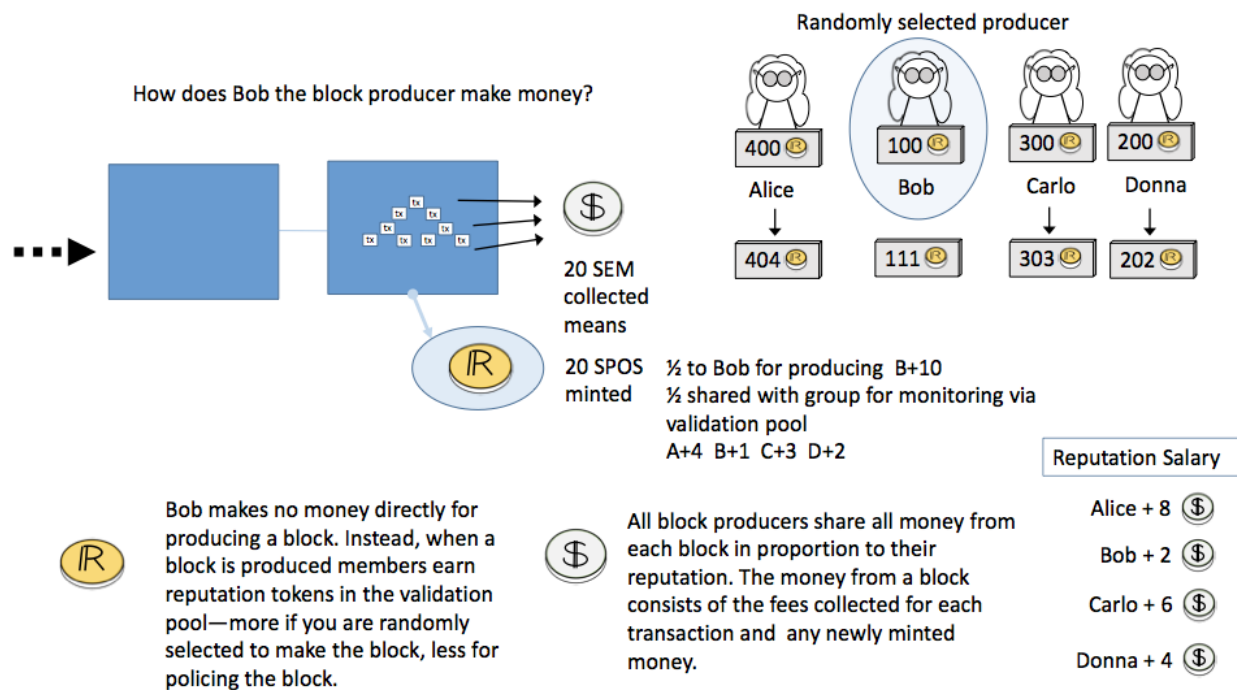


Figure 6: Figure 6 illustrates that after the block producer was awarded her SEM tokens for successful and validated block production, as illustrated in Figure 5, all Anchor token holders in the Anchor Protocol participate in the SEM token distribution from the block in proportion to their respective SEM token holdings.

Semada Reputation Salary Calculation Example

	Anch or		Proportional Anchor tokens		SEM Payout
Alice	404	$1020 \text{ Total} / 404 \text{ Anchor} =$	2.524752475	$20 \text{ Total SEM} / \text{Proportional Anchor} =$	7.92156863
Bob	111	$1020 \text{ Total} / 111 \text{ Anchor} =$	9.189189189	$20 \text{ Total SEM} / \text{Proportional Anchor} =$	2.17647059
Carlo	303	$1020 \text{ Total} / 303 \text{ Anchor} =$	3.366336634	$20 \text{ Total SEM} / \text{Proportional Anchor} =$	5.94117647
Donna	202	$1020 \text{ Total} / 202 \text{ Anchor} =$	5.04950495	$20 \text{ Total SEM} / \text{Proportional Anchor} =$	3.96078431
Total	1020		20		

How does Joe earn tradeable currency on the Semada Platform?

SEM tokens (traded on binance) are the tradable currency used for and within transactions (including as gas). Anchor tokens are the Semada block propagation reputation tokens available to the Semada block propagation DAO members.

The Anchor tokens determine who has power in the system for deciding:

1. who gets to make the blocks,
2. whether the blocks are valid in the validation pool, and
3. what percentage of the SEM token denominated reputation salary the Anchor token holders get).

The SEM tokens are the fungible (perfectly transferrable) currency of the system that are used in transactions contained in blocks, like bitcoin or ether. SEM is added to fees for each transaction by public users so block producers will add their transactions to the next block. These fees determine how many new Anchor tokens are minted for a block, then the fees are distributed to all Anchor holders in SEM denominated reputational salary.

New Anchor tokens are created in proportion to the number of SEM denominated transaction fees collected by the system in each block. Therefore, Anchor tokens are highly inflationary. To maintain his relative power, Bob must continue to participate.

Each time a block is produced, the SEM Token denominated fees from the transactions in the block are shared with the entire Anchor protocol DAO members as SEM Token denominated reputation salary (SEM Token is earned for each block in proportion to DAO members' Anchor token holdings). If Bob owns 1% of Anchor tokens, he earns 1% of all SEM token fees generated by transactions in the block (if block 1 has 50 SEM token and block 2 has 100 SEM, Bob always makes 1% of the SEM token fees in proportion to his 1% of total available Anchor tokens). Block producers do not gain immediate SEM token fees, only more Anchor tokens. If Bob doesn't participate in block production, e.g. Bob does not participate in the validation pool or does not stake an availability stake to be chosen for block production, he still shares the SEM token denominated reputation salary (for holding proportion of Anchor tokens as an Anchor DAO member) from the DAO member validation pool, but he does not share in the additionally minted Anchor tokens. Thus, Bob's relative power (as measured by his Anchor token holdings out of total Anchor tokens in circulation) and SEM token salary decreases.

Sockpuppet Protocol

Background:

The basic Web of Trust (WoT) works as follows: Keep track of your network transactions, and ask how well the people who are part of your transactions are satisfied with the interaction. If they also have a big reputation and are satisfied with the transaction then your reputation goes up. If you get a lot of these good transactions then you have a good reputation. It's bootstrapped with early adopters who are all trustworthy. If someone behaves badly their reputation will drop.

Here's the problem. If I use a lot of sockpuppet accounts, I can raise my reputation arbitrarily high, by behaving well for a while, then making a lot of transactions with myself and rating myself high.

So the solution that is always offered is to control entry by identity verification. The problem with this is, if the reputation is genuinely valuable, a sockpuppet account can afford to go through whatever hoops you have in place to create false identities (including stealing biometric data if necessary), then increase their reputation arbitrarily, as described above.

If the reputation is not valuable, then you won't be able to get honest users to go through the hoops required to identify themselves securely, since it's not worth it.

So the only time WoT works is when the service is not valuable, such as PGP (email which is essentially free). Then it's not worth it to create sock puppet accounts, so in that case you can trust the WoT network.

If you are trying to create an economic solution that is worth real money, where you need to be able to trust the other people in the network will behave well and follow protocol, you can't just assume their historical good behavior will prove their future behavior will also be good. Sockpuppet accounts allow us to automatedly game the system and falsely create valuable reputation, so we can leach whatever value there is out of the system.

The voting algorithm of Semada core is designed to combat that very system, so that it is not economically feasible to game the system without adding genuinely valuable improvements, as proven with the fees that are added to the system and the fair validation pool that every fee is subject to.

In summary, the Web of Trust is a traditional attempt to create decentralized reputation which is critically flawed and should not be used when fungible currency is at stake:

- It counts the number of transactions that are positive/honest and how much each member supports the other members (web of trust) - many DLT startups use this approach
- However, sockpuppet accounts can grow their value much quicker in the web of trust by validating each other. Honest users are much slower than the sockpuppets validating each other. Hence, the system is flawed.

Here is how Semada fixes this web of trust sockpuppet flaw:

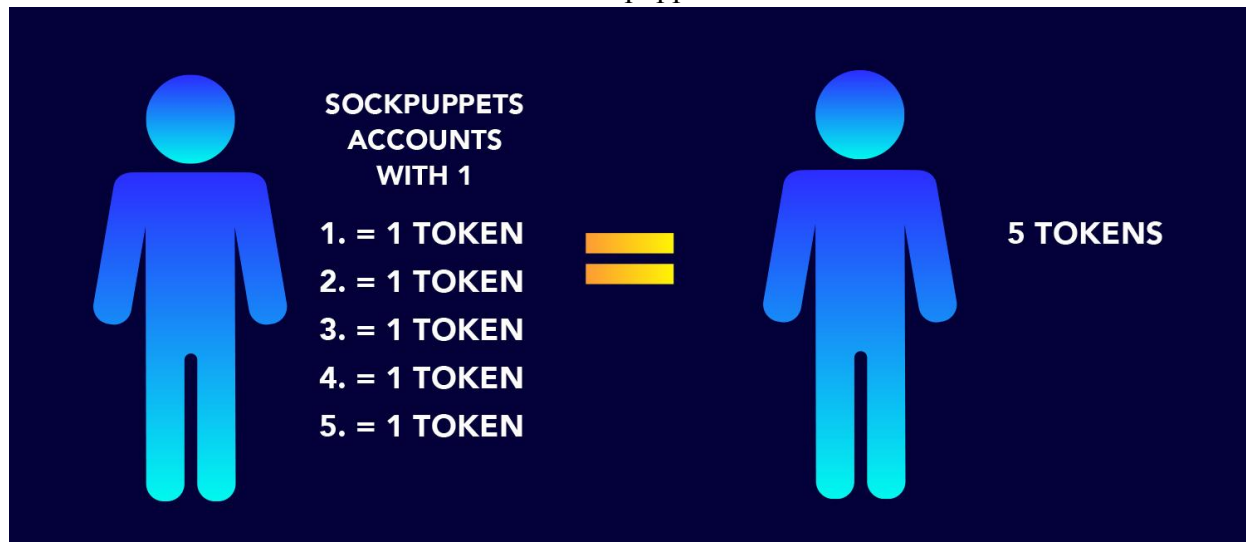


Figure 7: Figure 7 demonstrates that multiple sockpuppet accounts with 1 token each are still equal to a higher token amount of the same DAO member with only one account. In the Semada Persona Protocol, people, e.g. DAO members, can use sockpuppet accounts but they are wasting their efforts. Semada uses validation pools to make any change in rewards. All power comes from validation pools in relation to what DAO members stake, and all fungible currency rewards are shared fairly with the group in proportion to their individual reputation. The Sockpuppet Protocol thus breaks the incentives for Sybil attacks.

Persona Protocol

Background:

In the Semada Platform, anonymous DAO memberships define the reputation of their members by the amount of tokens the members hold in the respective DAO. The more DAO tokens members own the more the DAO, the system, and the platform respect the DAO member. The token is based exclusively on meritocracy. Physicality, group identification, race, culture language etc. are relatively superficial identifiers and do not play the same role in Semada as they have society historically. Semada may be seen as a forum for meritocracy, providing the most honest valuation of individual actions and contributions to a DAO.

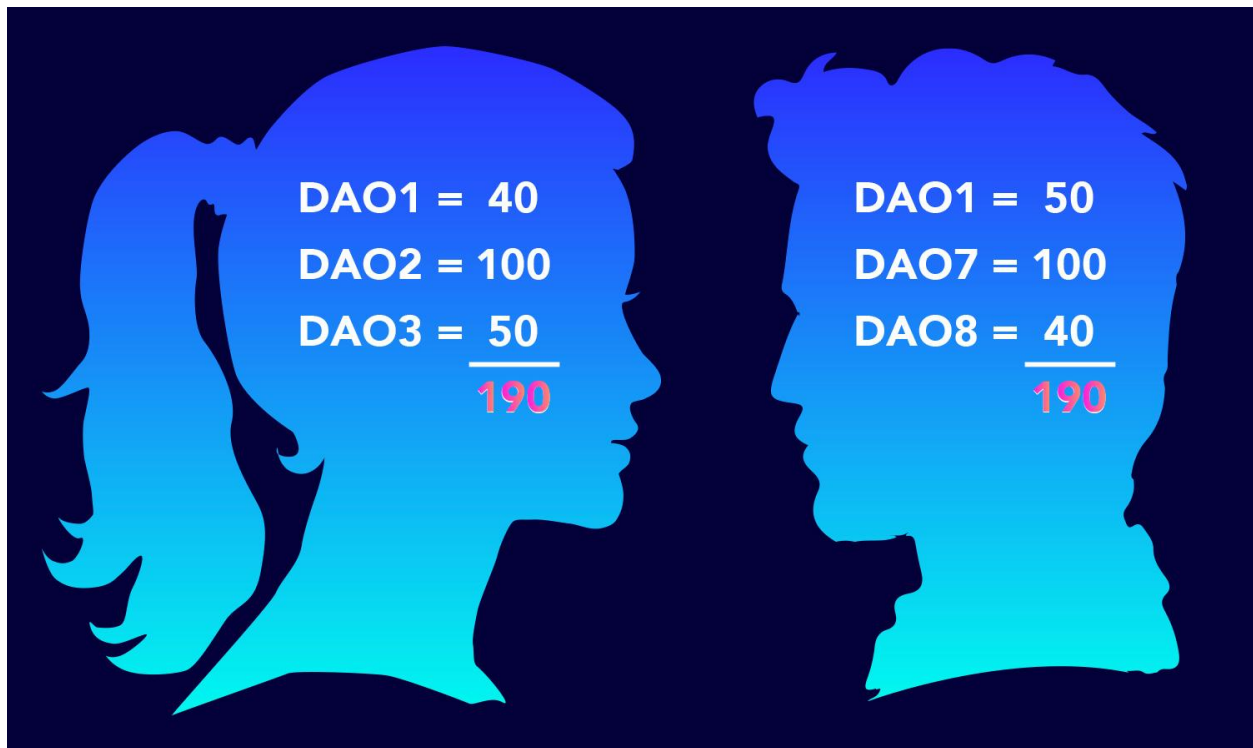


Figure 8: Figure 8 illustrates the respectively aggregated DAO memberships individuals on the Semada Platform may have that define their Self Sovereign Identity on Semada and ultimately the internet. In other words, Semada users are identified by their reputation scores in the respective DAOs they choose to become members of and participate in by staking their respective DAO reputations. Other commonly used identifiers such as social media provides, credit scores in centralized systems, etc., do not matter. The core identifiers are DAO token scores.

Different users may utilize such Persona Protocol Scores in different settings. The use cases for persona protocol scores are very wide ranging. Semada DAO scores are a conversation starter for people to engage with the platform and the individuals on the platform. For example, if person A has a very high reputation score in Semada Solidity Programming template Expertise tag / DAO, certain people will want to engage with person A just because of A's Semada Score in the respective DAO. Over time, the Semada team will use the Semada reputation scoring to engage with and emulate existing social identity networks.

From a social justice perspective, the Semada Persona Protocol takes power and spreads it out much further to people who have no agency in the centralized systems. In the existing systems very few audits exist that derive from the community itself. In any Semada DAO, community audits are at the core.

To facilitate DAO member onboarding and enable fully verified external wallets, SRI is developing proprietary mobile biometrics technology that allows users to sign in with their

biometrics into a particular wallet if they so choose. Semada uses zero knowledge proofs for its biometrics onboarding technology that guarantees continuing anonymity for users, once onboarded. User who wish to forego biometric identifiers via zero knowledge proofs on their mobile etc. devices can opt to become Semada DAO members in a completely anonymized way.

Evolutionary Blockchain Governance Protocol

The Semada protocol uses a weighted directed acyclic graph for a precedent system and DAO governance.

A graph is a collection of points, called vertices, with optional connections between vertices, called edges. The vertices of our graph are the posts to the forum. The edges are citations directed from one post (the referrer) to another (the reference). The edges give the graph direction, since references always point backward in time. Since there can be no time loops of references, the graph has no cycles, so it is acyclic. All in all, the forum is a directed acyclic graph (DAG).

DAO Governance Via Weighted Directed Acyclical Graphs

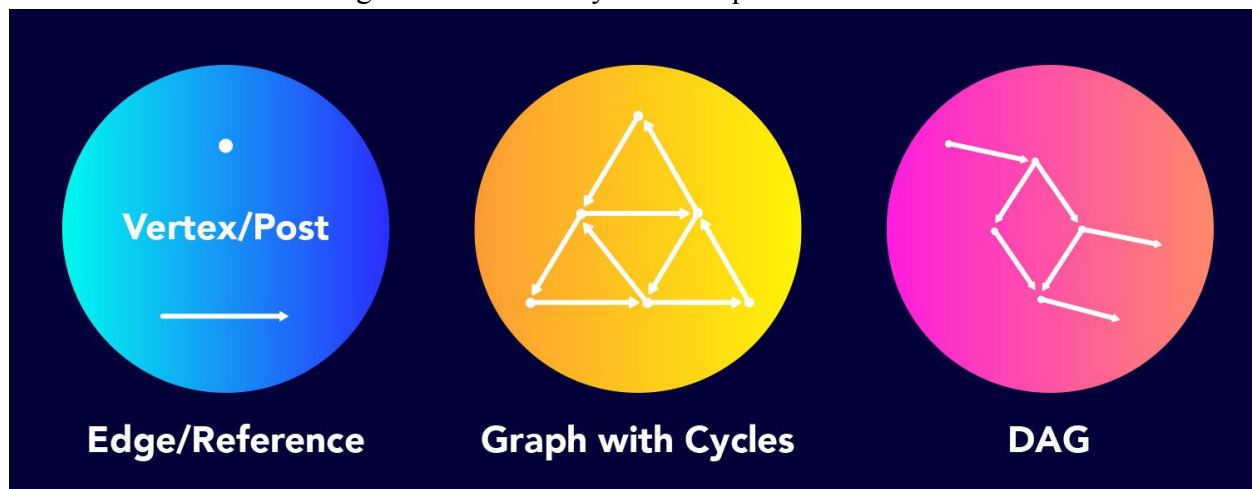


Figure 9: Weighted Directed Acyclical Graphs.

DAO Governance Precedent System via Weighted DAG

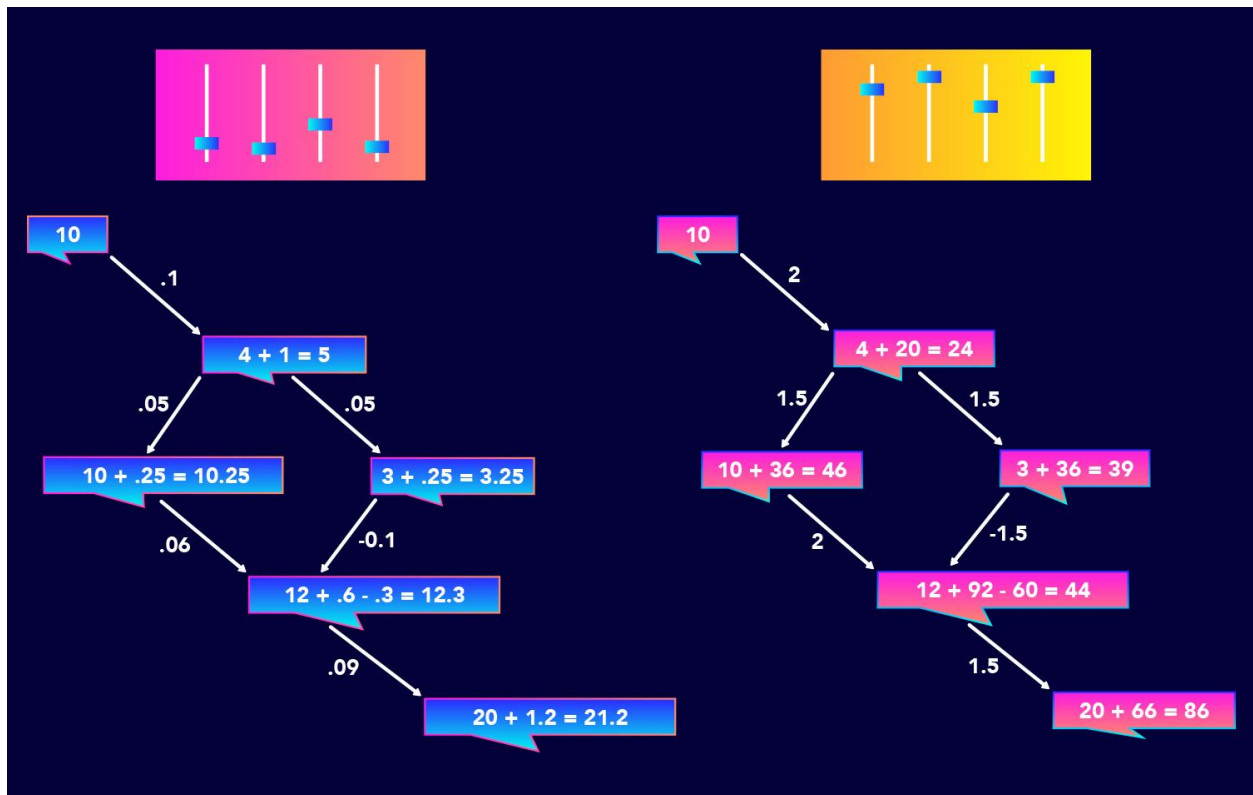


Figure 10: Weighted DAG Precedent System.

In the Semada Protocol, evolutionary DAO governance is enabled by the Weighted DAG precedent system. As Figure 10 above demonstrates, more reputation weight and salaries are allocated to posts on the Semada Forum that get continuously referenced by other posts. As a precedent dissipates over time, new precedence in the Semada Forum emerges naturally to replace older precedent. This is the essence of the evolutionary nature of the platform. As a matter of fact, entire expertise tags and DAOs on the Semada platforms can emerge and be replaced over time with new and improved systems naturally within the existing architecture of the platform.

Core Semada DAOs

Anchor DAO

The Anchor Protocol DAO is the Semada DAO responsible for block production. Each time a block is produced, the SEM Token denominated fees from the transactions in the block are shared with the entire Anchor DAO members as SEM Token denominated reputation salary (SEM Token is earned for each block in proportion to DAO members' Anchor token holdings). As Anchor DAO members participate in the block validation pools and join winning pools their Anchor token increases. Conversely, if they more often lose in validation pools, their Anchor holdings decrease.

Several subsidiary DAOs will be created based on technological protocol network needs to the Anchor DAO.

Network Improvement DAO

The Semada Network Improvement DAO (NIDAO) is tasked with network innovation for SRI .

Membership of the SRN DAO is contingent on being selected by the existing NIDAO members. Candidates for NIDAO membership only qualify if they posted valuable protocol upgrades and business proposals that were upvoted by the existing members.

NIDAO members get paid for their upvoted protocol contributions in both SEM Tokens and NIDAO Tokens. SEM tokens are fungible and traded on cryptocurrency exchanges. NIDAO Tokens are not fungible. NIDAO Tokens are the membership tokens that grant access to the NIDAO. Only the NIDAO Tokens are used for voting on incoming protocol improvement proposals.

Stability DAO

Semada's Stability DAO (SDAO) creates a core improvement over existing stability mechanism for cryptocurrencies. SDAOs is needed for multiple oracle functions in the stability mechanism and enables an unprecedented fully decentralized stability model. Some of its core improvements include:

- Fully decentralized policy decision making
- Full transparency of policy decision making
- Determination of the SEM / US Dollar exchange rate
- SEM monetary and fiscal policy decisions
- BOND token pricing and issuance decision [no. Market decides pricing via auction.]
- SHARE token pricing and issuance decision [I don't think so. SHARE tokens will probably all be gone to investors when SDAO starts.]
- Determine BOND expiration date (e.g. 5 years or less) for each BOND issuance [yes, but I suggest no expiration date; they should all be paid off.]
- Select a Consumer Price Index (CPI) for the peg (removing the US Dollar peg)
- SDAO determines artificial bond token price floor to ensure SDAO does not borrow excessively in attempt to limit SEM supply

Network Infrastructure for Decentralized Economies

Through its Internet of Trust protocols, SRI creates a network infrastructure for decentralized economies. The four core infrastructure solutions SRI created to facilitate decentralized economies include the DAO infrastructure for a network that continuously creates consensus for propagating transactions, the associated verification platform, the decentralized reputation economy, and the tokenization infrastructure.

DAO Infrastructure

Core to decentralized economies is a network that continuously creates consensus for propagating transactions irrespective of the device or its hardware capabilities. Over time, the Semada DAO Infrastructure will become the environment for hosting decentralized companies.

SRI's protocols facilitate autonomous self-governing networks of DAOs.

A good example that helps illustrate the DAO improvements over existing internet-based platform companies is Uber, the ride-sharing platform company. In essence, the DAO is a collective of people who decide to follow a certain protocol. Semada is the platform that helps the members of DAOs adhere to their own protocols. The Uber DAO on the Semada Platform can be seen as Uber the company with all its constituents except without the company, e.g. the entity, itself and its hierarchical governance structures. If Uber were a Semada DAO, the DAO collective of Uber drivers would become Uber, e.g. a fully decentralized company without hierarchies. The control and power over the Uber DAO would be completely in the hands of the DAO Uber collective. Yet, the staking mechanisms in the Semada protocols make the voting structure different than any previous attempts at creating liquid democracies.

Several core benefits are associated with the DAO infrastructure for decentralized platform businesses. First and foremost, the pricing should not be determined by the company Uber. The drivers and their passengers know best what pricing can work among them. The pricing for rides would be determined by the DAO members and their passengers. Hence, the marketplace is in the DAO itself. Second, the decentralized network of DAOs is significantly more efficient because the centralized fees, e.g. in Uber's case 25%, can be shared between the drivers / DAO members and the passengers. Third, the decentralized DAO business infrastructure is more efficient because the drivers themselves know best how to assess other drivers as members of the DAO. Fourth, the DAO collective enables unprecedented information symmetry among all constituents because unlike centralized internet-based platform businesses, DAO members continuously, iteratively, and incrementally evaluate all information pertaining to decision making metrics and protocols that govern the DAO. More complex DAO arrangements can be further governed by smart contracts. Because of the information history of the smart contracts, users can further get paid for improving smart contracts.

The combined efficiencies of DAOs over existing businesses suggest that DAO businesses could effectively overcome collective action problems and outcompete internet-based businesses such as Uber.

Verification Platform

Through its DAO infrastructure, the Semada platform enables expertise tags, e.g. individual DAOs on the Semada platform. Such DAOs can be used to verify otherwise uncertain or questionable information in both centralized and decentralized businesses. Verification DAOs help create direct and conscious as well as indirect and unconscious trust in the internet.

Examples of the DAOs that could benefit from the unified frontend UI that functions as Semada's verification engine include but are not limited to the following:

- Oracle DAO for decentralized business and blockchain connectivity and interoperability
- Wikipedia DAO. For example, compare Wikipedia today with Wikipedia on Semada. The Semada Wikipedia DAO would allow all DAO members to vote on each person's contributions. This would create a self-policed ranking of valuable contributions.
- Fake News DAO
- Decentralized credit score DAO
- Underwriting DAO
- Rideshare DAO
- Meetup DAO
- Publication Board DAO

Reputation Economy

SRI recognizes the shortcomings in internet-based platforms' attempts to use reputation. Based on that recognition, SRI has developed the core Semada Architecture as a new platform that enables a decentralized reputation economy.

Current internet-based platforms use reputation to improve their centralized control structures.¹² By contrast, SRI's core protocols facilitate the infrastructure for a decentralized reputation economy.

¹² See critique supra @[_].

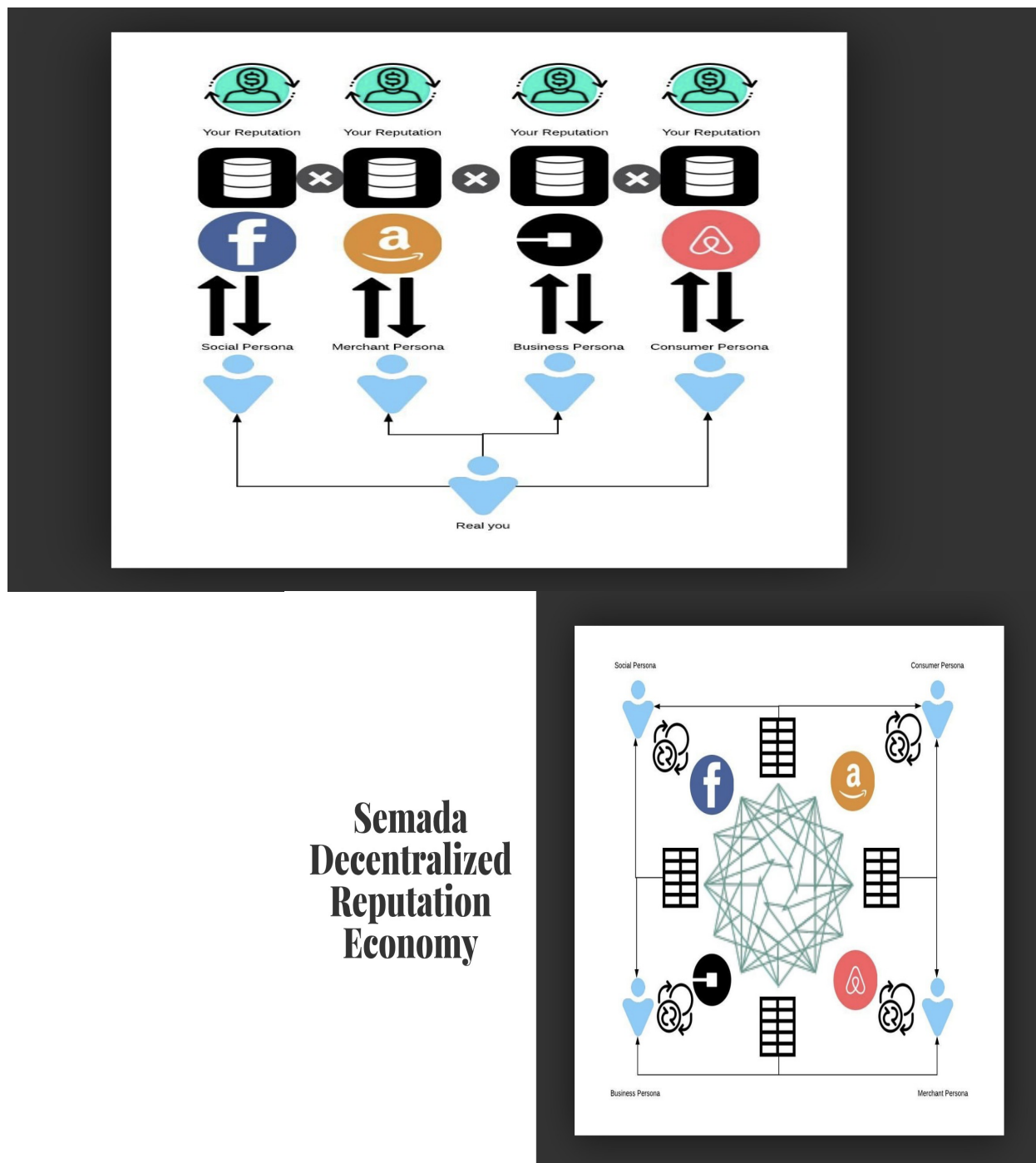


Figure 11: Comparison Existing Centralized Reputation Solutions vs. Semada Decentralized Reputation Economy.

SRI's decentralized reputation solutions have several advantages over existing internet-based platforms' attempts at utilizing reputation to improve their business models:

- Interoperable contextual reputation scores remove reputation data silos

- Reputation scores and reputation personas, e.g. profiles, cannot be created by fake internet accounts. The Semada Sockpuppet Protocol enables that through its sybil attack resistance
- Users build and actually own and control their respective reputations through the respective Semada DAOs in a fully decentralized way. The system is designed to avoid and disable any form of centralized corporate control over reputation
- Decentralized reputation scores allow users to build reputation-based social capital. Since the users own their own scores, they can now use their reputation scores to gain traction in various business contexts
- Complete privacy through anonymity of scores
- Users gain full reputation data autonomy

These core benefits of Semada's decentralized reputation solutions can create unprecedented business models and new forms of economic output that facilitate a decentralized reputation economy:

- **Network Effects:** are created by removing data silos via interoperable contextual reputation scores, combined with users' social capital, new network data, and users' self-sovereign identity
- **New Network Data:** The reputation solutions create an unprecedented kind of data SRI calls Rich Context Reputation GRAPHS which create new networks based on different kinds of reputation data
- **Social Capital:** Users' control over their reputation creates social capital that can be applied and utilized in unprecedented settings, facilitating new business lines and options for capital formation
- **Self-Sovereign Identity:** Semada Persona Protocol Human Uniqueness Identifiers enable users to control their own digital identity to identify or de-identify from the network

Decentralized Markets

- Decentralized markets as the next organic evolution of marketplaces through reputation verification
- How capital markets function today and how they would function in a decentralized market