Physical Freedom Requires Digital Freedom

The Digital Community Manifesto.

DIGITAL RIGHTS, GAME THEORY, AND GOVERNANCE OF SCALABLE BLOCKCHAINS FOR USE IN NETWORK STATES

FIRST EDITION MAY 2025

@theycallmedan, @starkerz

Chapter 1 – Pre-Word

The legacy economic system only responds to legitimate parallel competition that treats people better.

Introduction

This book (and accompanying audiobook) forms a go-to reference for understanding and achieving true decentralisation in social community blockchains and digital Network States. We believe in a model with:

- **No Pre-Mines** (*For further information see Annex I – Glossary of Terms and Acronyms*)
- **No ICO's (Initial Coin Offerings –** *for further information on ICO's see Annex I – Glossary of Terms and Acronyms***)**
- **No Companies or CEOs**
- **No Early Venture Capital**

Instead, the community should guide the technology and governance, maintaining the neutrality of the base layer for itself, ensuring freedom and participation for everyone.

We will explore the game theory of network attacks, attack vectors, how to defend against attacks, guiding principles for decentralisation, a realistic vision for the future, and the best technical stacks for censorship resistance and governance. You will find an in-depth discussion of:

- **Reputation and Governance Mechanisms**
- **Tokenomics and Immutable Communities**
- **DAOs and New Funding Models**
- **Future Implications of This Technology**

Throughout, we emphasize how these decentralised approaches may reshape society. We plan to illustrate our concepts with real-world examples of communities that have implemented them. This is a fully open-source, community-driven work, freely available to anyone who wants to replicate or expand upon these principles.

Why Document This Now?

The community forming what has become the back bone of the Hive Blockchain has endured years of conflict, evolution, and successful defence against multiple takeover attempts yet it remains decentralised. The ability to remain decentralised over almost a decade at the time of publishing, means there is noteworthy knowledge to be gained and lessons to be learned from dissecting how Hive's community achieved this resilience. In doing this, we reveal the critical requirements and pass on an industry standard for any other community network and Network State hoping to:

- **Stand the greatest chance of true decentralisation**
- **Remain censorship-resistant**
- **Thrive economically and socially**

Our ultimate aim is to document the "how and why" of proper and principled decentralisation, including the deeper implications for human freedom. In a world often controlled by entrenched power structures hostile to genuine decentralised, and therefore neutral systems, this knowledge is recorded immutably, and preserved under the account under the account @networkstate on the

Hive Blockchain one of the most principled, battle hardened and proven communities in decentralisation.

The next 25 chapters (you are reading Chapter 1) are the product of **20+ months of filming, writing, systematic break down of underlying principles and technology and continuous reflection**. Each topic builds on the last, culminating in a holistic framework for decentralised governance and secure digital communities.

For those of you interested in understanding more about how this book was created, go to https://hive.blog/@networkstate to see the discussions and conversations that went into the creation of this work, as well as see the immutable text version, stored on the blockchain, so that the ideas, essential for digital freedom within cannot be erased from our consciousnesses.

This is a new field of human understanding and so we invite your input. Constructive dialogue helps refine these ideas and is essential to the understanding of the principles required for this burgeoning field which is essential to the maintenance of digital freedom and digital rights into the future. It is long overdue that we share these methods in a digestible, publicly documented way, so others may replicate them and maximize their own decentralisation and digital self-sovreignty.

Scope and Purpose

Decentralisation, at present, is a term widely misunderstood in the crypto industry. Many projects, including Ethereum and most other leading, reputed crypto projects are not actually fully decentralised. Launched with conflicts of interest from ICO's, founder stakes, and pre-mines, amongst many other conflicts, such mechanisms often embed weaknesses that undermine genuine decentralisation in the long run.

We will contrast such pitfalls with a more robust formula for censorship-resistant design. In particular, we show how projects can thrive without centralised corporate structures or seed round investors. By removing these single points of failure, communities can achieve:

- **Self-Sovereign Token Economies**
- **Immutable Social Layers**
- **User-Owned Governance and Reputation Systems**

This work aims to become both an industry and societal standard on decentralisation for social and Network State type communities. By explaining the precise steps and technologies, we hope everyone can more easily understand and if they choose, build their own censorship-resistant networks, taking many of the foundational, timeless lessons explored in the following paragraphs about true decentralisation and what is required to achieve, maintain, attack, defend, apply, and expand it.

“You Must Know Your Worth Before You Can Be Worth Anything”

The Hive community has a history of being one of the only blockchain communities which successfully defended itself against centralised takeovers, removed exploitative stake, and fortified governance, and so sets a vital precedent which can be studied and replicated. These successes and the underlying lessons can serve the entire world as it searches for more equitable, secure ways to operate.

We believe there is a specific method for achieving and sustaining decentralisation, an approach offering genuine freedom and a more enlightened path on Earth. In a world where established power structures often oppose truly decentralised systems, it is crucial to document, debate, and preserve the knowledge gleaned from this text storage based blockchain community.

Make a Value4Value Donation to Support this work:

If you found the information in this work valuable, please do consider returning some of your value back to the authors way with some Value4Value. Value4Value is a monetisation model, a content format, and a way of life. It is about freedom and openness, connection and free speech, sound money and censorship resistance.

Time - Your time & attention are valuable. Spending them is valuable in and of itself.

Talent - It doesn't have to be money. Whatever your skills, there are many ways to give back.

Treasure - Thanks to the Bitcoin Lightning Network, Hive Backed Dollars, and other forms of monetary transfer, value can now be exchanged permissionlessly, instantly without friction and completely outside of the legacy economy.

Donate **Lightning** to:
networkstate@sats.v4v.app

Donate fee-less **HBD** (Hive Backed Dollars) to:
@networkstate

Use Hive Keychain
Wallet scanner

Contributors:

- **Voice for audio book** - @alohaed, **Cover graphics** - @rubencress, **Content assistance** - @eddiespino, **Technical Input and finding out literary and technical mistakes** – Thanks to various Hive Blockchain community members over the years for teaching us this stuff. And in particular: @alex-rourke, @blocktrades, @brianoflondon, @meno, @rubencress, @ura-soul, @vaultec for their reviews of this book and for spotting our mistakes!

We invite anyone to challenge the ideas in this book at the official blog spot https://ecency.com/@networkstate We will incorporate your ideas in future editions and mention your username in this contributors part

Our hope is that this book:

- **Clarifies what real decentralisation means.**
- **Shows how to maintain it practically.**
- **Establishes a replicable model for future projects.**
- **Assists the reader to participate in discussions about whether or not a project is actually decentralised.**

No single person or company can define “freedom” in a decentralised ecosystem it must emerge from the community itself. These chapters will detail our experiences, analyses, and guidelines to ensure your community can thrive, defend itself, and stay decentralised for generations to come.

In freedom, and in defence of it, let us begin.

@theycallmedan, @starkerz, May 2025

Table of Contents

Chapter 2 – Vision and Implications of Decentralisation for Network States

A peaceful way to opt out of past, present, future and increasingly oppressive legacy economic systems

Introduction

Decentralised technology extends far beyond the realm of digital payments; it gives communities the tools to form autonomous "Network States" online. As these groups gain genuine self-sovereignty, they can voluntarily exit failing systems and design their own economies and governance structures. This chapter examines how decentralised communities can evolve into fully realized digital sovereignties, ultimately achieving the kind of real-world recognition once reserved exclusively for traditional nation-states.

2.1 What is a Network State?

The Network-State is in contrast to the nation-state. Here we have a governance system that is based upon where one is geographically born. That is how citizenship is established. The rules of the land are based upon where one is physically. In comparison, the network-state is dependent upon which digital ecosystem or community one interacts and associates. This is paralleling the idea of nations and networks.

From the Definition in the book "The Network State" by Balaji Srinivasan:

"*A network state is a highly aligned online community with a capacity for collective action that crowdfunds territory around the world and eventually gains diplomatic recognition from pre-existing states.*"

2.2 Voluntary Migration to an Alternative, Parallel Economy

2.2.1 Why An Alternative, Parallel Economy?

In the current centralised model, true power rests with large institutions governments, mega-corporations, and global financial conglomerates. These entities operate in a system which is set up to extract more from everyday people than it returns, leading to an erosion of personal freedom. Technological advancements should have simplified our workloads and enhanced autonomy, but in practice, they primarily enrich a narrow elite controlling both infrastructure and money supply. As individuals, we lack genuine alternatives and often find our freedoms and free time dwindling while technology continues to improve.

2.2.2 New Options for Opting Out of Oppressive Economies

Decentralised economies offer a peaceful and genuinely empowering exit route. They allow people to:

- **Own Digital Assets Outright:** No single authority can block access or seize your holdings.
- **Speak Freely:** Immutable social layers ensure no corporate or governmental power can censor your voice.

- **Retain More Value:** Distribution models are built to reward contributors to the community, rather than siphoning gains off to distant Head Quarters or political cronies.

Initially, people may adopt these technologies alongside legacy systems. But as self-sovereign tools become more accessible and the central system's constraints grow intolerable, a larger exodus is likely. When you can genuinely own your voice, your currency, and your data why remain in a structure that limits them?

2.3 Communities Achieving Self-Sovereignty

2.3.1 The Historical, Town Square Context

In the past, small towns or local tribes held autonomous decision-making power yet they were confined by strict borders or overshadowed by strong neighbouring states. Modern digital platforms like Facebook, Twitter, and YouTube tried to become the "virtual town square," but they are run by CEOs and policed by regulations. Voicing "wrong" opinions can lead to an instant ban, removing your ability to participate. The essence of genuine community self-sovereignty had nearly vanished in the digital world until decentralised infrastructures offered a fresh solution.

2.3.2 Building Digital Self-Sovereignty

Using decentralised networks helps communities recapture the autonomy once found in small, self-governing bodies:

- **Immutable Accounts:** Neither governments nor corporations can suspend these financial or social profiles.
- **Self-Run Infrastructure:** Network "witnesses" or validators, elected by the community, maintain the chain. The project continues even if some nodes drop out.
- **Flexible Governance:** Communities can choose any model for governance and distribution of value; socialist, liberal, libertarian, anarchistic, capitalist, economically conservative, culturally conservative, or a fusion depending on their collective decisions on the blockchain.

Crucially, if there is no large corporate backer or centralised "founder stake," no single entity can sell or infiltrate the entire project. The community itself provides the real defence against hostile takeovers. It is the Layer 0 and is what the ecosystem ultimately derives its value from.

2.4 Creating One's Own Self-Sovereign Economy

2.4.1 Why Self-Sovereign Economies?

Local currencies have long been tested examples ranging from town-based scrip to the "Brixton Pound." Authorities typically shut these down swiftly, to preserve their monopoly on money. However, digital tokens can escape such crackdowns because they are:

- **Global in Nature:** No single jurisdiction can fully ban them.
- **Programmatically Distributed:** People earn tokens based on value added, non-monetary contributions to the community rather than political connections or inherited privileges.

2.4.2 Mechanics of a Community Economy

1. **Neutral Base Layer**
   A blockchain without major corporate investors or large "founder" allocations avoids centralised tampering with a consensus driven token minting schedule or token supply control.

2. **Value-for-Value Distribution**
   Contributors to development, social engagement, and infrastructure receive tokens. This system fosters genuine fairness no middlemen or external "gatekeepers."

3. **Stable Coin Integration**
   An over collateralised, algorithmic stable coin (for instance, "HBD" on the Hive Blockchain – for further information see Annex I – Glossary of Terms and Acronyms) shields community members from volatile price swings. This gives day-to-day stability, crucial for broader economic usage.

4. **Transparent Governance**
   A decentralised autonomous organization (DAO – for further information see Annex I – Glossary of Terms and Acronyms) might hold community funds, with decisions made via stake-weighted or reputation-based voting. Proposals get funded if the consensus views them as beneficial.

By minting and managing its own currency, a community breaks free from external authorities and their restrictive policies. Goods, services, and ideas flow within a network governed by its own participants.

2.5 From Online Community to Recognized Network State

2.5.1 Path to Recognition

A decentralised group with credible infrastructure can:

- **Resist Shutdown:** It has no CEO, no registered office, and no large chunk of tokens in a single wallet for regulators to freeze.
- **Develop Real liquidity:** Through stable coins and decentralised exchanges, its internal currency becomes practical for everyday transactions.
- **Fund Infrastructure & Social Projects:** A DAO can build community water wells, finance social ventures, create it's own Wi-Fi networks and physical infrastructure or support local commerce, much like a small municipality.
- **Improve Physical and Societal Quality of life in Locations Traditionally Difficult for to Government Reach:** Local people can take direct action where governments have found it impossible to in the past. Locals can campaign for funding from the blockchain community they are part of and build valuable, transparent initiatives in their local areas directly.
- **Provide local Governments a Tool with Which to Gain Transparent Legitimacy** The transparent nature of blockchains and especially those designed for social interaction, can allow local governments to contribute to society in a much more transparent way and dispel assumptions of corruption. This can lead to re-establishment of legitimacy over time.

As these digital societies exhibit tangible benefits economic productivity, peaceful collaboration, and mutual aid, external governments may start cooperating. Governments might find it financially worthwhile to trade with or even formally acknowledge these emerging Network States. Over time,

major global powers could sign treaties or agreements, conferring a form of legitimacy once unimaginable for an "online community" operating on the legacy Web2 social platforms.

2.5.2 Governments Joining New Parallel Economies

Some governments may not only recognize but also actively engage by:

- **Exchanging Reserves:** Converting parts of their national reserves into blockchain assets, earning yields or governance rights.
- **Leveraging On-Chain Reputations:** Public officials might validate their own standing within the transparent governance protocols used by the community.
- **Direct Cooperation:** Through joint infrastructure projects or social programs, aligning the interests of both the digital state and traditional government.

Revolutionary conflict becomes less likely when there are clear incentives for collaboration. By demonstrating tangible value, Network States can secure legal stature and self-determination without resorting to conflict.

Conclusion

A shift toward voluntary, digital-native economies is already in motion. Individuals are seeking alternatives where freedoms like unhindered speech and genuine financial autonomy are safeguarded, which the conventional system often fails to provide. As these decentralised communities expand, they:

- **Claiming Self-Sovereignty:** Controlling their own technical, financial, social and eventually physical architectures and infrastructure.
- **Issue Their Own Currencies:** Rewarding true contributors rather than serving centralised interests.
- **Evolve into Network States:** Gaining recognition from established nations and forming global partnerships.

What begins as a small collective of idealistic individuals can develop into a thriving society with a unique currency and governance model, potentially culminating in formal diplomatic acknowledgment. Far from being a "fringe movement," these new Network States could offer humanity's best chance at equitable prosperity and authentic self-governance in the digital age.

Chapter 3 – The Underlying Principles

When it comes to digital freedom, it is principles that matter most, economy is always a counter-intuitive 2nd

Introduction

Most blockchains claim to be decentralised, yet many have fallen short of delivering actual censorship resistance or meaningful digital rights. In this chapter, we explore the fundamental principles that support genuine decentralisation, why it is so hard to achieve, and how certain historical "freak events" accidentally resulted in the correct structural design. We also introduce the concept of the **Petri dish cultivation model**, where an ecosystem evolves organically rather than being "designed" from the top down.

3.1 Why True Decentralisation Is Difficult

3.1.1 Profit vs. Principles

Most project leaders focus on profit and convenience. They raise venture capital, pre ordain themselves tokens from the first day of the project in the form of large pre-mines or ICO's, or form legal entities. While these strategies may somewhat help to fund development, they inevitably compromise on decentralisation. Regulators can easily target corporations, foundations, or high-profile founders. For more detail on Pre-Mines and ICO's, see Chapter 15. "Censorship and the Morality of Pre-Mines"

3.1.2 Censorship Resistance is Binary

Either your system can be controlled by external parties, or it cannot. If a chain has a headquarters, a known CEO, or a large pre-mined stake in the hands of a few insiders with self-ordained pre-mines or ICO stakes, there are clear points of failure. True censorship resistance requires that no single entity or small colluding group can seize control.

3.1.3 Counter-intuitive Choices

Many of the decisions that yield true decentralisation look bad on paper. For example, not raising money or not giving a founder a large token allocation seems "unprofitable." Yet these moves are necessary to avoid creating central points of attack. At almost every juncture, founders who are profit-driven do so at the cost of decentralisation and so undermine censorship resistance. The key is in striking the balance to adequate decentralisation for the application in question. When dealing with digital rights, and maintaining neutral, decentralised layers this means putting counter-intuitive decision choices ahead of profit.

3.1.4 Freak Events and Serendipity

History shows that blockchains achieving genuine decentralisation rarely follow a neat, logical plan. Often, the original builders did not fully grasp what they had created. In retrospect, the intuitive "right" features that are typically chosen such as certain lock-up periods for founders or adding a centralised treasury turned out to be weak points in future which compromised the neutrality and decentralisation of the community. Repeating a sequence of events that are counter intuitive and principled enough in order to ensure decentralisation and digital rights is extremely difficult to deterministically plan for and orchestrate deliberately.

3.2 Everyone Did It Wrong Except a Few

3.2.1 What Bitcoin Got Right

Bitcoin avoided pre-mines, ICO's, and corporate sponsors. Satoshi Nakamoto disappeared, leaving no formal leadership. While Bitcoin's proof-of-work is excellent for store of value and permissionless access to liquidity, and a permissionless transaction layer for those that can afford fees. Its high fees and limited throughput make it ill-suited for scalable social or governance ecosystems.

3.2.2 What Most Proof-of-Stake Chains Got Wrong

Many proof-of-stake projects launched with large ICO's, venture backing, or corporate structures. They also adopted high fees and Layer-1 smart contracts (for further information on Smart Contracts see Annex I – Glossary of Terms and Acronyms), creating a "rich-get-richer" environment where governance is dominated by 2 or 3 naturally occurring large staking pools. Over time, these chains tend toward de facto centralisation: a few pools or validators control the system, and regulators can target them. This model is useful however for earning yield where social nuance is not an issue and many DeFi (Decentralised Finance) applications benefit from a financial passive earning system where the one with the largest stake has the most to lose from unfair treatment of users. (For further information on "DeFi" and "Staking" see Annex I – Glossary of Terms and Acronyms)

3.2.3 Steem and the Emergence of Hive

The Steem Blockchain (later forked into The Hive Blockchain) provides a rare illustration. Steem originally had a "ninja-mined" founder stake controlled by the company Steemit Inc. Unexpectedly, that stake was sold to a high-profile buyer, Justin Sun, founder of the Tron blockchain, sparking a hostile takeover attempt. The community through its DPoS (Delegated Proof-of-Stake – for further information see Annex I – Glossary of Terms and Acronyms) mechanism managed to fork away and create Hive, zeroing out the founder's stake. This forced event removed the largest point of centralisation and left the chain truly community-owned and operated

(See Chapter 11.4 De-Governance for further information on DPoS, See chapter 13.4.2 for more information on forking away from an abusive whale stake).

3.2.4 Why The Hive Blockchain Is a "Freak Event"

- **Founder Exit:** The principal developer left early, taking minimal continuous control.
- **Hostile Takeover:** The attempt to seize the chain triggered the community to unify and fork out the hostile stake.
- **No ICO, No VC, No Foundation:** Without a formal entity or large pre-mine, Hive has no single point of regulatory or financial capture.
- **Community-Focused Mechanics:** A 13-week power-down (for further information see Annex I – Glossary of Terms and Acronyms) of stake locked for governance dis-incentivises large custodial accounts from staking user deposits, making exchange-led takeovers far more difficult. This prevents exchanges from using custodial stake to vote against the interests of users who have deposited with the exchanges for purposes of trading.

Additionally a new, investor has to wait for 30 days in order to carry out governance votes after having staked their tokens to vote. In cases where the stake is large enough to affect the governance of the chain directly, the 30 days gives the community time to find out whether or not the new investor is a benevolent force and will act in the interests of the community before they are

able to carry out malicious votes. This also gives the community time to act and take defensive measures where it cannot establish a benevolent intent from the new investor.

3.3 Petri Dish Cultivation Model

3.3.1 The Need for Organic Growth

A Petri dish offers nutrients and the right environment, but you cannot force which organisms thrive. Similarly, a censorship-resistant chain must set the right "parameters" (like consensus rules, lock-up times, and governance models) so that a truly decentralised community can take root and expand.

3.3.2 Value-for-Value Incentives

When participants receive rewards for providing meaningful contributions whether running infrastructure or creating valuable content they build reputations and earn tokens without needing technical credentials or large initial investments. Users with stake earn when they vote on content, these votes direct tokens from a daily communal rewards pool to the content that is voted for. Over time, this democratizes token distribution and reinforces a healthy "middle class" of stakeholders.

3.3.3 Voluntary Participation

No chain can coerce people to stay. Individuals stay with the community if they see real benefits, like guaranteed speech, secure transactions, fairness, and sustainable token economics. Chains with poor governance, oppressive or extractive structures drive away genuine participants, lose credibility, and remain small or centralised.

3.3.4 Hard-to-Replicate Events

Forking away from a centralised founder stake or orchestrating a widespread volunteer development effort is extremely difficult and risky. Forks represent delicate moments in the history of a chain where communities can easily fracture due to idealogical disagreements and misalignments. Most new chains attempt to "engineer" a community through funding rounds or marketing. Whereas genuinely decentralised ecosystems often emerge from unexpected crises that unify participants around a single set of core principles.

3.4 Universal Digital Human Rights (UDHR)

3.4.1 Digital Self-Sovereignty

True decentralisation grants individuals irrevocable rights to their accounts, data, and tokens. If a chain's foundation or CEO can be pressured by authorities, it cannot guarantee those rights. Neutral, leaderless systems are what enable globally uniform digital rights.

3.4.2 Immutable Speech and Transactions

A robust DPoS or similarly parameterised consensus ensures no small group can censor or freeze accounts. By having a predictable, transparent on-chain governance, users know that no arbitrary decision from a corporate board or government office will invalidate their actions.

3.4.3 Beyond the Reach of a Single Country

When a chain is fully decentralised no headquarters, no corporate registration, no founder stake jurisdictional bans fail to shut it down globally. Any country that outlaws it simply loses the talent and economic benefits migrating to friendlier jurisdictions.

3.5 Key Lessons of the Required Principles

3.5.1 No Single Control Point

- Avoid pre-mines, ICO's, or founder stakes.
- Do not rely on a CEO or legal entity for development.

3.5.2 Parameterised Consensus

- An example of a parameterised consensus is Delegated Proof-of-Stake (DPoS) with a fixed number of elected validators can offer high throughput and strong security, ideal for social interactions and governance of community social nuance, if carefully designed, since the top validators can be elected and unelected by the community itself.
- Long un-staking periods for staked tokens for governance (e.g., 13 weeks), discourage exchanges from powering up custodial user tokens and using them to vote against the interests of the users themselves.

3.5.3 Distribute Tokens Broadly

- Encourage and distributing freshly mined tokens to non-technical users through rewarding positive, provable social actions or “value-for-value” rewards.
- A wide distribution prevents a few insiders from hoarding the majority of supply, leading to a more easily regulatable or corruptible system.

3.5.4 Freak Events Often Trigger Real Decentralisation

- True censorship resistance has historically emerged from crises: founder exit, hostile takeover, or unexpected forks.
- Trying to design a perfect system up front often fails because profit motives have been shown to override long-term security.

3.5.5 Censorship Resistance as a Social Phenomenon

- Technology alone is insufficient. A dedicated community that believes in censorship resistance and has the tools and social impetus to enact it is crucial.
- Reputation-based engagement and transparent on-chain governance foster collective responsibility.

Conclusion

Arriving at genuine decentralisation is counter-intuitive and rarely driven by immediate profit. Most chains chose easy funding routes pre-mines, ICO's, large outside investments and now face takeover risks or regulatory capture. History shows that robust digital rights grow from systems that lack a single controlling entity and operate on a truly neutral base layer, forcing communities to self-govern.

The **Petri dish** metaphor captures this perfectly. You can provide the right conditions no corporate ownership, fair token distribution, parameterised governance but you cannot fabricate real decentralisation just by declaring it. It requires a community voluntarily standing behind censorship resistance and self-sovereignty, with the right digital tools, often galvanized by crises or unexpected forks.

In the chapters ahead, we will detail how to maintain these principles technically and in practice, examining the deeper mechanics of consensus design, token distribution, and ongoing governance models that reinforce genuine network autonomy. Only by embedding these ideas deeply into the chain’s structure can we realize universal digital human rights that no centralised force can override.

Chapter 4 – What a Social Blockchain's Layer 1 Should Do

The Layer 1 should be as simple and as boring as it possibly can be. That's what scales

Introduction

Layer 1, also known as the Base Layer is the basis for immutability. Here is where decentralization takes place due to the node system. It also includes block time, the consensus mechanism deployed, programming languages, and rules pertaining to the network's core operations.

Layer 1 is the foundational tier of a censorship-resistant, community-governed blockchain. It underpins all core functions such as account creation, historical data storage, governance voting, and transactions that must remain immutable and easily retrievable by anyone. The guiding principle is to keep Layer 1 as simple and lightweight as possible, so it can:

- Be run by many independent operators without prohibitive hardware.
- Scale to accommodate network growth without becoming unmanageably large.
- Remain easily fork-able so a community can remove or "zero out" abusive oligarchs or malicious stakeholders by super majority consensus, however that consensus may be reached for each blockchain.

This approach contrasts with many other chains that overburden their base layers, often leading to high fees, low throughput, or compromised decentralisation. Below is an outline of which features belong on Layer 1 and why.

4.1. Data Availability (Text-Based Data Only)

Long-form text storage on the base Layer 1s a powerful tool. By limiting Layer 1 to text data (instead of storing large files like videos or images, or conducting compute and DeFi operations), nodes remain:

- **lightweight**: Operators can more easily store and playback an ever-growing blockchain if it is mostly text-based.
- **Censorship-Resistant**: A truly decentralised, text-based layer where the node operators and token holders are spread across multiple countries ensures people cannot be silenced by corporate or state actors.

When each node stores the same text ledger, no single entity can remove or change that record. This guarantees data availability for governance, on-chain reputations, and community discussions. Higher-bandwidth content and operations such as large media files and computation should live off-chain or on a Layer 2 specifically designed for larger data.

4.2. State Recall and Historical Record

A secure Layer 1 must provide historical state recall a full record of the chain's progression from inception to the present. Due to the fact that all text-based data remains accessible on-chain on such a blockchain, anyone can:

- Verify past actions (posts, votes, transfers, etc.).

- Reconstruct an account's exact history, ensuring transparency.
- Detect attempts to rewrite or delete historical events.

In effect, this "table of truth" is essential for accountability. If the chain experiences a hostile takeover, honest community members can use the historical record to fork away and preserve legitimate balances, reputations, and activities.

4.3. Table of Truth and Custom JSON

A table of truth is the immutable text ledger storing transactions and events. Sometimes, communities want to store structured data for example, metadata about a post or a custom vote type. This is enabled by:

- **Custom JSON Operations on Layer 1**: A feature allowing non-standard data fields to be written on-chain.
- **Indexing Layer**: A mechanism (often run by specialized nodes) that filters or organizes these custom JSON entries for easy query.

Although the base blockchain only sees text fields, custom JSON can represent many actions or data points (game moves, specialized votes, community tags, etc.) if those actions are still validated by the chain's consensus.

If this is followed to its natural conclusion, the result is that the chain can incentivise real world actions that benefit the community. This enables the chain and community to distribute value to valuable actors in the community that are doing real world actions. It becomes a Value for Value exchange that, if design correctly, can become accessible for the vast majority of people to involve themselves with, making earning crypto from a neutral layer accessible without the user having to know how to do technical activities such as crypto currency mining.

Ultimately, it makes newly created cryptocurrency accessible to all people, meaning everyone has the right to earn, regardless of their technical competency.

4.4. Accounts and Resource Management

Accounts are a core function of Layer 1. In a truly decentralised system:

- No user should be forced to rely on a centralised provider to create an account.
- Users can create public keys, store them locally, and sign transactions independently.

Additionally, an on-chain resource management layer (e.g., "resource credits") can replace transaction fees. By staking tokens, users gain the right to make a certain number of daily transactions for free rather than paying each time. This approach:

- Keeps transactions fee-less at the user level.
- Deters spam by requiring staked resources.
- Helps scale usage without imposing gas or high-fee structures.

4.5. On-Chain Actions: Posting Content and Commenting

Social content like text posts, comments, or community updates can be fully on-chain if the system is optimized for text. This:

- Preserves speech that cannot be retroactively edited or removed by a central party.
- Empowers front-end applications to display or filter content but not to delete it at the ledger level.
- Supports immutable communities where membership, discussions, and follower relationships are historically documented.

While full text records may sound large, modern compression and incremental storage can keep it manageable, especially when storing only text and not high-bandwidth media.

4.6. Communities and Followers list

Layer 1 can also track:

- Which accounts immutably “follow” which others.
- Community memberships or roles.

When these relationships live on-chain, centralised web2 style front ends cannot arbitrarily ban or eliminate entire groups. A user’s social graph (followers/following) is secure, and competing interfaces can tap into the same data. This is a huge leap forward from centralised social networks that can wipe your entire audience or content with a policy change.

The application of this technology means that no central party has the ability to delete or regulate online communities any longer.

4.7. Governance Voting (Further Details in Later Chapters)

To remain secure, a decentralised network needs a mechanism for the community to vote on:

- Infrastructure providers (elected witnesses or validators).
- Protocol-level changes (hard forks, parameter updates, token minting schedules and moderating inflation rates).
- Resource distributions (proposal funding, development grants, etc.).

All governance actions, voting, proposals and rank ordering should be recorded in the base chain’s text ledger. Governance on Layer 1 ensures the entire community can see and react to proposals, fosters accountability, and allows forks if a sizeable super-majority disagrees with major stakeholders.

4.8. Infrastructure Incentivisation (Micro-Payments for Node Operators)

Incentivizing core infrastructure (like witness/validator/block prodcuer nodes) is critical. By awarding block rewards or newly created tokens to elected operators, you avoid requiring them to form centralised businesses or rely on external VC funding. This:

- Keeps infrastructure neutral by letting the community elect whom they trust.

- Provides a steady reward for performing consensus, storing data, and serving it to the network.
- Minimizes external pressure or constraints that often lead to censorship or central control.
- Allows anonymous infrastructure operators to compete against large corporate entities that intend to outcompete them by cutting costs and fees, or running at a loss, knowing that they can put the individual, independent operator out of business over time. Other chains such as Bitcoin only incentivise their miners, but they do not incentivise their other critical infrastructure such as lightning Nodes or NOSTR relays from the Layer 1, neutrally created new currency. This leaves them susceptible to such a long term hostile attack from large corporate entities that comply to anti-freedom government regulations, prioritising those above the values of the community.

4.9. Transactions / Transfers

Finally, token transactions and transfers are fundamental on Layer 1. Users should be able to move assets from one account to another with:

- Instant finality or short confirmation times.
- Fee-less or low-friction operations if they have sufficient staked resources.
- Full immutability, forming the basis of the economy.
- All top witnesses (a small group of top community elected miners that run the community's preferred code) in the consensus should process all transactions, lest they be unelected by the community. This guarantees the rights of all users to transact apart from in special circumstances, when the chain is under attack and at existential threat of a hostile take over where the community may be supportive of some witnesses blocking transactions that threaten the chain's security.

  This is more efficient than small block Proof of Work systems, where there are many more Block Producers who are effectively voting with their infrastructure. This makes such layers slow and not suitable for low fee, large scale micro transactions.

4.10. Balancing Block Production with Efficiency in Voting and Operation

- It is in the community's best interest to elect witnesses that are among the top 20 or so most skilled operators of the code while also best reflecting the social ideology of that community. 20 is a minimum recommended number, each having equal weight in the governance decisions on the chain, regardless of their stake size. This means that witnesses are not only technically skilled, but they have to have a deep understanding of the social implications of the code they run, from setting interest rates, voting parameters, new token minting schedules and reviewing code to make sure upgrades meet community requirements and are secure.
- The top 20 witnesses are also the primary Block Producers (BP's) on the chain: they are responsible for the decision of which code to run and that code decides which transactions are recorded on the chain. These are the transactions and data which fill blocks of the blockchain and form the immutable, unchangeable history which the blockchain records. This is the heart of the blockchain: the block production process. Providing there is no centralising party, no ICO or pre-mine, there is a fair token distribution mechanism and no

company behind the blockchain, this process is what decentralises the storage of data on a PoS or DPoS chain and makes it un-censorable or tamper-proof. As a result the community members can operate permissionlessly on the chain with certain guaranteed digital rights, such as property rights, free speech rights, voting rights and others.

- The incentives paid from the chain to the BP's must be high enough that they are incentivised to remain as honest actors and not susceptible to corruption.
- The intuitive approach is that the more BP's a chain has the more decentralised it is and the more censorship resistant it is. However, things are not always as simple as this and counter intuitive approaches often apply.

4.10.1 Block Producer Rotation and Back-Ups:

- Often chains choose to have a top elected group of the best BP's as their witnesses and then have one or several rotating back up BP's. Having back up BP's means that:
    - there is a chance for more entities to earn and so more people run nodes
    - if an incumbent BP becomes malignant, they can always be elected out and a back up is ready to step in immediately
    - it keeps the other BP's on their toes, as those in the rotation positions are hungry to prove themselves and move up the rankings.
    - collaboration between the incumbents is more risky for those incumbents. A small group of elected BP's can be more easily held to account and replaced, if the community so wishes, by always on line back up BP's.
- Some chains choose only to have one back up BP, resulting in a top 20+1, where the back up is rotated in to the block production schedule at random, other chains have many hundreds or even thousands as future advancements in the technology are developed and tested.

4.10.2 Pros of Having Many Block Producers:

- More difficult to get a super majority to agree to censor transactions or speech
- More competition for top spots, keeping incumbents on their toes
- More difficult for a government to force their will on a community to censor transactions

4.10.3 Cons of having many block producers:

- More difficult to coordinate for forks or upgrades to technology
- More difficult to tell if all BP's are all individuals or just one entity running many nodes
- Where ICO's or companies are involved in the inception stage of a project, they naturally gain a centralising influence over the BP pool making the chain seem more decentralised than it actually is
- Each BP gets paid less, as there is less money to go around per BP and so the chances of dishonest BP's increases since they have more to gain by coordinating with other BP's to corrupt the chain and steal funds. Alternatively, the more BP's there are, the more of a

chain's inflation must be dedicated to them in order to pay them enough to remain honest actors

- Can reduce efficiency, speed and scalability of a blockchain.

4.10.4 Optimising for Reality:

- The reality is that each community must strike a balance between too large an amount of BP's and too small a number. On social or community driven chains using DPoS or similar technology, the BP's build their on-chain reputations over time. This means that there is a theoretical optimum number of top class BP's with which a community can operate in an adequately decentralised, censorship resistant way which is resistant to Sybil attack, while not being so small that it can be easily co-opted by government, other types of attack or become easily corrupted.
- Over time, as the market capitalisation of a chain grows, it can afford to incentivise more BP's and should look to incorporate modern technologies to allow for an increase of BP numbers while not sacrificing the scalability and speed of the chain.
- Based on the experience of the fork away from Steem that created the Hive Blockchain, it seems that a top 20 is an adequate number of BP's. It allows coordination when it makes sense to block a transaction, but makes it difficult enough to get consensus that such measures won't be taken lightly. In cases where there is one entity that can easily elect all of the top 20, this of course does not work, so attention must be paid to this issue on a chain by chain basis. Communities with lopsided token distributions are often better having a much larger BP pool, however, in the cases where a small group of entities control the majority of the tokens they are often known to run the majority of the BP's anyway. This means that just because a chain has a large number of BP's it does not necessarily mean it can't be pressured into unfairly blocking transactions or other unfair actions, that centralise the chain in critical moments when decentralisation and censorship resistance is needed most. The issue often comes about as a result of whether or not the chain had an ICO or Pre-mine. If there was a Pre-mine, then a lopsided distribution is normally present and so even chains with large numbers of BP's are often easily pushed into making decisions that effectively centralise the chain, particularly in times of need, such as in hacks, takeovers or when subject to government pressure or regulation.
- It is unclear as to how much more secure a chain is based on an increased number of BP's. After all a government can just as easily pursue a top 200 as a top 20 to achieve the censorship it wants. It seems that only once the number of BP's increase by an order of magnitude does increasing the number of BP's start to have a significant affect. This however, increases the cost to the chain of incentivising these BP's to remain honest actors. Communities should design their systems to suit their own situation based on these factors.
- A serious defence against an organised attack would be where many thousands of BP nodes could easily be spun up by community members at any time for almost no cost, in a similar way to how torrent sites evade shut down but re spawning a new version of the site shortly after the original site was legislated out of existence.

4.11 Why Keep Layer 1 Minimalist?

- **Scaling**: The more complicated the base chain, the more likely it becomes bloated, expensive to run, and difficult to fork.
- **Forking**: A simpler, smaller codebase is easier for the community to adopt in a fork, safeguarding against hostile actors or “rich whales” who attempt takeovers.
- **Performance**: Text-based data alone can be compressed and synchronized efficiently, making it accessible for diverse operators in many regions without requiring specialized hardware.

Everything heavier like complex smart contracts, large file storage, or advanced application logic should move to a Layer 2 or specialized network that references the trusted state from Layer 1. This architecture avoids turning the core ledger into a single point of failure or bottleneck.

Conclusion and Implications

A well-designed Layer 1 is the bedrock of any censorship-resistant, community-driven blockchain. By keeping it limited to text-based data availability, historical state recall, basic governance mechanics, and secure transactions, you ensure:

- High decentralisation and easy operation.
- Human-readable transparency for all critical updates, votes, and account histories.
- Flexibility to fork when necessary, preserving community rights.
- Optimum number of Block Producers and block production alogrithm for the network

Adhering to these Layer 1 principles lays the foundation for truly self-sovereign digital communities and Network States. Layers above can then innovate with large-scale data, complex smart contracts, or specialized applications without jeopardizing the core security that lives on this minimal, robust base chain.

Chapter 5 – Zero Fee Structure

Zero fees means the masses can use it and the complex operations can remain trustless

Introduction

Transaction fees on a blockchain can make or break its usefulness and decentralisation. Many projects overburden their Layer 1 with features that dramatically raise fees or force it to become overly complex and resource-heavy. This leads to two typical problems:

- High fees that discourage on-chain activity, making the network exclusive to wealthy users that can afford the fees, especially when carrying out the large volumes of micro transactions required in social communities.
- High volume and throughput fat nodes where only smaller numbers and groups of well-funded operators can run the chain's infrastructure, reducing community self-sovereignty.

Below, we explore how to address spam, infrastructure incentives, and why a fee-less or low-fee Layer 1 model best serves a truly decentralised community when it comes to social interactions and Network States.

5.1. Spam limitation & Resource Credit Systems

A common objection to free transactions is: **"Won't it be spammed?"** The answer is to require staked resources (sometimes called **Resource Credits**) instead of charging individual fees per transaction. The system:

5.1.1 Requiring Users (or Apps) to Stake

- To transact, an account should lock up a small amount of the chain's native token.
- The larger your stake, the more daily (or hourly) Resource Credits you receive, the more free, on-chain transactions one can carry out per day.

5.1.2 Eliminates Per-Transaction Fees

- Each operation (post, vote, transfer) consumes a small portion of these credits but does not charge you a fee.
- Resource credits recharge at a certain daily rate, say 20% per day. meaning, if an account executes enough transactions in a particular day that the Resource Credits drop below 80%, it will take more than 24 hrs. for the account to regenerate to 100%
- Once credits recharge, you can transact again at no extra cost.

5.1.3 Deters Spam

- Malicious spammers must stake substantial tokens to sustain large-scale attacks, making spam expensive.
- Honest users who do not overshoot transaction limits continue accessing the network without paying fees.

5.1.4 Fosters App-Level Staking

- Applications can stake and delegate tokens and their associated resources in bulk so their end users can transact for free, using the resources of a larger stakeholder. The token or resource delegation happens in such a way that the delegator's tokens are never at risk of being stolen by the account receiving the delegation. Resource delegations can be withdrawn at any time (See Chapter 7.3 " Making Spam Costly and Creating Competition for Resources Increasing Buy Pressure with Increasing Network Affect" for further information on delegations of resources).
- This further democratizes access because everyday users do not need to buy or hold tokens personally.
- Apps become **"holders of last resort,"** maintaining large stakes to serve their communities (see more information on this matter in Chapter 12.11 "DApps and Services as Holders of Last Resort").

This approach banks the unbanked: people in low-income regions can post, comment, or transfer value without paying fees, so long as the application or a sponsor account stakes enough to cover them.

5.2. Incentivizing Community-Run Nodes & Infrastructure

In a genuinely decentralised model, elected community members run the nodes not giant corporate data centres or venture-funded teams. To make that viable:

5.2.1 Paying Infrastructure Operators from the Protocol

- The base chain's inflation or block rewards should fund node operators directly.
- This prevents infrastructure operator sole reliance on business models or venture capital.

5.2.2 Reputation & Community Voting

- The community votes for reputable infrastructure operators.
- Elected operators receive predictable rewards to maintain servers, store data, and confirm blocks. This does not need however, to be the full daily rewards pool, but only a portion of it. Remaining rewards can be distributed to other types of value creators and infrastructure operators in the ecosystem.
- If they fail or behave maliciously, they lose votes, and therefore rewards.

5.2.3 Freedom to be Anonymous

- Operators can receive block rewards from the chain without revealing their identities.
- This protects them from external pressure, enabling truly neutral infrastructure which creates the foundation for protection of Digital Rights for all users.

Combining **fee-less end-user transactions** with **direct infrastructure rewards** ensures the network remains inclusive while node operators have the incentive to keep running services that benefit everyone.

5.3. Why High-Fee Layers are Bad for Communities

Many blockchains impose high fees especially if they:

- Store everything on one layer (heavy code, complex smart contracts, large data).
- Have limited throughput that forces bidding wars for transaction space.

5.3.1 High fees cause:

- **Exclusion:** Everyday users, especially in low-income areas, can't afford consistent on-chain activity.
- **Stunted Growth:** Apps cannot embed frequent transactions or user-generated data if each operation is expensive.
- **Centralisation:** Only wealthy entities can transact heavily or run specialized infrastructure.

When base-layer fees become high, communities cannot harness the blockchain for everyday speech, social features, or micro-transactions. Instead, usage reverts to speculative DeFi and whales who can afford to pay high fees, undermining the vision of broad, censorship-resistant participation for the widest possible user base.

High fee layers also mean that Layer 2 systems cannot clear to the Layer 1 security layer very frequently due to having to constantly pay Layer 1 fees in order to do so. The result is that one has to trust Layer 2 with information until it clears to the finality layer (L1).

On a fee-less blockchain, this is not an issue since one can always afford to clear to Layer 1 as long as it has enough stake in the ecosystem to control the resource credits necessary to clear to Layer 1 on a continuous basis proportional to its usage.

5.4. Why a Low-Fee or Fee-less Layer 1 is Preferred

A fee-less or near-zero-fee system on Layer 1 is crucial for:

5.4.1 Universal Access

- Anyone can create content, transfer funds, or engage in governance without cost barriers.
- This ensures that economic class does not dictate who can speak on-chain.

5.4.2 Circular Economies

- When transactions are free at the user level, the network can become a platform for day-to-day exchanges.
- Enables sending small tips, micropayments, or publishing social posts.
- Fosters a vibrant on-chain community rather than a speculative clique.

5.4.3 Strong HODL Incentives for Decentralised Applications

- Applications stake tokens to cover user interactions.
- They must keep those tokens staked long-term to serve their audience.

- This effectively locks supply out of circulation, providing floor demand and lending intrinsic value to the token.
- This means that the majority of Dapps (decentralised applications) wont sell their stake at any price, since if they did, their Dapps would stop being able to post to chain through lack of resource credits. This means Dapps are holders of last resort and thus create an intrinsic value and floor price to the token providing resource credit staking in the ecosystem (see more information on this matter in Chapter 12.11 “DApps and Services as Holders of Last Resort”).

5.4.4 Equitable Distribution for Everyday Users

- Fee-less usage makes it far easier to distribute tokens to everyday participants.
- Example: Rewarding posted content or community contributions / real world, document-able actions in a low-cost environment.

Conclusion

Fee policies shape who can use your chain and how. If you want mass adoption, true censorship resistance, and a community-run architecture for social based Network State systems, you must ensure:

- **Staked Resource Credits** instead of per-transaction fees.
- **On-chain incentives for node operators,** allowing them to remain independent.
- **lightweight (mostly text-based) Layer 1** so many people can run it without specialized hardware.
- **Simplicity** that keeps the system forkable and avoids centralisation by complexity.

With a **fee-less or near-zero-fee model,** you empower a global user base far beyond crypto speculators to store text, engage in social communities, and exchange value via cheap or zero fee utility systems, not speculation alone. The chain’s **neutral funding of infrastructure** ensures longevity and true decentralisation, preventing regulatable corporate takeover or excessive corporate influence, leaving the community to be governed and regulated by itself.

This is the bedrock for building **scalable, censorship-resistant Network States** where anyone can join and freely transact without gatekeepers.

Chapter 6 – What a Social Blockchain's Layer 2 Should Do

It's not that difficult to understand why trying to put everything on Layer 1 is a fruitless task

Introduction

The second layer (or Layer 2) refers to the secondary layer or protocol that is built on top of a blockchain. These are designed to enhance the scaling of the ecosystem far above what can occur at the base layer. Blockchains tend to be limited in the number of transactions they can process. There are also memory concerns since individual nodes have limitations

A well-designed Layer 2 (L2) is where most application logic, heavy data, smart contracts, and computationally intensive operations should live, while still relying on Layer 1 for security, finality and account management. By keeping Layer 1 lightweight mainly storing text-based data, social actions, and essential governance, Layer 2 can handle large-scale application services, smart contracts, and non-text data without bogging down the base chain. This division lets the community-run Layer 1 remain forkable, scalable and fee-efficient, while Layer 2 delivers complex functionality to end users.

This chapter explains what Layer 2 should do and how it can build upon a secure, fee-less (or low-fee) base layer.

6.1. Application Operations and Services

6.1.1 Offloading Heavier Logic

- Instead of stuffing all computation into Layer 1, the "business logic" runs on Layer 2.
- Keeps the base chain from becoming overloaded with code or inflated transaction fees.

6.1.2 Front-End Interactions

- Social platforms, smart contracts, games, collaborative editing tools, or advanced finance products can store heavier data or run specialized computations off-chain (or partly off-chain) and only anchor key results and checks to Layer 1 when needed.

6.1.3 Data Efficiency

- Large media files or high-volume data like videos, images, or complex transaction logs are better suited for Layer 2 networks or off-chain storage solutions.
- Layer 1 records essential references (e.g., pointers/hashes) to ensure immutability and censorship resistance for crucial metadata.

This synergy lets Layer 1 remain nimble and secure, while Layer 2 fosters rich application ecosystems.

6.2. Rely on the Security and Account System of Layer 1

6.2.1 Leverages Layer 1 Accounts

- User identities and private keys are established on the base chain.
- Layer 2 applications rely on these same accounts, ensuring a single source of truth for ownership.

6.2.2 Anchors Critical State

- Key events like finalizing token transfers or verifying integrity are committed back to Layer 1 to prevent manipulation. With a zero fee base layer this can happen instantly, all day long, providing the Layer 2 has the required amount of resources staked on Layer 1. This minimises trust in Layer 2's as they can affordably and instantly clear to the base layer (L1) security for finalisation.

6.2.3 Avoids Duplicating Security on Layer 2

- Layer 2 should not require a separate "miner" or "validator" set to replicate the entire chain's security.
- Reduces complexity and resource consumption while maintaining trust in the Layer 1 consensus.

Because Layer 2's can inherit the reliability and user identity from layer 1, each new application or service does not have to solve security from scratch. This means Layer 2 builders can focus resources in what they are good at, and not on having to replicate Layer 1 blockchain features and maintaining operation of a decentralised network.

6.3. If Done Correctly, Layer 2 Does Not Need Layer 1 Security

6.3.1 Minimal On-Chain Dependencies

- Layer 2 can store ephemeral or detailed data on specialised, distributed "off-chain," storage systems such as SPK Network, referencing only final states or signatures on Layer 1 (see Chapter 18. "Off-Chain Data Availability Layer for Non-Text Data"). Layer 1 therefore, functions as a final settlement layer rather than a global CPU or data warehouse.

6.3.2 Reduced Attack Surface

- Since Layer 2 uses Layer 1 only for account identity, finality, and minimal checks, the base layer remains robust. Layer 2 systems can therefore innovate freely without risking or having to replicate the entire network's stability.

6.3.3 Separate Upgrades

- Layer 2 services can evolve at their own pace and scale independently without putting load on the entire chain.
- Boosts flexibility while preserving Layer 1 continuity and neutrality.

6.4. Smart Contracts / Heavy Data (Non-Text) & Computation

6.4.1 Smart Contracts

- Complex scripting logic, DeFi protocols, advanced NFT mechanics, or multi-step financial flows operate off the base Layer 1 chain, keeping the base Layer 1 light and scalable, while modularised Layer 2 systems can scale individually based on demand and usage while, as a result, not putting additional load on the base layer.
- Only essential confirmations (like final balances or contract triggers) settle on Layer 1. Inter computational information can be kept on the Layer 2 until computation reaches points at which it needs Layer 1 security

6.4.2 Heavy Media / Non-Text Storage

- Videos, large documents, or images do not belong on the base layer chain and can be stored on Layer 2 storage systems.
- Layer 2 or other off-chain networks (e.g., IPFS, SPK Network) store these files, referencing them via hashes or pointers on Layer 1.
- This allows the Layer 1 to scale significantly more. Any non essential action or piece of data can be stored on Layer 2 instead of on the Layer 1.

6.4.3 Computationally Intensive Operations

- Simulations, gaming logic, aggregator queries, or batch updates can operate on Layer 2 nodes or specialized side-chains.
- Summarized or finalised results are recorded on the base layer.

This prevents Layer 1 from becoming bloated and requiring centralised super-nodes.

6.5. Tokens, Wrapping, and Decentralised Finance (DeFi)

6.5.1 Custom Tokens

- Communities can create Layer 2 tokens representing digital assets, reward points, or governance stakes pertaining to that community only.
- Such tokens can be managed by Layer 2 logic but recognized or mapped at Layer 1 for authenticity and security.

6.5.2 Instant, Low Cost Swaps and Wrapping

- External or cross-chain tokens can be "wrapped" into Layer 2 equivalents.
- Multi-sig or bridging mechanisms facilitate this process.
- Fast, Fee-less transfers means that liquidity can be held on both chains by the Layer 2 Smart Contract multi-sig system and thus instant, low fee swaps can be facilitated.

6.5.3 Fee-less DeFi

- DEX's, lending protocols, and yield farms operate on Layer 2.
- They frequently specialise in DeFi lending and value / token swap transactions, which require low-cost execution, making a zero fee Layer 2 the ideal environment for such systems.

By relying on Layer 1 for final settlement and accounts, Layer 2 tokens or DeFi remain trustless, auditable and tamper-resistant.

6.6. Implications: Efficiency, Scale, and User Experience

6.6.1 Lower Fees

- Using this Layer 1/2 division of responsibilities approach, Layer 1 can optimally reduce its load from computations and other high intensity transaction types. Layer 1 transactions can therefore more easily remain near-zero fee or Resource-Credit-based when the chain operates at scale.
- Layer 2 handles heavy transaction flow. This flow can be modularised per Layer 2 smart contract meaning the cost of demand does not have to be passed to the whole community, as it does on many other chains where Layer 1 executes almost everything, including smart contracts and compute. This results in a general reducing of costs across the network and costs raise only in areas where demand is high, not for all end users, as with many of the early blockchains.

6.6.2 Fast, Rich Apps

- Layer 2 is able to offer real-time updates, large datasets, and interactive Dapps at scale, where as Layer 1 can focus on being the security and finality layer. This means Dapps can specialise in making their user experience top quality, and not have to worry as much as with traditional blockchain tech stacks about operating at scale

6.6.3 Protection of the Base Chain

- If something goes wrong with a Layer 2 app, the underlying chain remains intact.
- Financial risk assets and operations can be minimised on Layer 1 and risk taking can be moved to the Layer 2 systems that specialise in generating high economic yield to users for increased risk taking. This reduces risk on the community base layer (Layer 1) and isolates mistakes and over leverage to Layer 2, helping to protect and preserve the Layer 1 in times of financial uncertainty.

6.7. BLS Multi-Sigs on Layer 1 and Escrow & Liquidity Pools on Layer 2

6.7.1 BLS & Escrows

- This type of feature allows two parties to lock funds or assets until certain conditions are met at which point funds can be released.
- These are governed by Layer 2 logic, often with multi-sigs with final "release" transactions on Layer 1.
- If the collateral involved in such transactions is large, in the tens, or hundreds of millions of dollars, the community may opt to use BLS Threshold signatures on the Layer 1, where a multi sig in which a preferred method of on chain fund release requires many hundreds of signatures be obtained in order for funds to be released from liquidity pools or escrow systems.

6.7.2 Layer 2 Liquidity Pools

- Layer 2 automated market makers (AMMs) or multi-asset pools can handle continuous swaps and yield strategies away from the Layer 1.
- High-frequency operations stay on Layer 2, reducing contract calls on Layer 1 where finality clearances happen.
- Some communities may wish to create their own dedicated Layer 2 liquidity pools separate to the Layer 1, reducing risk of hacks on the Layer 1.

Conclusion

Layer 2 is the engine for advanced functionality, heavy data, and day-to-day Dapp logic. By leaning on the secure, fee-less (or low-cost) Layer 1:

- **Accounts and final settlements remain tamper-proof.**
- **Smart contracts, heavy storage, and complex computations stay off the base chain.**
- **Tokens and DeFi gain flexibility without increasing Layer 1 congestion.** Communities and Dapp operators can expand freely, confident their basic user identities and transaction proofs are anchored in an un-bloated, decentralised base layer.

This complementary design empowers vast application ecosystems such as community social tokens, advanced financial instruments and data-rich content platforms while preserving true decentralisation and fork-ability at the root. By separating what Layer 2 should do from what Layer 1 must do, you maximize scalability, lower costs, and open the door to censorship-resistant digital communities at real-world scale.

Chapter 7 – Sustainable Economy & Decentralised Coin Distribution

Distributing tokens fairly and making it sustainable is amongst history's most difficult challenges

Introduction

A sustainable economy in a decentralised blockchain hinges on properly distributing the coin supply so that no single entity or small group can dominate. Unlike many existing, more centralised models that rely on large pre-mines, ICO's, or purely profit-driven validation, a truly censorship-resistant system needs a continuous, community-driven distribution that rewards actual value creation.

7.1. Token Distribution Methods

Current Main Distribution Methods Include:

- **Mining or Validating** – Earn by providing infrastructure (proof of work or proof of stake).
- **DAO Proposals (On-Chain)** – Fund work or community projects through inflation or a treasury, as voted by stakeholders.
- **Direct Trading** – People buy the coin from existing holders, though this alone does not ensure fairness or broad distribution.
- **Incentivized Stakeholder Distribution (ISHD)** – Also called Proof of Brain, where community members are incentivised with a portion of the daily rewards pool when they vote tokens to those producing valued content or services (for further information see Annex I – Glossary of Terms and Acronyms).

Most blockchains rely on a narrow set of these, often resulting in whales accumulating large amounts of the supply. A robust model should leverage multiple mechanisms ensuring that miners, validators, content creators, infrastructure operators, and general contributors can all earn.

7.2. Incentivized Stakeholder Distribution (ISHD / Proof of Brain)

ISHD awards tokens based on recognized value creation: publishing, curating, developing, marketing, or performing tasks that the community deems worthwhile. Stakeholders vote, and the protocol mints new tokens to reward both creators and voters. This:

- **Aligns Incentives** – People who have a stake in the network (by staking tokens) benefit from finding and rewarding good content or valuable work.
- **Invites Broad Participation** – Non-technical users earn most of the newly minted tokens by contributing ideas, media, or organizational help, rather than being limited to buying or having to do prohibitive technical mining by running infrastructure.

This model counters the typical "pay-to-play" approach, letting anyone enter permissionlessly and earn if they provide real value to the community.

7.3. Making Spam Costly and Creating Competition for Resources, Increasing Buy Pressure with Increasing Network Effect

A major problem with public blockchain systems is spam. The chain can easily become clogged up with data of users who are attempting to drain bandwidth on the chain and make it difficult for others to post their own data. The problem is that if fees are charged on each transaction, this can become highly costly and a prohibitive barrier to entry for many users. Each user now requires additional tokens that they must first obtain from an exchange, so that they can pay the transaction (gas) fees in order to post to chain. In social media systems, this becomes prohibitive to users, especially where there are thousands of tiny, micro interactions each day, in replies, likes and distribution of rewards.

This can be solved by making a competition for resources on chain. This may manifest in users being required to stake small amounts of the token. The users who stake the most get access to the most free transactions each day.

In order to help new users onboard, an existing user may wish to delegate some of their tokens such that new users can access zero fee transactions to post to chain straight away. A delegation is a process whereby an existing user can delegate the power or resources of their tokens to a new user, without actually giving them their own tokens. This means that the new user cannot steal the tokens of the existing user, but they can access the chain for free with some of their resources.

Staking for access to resources on chain (transactions, processing, storage, voting, curating etc.) brings about a sustaining buy pressure for the token as long as a network effect takes hold and demand to post information to chain grows over time. This results in a sustainable token price which is proportional to the network effect of the chain as well as the number of new users signing up.

7.4. Social Distribution as a Trojan Horse

Social content distribution can serve as the entry point for far broader decentralised ecosystems:

- **Wider Token Spread** – Many people can create or curate content (e.g., blogging, video, discussions) rather than just a few technical validators or miners receiving all of the freshly minted tokens.
- **Ongoing Token Flow** – Every post, comment, or contribution that gains upvotes injects new tokens into many individual wallets forming a de facto distribution engine to those who contribute and create value.
- **Moving Beyond "Lunch Posts"** – Over time, the community can prioritize content related to actual value (e.g., building projects, marketing the chain, developing infrastructure). This becomes a Trojan Horse for encouraging real productivity and value creation, not just social media.

By starting as a user-friendly content system, the ecosystem indirectly bootstraps mass token distribution and engagement, ensuring the coin doesn't end up in just a few technically capable hands, but rather, also in the hands of many regular people who add value to the network in their own ways.

7.5. Distribution to Multiple Parties & Ongoing Issuance

A single distribution path (e.g., only validators, or only an ICO) creates central points of control. Instead:

7.5.1 Multiple Mechanisms of Distribution to:

- **Validators / Infrastructure Providers**
- **Social & Curation Rewards**
- **DAO/Treasury Proposals**
- **Developer Bounties**
- **Community Sponsorships**

7.5.2 Continuous, Controlled New Token Minting:

- The protocol can continuously mint tokens (at a strictly controlled rate controlled by the community consensus), directing them toward contributors who deliver recognizable value.
- **Zero Founder or Early Stake** – Founders should earn tokens alongside everyone else. With no large pre-mine that cements early dominance, founders are more aligned with their community members to add value instead of using them as exit liquidity as is so often seen in many of today's "decentralised" blockchains. For more information on Pre-Mines and ICO's see Chapter 15. "Censorship and the Morality of Pre-Mines".
- Ongoing issuance means new participants and future contributors can still obtain tokens without purely "buying in." This fosters dynamic growth and social mobility. It also means new participants do not have to take risks to earn stake in the community, they can just contribute and earn from community votes.
- Continuous new token minting means that the community can continuously reward users for contributing value and it can also direct some of this supply to subsidising transaction fees, keeping them as low as possible into the future.
- As long as the value created via the incentivisation with freshly minted tokens exceeds the value of freshly minted tokens that are distributed, it is possible to achieve a sustainable, growing token price into the future.

7.6. The Importance of Earning Your Tokens

Many blockchains feature founders or Venture Capital firms (VC's) receiving large stakes via ICO or pre-mine, which often:

- **Centralises Control** – Eventually invites regulatory scrutiny as an unregistered security.
- **Turns Users into Exit liquidity** – Early insiders sell off tokens, depleting value for later entrants.

By contrast, in a free, permissionless system:

- **Tokens Are Earned by Contribution** – Documented value creation (e.g., infrastructure operation, marketing, code, or social content) is rewarded.

- **Founders Earn From Zero Tokens, Fairly like Everyone Else** – Community recognition determines ongoing rewards.
- **Avoiding Scams** - Often, tokens that are scamming their users will inevitably bring the conversation around to "buy our token". However, in ecosystem's that are not scams, users should be able to earn their tokens from a neutral, CEO-less protocol. As such, one can do beneficial actions for the community, earn stake from the protocol itself and thereby not take any financial risk at all. This significantly lowers the possibility of users being scammed for their money

For more information on Pre-Mines and ICO's see Chapter 15. "Censorship and the Morality of Pre-Mines".

All parties starting at zero tokens and having an equal opportunity to earn tokens from a neutral protocol ensures that no party can claim an unfair proportion of tokens by fiat or capital alone. This aligns the incentives of all members of the community, in that they must first add value before they can take any out as profit. Be it by building of code, purchasing the tokens on the open market, running infrastructure, creating valuable content, documenting their usage of the system or running events to promote the community, amongst other things all participants can contribute and earn a stake in the system as long as what they are doing adds value. This minimises extractive behaviour in blockchain systems where founders have large pre-mines and ICO stakes that they have obtained by decree, without adding value and therefore unfairly compared to the other participants in the system. For more information on Pre-Mines and ICO's see Chapter 15. "Censorship and the Morality of Pre-Mines".

7.7. Keeping Inflation in Check

Unlike Bitcoin's capped supply, a content or community-focused chain might retain continuous tail inflation but at a controlled rate:

- **Start Higher** (e.g., 15% per year) to bootstrap distribution.
- **Gradually Decline** annually until stabilized at a nominal rate (e.g., 1–2%).
- **Consensus Governance Adjustments** – Community-consensus-driven adjustments to inflation based on needs.
- In contrast to a capped inflation schedule like on the Bitcoin Blockchain, where fees will remain high in order to pay for the security budget of the chain, a chain with a long tail emission can keep fees very low or free, which is more applicable to social layer with high interaction and transaction volumes on chain.

The real test is whether the community's total value output (value creation and demand) outweighs the value of new token minting.

7.8. What You Want to See Vs. What You Don't

What You Want to See:

- **No Pre-Mine, No ICO**
- **Multiple Distribution Paths**
- **Small, Controlled, Consensus Driven Inflation**
- **Broad Middle-Class Growth or Path to it**
- **Permissionless Entry**
- **Ability for Low Tech Users to Earn Stake Without Taking Financial Risk**

What You Do Not Want to See:

- **Massive Founder Stake** controlling a disproportionate supply.
- **Single Distribution Channel** funnelling all tokens to only a few, often technically capable entities.
- **Excessive, Open-Ended New Token Minting** leading to token devaluation.
- **Stagnant Social Mobility** preventing smaller holders from growing, even when they voluntarily add value to the community.

7.9. No Compromise on Free Speech & Censorship Resistance

Projects aiming to secure digital human rights cannot allow:

- **Pre-Mined Central Control** – Easily coerced by governments or powerful interests.
- **CEO/Company Structures** – Single legal entities are direct regulatory targets. they are also more coercible than anonymous individuals operating on such systems who are mobile and can move jurisdiction when pressured.

A neutral, ownerless base layer ensures speech and user accounts remain unstoppable.

Conclusion

A sustainable coin economy arises from continuous and equitable distribution to those providing recognized value. Systems relying on single distribution channels, large pre-mines, or purely fee-based mining tilt toward centralisation. In truly censorship-resistant networks:

- **ISHD (Proof of Brain) must be a major pillar of governance token distribution.**
- **Low Inflationary Tokenomics** prevents excessive dilution while funding future participants for providing value to the community.
- **Strict Vigilance** against centralising whales or external money attacks that do not align with the values of the community.
- **No Founder Pre-Mines** for chains protecting digital rights.

By following these principles, a blockchain fosters a self-reinforcing, sustainable economy while remaining resilient to both internal power grabs and external regulatory pressure.

Chapter 8 – Reputation

How do you know who to trust when you are under attack?

Introduction

Most blockchains rely on pseudonymous wallet addresses (long strings of letters and numbers) that do not clearly reveal who you are, how much you contribute, or whether others in the network find you trustworthy. By contrast, named account systems such as those used by Hive blockchain let you appear under a human-readable name (e.g., @starkerz or @theycallmedan). This approach opens the door to reputation: not only can people see your on-chain actions, they can also develop a subjective sense of who you are and what you contribute to the network. It should be noted that it is the user's own choice as to whether or not they reveal their true identity.

Reputation in decentralised systems functions on two layers:

- **Tangible, on-chain reputation** (measurable community votes, account history, stake-related indicators).
- **Intangible, human-to-human reputation** (subjective assessments by community members over time).

When combined, these give each user an identity within the network. It takes a user a significant amount of time to build both tangible and intangible reputations and relationships on chain. As a result the value of these reputations to the user often means more than the token balance in their accounts. This has interesting improved escrow and trust implications as will be discussed below.

8.1. Why Reputation Matters

8.1.1 Social Trust Over Trust in Code

Blockchains pride themselves on “code is law,” but in crisis scenarios (takeovers, chain splits), people look to trusted individuals. A strong group of reputed accounts can be more decisive than any purely technical solution during an attack or time of crisis.

8.1.2 Accountability and Skin in the Game

If you spend years building a good reputation, it becomes very costly to betray the community. Losing a high-trust status can hurt more than even losing tokens you hold.

8.1.3 Support of Nuanced, Complex Social Interactions

Named accounts with recognized reputations enable user-to-user escrow, collaborative proposals, delegated voting, and similar advanced features.

The intangible trust you build through honest interactions and consistent contributions underpins these unwritten social contracts.

Reputed users can provide on chain legitimacy to real world physical locations such as businesses. With a user carrying out an action in a trusted business, such as making a purchase, with a timestamp, product purchased, photograph of the purchase, price, geolocation amongst other information, this allows Proof of Person systems to be built using trusted real world locations. These locations are identified based on the reputation of certain trusted users within the community.

8.2. Two Types of Reputation in Decentralised Systems

8.2.1 On-Chain, Numeric Reputation

Often tracked via a "reputation score" or stake-based metric. Every upvote, downvote, or curated activity leaves a digital trail. Over time, these accumulate into a visible on-chain record and reputation.

- This numeric score is transparent; anyone can inspect an account's history and voting record.

8.2.2 Intangible Human-To-Human Reputation

Beyond metrics, people form personal judgments about your character, reliability, and expertise.

- This intangible layer allows you to gain influence even if your numeric on chain reputation score is moderate, because active community members may appreciate your attitude, problem-solving, social or code contributions.

Both layers reinforce each other. Good numeric signals usually reflect consistent quality, which boosts intangible reputation and intangible credibility often translates into stronger numeric endorsements from top stakeholders.

8.3. Building Reputation

8.3.1 Consistent Value Creation

- Write informative posts, produce helpful tools, run infrastructure, or moderate community forums. Over time, repeated value-added behaviour raises your standing in the community.
- Being active, responsive, and transparent goes a long way.

8.3.2 Stakeholder Validation

- On such DPoS systems like The Hive Blockchain, large stakeholders can give upvotes that significantly affect an account's on-chain reputation and earnings.
- If recognized stakeholders repeatedly endorse you, it signals broader trust in your work.

8.3.3 Social Presence and Visibility

- Engage in discussions, help onboard newcomers, run meetups or digital events. People gradually learn you are reliable.
- Reputation is earned: the more you prove yourself and carry out actions that benefit the community, the more intangible weight your account carries.

8.4. Reputation-Based Trust and Account Value

8.4.1 Account Reputation as an Escrow

- If you hold significant stake and a solid reputation, others can safely entrust you with temporary custody of tokens (e.g., for trades or proposals).
- Because your intangible reputation often exceeds the face value of your tokens, you have enormous incentive not to risk losing community trust.

8.4.2 Increasing Account Valuation

- Your personal intangible capital can exceed the raw dollar value in your wallet because it reflects long-term engagement, verified contributions, and community goodwill.
- You might even help resolve disputes or coordinate tasks purely on the strength of your good name.

8.5. Reputation-Based Delegation and Voting

8.5.1 Why Users Delegate

- Not everyone has the expertise or time to actively vote on governance proposals or curation. They choose to delegate their voting power to accounts they trust. This helps with distribution of tokens and allows the trusted delegatee to earn stake from curation rewards when ever they vote.
- Such delegations of voting power often goes to accounts with high on-chain and intangible reputation.

8.5.2 Scaling Influence

- As your reputation grows, people may delegate more stake to you, amplifying your decision-making influence in governance or curation pools.
- Over time this can make you a de-facto community leader. If you misuse that power, your entire social investment in the community may collapse.

8.5.3 Defence Against Attacks

- High-reputation delegates are less likely to act maliciously because losing that reputation is worse than any short-term gain.
- Attackers might buy tokens, but without trust, they cannot easily sway user delegations in the face of well-established reputable entities.

8.6. Reputation in Times of Crisis or Forking

8.6.1 Communities Rally Around Known Leaders

- In a split scenario, the question isn't just "what code do we run?" but also "which people do we follow?" Named, reputable figures can mobilize a critical mass for a successful fork.

8.6.2 Long-Term Commitment

- Reputed, long-term token holders typically have spent years building trust. The personal cost of abandoning the chain or acting maliciously is enormous, which helps anchor community stability.
- Newcomers, even with large token balances, lack that intangible goodwill from the community, so they can't match the social capital of long-standing high-reputation contributors.

(See chapter 13.4.2 for more information on forking away from an abusive / malevolent whale stake)

Conclusion

Reputation is the social lifeblood of censorship-resistant, decentralised systems. It transcends the purely mechanical realm of token balances and block production. When crisis hits or when the community needs leadership and integrity, people turn to those with established, trustworthy track records.

By embedding both numeric (on-chain) and intangible (human-based) reputation layers, digital communities following such a model as described in this book can:

- **Incentivize long-term behaviour that consistently benefits the community.**
- **Enable advanced trust mechanisms such as escrow and delegation.**
- **Foster a resilient culture where user names, histories, and reputations matter just as much if not more than raw token stakes.**
- **Identify trusted real world business networks where reliable trade and Proof of Person systems can be built**

Ultimately, combining strong Tokenomics with healthy social dynamics (via reputation) creates far more robust ecosystems than code alone can provide.

Chapter 9 - Why Free Open Source Software (FOSS) Is Needed for Security

If its Free and Open Source Software, eradicating it is like playing "Whac-a-Mole"

Introduction

As decentralised ecosystems grow in scope especially those aiming to preserve individual freedoms, resist censorship, and protect digital human rights **free and open source software (FOSS)** proves indispensable. When projects rely on proprietary code, they introduce single points of failure and compromise transparency, directly weakening collective security. Below, we delve into why FOSS is central to reliable blockchain governance and how it upholds the deeper principles of decentralisation and self-sovereignty.

9.1. Ensuring Transparency and Trust

Visible Codebase

- **Enhanced Accountability:** Making the full codebase public forces developers to maintain high standards. It becomes infinitely harder to hide malicious backdoors or unauthorized "special privileges."
- **Community Verification**: Users are no longer forced to trust the word of a core developer or a single entity. Instead, they can rely on the global community of developers, researchers, and even curious laypeople to confirm the absence of hidden flaws.

Verification Instead of Blind Faith

- **"Many Eyes" Principle**: Open source code benefits from a wide pool of auditors. From security professionals to part-time hobbyists, more people scrutinizing the code leads to quicker bug detection and fixes.
- **Immutable Ledger, Transparent Software**: A blockchain's immutability rings hollow if the software itself is opaque. FOSS ensures that every aspect of a system designed to be "trustless" can genuinely be trusted.

Why This Matters
True decentralisation hinges on the absence of privileged actors. FOSS inherently levels the playing field: all participants can assess the rules, confirm they're applied uniformly, and hold each other accountable.

9.2. Long-Term Sustainability and Fork Resilience

No Single Point of Failure

- **Avoiding Lock-Ins**: Closed-source projects become hostage to the company or individual controlling the code. If they abandon it or are forced offline, the project stalls or dies.
- **Seamless Continuity**: By contrast, open sourcing the code frees the community from sole reliance on a particular maintainer. If key developers leave or face pressure, others can immediately step in code in hand.

Forking and Evolution

- **Necessity of Forks**: Healthy blockchain ecosystems sometimes need to "fork" whether to thwart a hostile actor or adopt new beneficial novel features. With FOSS, forking the entire project is effortless when compared to doing this where the core code is held in the hands of a corporate entity whose intentions may not fully align with the community.
- **Censorship Resistance**: Because code is publicly replicated, targeting or "shutting down" one repository or developer does little. Another team can re-host the code, re-deploy the network, and ensure continued functionality.

  (See chapter 13.4.2 for more information on forking away from an abusive whale stake)

Community Ownership

- **Decentralised Upgrades**: When nobody owns the code's rights, no single authority can demand licensing fees or deny others the ability to enhance or customize.
- **Collective Responsibility**: Everyone in the community has the autonomy to push improvements. This promotes a sense of stewardship where users and developers become co-owners, not passive consumers.

Why This Matters

Blockchains are designed for permanence and resilience. Proprietary code contradicts these aims by tying crucial operational elements to a central gatekeeper. FOSS on the other hand, cements the system's self-sufficiency and the community's role in directing its own destiny via open source code maintenance, operation and development.

9.3. Mitigating Legal and Regulatory Risks

Reduced Central Targets

- **Choke Points Removed**: A proprietary codebase can be legally coerced leading to potential sabotage or closure. By distributing the code (and its rights) across the community, no single party can be easily bullied.
- **Ecosystem Continuity**: Because the code is "in the wild," attempts to suppress the network by targeting individual developers or maintainers become largely futile.

No Patents or Licensing Traps

- **Permissionless by Nature**: A decentralised network thrives on open participation enforcing patents or restrictive licenses contradicts the collaborative ethos of blockchain technology.
- **Neutral Infrastructure**: A platform that withholds core software or demands fees cannot claim to be neutral or fully community-driven.

Why This Matters

Censorship resistance extends beyond the technical sphere; it also includes defence against legal or regulatory manoeuvrers. FOSS disperses liability and control, putting the community rather than a single entity in the driver's seat.

9.4. Enhancing Community Innovation

Permissionless Contribution

- **Global Developer Pool**: When code is public, any skilled developer worldwide can contribute bug fixes, implement new features, or build complementary applications.
- **Vibrant Dapp Ecosystem**: lively innovation drives the creation of decentralised exchanges, games, marketplaces, social platforms, and more, all of which extend the blockchain's value.

Faster Iteration

- **Parallel Experimentation**: Multiple developer teams can work on improvements simultaneously. Competing ideas drive healthy innovation.
- **Agile Decision-Making**: If the network's stakeholders approve a change, it can merge swiftly. Stagnation is minimized, and the project remains competitive in the fast-evolving blockchain sector.

Why This Matters
Innovation and network effects often determine which blockchains endure. FOSS invites a global tapestry of creativity making the system more adaptable and faster to incorporate new technology or user demands.

9.5. Security Through Community Collaboration

Crowdsourced Security Audits

- **Sophisticated Attack Vectors**: Modern blockchains face advanced exploits, from consensus attacks to smart-contract vulnerabilities. An open codebase means thousands of potential auditors.
- **Rapid Response**: When a flaw is detected, public collaboration typically fixes it in hours or days, rather than waiting on a closed-source entity to "do the right thing" in private, behind the scenes.

Lower Attack Incentives

- **Minimal Payoff**: Compromising a closed-source repository can yield total control. In contrast, FOSS-based systems can be mirrored or restarted. The cost-to-benefit ratio for attackers worsens significantly.
- **Redundant Architecture**: Because everyone can host, study, and tweak the code, an attacker cannot stealthily modify it to gain lasting advantage.

Why This Matters
Security in decentralised systems hinges on distribution of data, governance, and development. FOSS intensifies this distribution: the software's design fosters "anti-fragility," becoming stronger as it endures challenges.

Conclusion

For blockchains to achieve **true decentralisation** where no single party can unilaterally alter the chain or silence users **free and open source software** is indispensable. It underpins:

- **Transparency and Trust**: No hidden code can undermine the community's confidence in governance or operations.
- **Community Resilience**: Quick forks and replacements become possible if a lead developer leaves or is compromised.
- **Legal Safeguards**: Distributing code among many stakeholders thwarts attempts at legal or corporate take downs.
- **Active Innovation**: A worldwide developer community can rapidly iterate, preventing stagnation.

Ultimately, **FOSS** lifts a blockchain project from a vulnerable, centralised product to a collectively owned, **public good**. Coupled with robust governance mechanisms and globally distributed infrastructure, open source technology stands as a **cornerstone** of secure, scalable blockchains, empowering digital Network States to flourish without fear of censorship or capture.

Chapter 10. Bridge to Decentralised Governance

Why Effective Consensus Mechanisms Are Essential

Introduction

Every blockchain, no matter how it's structured, ultimately needs a way for people to *agree* on what the chain's rules are, how to update them, and who owns which assets. This process of collective decision-making often called "governance" is how a decentralised project remains stable and evolves over time.

In practical terms, governance answers questions such as:

- How do we decide on changes to the protocol, like bug fixes or new features?
- Which individuals or entities have a say in these changes?
- How do we resolve conflicts when the community is split on major issues?

Understanding *why governance matters* and *what forms it can take* is crucial for anyone interested in building or contributing to scalable blockchains that uphold genuine digital self-sovereignty and censorship resistance.

10.1. What Is Decentralised Governance?

Definition
Governance is the process by which a community makes decisions about shared rules and resources. In a blockchain setting, these shared resources include the digital ledger (the record of all transactions) and the underlying software (the protocols that define how transactions are processed and validated).

Consensus as the Foundation
Because blockchains distribute data across many computers worldwide, there must be a *consensus mechanism* a way for all participants to confirm the state of the ledger (historical data, current balances, etc.). Governance is the umbrella under which this consensus mechanism operates, ensuring everyone agrees on not just daily updates but also fundamental protocol changes over time.

Why You Cannot Avoid It
Some projects claim "no governance" or "governance-free" systems. However, *any* distributed database that requires updates whether bug fixes, performance improvements, or new features relies on humans to come to an agreement. This agreement must be structured in a way that is as decentralised as possible, or else the system risks being dominated by a small group.

10.2. Why You Need Governance in Decentralised Systems

1. Resolving Protocol Updates
Blockchains are not static. They need software upgrades, security patches, and new features. Governance decides *how* and *when* to implement these changes so that the chain can grow without abruptly splitting the community or becoming vulnerable to attacks.

2. Handling Emergencies
When crises arise such as hacks or hostile takeovers communities must act quickly to defend the network. Governance mechanisms allow participants to coordinate a response, possibly "forking"

(copying and modifying) the chain to exclude an attacker's influence or fix a critical bug (See chapter 13.4.2 for more information on forking away from an abusive whale stake).

3. Funding and Collective Projects
Fully decentralised blockchains often rely on some form of on-chain funding (like a DAO) for development, community initiatives, and infrastructure. Governance determines who receives that funding, on what terms, and how to track accountability.

4. Maintaining Long-Term Vision
Without a structured process, short-term profit motives can overshadow the chain's long-term mission of free speech or censorship resistance. Proper governance gives the community a voice, preventing a single founder or entity from unilaterally controlling the chain's direction.

10.3. Data Availability and Agreement

Data Availability Layer
A blockchain's "data availability layer" stores all the historical records transactions, smart contract states, social posts, etc. These records must be reliably accessible worldwide. If only a handful of nodes retain full history, the system becomes centralised and prone to data loss or manipulation and decentralised governance becomes compromised.

Distributed Around the Globe
To remain censorship-resistant, multiple independent operators (often called validators, witnesses, or miners) hold copies of the ledger. This distribution ensures no single party can erase or alter historical data without everyone noticing. If one server goes offline or gets compromised, many others still have the verified history.

Coming to an Agreement
Every time new information is added like a batch of transactions these independent operators must *agree* on its validity. They use consensus rules (e.g., Delegated Proof-of-Stake, Proof-of-Work, or another protocol). Governance is the higher-level process that can tweak or overhaul those consensus rules if needed, but only with broad community support.

10.4. Forms of Consensus and Voting

All Systems Have Consensus
Regardless of ideology be it coin voting, node infrastructure voting, or something else a blockchain must converge on a single "truth" about who owns what. This single truth emerges from a *vote* of some kind:

- *Coin Voting:* Users stake tokens to influence upgrades or select block producers (traditionally known as Proof of Stake or PoS).
- *Infrastructure Voting:* Users with specialized hardware or reputations decide the chain's next block (traditionally known as Proof of Work or PoW - for further information on PoW see Annex I – Glossary of Terms and Acronyms).
- *Reputation or Hybrid Systems (Parameterised Coin Voting):* Some networks might incorporate identity or other parameters to weight votes (Known as Delegated Proof of Stake (DPoS)).

Parameterising On-Chain Governance
No single voting method is perfect. For social Networks and Network States, the art of governance lies in *parameterising* how votes are cast and counted. This allows for social nuance to be built into the community decision making process.

An example, of a parameter put on voting maybe where a chain wants to prevent large exchanges from dominating the voting with custodial stake that it did not earn itself. The blockchain might require a long un-staking period (e.g., 13 weeks) before someone can use newly acquired tokens for governance. These parameters can drastically change the power dynamics within the network.

10.5. Potential Governance Models

1. One Token, One Vote

- *Pros:*
    - Aligns influence with financial stake; people who invest more have a bigger say.
    - Collateral Provision Accountability - the user with the most tokens also has the most to lose if being used in a collateral provision or DeFi system
- *Cons:*
    - Wealthy participants can accumulate disproportionate control, risking centralisation.

2. One Account, One Vote

- *Pros:* Every user with an account is treated equally, in principle.
- *Cons:* Difficult to enforce; requires identity verification that can reintroduce central control. Newly joined, uninformed users have the same weight as long-term contributors, and it's prone to "bot-farm" attacks, if not carefully managed, where one user can control multiple accounts.

3. Reputation-Based Voting

- *Pros:* Encourages long-term commitment and trust-building. People who add proven value over time gain more say.
- *Cons:* Hard to quantify reputation objectively, and might still require coin or identity layers for synergy.

4. Hybrid Approaches

- *Pros:* Combines financial stake, reputation, and possibly time-locked tokens (like a power-down period) to balance power distribution.
- *Cons:* More complex to implement and explain. Possibly confusing for newcomers, but can address many pitfalls of simpler models.

5. Top Elected Infrastructure Operator Voting
Many DPoS chains, in order to take into account social nuances of communities elect their top 20 validators (or witnesses) who run the software of the chain. They elect them usually using stake weighted voting. These witnesses then become social representatives of the community, running only the code that they are elected to represent. This code contains all of the governance systems that best reflect the communities values. See chapter 11.4 for further details on top witness voting.

10.6. Governance and the Human Element

Social Coordination Is Key

Even the most elegant on-chain mechanisms ultimately rely on *human* agreement. If a large fraction of the community rebels against a proposed update, they can "fork" the chain. Technology does not settle disputes; it only provides pathways. People must use those pathways wisely.

Reputation and Trust

Successful governance also hinges on intangible social factors like reputation. Leaders who have consistently acted in the network's best interest earn community trust over time. At crisis moments, such leaders can guide the network to fork or adopt specific policies. Without this social cohesion, governance devolves into chaos or central authority.

Conclusion

Governance in a decentralised blockchain isn't an optional add-on; it's the backbone that coordinates consensus, updates, and community direction. Even if a project tries to minimize "human decision-making," it still depends on individuals to maintain code and respond to emergencies. Recognizing that *all distributed systems require some form of structured governance* is the first step in building blockchains that remain truly open, censorship-resistant, and capable of scaling into digital Network States.

Key Takeaways

1. **Governance Underpins Consensus:** Whenever multiple nodes hold the ledger, they need a method to agree on updates and fixes.
2. **No "One-Size-Fits-All" Voting:** Different chains use different models (coin stake, node infrastructure, reputation). Each has strengths and weaknesses.
3. **Parameters Shape Power Dynamics:** Lock-up times, voting weights, and reputation scoring can prevent unhealthy centralisation.
4. **Human Community Is Inseparable:** Technology alone does not ensure freedom. Dedicated people defending open source, decentralised processes are vital.
5. **Crucial for Network States:** As communities evolve into full-fledged digital sovereignties, robust, social nuanced governance becomes the cornerstone of self-rule and stability.

By grasping these governance fundamentals, communities can design systems that genuinely live up to the promise of decentralised power resisting censorship, welcoming newcomers, and fostering the trust needed to build entire online nations.

Chapter 11. De-Governance

Where Consensus Meets Human Judgment

Introduction

Blockchains inevitably require a *consensus* mechanism some form of governance to decide how data is validated, how upgrades occur, and who ultimately exerts control. Yet many projects misunderstand governance, defaulting to simplistic models that invite centralisation. This chapter examines three major paradigms Proof-of-Work, Proof-of-Stake, and Delegated Proof-of-Stake while highlighting how true decentralisation for communities and social systems requires more refined "parameterised" voting systems. We then show why neutral, ownerless blockchains must avoid founders, VC's, and pre-mines, and how community-driven governance can act as a counterbalance against takeover attempts and regulatory threats.

11.1. Governance Is Unavoidable

Why We Need It
No matter how "hands-off" a blockchain claims to be, *someone* must decide on software patches, security fixes, and emergency measures. Even "code-is-law" projects have humans writing and changing that code. When attackers strike or improvements are needed, effective governance enables swift, community-backed decisions rather than letting one party (like a founder or corporation) take over.

De-Governance?
Some blockchains say they have "no governance" or "minimal governance," but that usually means governance is hidden or de facto centralised. True decentralisation *conducts* its governance out in the open and spreads it among stakeholders, rather than pretending it can be removed entirely, or conducted on a separate, web2 layer such as Reddit, which is often the case in existing blockchain systems.

11.2. Proof-of-Work (PoW) Otherwise Known as Infrastructure Voting

In PoW, *computational power* (energy plus hardware) is the mechanism to secure the chain. Nodes around the world expend resources to compete for block rewards, effectively "voting" with their electricity bills.

Security vs. limitations:

Advantages of Proof of Work:

- **Highly resistant to censorship** If enough miners operate globally it is difficult to fake mining since you need real hardware and energy expenditures.
- **Good for large amounts of permissionless liquidity and collateral**. It allows everyone access to liquidity as long as they can afford the high fee.
- **Global Infrastructure and High Security**: The sheer capital required to replicate or outvote the network discourages attacks.
- **Censorship Resistance**: Dispersed mining pools and hardware prevent easy shutdown or forced compliance (in theory).

Disadvantages of Proof of Work:

- **Centralising Tendencies**
  Over time, mining typically coalesces into a handful of pools (e.g., two or three major ones). Smaller participants must *join* these pools, eliminating the grass-roots, democratic element.
- **Limited Governance Flexibility**
  PoW is primarily designed to confirm transactions and maintain an immutable ledger. It does not inherently solve *on-chain governance* it cannot easily upgrade network rules or incorporate dynamic features for social media or consensus-driven proposals.
- **Scaling Constraints**
  Storing large volumes of data or performing fast transactions under PoW is cumbersome. Blocks with high throughput require more computational and energy overhead. Miners rarely want to expand block sizes indefinitely because it increases node storage demands and can hamper decentralisation.
- **Exclusive to Elites Only**
  Exclusive to those elites who can afford the fee, by design. It must be high fee to preserve the security budget, since there is no other way to incentivise this with the dominant PoW chain at present (Bitcoin) having a capped supply.
- **Centralised Mining**
  Mining typically centralises into large pools or in it being expensive to operate a validator, since everyday people can't afford specialized infrastructure.
- **Validators Not Accountable to Community**
  The validators are not accountable to the community, since they vote themselves into consensus with their own hardware power.
- **51% Attacks Cost Money to Defend**
  During a money attack (51% hashing rate) takeover, there is no way to fork away from the attacker without it costing the community money since the defender must outcompete the attacker and gain back 51% of the hashing power on the new fork. You also cannot identify the attacker since you cannot see who they are due to the fact that there is no on-chain reputation system.

Replicating Bitcoin's Scale
Bitcoin's success in censorship resistance rests on a massive, expensive global mining network. *Starting a new PoW chain* at that scale is nearly impossible today, because you'd have to attract billions in hardware investment. Smaller PoW chains can be 51% attacked more easily by the main chain, unless they can convince PoW miners to switch to their own hashing algorithm. There is therefore, most likely only one winner in PoW mining.

Using the most expensive hardware, with the most resource intensive hashing algorithm to secure the network is the most logical solution since it makes the network more expensive to attack. If an alternative fork attempts to go to a cheaper hashing algorithm, then the dominant chain can 51% attack the new fork if it was seen as a threat.

11.2.1 Mitigations for Proof of Work Attacks

- **Non Custodial Layer 2 Options**
  Make sure Layer 2's are non custodial, since Layer 1 fees will be so high, there will be a tendency for exchanges and Layer 2 systems to custodialise funds. With enough custodial funds collaborating and unsuspecting people operating on them, it is possible for the custodial stakes to fork the original chain and dictate which version of Bitcoin will be accepted on their custodial systems.

11.2.2 Longer Term Accumulation Attacks on a PoW Chain

In a Proof of Work chain, a group of people who collaborate with a large amount of the total stake can collude with other major stakeholders, exchanges and businesses to create a new fork of the original chain and dictate which version (their version during an attack) that the on and off ramps will use, excluding the original (and legitimate fork). This can be more easily defended against on DPoS chains where human readable, named accounts that have built reputation via long term stake distribution and voting mechanisms can form a popular, community fork made up of reputed community members, regardless of their total stake size, around which the legitimate community can gather to continue on away from the attackers.

Conclusion (PoW): Proof of Work is a powerful security solution analogous to a “Panzer tank” but is less flexible and not easily repurposed for rapid governance, high-volume social use, or swift on-chain decision-making.

11.2.3 Attacking the Largest Bitcoin Block Producers

There are only a few large block producers on Bitcoin where most of the hashing power that secures the chain is centralised. Coordinating governments could physically cut the honest actors of those block producers off from the network, write legislation that prohibits them, or force them to operate under mining licenses, while setting up competing, government compliant block producers. Small “free” block producers could then try to “pop up”, but the larger governments would potentially overpower them.

11.2.4 Why We Call PoW "Infrastructure Voting"

This system should also be referred to as Infrastructure Voting, since the community recognises the longest chain when forks split the consensus. The longest chain is normally formed only by the chain which has been able to deploy the most infrastructure and thereby the most computing power to secure the consensus. Eventually infrastructure operation becomes expensive and resource intensive, making it economically viable only to those who have the money to invest in large amounts of expensive equipment. Such a system is only therefore able to account for liquidity and collateral, but not the social nuances of communities and social governance.

11.3. Proof-of-Stake (PoS)

11.3.1 Otherwise Known as Un-Parameterised Coin Voting

In basic PoS, whoever holds the most tokens wields the most influence. Stakeholders "lock" coins to validate transactions or produce blocks. Over time, large holders typically become even larger, leading to potential centralisation around wealthy interests.

11.3.2 The Fundamental Idea

Pure Proof of Stake (PoS) equates the *proportion of tokens owned* to *governance power*. Each stakeholder's influence stems solely from the size of their balance. On paper, this creates a "skin-in-the-game" scenario: attacking the network undermines the value of one's own stake.

However, early real-world implementations of PoS often introduced no *parameters;* no rules to prevent or discourage centralising forces. Large token holders or custodial services (exchanges, pooling services) quickly dominate, rendering the chain effectively controlled by a few "whales."

This makes PoS systems excellent for financial services and liquidity systems where there is no social nuance involved in making decisions. Money and yield are generally non political and do not directly affect culture and social systems. Having the top validators in a finance system those who have the most to lose is one of the best ways to make sure your financial yield stays neutral.

(For further information on PoS and UPCV see Annex I – Glossary of Terms and Acronyms).

11.3.3 Why Un-Parameterised Coin Voting (PoS) Tends to centralise

In "Un-Parameterised Coin Voting (UPCV)," **staking pools** become inevitable:

- **Pooling of User Funds**
  The paradox with PoS is that you do not want too many validators as it can necessarily overburden the network and validators with small stakes are not really contributing to the security of the block production process with such small skin in the game. Therefore, often a minimum staking for governance threshold is set where if users stake above this amount they can earn when mining in the network (on Ethereum for example, this limit is set to 32ETH or $80K as of time of writing). However this results in people who want to run validators but don't have enough to stake and so they pool their stakes into mining pools in order to share mining rewards.

- Most small participants lack enough tokens or technical know-how to run a validator node. They deposit stake into large third-party pools, which then yield better returns through economies of scale. Eventually and naturally, one to three major pools emerge, dominating block production, making the chain far more centralised than it appears.

- **Staking to Vote Delays**
  Without mandatory waiting periods, exchanges can temporarily "power up" user funds to vote in governance without users' explicit consent. This has happened historically on certain chains, allowing custodian-led attacks or hostile takeovers (for further information on Powering up and Powering Down see Annex I – Glossary of Terms and Acronyms). Both DPos and PoS chains must have lock up delays for governance voting when staking to vote in order to defend against custodial stake attacks by entities such as centralised exchanges. The same issues are true for hostile attackers with large stakes. The idea is that the delay for voting after staking to vote (often 1 month) allows the community time to determine if the entity staking significant amounts is hostile and take action to protect the chain.

- **Long Lock-ups**
  PoS (and DPoS) chains that do not have long lock ups when staking to vote often are susceptible to takeover by those holding custodial stakes (such as large, centralised exchanges). This is because exchanges can use custodial, user funds that are deposited into their accounts for trading and stake them for short periods of time without the permission of the depositors in order to take control of the chain's governance and carry out hostile takeover. There have been several instances of this occurring in the past and so this threat is very real. Exchanges can do this since they can use the short un-staking period to make depositors whole in a timely manner when they request to withdraw funds. With long lock up periods for governance, this type of attack is not possible. PoS chains that are not susceptible to this type of attack typically have 3 to 6 months lock ups for governance.

> *"Coin voting is amazing if parameterised correctly. UPCV (Un-Parameterised Coin Voting) is lazy: it centralises over time into massive staking pools that overshadow smaller individual stakeholders and somewhat centralise the network."*

11.3.4 Mitigations for PoS Attacks

In order to avoid centralising governance issues, users should be encouraged not to stake with large staking validators or exchanges and be informed on which forks that suit them ideologically in order to follow their best suited fork.

11.3.5 Danger of Centralisation

- **Staking Pools Dominate:** Users often stake through third-party pools (like lido Finance), which ends up resembling the pool dominance also seen in PoW mining.
- **VC & Founder Advantage:** Early insiders can hoard tokens cheaply, keeping governance under their control.
- **High Fees, Slow Upgrades:** Many proof-of-stake chains aim for "general-purpose" Layer-1 smart contracts processing not only transactions but also computation on the Layer 1. This often results in high fees to reward infrastructure operators and stakers, making day-to-day usage expensive and discouraging broad adoption.
- **Fat Nodes:** A common occurrence in blockchain where the operation of smart contract processing as well as transaction processing on all base layer nodes becomes the norm. This makes the standard on the chain the operation of large, heavy duty and therefore expensive, unprofitable nodes that have to be kept afloat by constantly minting new tokens (inflation) due to the chain charging artificially low fee transactions on the base layer. The point here is that most such chain validators are uncompetitive and as they scale, they have to charge proportionately higher fees which over time cannot compete against systems that keep the base layer simple and light weight and move the computation layer to the Layer 2.

11.3.6 The Necessity of Guardrails

To avoid these pitfalls, PoS (UPCV) needs constraints time-locks, minimum validator counts, voting delays, and so forth. We'll see in the next section how **Delegated Proof of Stake** introduces precisely these guardrails to preserve the core "skin-in-the-game" feature while preventing consolidation into a handful of players.

11.3.7 Why We Call This "Un-Parameterised Coin Voting (UPCV)"

The method should also be referred to as Un-Parameterised Coin Voting (UPCV) since consensus is set by stakeholders voting with their coins meaning the largest stake holder has the biggest influence on the governance of the chain, hence there are no parameters in place to prevent a “rich get richer” scenario or to incorporate any social nuance of the community into the governance system.

11.4. Delegated Proof-of-Stake (DPoS) or Parameterised Coin Voting (PCV)

Otherwise Known as Parameterised Coin Voting (PCV)

DPoS starts with the premise: Staked coins = skin in the game. Then it *adds parameters* to prevent the pitfalls of raw PoS.

Delegated Proof of Stake can be considered *an evolution of coin voting*. Rather than letting raw stake automatically produce blocks:

1. **Named Validators**
   Stakeholders elect a fixed number of block producers, commonly called “witnesses” or “validators.” They are elected by the community using stake weighted voting (not one account one vote) and the top 20 or 21 block producers are paid for securing the network and upholding consensus.

2. **Parameter Constraints**
   - **Stake Lock-ups**: Voters must stake tokens for a certain duration (e.g., 13 weeks). This prevents custodial wallets (such as exchange accounts holding users funds) from freely flipping user deposits into governance attacks. This process is known as Powering Up on some DPoS chains. Un-staking is known as powering down (for further information see Annex I – Glossary of Terms and Acronyms).
   - **Voting Delay**: The chain might enforce a waiting period say, one month before newly staked tokens can actually cast votes. This gives the community time to spot potential aggressors powering up a suspiciously large stake.
   - **Minimum Validator Requirement**: The protocol guarantees multiple active validators, e.g., 20 block producers instead of an unlimited or undefined number. The chain can then sustain high throughput (thanks to a limited set of block producers) but remain decentralised enough to prevent collusion.

3. **Community Accountability:** Stakeholders can remove validators at any time if they fail or collude. This fosters an ongoing “immune system” against malicious actors.

4. **Many Elected Equally weighted Top Validators:** A top 20 elected validator set are more akin to having 20 equally weighted staking pools, even though each validator can have a different stake size in the ecosystem. They are elected in and so, for example, the largest account in the ecosystem at best has equal influence to the other 19 elected validators, even though their stakes are likely much smaller in comparison. This is in contrast to most chains using other consensus mechanisms that cumulate into 2-3 more centralised staking pools staking custodial stake on behalf of users and thus becoming over bearing forces on governance, while having provided no value to earn such a position.

11.4.1 Community Reputation and Named Accounts

A key feature of many DPoS systems is **human-readable account names**. This fosters a social aspect:

- **Users Earn Reputations**: Engaging in core development, running reliable infrastructure, or promoting the ecosystem can earn community trust, which translates into witness votes.
- **Social/Community-Driven**: Instead of the "richest account wins," smaller players can rally around a witness candidate who has proven contributions but may not hold much stake personally. The entire system becomes more *social* and less purely financial as a result.

11.4.2 Advantages Over Basic PoS

- **Battle-Tested Against Exchange Attacks**
  By requiring lock-up periods or a "period of time before vote," the chain can detect malicious power-ups (like large exchanges powering up user deposits to sway governance).
- **Faster and Cheaper Transactions**
  With a limited, predictable set of elected block producers, block times can be short, fees minimal or non-existent, which is critical for social networks or content-based Dapps.
- **Continuous Distribution**
  Many DPoS systems reward users for content creation or running infrastructure, enabling them to acquire stake organically. This counters a "rich-get-richer" scenario.
- **Faster Block Production:**
  A fixed number of well-equipped witnesses can confirm transactions quickly.
- **Neutral Base Layer:**
  Protocol-level parameters (lock-up times, voting delays) prevent centralised takeovers.
- **Human Element:**
  Probably the most important distinction is that reputable people with smaller stakes, or even no stake at all can rise to validator positions *without* having the largest stake, because the community can delegate tokens to them or vote for them. This adds social nuance to the raw coin-vote model where they user or mining pool with the largest stake is the most influential in the network.
- **No Minimum Staking Threshold**
  In contrast to PoS, DPoS does not need a minimum staking threshold for voting in governance. Instead witnesses are ordered in relevance to the block production process based on the amount of stake weighted voting they receive from the wider community. Since the chain dedicates a certain amount of newly minted tokens to pay witnesses, there is a limited amount of them that can operate profitably. After this limit witnesses operate at a loss or voluntarily. It is up to the chain to make sure it is as cheap as possible for a community member to run a node in order to maximise the number of back up witnesses. However, the advantage of this is that it makes the staking pools that are so common in PoS pointless and ensures that the chain forms into a minimum sized top witness set of 20 each with equal voting weight, regardless of their own stake or the stake voting for them (as long as they get enough votes to reach the top 20). This means that DPoS chains really are like having a minimum of 20 equally weighted staking pools, whereas PoS and PoW naturally settle to 2-3 major staking or mining pools, which is far more centralised when it comes down to defending against an attack.

11.4.3 Disadvantages of DPoS

- **Voter Apathy**
  If the active stake that is voting is not the majority of stake in the ecosystem, then the ecosystem is subject to takeover. the community should therefore monitor to make sure at least 51% of the voting stake is constantly voting.
- **Preventing Voter Apathy:**
  A potential risk is that once voters pick witnesses, they leave their votes unchanged indefinitely. Some chains solve this by **witness vote decay,** an automatic reduction of vote weight over time, forcing users to reconfirm votes periodically. This "refresh cycle" fosters dynamic governance, ensuring people stay informed and new voices can emerge.
- **Large Stakeholder Risk**
  The biggest stake holder may accumulate a significant enough stake as to become a security risk when it comes to voting. The community should move to mitigate any such risk
- **Long Term Take Over**
  Susceptible to long term, slow accumulation of stake where the top elected witnesess are slowly replaced overtime without the community taking note and the new top witnesses operate code that is not in the best interests of the community. To mitigate this, the community should note the state of witnesses from a time when the chain operated in a way that reflected the ideals of the community and fork to return to this more representative validator set

---

11.5. The Importance of Parameterisation

Why Parameters Matter
Without guardrails, simple PoS (UPCV) quickly centralises around whales or single staking pools. Parameters act like traffic rules or guardrails on a winding road. Each parameter (e.g., minimum validator count, witness vote decay, lock-up times) is a protective measure so that real-world attacks don't succeed.

Examples of Useful Parameters

1. **Minimum Validator Count:** Ensures at least a set number (e.g., 20) of independent validators must coordinate, preventing one or two major pools from dominating.
2. **Lock-Up Before Voting:** Newly staked tokens must wait weeks, giving the community time to spot suspicious activity (e.g., an exchange powering up customer deposits).
3. **Vote Decay:** Stakeholders must periodically renew their votes, preventing perpetual voter apathy and forcing validators to remain accountable.
4. **Time-Delayed Un-staking:** Prevents attackers from quickly exiting after a hostile manoeuvrer; they risk their stake being stuck if the community forks out hostile funds.

Distribution First
Even the best governance parameters fail if most tokens sit with early insiders or VC's. A *broad* token distribution, ideally through "value-for-value" earning mechanisms, is vital for meaningful decentralisation. Having people worldwide *earn* tokens from a neutral Layer 1 by contributing something valuable rather than buying at scale helps create a large middle class of voters.

Why We Call This "Parameterised Coin Voting (PCV)"
DPoS should also be referred to as Parameterised Coin Voting or PCV, since it is able to use parameters in the consensus that avoid a “Rich-Get-Richer” scenario. The parameters it uses mean the largest token holder seldom wields the most sway over governance. This maximises the chance that the social nuance of the general community and its values are reflected in the governance process and makes it ideal for self organising social, digital communities and Network States.

11.6. Why No Founders, No ICO, and No VC's

Central Attack Points

- **Founders & CEOs:** A single “visionary” becomes a legal or regulatory target. Governments can coerce them into compliance, leading to censorship or policy changes.
- **VC Pre-Mines & Early Sales:** Venture capital often demands a controlling stake, undermining decentralised governance. Unsuspecting retail users later serve as exit liquidity, and the interests of the founders and the late entry users are often therefore misaligned.
- **Formal Companies:** If a blockchain “company” holds trademarks or controls critical code, lawsuits and cease-and-desist orders can force compliance.

Community-Built & Ownerless
A truly decentralised chain has no formal owner or headquarters, making legal threats difficult to enforce. This was illustrated by the Hive community when a mining company attempted legal action over the “Hive” brand name. With *no single entity* to serve or respond to a lawsuit, it was later dropped.

11.7. Voting Models Are Everywhere

All Consensus Is Voting
Whether PoW (miners “vote” via computational work), PoS (largest stake “votes”), or DPoS (parametered stake “votes”), *every system is some form of voting.* Pretending “code is law” eliminates humans is naive. People *choose* how code upgrades, and they *enforce* or *reject* forks in emergencies. The distinction lies in:

- **What** do you vote with? (Mining power, tokens, or delegated tokens?)
- **Which** parameters ensure fair distribution? (Lock-ups, whitelists, minimum validators, etc.)
- **How** do you handle staked reputations, backups, or emergent crises?

Delegation and “Politicians”
Delegation allows a less technical holder to transfer voting power (not ownership) to a trusted witness or community leader. This replicates the concept of **political representatives**:

- **Accountability**: If the delegate misuses votes, the original stakeholder can revoke delegation.
- **Reputation Building**: Ambitious or service-oriented community members can gather delegated stake by proving themselves helpful, honest, and aligned with the network’s ethos.

In this way, stakeholders can delegate votes to witnesses or proxies, much like electing politicians. This ensures smaller holders or those without technical knowledge can still influence governance through trusted representatives. Reputation systems help identify benevolent proxies.

11.8. Accountability and Preventing AI/Big Tech Takeover

Human Element
Some blockchains incorrectly assume purely algorithmic approaches can settle disputes. Real communities need human judgment *the chain's social layer must be able to override purely technical missteps.* Delegated Proof-of-Stake excels here because stakeholders can intervene if an actor (or an AI) accumulates stake maliciously.

As artificial intelligence matures, AI "sock-puppet accounts" could appear credible in online communities, slowly accumulating stake. However, a chain that places value on:

- **Long-standing History**
  Accounts building trust over years are less likely to be AI, particularly if they started prior to AI's rise.
- **Community-based Identity**
  Reputations *subjectively* determined by real humans can guard against an AI that merely "posts content."
- **Participate in Proof of Person systems** where a known, trusted and reputed, real person holding an on chain account identifies a business such as a shop. Users who buy products and document the purchase on chain can prove they are a person without having to KYC (Know Your Customer – for further information see Annex I – Glossary of Terms and Acronyms).

This interplay of parameter coin voting, reputation, and human oversight forms a bulwark against AI-driven infiltration.

New "AI accounts" will lack such historical footprints, letting the community discount them in governance decisions.

11.9. Defining Web 2.5

Most self-proclaimed "Web3" protocols still rely on:

- **Centralising Venture Capital**: Early token pre-mines or private sales create small, powerful cliques controlling governance.
- **High-Fee Layer 1**: Forcing developers onto "Layer 2" solutions that are often themselves centralised.
- **Corporate Entities**: A chain might have an "official company" or "foundation" that can be targeted or regulated, leading to partial, superficial decentralisation.

These projects are best categorized as **Web 2.5**: they adopt some blockchain elements but remain vulnerable to corporate or government pressure.

Big Tech vs. Web 2.5
Traditional corporations (Web 2.0) profit from user data and can easily create "Web 2.5" solutions semi-centralised "blockchain-based" services where they still hold keys or run crucial servers. True Web3 demands protocols incentivize independent infrastructure globally. Without a genuine neutral layer, "convenience monsters" like large platforms can undercut smaller operators and reintroduce central points of failure.

11.10. Achieving True Web 3

A truly decentralised system has:

1. **No Pre-Mines or Founder Stakes**
   The network is community-owned from inception, so no single authority can be coerced into compliance or censorship.
2. **Parameterised Coin Voting**
   Long lock-ups, minimum validators, well-tested distributions, and social reputation layers prevent *accidental or malicious* centralisation.
3. **Community Accountability**
   Voting is frequent or re-evaluated; large custodial wallets cannot quietly hijack consensus.
4. **Neutral, Incentive-Driven Infrastructure**
   Nodes and Dapp operators are rewarded from the protocol's minting of new tokens or fees, reducing reliance on corporate business models or KYC requirements.

Key Point: *If a blockchain surrenders to large-scale pre-mines, venture capital dominance, or minimal parameters, it drifts into Web 2.5. Realizing the full promise of Web 3 requires structural safeguards and widely distributed stake, combined with robust governance that no single entity can subvert.*

11.11 Putting It All Together

1. **PoW**: Effective for base security at massive scales (like Bitcoin), but lacks governance flexibility, speed, low cost transactions and is nearly impossible to replicate in new projects. Ideal for large, permissionless liquidity and collateral provision.
2. **Basic PoS**: Unchecked stake accumulates power; quickly centralises around whales, VC's, or exchanges. Ideal for financial yield systems.
3. **DPoS / Parameterised Coin Voting**: Builds on stake = skin-in-the-game while adding crucial guardrails lock-ups, vote decay, minimum validator sets, reputation, etc. to foster *true* decentralisation. Ideal for socially nuanced communities and Network States
4. **Web 2.5 vs. Web 3** – Many "crypto" platforms remain significantly centralised. True decentralisation emerges when no founder, company, or small clique can capture the chain, and governance decisions arise from a fair, widely distributed stake, informed by real human reputations.

Crucial Tenets

- **No Founders, No Pre-Mine, No VC**: Removes single points of control; no one to coerce or sue.
- **Open Infrastructure Incentives**: Protocol must pay community-run nodes and developers, avoiding Web2 business models (data sales, ads, KYC).
- **Large & Active Voting Base**: Broad token distribution and user engagement protect the chain from hostile takeovers.
- **Reputation & Human Oversight**: Genuine communities rely on trust built over time. When code fails or AI tries to infiltrate, humans must step in.

- **Long Voting Stake Lock Ups** multi-week or multi-month stake lock-ups to vote.
- **Minimum number of top validators** and transparent reputations for block producers.
- **Everyone Can Earn** Users with small stakes to earn stake through proven contributions (content creation, infrastructure, etc.).
- **Voting Decay & Ability to Delegate Votes** healthy re-voting and proxy delegation to reduce voter apathy and ensure dynamic leadership.

Conclusion

De-governance is not about removing governance it's about removing *centralised* governance and replacing it with a robust, multi-parameter system that's hard to capture. Proof-of-Work provided a censorship-resistant *foundation* for Bitcoin, but it's impractical to re-create and offers little room for social or high-throughput applications. Un-Parameterised Proof-of-Stake tends to centralise around large holders or exchanges and makes the person or mining pool with the most stake the most powerful and most rewarded on the network. **Delegated Proof-of-Stake (DPoS) or more generally "Parameterised Coin Voting"** adds social nuance: reputation, timed lock-ups, witness vote decay, stable, minimum node counts, and open development funding and allows even the people with the smallest accounts rise to the top of the witnesses and gain significant influence on the chain, provided they carry out the will of the community.

Under these conditions, communities can sustain vibrant digital ecosystems, censorship-resistant social networks, governance systems, economies which are truly owned and operated by the people who rely on them. This is the vision of a *scalable*, *democratic*, and *resilient* blockchain, finally delivering what many call **Web 3**.

By enforcing decentralisation at the **protocol level** through no founders or companies, fair distribution, and layered defences against collusion these systems can achieve genuine freedom from censorship and regulatory strangleholds. The result is an *ownerless*, community-driven blockchain that stands the greatest chance of scaling into a fully fledged "digital Network State," where user rights are coded *and* guarded by human consensus.

Chapter 12. Coin Voting Parameters

How Time Locks, Stable-coins, and Infrastructure Incentives Strengthen Governance on DPoS Chains

Introduction

Once a blockchain community agrees on "Parameterised Coin Voting" (often called Delegated Proof-of-Stake, or DPoS), it must also define *how* the ecosystem's voting power is distributed and exercised. These "coin voting parameters" determine everything from how long stake must remain locked when powered up, protective time delays for stable coin token swaps on the base layer, to how new tokens are issued or taxed as well as many other variables. Each parameter serves as a safeguard against centralised takeovers and short-term manipulation, while also incentivizing community members to hold, build, and coordinate in the long term.

This chapter details key parameters such as lock-up durations for governance, stablecoin security rules, token minting and inflationary controls, and more. It explains why collectively they form the backbone of secure, censorship-resistant on-chain economies.

12.1. Importance of Long Lock-Ups for Governance Participation

Why Locking Matters
When stakeholders lock (or "power up") tokens for an extended period, they reveal genuine "skin in the game." Someone who can instantly withdraw has far less risk and can more easily perform a short-term attack or manipulate votes. By contrast, a locked-in stakeholder must carefully choose who or what they vote for, because they can't exit quickly if they cause harm or fail to benefit the community.

Preventing Custodial Attacks
Long lock-ups also prevent custodial wallets (like centralised exchanges) from freely using *other people's* tokens to hijack governance. If tokens must remain staked for months, it's much harder for an exchange to suddenly vote without telegraphing its move. The community gains time to see large power-ups and respond if malicious behaviour appears.

Time as a Security Factor
Time itself becomes an integral part of security. With a multi-month lock-up requirement, any new whale is effectively "on probation" for that period before it can fully influence governance. This discourages opportunistic short-term attackers who want to "buy in, vote, then sell."

12.2. One-Month Voting Delay

Seeing Attackers Coming
A "voting delay" is a specific parameter stating that *even after* you lock your tokens for, say, three months, so that you can vote in governance decisions, you must still wait an additional period (e.g., one month) *before* you can cast those governance votes. This delay means:

- The community can observe and reach out to new, large stakeholders and see if they're legitimate or a threat.
- Any suspicious movement of funds from, for example, a major exchange's wallet, becomes immediately visible and can be monitored in case it is going to be used in an attack on the community.

Critical Defence
Had such a voting delay existed on certain DPoS chains in the past, major hostile takeovers by custodial exchanges would have been thwarted or significantly hampered (See STEEM blockchain takeover). The extra time window lets defenders rally: they can withdraw support from compromised witnesses or even prepare a hard fork to nullify an attacker's stake if it's obviously stolen or the intention is to use stake against the super majority's will which represents the community's consensus.

12.3. Why a Three-Month Lock-Up

Why Three Months?
Three months is a good lock duration for governance participation, but similiar lengths are good as well. It strikes a balance: long enough to deter "drive-by" attackers, but not so long as to alienate ordinary users. During this period:

- Stakers cannot instantly sell their tokens, so they share in the chain's volatility and remain committed.
- Potential attackers must accept that if they sabotage the system, their funds remain at risk to volatile price movements and community, consensus driven mitigations for months.

Future Variations
Some ecosystems might experiment with different lengths or even *tiered* lock-ups with longer commitments giving even greater voting power. The core idea is consistent: time-bound staking cements accountability and weeds out short-term exploiters.

12.4. Stablecoin Security

Why a Decentralised Stablecoin Is Crucial
For an on-chain economy to function, especially one prioritizing censorship resistance, users need a stable unit of account that *doesn't* rely on centralised issuers or banks. A purely "speculative" chain with a volatile native token won't serve everyday commerce or wages. Algorithmic stablecoins fill this gap by:

- Maintaining a peg (usually $1, but could be pegged to some other stable asset, commodity or basket of the same, should the community consensus wish it so)
- Relying on on-chain mechanics, free of direct fiat banking
- Allowing users to buy goods, save money, or transact in a familiar unit instead of an unfamiliar, volatile priced asset.

Collateralised by the Base Token
The main token is often 20-30 times larger than the stable coin which it collateralises. There should be multiple controls built into the base layer protocol which ensure the stable asset is always vastly over collateralised by the main token.

A robust *algo-stablecoin* typically uses the chain's main token as collateral. For example, if you hold one "Hive Backed Dollar" (HBD), you can always convert it into $1 worth of Hive (the main token), provided certain parameters remain healthy. To prevent runaway issuance, the chain includes "haircut rules" and time delays on large token swaps, ensuring the stablecoin supply can't surpass the market capitalisation of the underlying collateral in a way that threatens the peg. An example of where these rules were not followed, ending in inevitable disaster was Terra Luna which

incorporated none of the above mitigations into its protocol, resulting in a hyper inflationary collapse.

12.5. Haircut Rules

Preventing Over-Issuance
A "haircut rule" puts a hard cap on how large the stablecoin's total market cap can be relative to the base token's market cap (e.g., 30%). If the stablecoin ever approaches or exceeds this threshold:

1. The chain can **stop** creating additional stablecoins (e.g., halting certain reward distributions in stable form).
2. It may **devalue** the internal stablecoin peg (to 90¢, 80¢, etc.) to ensure overall system solvency, by prioritising the limitation of the creation of new main governance / collateral tokens during conversions back from stable coins at the cost of the stable coin peg value. This prevents a hyper inflationary event of the main collateral token, protecting the ecosystem, albeit at the cost of a temporary de-pegging of the stable coin asset's price.

Adaptive Mechanism
This dynamic protects both the stablecoin and the chain from a "bank run," where too many stablecoins chase too little collateral. Over time, once conditions improve and the chain's base token regains value, the stablecoin's internal peg and issuance can return to normal. This cyclical approach allows algorithmic stablecoins to recover from market dips without collapsing irreversibly.

12.6. Time Delay on Bulk Token Swaps

Slow Conversions, More Safety
If large holders could instantly swap massive amounts of tokens into stablecoins (or vice versa), they could destabilize the market or execute rapid attacks by building short positions in the main token and then instantly converting large amounts of stable coins to the main token. This causes massive inflation of the main token and devalues it, resulting in large payouts for the attacker's short positions. Imposing a three-day (or similar) delay on major conversions:

- Gives the community consensus driven protocol time to adjust supply and internal pricing.
- Alerts the community to suspicious behaviours well before the conversion finalizes.
- Creates a highly risky situation for the attacker, who now has to wait for 3 days with a large short position that can be liquidated by a move higher in the base layer asset, causing a huge short squeeze against their position. This makes the potential losses to the attacker infinite and the inherent risk of such an attack far greater than carrying out such an attack without the time delay on internal stable coin conversions mitigation in place.

Avoiding System Shocks
A delayed swap mechanism prevents sudden surges in the stablecoin or base token supply, reducing manipulative volatility. This resembles "capital controls," ensuring a healthy conversion pace rather than abrupt floods that can crash markets.

12.7. Inflation Control

Steady, Transparent Token Issuance
Blockchains commonly issue or mint new tokens as "inflation," distributing them to infrastructure operators (validators) or to individuals providing value (content creators, developers, liquidity providers). However, the inflation rate must remain carefully managed:

- **Too high** and the token's value dilutes, undermining long-term growth, inflating it away to zero.
- **Too low** and the chain can't adequately fund community projects or incentivize widespread distribution of the token.

Community-Defined Parameters
Many DPoS-like systems use scheduled token minting curves (e.g., starts at 12% then drops 0.5% per year until 0.5%) or allow consensus decision by governance voting to adjust annual rates. The key is that *no central party* arbitrarily mints unlimited tokens. When stakeholders collectively control inflation, they align it with network health.

12.8. Importance of Transaction Taxes

(*Note: Some chains opt for "resource credits" instead of explicit transaction fees, but the concept is similar.*)

Prevents Spam
Tiny taxes or "resource credit" costs in zero transaction fee systems on each transaction deter malicious actors from flooding the network with meaningless transactions.

Funds Public Goods
If designed properly, transaction fees can be channelled into a decentralised community fund (a DAO), financing infrastructure upgrades, marketing, or development without relying on external venture capital funding.

Trade-Off
High fees can stifle usage, pushing users to centralised layers or competitor chains. Low or zero-fee designs risk spam unless you stake tokens to earn "resource credits." The right solution typically involves parameterised resource models that scale usage based on staked token amounts.

12.9. Backing the Token with Community Interactions

Real Economic Activity
A chain's main token gains lasting value not through speculation alone, but from genuine utility. If people need to stake tokens long term in order to:

- Post or comment,
- Run apps,
- Vote on governance proposals,
- Earn stablecoins or other rewards, then they *compete* for access to on chain resources in exchange for holding and staking those tokens. As network effect takes hold and the community grows, the demand for transactions grows and thus competition for access on

chain resources also grows with it. This usage is what "backs" the token's worth *far* more stable than mere hype, speculation and venture capital backed market makers.

Circular Incentives
Users earn tokens for creating valuable content or running infrastructure. They then stake (lock) those tokens to gain influence or resource credits, enabling them access to more on-chain activity, which further enriches the ecosystem. This positive feedback loop cements real demand for tokens that pure speculation cannot match.

12.10. Rewards for Holding and Locking In

Staking Benefits
Long-term stakers may earn extra yield or command stronger voting power. This can:

- Counterbalance short-term traders,
- Incentivize early believers and builders,
- Foster and favour a middle class of stakeholders who have earned their tokens from the protocol over time, over whales that merely buy big positions on day one.

Proof of Commitment
These "hold-and-earn" or "stake-and-earn" models on social blockchains where community stake weighted voting of valuable content show that one can support the chain's vision long enough to shape its governance responsibly. In many systems, staked accounts also receive a portion of newly minted tokens or content curation rewards over time. This incentivises long term, staked holders with skin in the game to continue to contribute to the community while earning additional stake as a result of their value added contributions.

12.11. DApps and Services as Holders of Last Resort

Why They Don't Sell
Applications built atop a chain (social media platforms, games, DeFi protocols) need guaranteed access to transactions, bandwidth, and resource credits for their users. They must lock large amounts of the base token:

- If they become distressed sellers and sold under times of price pressure, *their entire app* would cease to be able to post to chain and thus lose much of its functionality.
- This creates a class of "holder-of-last-resort" entities, who keep tokens *no matter* how low the price dips, in order that they can continue to operate their applications on chain.

Intrinsic Value Floor
When multiple serious DApps stake substantial amounts of tokens, you get a "demand floor". An intrinsic value to the token. Even in market crashes, these services can't afford to offload their stake. This underpinning helps prevent token value from hitting zero purely from panic sells.

12.12. Anonymous Accounts vs. Known Accounts

Freedom vs. Trust
A truly censorship-resistant chain lets users create accounts without government-issued IDs or personal details. However, if people want to build public reputations or operate recognized infrastructure, they may choose to "dox" themselves revealing their identity. Both approaches matter:

- **Anonymous** (or pseudonymous) users enjoy privacy, crucial for free speech in hostile regimes.
- **Known** users gain trust more quickly and may have "official" track records.

Hybrid Ecosystem
Chains typically end up with a mix: some top validators or developers might be pseudonymous, while others are open about who they are. Reputations can form around handle names, proven over time by consistent participation.

12.13. Importance of Locally Run Desktop Apps for Censorship Resistance

Web Apps Are Vulnerable
If an application only exists as a website (e.g., *something*.com), governments or ISPs can block the URL. Domain registrars can seize or censor it, pressuring the app to follow local regulations.

Desktop Clients
By contrast, user-installed desktop or mobile clients directly query the blockchain's node infrastructure. No single domain or centralised server can be shut down. Even if a front-end website disappears, the *community-run blockchain* remains accessible through these locally operated apps.

True Decentralised Access
Desktop clients shift control back to users. They choose which API nodes to connect to, or even run a node themselves. This fosters unstoppable digital communities no domain take down or corporate compliance order can erase the chain's content or access to it.

Conclusion

Coin voting parameters might seem like small technical rules, but collectively they fortify an ecosystem against takeover, ensure broad participation, and maintain the stablecoin foundation crucial for everyday transactions. **Long lock-ups** and **voting delays** deter short-term money attacks, while stablecoin **"haircut rules"** and **time-delayed swaps** prevent systemic collapse. **Transaction fees or resource credits** control spam and fund public goods, and **Dapps** become "holders of last resort," sustaining demand for the base governance / collateral token.

Whether your account is anonymous or publicly known, these governance parameters allow a robust, censorship-resistant environment where individuals can operate desktop apps, earn tokens from the rewards pool, and shape policy over time. By weaving all these elements together economic, technical, and social blockchain communities can grow into truly self-sovereign digital Network States, immune to the centralising forces and quick-profit motives that undermine so many freedom / self-sovereignty based projects.

Chapter 13: Defending Decentralised DPoS Communities

Attack Vectors, Security Mechanisms and the Power of Layer Zero

Introduction

Decentralised ecosystems promise censorship resistance, transparent governance and community ownership. Yet these aspirations come under threat the moment someone attempts to gain disproportionate control. Whether through direct purchase of tokens, stealthy accumulation, or coordinated influence, attackers seek to seize the reins of power or, at the very least, disrupt the shared values that hold the community together. As a result, the community must be highly vigilant to monitor its systems for signs of centralisation and be ready to defend itself at all times. This chapter explores the key attack vectors in delegated proof-of-stake (DPoS) blockchains, the defences that resilient communities employ, and how reputation, distribution, and circular economies become powerful shields against hostile takeovers.

13.1. Understanding the Direct 51% Attack

A **"51% attack"** in the context of many blockchains typically refers to controlling the majority of mining hash power (in proof-of-work) or the majority of total stake (in proof-of-stake). In a **delegated proof-of-stake (DPoS)** chain, the equivalent is controlling over 51% of the ***active voting stake***, not necessarily 51% of total tokens in existence. A large fraction of tokens may be non voting, dormant or held by long-term investors who choose not to participate in governance, so the threshold to seize decision-making power might be lower (e.g., 30–40% of total tokens) if it translates to half of the actively voted stake.

The goal of gaining 51% of the voting stake in either POW or DPOS governance systems is to control or change the underlying consensus software of the blockchain. The group which controls 51% of the active voting stake has the power to nullify balances, change the rules or carry out any number of wide ranging nefarious actions which may act against the best interests of the wider community. Some of these actions may even be subtle and hard to detect without deep knowledge of the base code.

13.1.1 Calculating the Threshold in Practice

- **Dormant or apathetic stake.** Many investors do not wish to use their governance rights. Some have lost access to keys; others simply hold tokens passively, others are ill informed as to the importance of maintaining activity of their tokens in governance decisions.
- **Voting delays.** DPoS platforms often include powering-up requirements and waiting periods (also known as staking). For example, once tokens are staked ("powered up"), an attacker must wait (e.g., 30 days) before being able to vote for witnesses (the block producers).
- **Community "immune response."** During peaceful times, only 30–40% of total supply might be actively voting. Under attack, additional dormant stake frequently awakens, pushing the actively voted stake higher. An attacker who has purchased 30–40% of the total tokens might suddenly face 50–60% of active stakeholders voting against them, when these voters were apathetic before their attack.

13.1.2 Over-the-Counter (OTC) Acquisitions

Attackers sometimes attempt **shock acquisitions**: buying large stakes through private Over the Counter (OTC) deals with major token holders to avoid moving markets. Even so, a month-long lock or similar delay feature grants the broader community critical time to observe the build-up, approach the new party about their intentions and organize a defence if necessary.

13.2. Indirect or Slow Accumulation Attacks

An alternative method is the **slow, stealthy** approach, gradually buying tokens over a long period so that no sudden price surges draw suspicion. The attacker attempts to outpace inflation and avoid spooking community members. This is often described as a **"Red Queen Race or Game,"** where the attacker has to keep running, constantly purchasing stake to maintain or grow their position because:

1. **Inflation** issues new tokens to existing stakers, continuously diluting outsiders attempting to accumulate stake over the long term for an attack.
2. **Community awareness** can lead to counter-buys. If accumulation becomes obvious, others may accumulate too, driving up price and making the attack prohibitively expensive.

In practice, truly stealthy long-term accumulation on a healthy DPoS network proves extremely difficult. Because continuous buying raises a token's profile, it can also raise the price, creating a negative feedback loop that the attacker has to outpace.

13.3. Distribution as Security

Well-distributed token ownership is the most fundamental defence against takeover attempts in DPoS. If a small group of large holders controls the majority of tokens, an attacker may simply collude or purchase those stakes. Conversely, if significant token supply rests in the hands of numerous mid-level stakeholders ("dolphins" or "orcas" in some ecosystems), no single OTC deal can guarantee majority control.

1. **Healthy Middle Class.** A broad "middle class" of token holders ensures that a handful of whales cannot single-handedly decide governance.
2. **Ongoing Community Allocation.** Continuous reward mechanisms (e.g., content creation rewards, infrastructure rewards, gaming, or curation) spread tokens widely among active participants, reinforcing decentralisation.
3. **Fair Launch or Post-Launch Distribution.** Token systems with large pre-mines or concentrated early investors may face outsized risk of governance capture. Over time, these chains must actively work on distributing tokens to genuine, productive community members, otherwise they undermine their own security model.

For more information on Pre-Mines and ICO's see Chapter 15. "Censorship and the Morality of Pre-Mines".

13.4. How to Defend Against Attacks

13.4.1 The Immune Response

In the event of an attempted 51% attack, a DPoS community often springs into action much like a biological immune system. Dormant stakeholders rally to vote; whales who had previously been indifferent secure the network to protect their own investment. This sudden rise in active voting power can defeat or mitigate the attacker's advantage. The lower the level of dormant or apathetic voting stake during times of normal operation, the more of a deterrence it is to an attacker.

13.4.2 Forking: The Ultimate Escape Hatch

Even if an attacker somehow takes control of the main chain, **forking** remains a final check on malicious power.

- **Copying State and Excluding Attackers.** Communities can duplicate the blockchain's history but exclude or freeze the attacker's stake. Everyone else's balances are preserved on the new fork where the community will move to in order to isolate an attacker (on the old fork).
- **Migrating to a New Brand.** Though the original chain may keep its name under the attacker's control, the "real" community can move to a new chain, complete with code and state continuity. In this case, the community should do everything it can to communicate what the new brand is, where to find the new chain and what changes the new chain has made in order to mitigate the attack on the previous fork. Failure to do this is often as bad as not forking away from a hostile attacker.
- **Winner Takes All.** In most scenarios involving DPoS chains which are being attacked, the community-led fork becomes the de facto chain. The attacker, holding no tokens on the new fork, discovers that "you cannot buy a community." Without people to give the token utility, the original chain withers.

Forking therefore holds large token holders accountable, compelling them to act benevolently towards the community. If whales push too hard or threaten the ecosystem's values, the rest of the network can simply leave. This "veto power" ensures that smaller stakeholders, though individually less wealthy, collectively hold enormous influence which far outweighs that of any of the whales (large stakeholders) in the ecosystem.

13.5. You Can't Buy a Community

Centralised startups or traditional corporations may be acquired by buying out a single entity or board of directors. In a **community-governed ecosystem**, no single gatekeeper can sell the "heart" or values of the community. If an attacker attempts a hostile takeover:

- **Rebellion.** The moment members sense motives detrimental to the network, they organize resistance.
- **Fork Off.** Communities fork away if necessary, taking the developer talent, user engagement, and brand loyalty with them.
- **Moral Imperative.** Decentralised communities often coalesce around values like censorship resistance or autonomy. Members who have already "tasted digital freedom" are notoriously unwilling to forfeit control or make a deal with the hostile attacker, especially when the new "overlord's" intentions are questionable.

13.6. The Community Is the Layer Zero

In blockchain architecture, we often hear about **Layer 1** (the core protocol, consensus, and data availability) and **Layer 2** (applications, smart contracts, Dapps). Missing from many discussions is **Layer 0**: the **community of people** who participate, build, and govern.

- **Ultimate Source of Value.** DApps, transactions, and social engagement bestow real-world relevance and demand upon a token. Without active users and developers, the network is merely code.
- **Immune Response.** Layer 0 unifies in times of crisis, bringing otherwise dormant stakeholders to defend the chain.
- **Collective Veto.** When whales or outside attackers threaten the ecosystem, it is the community, Layer 0, who can coordinate a new fork, rendering any hostile stakes worthless.

In proof-of-stake systems which usually lack engaged community members due to the typical nature of the passive earning for staking model in PoS systems, a wealthy minority can capture governance outright with no recourse for remediation for the majority individual members of the community. By contrast, well-distributed DPoS networks rely on their engaged, vigilant user base; the crucial layer zero to monitor, maintain control decentralised, and fight for it digitally when necessary.

13.7. Reputation Building and Trust

When under attack, it is almost impossible to know who the honest acting block producers or witnesses are unless their accounts are named with human readable identifiers and already have reputation that has been built over many years of reliable operation. This is the only way to reliably identify who your adversaries and allies are during an attack and why reputation in a group of top witnesses who are known entities, even where they are pseudo-anonymous is so important. Why would one move to a fork of unknown, or unidentifiable witnesses after all?

Additionally, having reputed, elected witnesses signalling which version of the blockchain's code they are running from the open source repository is far more secure than in cases where a small number of people communicate this on twitter or other censurable Web2 social platforms, as is the case with the vast majority of top blockchain of today.

One of the questions to be asked when deciding for oneself whether or not a community will defend your digital rights is "How many of the top elected witnesses will not bend the knee to state pressure?" and "If they do will the community quickly elect back up witnesses into place?" While one cannot know the answer to this directly, one has to use judgement to decide which chain has the technical ability, and back-up witnesses to cope with pressure and external attacks best? Their actions and how they acted in pressing times will be on chain forever, for history to judge.

As long as a community requires censorship resistance, demand for competent, honest witnesses / block producers, who are loyal to the community and exist outside areas from which government pressure arises will increase during attacks. In cases where incumbent witnesses submit to unjust or forced government requirements, demand for back up witnesses will increase as the wider community will incentivise those who preserve censorship resistance.

13.7.1 The Value of On-Chain Reputation

Reputation in decentralised systems combines intangible social capital ("trust" among peers) and ***tangible*** on-chain achievements (e.g., track records of contributions, proposals funded, or community-voted posts).

- **Transparent History.** Actions such as authorship, writing new code to improve the base system, identification and curation of valuable or infrastructure operation are typically logged publicly on chain, making it easier to verify a participant's long-term involvement.
- **Community Voting.** Projects can highlight individuals through initiatives like "Community Member of the Month," distributing tokens or issuing badges/NFTs to credible contributors.

13.7.2 Reputation Damage

Acting against communal interests, voting in malicious witnesses or exploiting / gaming the system to unfairly extract community rewards can destroy an individual's reputation. In a small, tight-knit community, reputation damage is often irreversible; one cannot easily hide or rebrand to escape on-chain records. In many ways, on-chain accountability can be more powerful than any legal or centralised penalty.

13.7.3 NFTs for Reputation

Non-fungible tokens can also reflect reputational milestones. For example:

- **Early Contribution Badges.** Testing, bug-hunting, or evangelizing a new application might earn you a unique NFT that can be displayed on many of the ecosystem's front end platforms as badges of honour and status.
- **Long-Term Involvement.** An account that has built up multiple such NFTs over the years signals genuine commitment to the community and the continuation of its values.
- **Fork Coordination.** In a contentious fork, it becomes easier to identify trusted participants who have proven social and achievement based track records of positive contributions (shown through their NFT collections or verifiable participation).

Because forging an entire history of valuable actions is expensive and time-consuming, NFTs serve as an additional line of defence. Attackers trying to infiltrate the community would have to do real, beneficial work for years to build up a similar standing; an ironic deterrent that strengthens the network they aim to subvert.

13.8. Infrastructure Operation and Security

A distributed blockchain stands or falls on the breadth and redundancy of its infrastructure:

- **Validators/Witnesses.** In DPoS, the top 20, community elected block producers secure the network. Decentralising their ownership and distribution of block rewards curtails single points of failure.
- **Node Operators.** More community-operated nodes ensure that malicious actors cannot easily shut down or censor the network.

- **Funding and Incentives.** Systems that autonomously reward node operators (through new token minting or block rewards) help maintain a wide base of infrastructure providers without relying on trust in third parties.

When the community invests in multiple forms of off-chain infrastructure storage solutions, front-end interfaces, decentralised identity and Proof of Person systems it becomes substantially harder for an attacker to sabotage the ecosystem in one fell swoop.

13.9. Achieving Circular Economies

Circular economies arise when members not only earn tokens for contributions but also *spend* tokens within the same network. Real-world examples include:

- **Contractors and Service Providers** willing to accept the ecosystem's stable coin as payment.
- **Local Projects** (e.g., well-drilling, community parks) funded directly in the native token.
- **Cross-Border Use** where members send tokens internationally without KYC friction, using them for day-to-day transactions.
- **Physical shops** accepting the currency in daily commerce, paying employees with it and accepting it as payment and providing clients with benefits such as cash back for using the currency.

A robust circular economy means a token is no longer just a speculative asset. Instead, it becomes an everyday medium of exchange, weaving itself into the fabric of local businesses and communities. At that point, attacking or banning the token outright becomes politically and practically difficult. Governments risk backlash if they disrupt livelihoods of projects that rely on blockchain funding, commerce or censorship-resistant transactions.

13.10. "You Can't Attack a System That's Helping People"

When a blockchain funds initiatives that *truly* improve lives such as building **water wells in underserved regions**, supporting **food drives**, or financing **local commerce** the optics of any crackdown become dire. Governments or wealth-driven attackers have little moral high ground to justify shutting down an entity providing essential services. People defending the chain can credibly argue that any ban or hostile takeover punishes those most in need, galvanizing country wide as well as global sympathy, garnering political pushback.

13.10.1 Benevolent Acts and Resilience

By design, DPoS communities can sponsor benevolent acts through their on-chain decentralised autonomous organizations (DAOs). The **transparency** of these charity-like distributions where every transaction is visible, reduces or even completely removes suspicion of corruption. The result is both:

- **Concrete Impact.** Villages gaining clean water, clinics improving medical supply chains, or impoverished regions finding alternative commerce channels.
- **Strategic Strength.** A network doing widespread good is more difficult for bad actors to undermine without risking huge reputational fallout.

13.11. Bringing Governments into the Ecosystem

Beyond passively tolerating blockchain projects, governments may be invited to **participate** in ways that align with community values such as issuing community **bonds** on the blockchain or adopting tokens for local governance or budgeting. Once governmental bodies see tangible benefits and even cost savings from decentralised, transparent record-keeping, the incentive to ban or attack the platform drops further. In some scenarios:

- **Municipal Bonds on a Blockchain.** A city might raise funds from the global community by issuing interest-bearing tokens, with repayment schedules transparently tracked on-chain.
- **Local Tax Initiatives.** Governments might accept partial taxes in tokens if they see that usage benefits the region.

Such measures weave state-level actors into the community itself, transforming potential antagonists into stakeholders who would defend the network and giving incumbent political actors tools to build genuine, community supported legitimacy for their blockchain documented good deeds to the communities they serve.

Conclusion

Delegated proof-of-stake ecosystems are uniquely positioned to fend off attacks from dramatic 51% takeover bids to subtle, stealthy infiltration provided they uphold a core set of principles:

1. **Widespread Token Distribution.** A thriving middle class of stakeholders dilutes takeover risk and empowers the broader community.
2. **Robust "Immune Response."** Dormant voters wake up when threatened, forming a collective shield.
3. **Forking as the Final Safeguard.** The community's ability to abandon a compromised chain neutralizes the power of malicious whales.
4. **Reputation and Trust.** Social capital, verifiable on-chain contributions, and NFTs that certify long-term engagement make infiltration extremely expensive.
5. **Benevolence Breeds Resilience.** Funding real-world projects fosters local loyalty and global goodwill, making the chain even tougher to suppress.
6. **Embracing Circular Economies and Government Partnerships.** Widespread daily usage and state-level integration in the real economy render token-based services indispensable and resistant towards hostile interference.

Ultimately, no one can simply "buy a community." While an individual or institution might acquire tokens, the heart of a decentralised ecosystem resides in its people. When those people champion transparency, freedom of speech, and open collaboration, they create a formidable system that cannot be so easily captured or coerced. In this way, **Layer Zero (the community itself) remains the bedrock** of genuine decentralisation and, indeed, the ultimate guardian against all forms of attack.

Chapter 14. Balancing Scalability and Censorship Resistance (Disproving the "Scalability Trilemma")

How to Achieve High Throughput Without Sacrificing Security or Decentralisation

Introduction

The so-called "Scalability Trilemma" asserts that a blockchain must compromise on either *security*, *decentralisation*, or *scalability,* it seemingly cannot excel in all three. This idea, widely attributed to certain high-profile developers, has shaped much of the industry's design choices, often leading to high fees, heavy Layer-1 "smart contracts," or reliance on centralised second layers. However, **the Trilemma itself is based on flawed assumptions**. By distinguishing data availability from computation, optimizing for truly low-fee base layers, and ensuring fair token distribution, we *can* build systems that are both highly scalable and censorship resistant without sacrificing security.

14.1. Why the "Scalability Trilemma" Is Misleading

14.1.1 Security and Decentralisation Are the Same Goal

A core claim of the Trilemma is that security, decentralisation, and scalability are three separate pillars that a blockchain must juggle. Yet, in reality:

- **Security** in a censorship-resistant blockchain *derives* from **decentralisation**.
- If a network can be censored, it is *not* secure.
- Hence, these two "pillars" are really just one: a network's *degree of decentralisation* determines its censorship resistance, which determines its security.

Any framework that treats security and decentralisation as separate categories is already conflating the same property in two forms. This conceptual redundancy leads many projects astray.

14.1.2 Mixing Computation With Data Availability

Many protocols that attempt to handle everything including smart contract computation *and* data storage at the base layer end up with:

- **High fees**, because on-chain computation is both expensive and socialized.
- **Unpredictable throughput**, any popular app (such as "CryptoKitties", an early meme ecosystem that bloated all Ethereum transaction fees when it attempted to scale with its popularity) can clog the network, driving fees sky-high for everyone else.

These symptoms are not *inevitable* but arise *if* you force every node to perform all heavy computations on every block. By separating the roles leaving text-based data availability to the base layer, while pushing complex computations to Layer-2 systems blockchains can avoid the trade-offs that the Trilemma insists upon.

14.2. Rethinking Scalability

"Scalability" often means the network can handle many transactions per second (TPS), but ironically, many "scalable" chains impose *high* base layer fees or complex Layer 1 logic that undermines widespread usage and results in fat nodes that are not profitable to operate without passing excessive costs onto the user base.

14.2.1 Lightweight Base Layer for True Layer-2's

A truly scalable Layer 1 should focus almost exclusively on being a **data availability layer** with near-feeless (or staked-resource) transactions. Layer-2 solutions, which rely on that base-layer security, can then run intensive computations or store large non-text based data *off-chain*, referencing the base chain for its immutability requirements. If the base Layer 1 is *too expensive* to write to, then any purported Layer-2 will become centralised because it cannot afford to commit its data or proofs back on-chain on a regular enough basis without having to "trust" the Layer-2 system. This undermines the "trustlessness" that blockchain technology was supposed to minimise.

Example

- **Bitcoin's Lightning Network**: Channels are expensive to open/close, so users rely on a few large node operators which form transaction hubs, through which much of the network's traffic passes. Decentralisation suffers as a result. Lightning effectively forms a small cluster of well-funded custodians. Lightning nodes are not forced to process all transactions and therefore there is a level of censorship capability built in, without having to risk losing mining rewards from the Bitcoin Layer 1.
- **High-Fee Smart-Contract Chains**: When "Layer-2" operators cannot frequently submit data on-chain due to high Layer 1 transaction costs, they must store it off-chain, losing the guaranteed immutability from the Layer 1. They turn into "trusted", centralised services as a result.

14.2.2 Resource Credits vs. Fee Auctions

Standard blockchains often rely on fee auctions: users outbid each other, so the chain always "chooses" the highest-paying transactions first. This leads to:

- **Spikes in fees** whenever demand surges (the "CryptoKitties problem").
- **Poor user experience** and unpredictability, making it impossible for typical apps to guarantee stable transaction costs to their user bases.

By contrast, a **resource-credit or stake-based** model requires:

- Users or applications to stake tokens to gain an *allotment* of daily transactions (credits).
- No one else's willingness to pay can "steal" your bandwidth; as long as you hold enough stake, you can transact or store text data at minimal cost.
- This approach remains stable *even during high usage* because your right to transact is locked in by your stake, not by ephemeral, variable fees which always increase in times of high demand, when the user needs to transact the most.

Result: By applying a fee-less, resource credit model, you get a chain that can handle large volumes of traffic without punishing normal users with unpredictable fee changes.

14.3. Censorship Resistance = Security

If a project claims to solve "the Trilemma" by scaling up yet remains easily censorable, it fails on security. *Real security means no single entity can freeze accounts or remove data.* This is only feasible if:

- **Token Distribution** is broad enough that no whale, foundation, venture capital firm or centralised exchange can unilaterally dictate governance.
- **Block Production** is parameterised so a fixed amount of top, independent validators, each accountable to the community and replaceable by stake weighted election, remain spread worldwide.
- **Low Fees** or staked resources ensure that usage doesn't centralise around large corporate infrastructure.

14.3.1 Un-Parameterised Proof of Stake vs. Parameterised Coin Voting

Proof of Stake systems without guardrails ("Un-Parameterised Coin Voting") often devolve into a handful of (2-4) large staking pools (e.g., lido Finance) controlling consensus. Unless carefully designed, this leads to:

- **High centralisation**, where the votes of one or two large pools overshadow smaller validators.
- **Easy regulatory targeting**, since large staking services become choke points for governments or corporations.

A better approach, especially for social and highly nuanced community governance is **Parameterised Coin Voting** (e.g., Delegated Proof of Stake with a fixed number of validators and mandatory stake lock-ups). This ensures:

- No single entity can spin up infinite validators and manage to have them all simultaneously elected into the consensus by the community's votes.
- Full transparency if anyone attempts to buy excessive influence.
- Time-locked stakes for governance voting create real accountability; people can't just vote maliciously and dump.

14.4. Governance and Stake Distribution: The Most Difficult and Most Crucial Element

A Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) blockchain can only be censorship resistant if its tokens are meaningfully and widely distributed. If a small group of venture capitalists, founders, or pre-miners holds the majority of tokens, they can override governance or be legally pressured into compliance that ultimately represents a take over of a community causing it to operate against its own best interests. Achieving broad distribution typically requires:

1. **No Pre-mines, No ICO's**: Nothing seeds an imbalance and centralisation more than giving a few insiders large shares at launch.
2. **Low Barriers to Entry and to Earning**: Anyone, anywhere should be able to earn tokens by providing value running infrastructure, creating content, building apps, or other socially beneficial actions.

3. **Long-Term Engagement**: Communities that *improve* everyday life (e.g., enabling people in countries where their currencies experience high levels of inflationary devaluation to save in a currency which is pegged to a stable value) attract organic users who value and hold the token, forging deeper loyalty and distribution and as a result, increased security for the community's economy and governance.

14.5. Zero Knowledge Roll-ups for Scaling and Privacy

Scaling blockchain networks for mainstream use has been challenging due to network congestion and high transaction costs on layer 1's. Zero-knowledge (ZK) roll-ups, a layer-2 solution, address these issues by moving computation off the Layer 1 chain and validating transactions with compact proofs on layer 1, reducing congestion and costs.

ZK proofs work, essentially by allowing someone to prove that they have access to information without actually showing that information to the party asking for proof. For example, if the information that they posses allows them to correctly solve a complex mathematical problem over numerous iterations and adjustments in input variables so that expected outputs are received in return, then after a number of repeated correct responses in a row, the party asking for the proof can be satisfied that the party with the information actually has it, even though they do not know what the information is and do not need to reveal it.

A simple example of a ZK Proof is where you ask a friend to tweet out a word from a Twitter account that they say they control. They oblige and a few minutes later you see the Twitter account in question has posted the word you requested. There is now a good chance that your friend is proven to be the owner of this account, but to be sure you ask them to repeat the process several times, each time posting a different word that you have specified. After several correct tweets, you have enough evidence to be convinced that your friend controls the password to that Twitter account. Your friend does not need to reveal to you the password to their Twitter account to prove to you that they do in fact have the keys to that account. This is a Zero Knowledge Proof.

The process of ZK roll-ups is where the computation to carry out and verify transactions is not done on the blockchain Layer 1, but on a ZK capable Layer 2. ZK Roll-ups on such a Layer 2 can batch or roll up many thousands of transactions. Then a ZK Proof can be published to the Layer 1 for final clearing and security, verifying the correctness of the transactions in the process.

The important thing to note here is that these ZK proofs are far smaller than complete Layer 1 transaction data making the Layer 1 far less congested when it uses ZK Proofs to scale while not adding to the cost of transactions.

Because of their Zero Knowledge nature, these proofs can be adapted to enable Layer 1 block producers to validate Layer 2 transactions without needing the transaction information itself. This makes the transactions private, obscuring information from both the Layer 1 block producers, third party observers and even the person receiving the transaction.

14.6. Real-World Example: Community Forks

The evolution of certain DPoS systems shows how distribution often arises from unexpected events like hostile takeovers or forks rather than neat, planned "token sales." When a community must set aside its internal differences and unify to fork out a malicious actor's stake, distribution can become more *organic*:

- Many previously inactive holders in voting become active voters to defend the chain - like an immune system kicking in, it increases the inherent security of the chain by reducing apathetic voters.

- Founder stakes or investor stakes get nullified if they attack the community.
- The result is a large class of committed stakeholders who align around genuine and continued decentralisation.

  (See chapter 13.4.2 for more information on forking away from an abusive whale stake)

Conclusion

The so-called "Scalability Trilemma" posits that a chain must sacrifice security (decentralisation) for scalability or vice versa. In practice, this trilemma stems from conflating *data availability* with *computation* and ignoring the power of Parameterised Coin Voting combined with a widely distributed token.

Key Lessons

1. **Separate Computation from the Base Layer**
   - Keep Layer-1 minimal: text data availability and lightweight transactions.
   - Push heavy smart-contract logic, large media storage, or advanced computations to Layer-2.
   - This allows near fee-less base layer transactions, crucial for censorship resistant usage.
2. **Resource-Credit or Staking Models**
   - Eliminate high, unpredictable base layer fees so layer-2 solutions and normal users can reliably store data or do basic transfers.
   - Guarantee that the success of one application doesn't undermine the cost of transactions on others through universal "fee auctions."
3. **Ensure No Single Entity Can Dominate**
   - Avoid pre-mines, large ICO's, or central staking pools that accumulate majority control.
   - Parameterised consensus (e.g., a fixed set of elected, replaceable block producers) and lock-up stakes for governance. (For more information on Pre-Mines and ICO's see Chapter 15. "Censorship and the Morality of Pre-Mines").
4. **True Security = Decentralisation**
   - "Security" is not separate from "decentralisation." A chain is only secure if no single party can impose censorship or freeze assets.
5. **Broad Distribution Is Non-Negotiable**
   - Let anyone earn the token from real value-added activities such as building, content creation, infrastructure support.
   - Community forks or "freak events" often achieve fair distribution more effectively and organically than any top-down design.

By following these principles, a blockchain can deliver robust throughput *and* maintain censorship resistance disproving the notion that one must compromise "security vs. decentralisation vs. scalability." Properly built systems show these are not mutually exclusive trade-offs but rather

aspects of a carefully designed, parameterised network where *no single dimension* has to be sacrificed.

Chapter 15. Censorship and the Morality of Pre-Mines

How Pre-Mined Tokens Enable centralised Control and Why True Decentralisation Demands Fair Distribution

15.1. Understanding the Moral and Practical Issues of a Pre-Mine

15.1.1 Defining a Pre-Mine

A **pre-mine** occurs when a blockchain's token supply is minted, sold to or allocated to specific insiders (founders, VC funds, early investors) *before* it becomes available to the broader community. This may happen in an ICO, private sale, or "seed round."

- **Moral Concerns**
    - **Unearned Privilege**: Those who receive a large portion of tokens at negligible or no cost gain disproportionate power over governance, essentially "buying out" a community that doesn't even exist yet.
    - **Misalignment of Incentives**: Early insiders can exit ("dump") on future participants, who then become de facto exit liquidity. The project's "community" and the insiders do not have the same goals as a result.
- **Regulatory Exposure**
    - If the same small group has significant control (e.g., 20%+ of the supply), that project can be classed as an unregistered security under various interpretations. Even if it is *not* formally regulated by the SEC or CFTC, it remains susceptible to political or legal pressure due to its obvious central points of failure.

15.1.2 Hidden "Regulation Through Pressure"

Even when regulators officially classify a token as a "commodity", where it falls outside of the regulation of the governing bodies **informal leverage** still exists:

- **Centralised Owners:** Large token holders often operate in major financial jurisdictions. If pressured by authorities, they can be forced to comply, or risk legal consequences.
- **Control of Infrastructure:** On a chain that is majority-owned by a handful of entities, governments (or powerful corporate interests) can persuade infrastructure operators, or coerce them to censor certain users or transactions, particularly if they are operating a significant amount of an ecosystem's infrastructure under one corporate entity.
- **No Official "Crackdown" Needed**: The project appears "unregulated," yet it's quietly *controllable* by anyone who can influence those few whales or well-funded validators or infrastructure operators. This is the case with most blockchain projects operating today. Particularly those with the largest market capitalisations.

Key Point: *Pre-mines hand regulators and large stakeholders a built-in "attack vector." They can shape the chain's rules or impose censorship indirectly because the underlying distribution is centralised.*

15.2. How Pre-Mines Undermine Censorship Resistance

15.2.1 Coin Voting Without Parameters

- Many chains use **un-parameterised proof of stake** which is effectively "coin voting" with no strict guardrails.
- If pre-miners hold large stakes, they can dominate every decision without having earned their positions of influence on a fair basis. Legitimate community members hold far less influence and cannot effectively resist if these big holders choose to censor certain addresses or content.

15.2.2 Tying into centralised Nodes

- Large token holders often fund massive infrastructure, especially when the chain's nodes are expensive to run (e.g., requiring high-end hardware).
- This fosters a network of large, centralised validators often operating in "regulation friendly" jurisdictions. If governments demand blacklisting or freezing, this small circle of validators will likely comply, no matter how "officially decentralised" the chain claims to be.

15.3. Moral Arguments Against Pre-Mines

- **Fairness and Earning**
    - A chain that launches without pre-mines (or large ICO allocations) forces *every* participant to "earn" their position, whether by early mining, meaningful contributions, buying tokens on the open market or earning social "value-for-value" rewards.
    - This fosters alignment: all holders have sacrificed time, labour, or resources, so they *want* the system to be robust and censorship resistant. Where there is no pre-mine or ICO, even if the stake holder wants to buy and exit quickly, they will at least have already added value to the ecosystem in some way. Where they obtained their tokens by pre-mine, this is not always the case since no value was added when the stake holder was ordained tokens since they added little to no value to obtain that stake.
- **Avoiding Exit-liquidity and Exploitation**
    - When venture capital or founders hold a massive early stake, they can, and often do, sell those tokens after hype builds, leaving later arrivals holding devalued coins.
    - This dynamic cripples trust and channels wealth to insiders rather than distributing it among actual and organic community builders.
    - Why would you run a validator on a chain which is clearly owned by others? This means that all of your efforts and work are going into supporting increasing the value of other people who didn't actually earn that value fairly, since they obtained their tokens, pre-ordained, in a pre-mine.
    - Most chains with pre mines are making it look like many people run validators, where as in reality, no person who genuinely values freedom would would run a node in a chain that was pre-mined by someone else, as you are working for them by proxy

- Once pre-mines are removed form a community, or on projects where there is no pre-mine from inception of the project, often more open source contributions are observed from community members, since they know that the value of the work they do is not going back to a corporation, owner, founder, CEO or early venture capitalist firm.

- **True Decentralisation from Day One**
  - If no single party holds, say, more than 7% of tokens, there is less risk that an external, hostile force can capture the network by coercing that party, or obtaining their tokens in an over the counter private purchase.
  - The network's governance emerges naturally: participants vote proportionally to how much effort or value they have added, not how cheaply they acquired tokens at launch or even are ordained tokens at zero cost as happens in some cases.

15.4. Censorship Implications of Centralised Coins

The more centralised a blockchain is the more likely it is to succumb to corruption, regulation and shut downs. The following are some of the ways centralised entities can corrupt a seemingly decentralised ecosystem given just enough centralised control to tip the balance of power in their favor:

- **Layer-1 Manipulation**
  - Given enough stake and coordination from centralised exchanges, that hold significant amounts of custodial stake or Large stakeholders can simply impose code changes and only reorganize the chain, or block addresses that centralised entities who do not have the best interests of the community at heart if so demanded by a regulating agency.
  - Users have no recourse; the chain's rules can be rewritten without broad consensus in this scenario.
  - A chain's users must be vigilant, always monitoring for such vulnerabilities and attack vectors taking place or forming on the chain and in its governance token distribution.
  - Early Venture Capital, Pre-mine, ICO or company backed chains will appear decentralised under normal operational periods, however, in times of defending against catastrophe, when the community needs the chain to be the most censorship resistant, the ability for these centralising entities to censor transactions often becomes overwhelmingly clear. Even in times when the chain is not undergoing catastrophic attack, such as during a hack or when new, more restrictive government regulation is released, code changes can be passed that go completely against the community's wishes. In such cases, the community has little recourse.

- **Censorship on Layer-2**
  - If the base chain is compromised then so are "layer-2" apps. Artificially imposed high fees by bad actors on Layer 1, or central gatekeepers hamper true censorship resistance, because it can become expensive to clear to Layer 1 for immutability in such cases.

- Many “layer-2” solutions rely on Layer 1 stablecoins, which may become controlled by a few large token issuers (again, pre-mined or pre-funded). Authorities can freeze or reverse transactions on these assets easily in such scenarios.

- **No Grass-roots Defence**
  - In truly decentralised systems, communities can “fork out” malicious large holders. But if the majority stake belongs to a handful of powerful investors or exchanges holding custodial stake that can be used for governance voting, forking to remove them is nearly impossible. The entire infrastructure effectively obeys or is operated by the largest stakeholders.

15.5. Case Studies & Real-World Consequences

- **Steem–Hive Fork**
  - When Steemit Inc., the company behind The Steem Blockchain sold its large “ninja-mined” stake to an external buyer, that buyer (Justin Sun) attempted to dominate chain governance and stated that the ecosystem’s decentralised applications would now be migrating across to another chain, without first getting approval from the Dapps in question, the community quickly forked Steem, creating the The Hive Blockchain which removed the hostile ninja mined stake on the new fork. Since there was one identifiable hostile stakeholder and many opposing whales and community members that supported the community, the new fork was sufficiently decentralised after having forked out the hostile entity, and so the Hive fork was a success. However, had there not been sufficient decentralisation of large stakeholders, it may have been the case that the new fork created a situation in which a new group could easily form an alliance to dominate and dictate the new fork's governance, making it a failure.
  - *Key Lesson*: If a chain can unify and remove an overbearing founder stake by forking, it avoids permanent capture, but only if distribution is already broad enough to resist takeover on the new fork.

- **Ethereum’s Regulatory “Gray Area”**
  - Ethereum pre-sold tokens in its Initial Coin Offering, yet it still ended up under partial regulatory capture because it is big enough and has signalled compliance (e.g., censored Tornado Cash transactions at the protocol level based on regulatory body actions, causing compliance among major validators).
  - *Key Lesson*: Even if not formally labelled a “security,” the chain is still vulnerable to censorship demands because large validators and infrastructure operators, especially those who obtained their stake by being sold cheap tokens by the founders in a pre-mine, can be pressured indirectly by regulatory and government bodies.

- **Highly-centralised “Chains”**
  - Some networks remain so heavily pre-mined that a founder or VC sees almost all future “community” participants as exit liquidity. They seldom resist censorship or they bow out to regulation if it threatens the early insiders’ majority stake.

15.6. How a Pre-Mine Hurts Everyday Users

- **Misaligned Incentives:** Insiders may not care about genuine freedom of speech or censorship resistance; they often care only about short-term ROI. They will normally comply with any authority if it sustains token price or personal safety.
- **No Real Vote:** Even if the chain claims to have on-chain governance, smaller user stake is dwarfed by whales who were self ordained pre-mines and who never earned their tokens, making "community voting" largely symbolic.
- **Susceptibility to Attacks:** A single compromised entity (venture fund or centralised exchange) can pivot chain policy, effectively turning the network into a lightly disguised corporate product.

15.7. Moving Forward Without Pre-Mines

- **Founder-less / No-ICO Launch**: It is critical to allow people to mine or contribute from day one without privileged allocations on a fair bases, so that as many people, technical and non-technical alike, can mine the token from a neutral base layer. The result is a much wider, organic distribution, where the goals and interests of the vast majority of players are aligned, and people trying to exit have already added value in some form.
- **Stake Distribution**: Encouraging "value-for-value" earn models, so tokens flow to users who actually run nodes, create valuable content, or provide valuable services rather than early self ordained pre-mine holders.
- **Parameterised Coin Voting**: Long lock-up periods and other distribution and voting constraints make it harder for one group to seize control.
(As described in chapter 11.4 De-Governance, Delegated Proof-of-Stake (DPoS) for further information on DPoS)
- **Community Watchdog**: If any large entity accumulates too much power and becomes hostile or is perceived as a security risk, the community is prepared to fork or vote them out. This is impossible if pre-mines gave them a large enough majority stake that the community becomes fragmented following the defensive fork. The community needs therefore to self regulate this dynamic and make sure it does not become susceptible to such a situation.

Conclusion

Pre-mines are more than a funding shortcut: they are a structural vulnerability that undermines the very decentralisation many blockchains claim to champion. By empowering a small elite or large investors from inception, such projects pave the way for censorship, regulatory capture, and moral hazards, *no matter what the official legal label might be.*

Key Takeaways:

1. **Moral Misalignment**: Pre-mined coins let a handful of insiders profit off later participants.
2. **Regulatory Pressure**: Even if not formally classed as "securities," large holders can be coerced to implement censorship or "comply" with government mandates.
3. **Weak Community Defence**: When a chain is top-heavy, resisting takeovers or forks that remove corrupt actors is nearly impossible.

4. **True Freedom Requires Fair Distribution**: Launching without pre-mines or ICO's compels all to earn tokens *proportionately* to contributions, building a naturally decentralised governance system in which all have a fair chance to build stake and participate, without serving someone else who has not already added value to the eco system themselves.
5. **Mis-Alignment of Incentives** Early, pre-ordained token holders have an incentive to use unsuspecting, new users as exit liquidity, without first adding any value themselves.

Refusing pre-mines and demanding fair, open distribution isn't just an ideological stance, it is a practical necessity for any blockchain that aims to be **censorship-resistant** and provide **neutrality** and therefore **Digital Rights** to its users, ethically aligned with user interests, and *beyond* easy regulatory capture.

Chapter 16. Three Pillars of Decentralisation

Three Pillars that all digital communities need for self-sovereignty

Introduction

Many projects struggle with decentralisation because they focus on the wrong goals or mix too many complex features into their base layer. By contrast, truly censorship-resistant and scalable systems can emerge from **three core pillars**. When these pillars exist at the base layer, the entire ecosystem gains self-sovereignty, freedom of speech, and economic resilience.

16.1. Text-Based Data Availability

Freedom of Speech
A system must store text (or fundamental data) in a globally replicated way. This ensures everyone can freely post or read, without a single entity able to delete or block content.

Simplicity and Cost
Only storing text keeps overhead predictable and minimal. Complex computations or large file storage on the base layer lead to huge costs and limited scaling.

Neutral Infrastructure
Because text is universal and lightweight, it can be distributed across many jurisdictions. Attempts to censor or alter historical records fail unless the entire network agrees, ensuring true data availability.

Key Point: *Text-based storage on the base Layer 1's the foundation of free speech and collaboration across any border.*

16.2. Zero-Fee Transaction Layer

Skin in the Game Instead of Fees
Rather than paying every time you transact, you stake (lock up) tokens to gain transaction bandwidth. This model is often called "resource credits" or "regenerative fees." It eliminates unpredictable costs and fosters global usability for all people, whereas chains with fees on transactions can become prohibitively costly to people without economic means to pay such fees.

High Throughput, Low Friction
When you remove transaction fees, you open the door for real-time micropayments and rapid app development. Users do not abandon the network under surge pricing or fee spikes.

Expanding Ecosystems
Zero or near-zero fees make it viable to build truly decentralised applications (on Layer 2's) that reference data from the base layer. Expensive layer 1's cannot host decentralised apps effectively because each action that clears from layer 2 to layer 1 (so that the Layer 2 application gains trustless security) becomes too costly.

Key Point: *A zero-fee transaction layer (backed by staking) ensures anyone can use the network, allowing broad adoption and preserving censorship resistance.*

16.3. On-Chain Stablecoin

Essential for Daily Use
A stable form of payment is critical for real-world transactions. If the native token always fluctuates in value, most people will not rely on it for routine expenses, business transactions or savings.

Decentralised & Backed
An on-chain stablecoin can be algorithmically backed by the main governance token. As long as the stablecoin's market cap remains well below that of the base token, the system remains secure.

Self-Sovereign Conversion
Because this stablecoin resides entirely on the base chain, users exchange value without external markets or centralised "gatekeepers." True on-chain liquidity means no forced reliance on outside exchanges for dollars or stable value exchange. Essentially this means that the eco system can continue to function and provide itself with liquidity, without Centralised or even decentralised exchanges

Key Point: *A decentralised stablecoin, fully integrated on the base layer, is the final piece that allows people worldwide to store and transact in stable value without leaving the protocol.*

16.4 Why These Three Pillars Matter

- **Censorship Resistance**
  Text-based storage protects free speech. Distributed nodes ensure no single jurisdiction or entity can delete what you say, post, your followers, your community or its economy.
- **Zero-Fee Transactions**
  With staked tokens, users bypass unpredictable network fees. This opens the door to everyday usage, micro-transactions, and diverse decentralised apps where users do not require gas, a prohibitive hurdle to access in order to interact with the ecosystem.
- **Stablecoin Integration**
  People need a stable unit of account for commerce. An on-chain stablecoin allows real economic activity without centralised intermediaries.

Together, these pillars form a self-reinforcing network:

- **Free Speech** (data availability) increases the system's inherent value and communication.
- **Zero Fees** encourage participation and app development for all people.
- **A Base layer Stablecoin** empowers real-world trade without needing external exchanges.

When combined, they create a **truly self-sovereign** ecosystem: no central point of failure, no single jurisdiction in control, resistant to blockages of on and off ramps, and no reliance on external stablecoins or exchanges. This model is already demonstrated in systems like The Hive Blockchain, which integrates text-based data, near-feeless transactions through staking, and an on-chain stablecoin. By mastering these three pillars, a blockchain can achieve a higher degree of decentralisation and practical everyday utility.

Chapter 17. Algorithmic Stablecoins on Layer 1

A fee-less, permissionless, non banking asset backed Layer 1 medium of exchange and liquidity is essential

17.1 Why We Need a Truly Decentralised Stablecoin

Many blockchains rely on **centralised stablecoins** (like Tether or USDC) that hold reserves in fiat accounts. These assets can be seized, frozen, or regulated at any time. A censorship-resistant blockchain must have an **algorithmic stablecoin** backed only by digital value that no single entity can control or confiscate.

17.2 Backing the Stablecoin with Digital Real Estate (Social Tokens and Bandwidth in the Ecosystem)

A stablecoin has to be backed or collateralised by something. In a censorship-resistant system, backing cannot be gold, dollars in a bank, or any physical good vulnerable to seizure. Instead, it should be backed by a **Layer-1 governance token** that represents valuable digital real estate or bandwidth to post data on chain, relative to other users or apps also wishing to post data to chain.

The governance token should grant:

- **Access to on-chain resources** (e.g., text storage, zero-fee transactions otherwise known as bandwidth access to upload to the database).
- **Payouts in newly minted tokens** for community contributions.
- **Proof-of-stake governance** with strong parameters to prevent takeovers.

This “digital real estate” has fundamental demand because it secures data availability (free speech) and zero-fee transactions. The main token can then back or over collateralise an on-chain stablecoin, algorithmically pegged to the dollar without the need to hold collateralising assets in a traditional bank, which are subject to seizure or censorship.

17.3 How It Works

1. **Pegging to the Dollar**
   The stablecoin maintains a target value of one US dollar. It does so by letting holders redeem the stablecoin for one dollar’s worth of the base token. As long as the base token has a higher market cap than the total stablecoin supply, redemption is secure and the stable asset remains adequately over collateralised.
2. **Haircut Rule**
   To avoid the fate of projects like Terra/Luna, a **debt limit** or “haircut” parameter is set (often around 20–30%). If the stablecoin supply approaches such a set percentage of the base token’s market cap, the chain stops issuing new stablecoins. This prevents the stablecoin’s market cap from exceeding its collateral.
3. **Delayed Conversions**
   Attacks happen when a stablecoin is instantly swapped for the governance token and dumped on the market. To counter this, conversions take place over a few days (3.5 days is

typical). Large conversions face **time risk** and possible fees, making quick takeovers highly risky for the attacker and most likely unprofitable.

4. **Fee or "Haircut" on Bulk Conversions on the Base Layer**
   A small fee (e.g., 5%) can apply to mass conversion, discouraging sudden attacks. Genuine users pay the fee only when moving large sums, while attackers find it prohibitively expensive to destabilize the system.

5. **Reward Pool Funding**
   These stablecoins often emerge via new token minting to a daily rewards pool that the community competes for. The more stake weighted votes your contributions receive, the more of the rewards pool you receive in turn: half of the daily rewards go to users in stablecoins, and half in the base governance token. This slow, steady issuance avoids reliance on centralised reserves. Over time, the stablecoin organically expands alongside the flow of tokens to the community.

17.4 Infinite liquidity Through Base-Token Conversion

Even if centralised exchanges list only small amounts of the on-chain stablecoin, true liquidity can be **effectively unlimited**. A large holder can:

1. **Buy the Base Token On the Open Market**
   Purchase the governance token on open markets.

2. **Convert Over Time**
   Convert that token supply into stablecoins via the protocol's built-in mechanism on Layer 1.

3. **Haircut Rule Enforcement**
   If the conversion is large, the base token's price likely rises. This increase keeps the ratio below the debt limit, preserving stability, in fact it may lower the debt limit as the supply of the stable coin is increased, since in this scenario it is likely that the market cap of the base layer token being bought on the open market and used to convert to stable coins will increase at a higher rate than the increase in supply of the new stable coins being created by those conversions.

This process mirrors how centralised stablecoins work except there's no single issuer to "call" for a mint or redemption. The protocol itself autonomously executes conversions.

17.5 Example: Hive Backed Dollars (HBD)

- **Non-Custodial**
  No single wallet, company, or government can KYC, freeze HBD or seize its collateral.

- **Three-Second Confirmations**
  Transactions are nearly instant and effectively fee-less thanks to resource staking.

- **Parameter Rules**

  - **30% Debt limit (Haircut):** If HBD nears 30% of the governance token's market cap (Hive), no more HBD is issued.

  - **Conversion Delay:** Conversions from HBD to Hive (or vice versa) take several days and may incur a fee.

- **Organic Expansion**
  HBD supply grows through daily new tokens mints which are allocated to content creators and community members via decentralised community, stake-weighted voting systems.

If large financial players want millions in decentralised stablecoins, they simply acquire Hive on the open secondary market, then convert day by day into HBD. This pushes Hive's price up such that its market capitalisation increases more than the newly minted stable coins, lowering the debt ratio. Thus the stable coin issuance system scales while maintaining an adequate collateral buffer.

17.6 Resilience Against Attack

Comparisons to Failed Models
Un-parameterised algo stablecoins like Terra/Luna had no effective cap on supply or redemptions. When attackers mass-converted the stablecoin to Luna, it collapsed the token's value. In contrast, parameterised systems employ:

- **Haircut thresholds**
- **Delayed conversions**
- **Optional conversion fees**

These dampen flash manoeuvrers, vastly increase financial risk to the attacker and reduce exploit potential.

Fork-Out Option
Even if a large actor gains a huge stake, reputation based, censorship-resistant communities can fork the chain and exclude hostile balances. This threat deters malicious governance attacks.

17.7 Toward a Parallel Dollar Economy

A reliable Layer 1 stablecoin sets the stage for a **true parallel economy**, allowing everyday people to:

- **Transact globally with no KYC**
- **Store value in a stable currency**
- **Move into or out of local currencies without permissioned gateways**
- **Access zero-fee settlement in seconds**

Because these stablecoins are algorithmic and fully on-chain, they also enable advanced financial instruments like **bonds and collateralised loans** mirroring "pristine collateral" (akin to US Treasuries) but free from legacy banking restrictions. Over time, such systems can mirror or replace major components of traditional Euro Dollar international finance system without centralised reserves or permissioned intermediaries.

Conclusion

- **No Physical Reserves**
  Backing must be purely digital, immune to seizure or control by a single entity.
- **Parameter-Based Algorithm**
  Enforce haircut rules, delayed conversion, and optional fees to maintain the peg and prevent sudden attacks.
- **Infinite liquidity**

  As long as the governance token is valuable (due to real utility), large amounts of stablecoins can be created by buying the base token.

  Stable, Parallel Currency
- Distributed newly minted tokens and community-driven enforcement produce a sustainable on-chain dollar for everyday use and financial services.

Algorithmic stablecoins on Layer 1 are an essential pillar for any genuinely decentralised blockchain ecosystem, powering commerce, savings, and economic growth outside centralised oversight.

Chapter 18. Off-Chain Data Availability Layer for Non-Text Data

Storing More Than Text

Introduction

A text-based storage layer on the base chain is critical for censorship-resistant records, but what happens when you need to store large files like videos or software? Storing them directly on a lightweight, text-focused chain would bloat the network. Once you move beyond text, you need an **off-chain data availability layer** to keep blockchain nodes lean while still distributing and verifying heavier content.

18.1 Why Not Just Put It All On-Chain?

- **Data Density**
  Large files (videos, high-resolution images, or entire software packages) are too big for most blockchains to handle without enormous storage overhead.
- **Performance Bottlenecks**
  Even if you tried, nodes would become "fat" and resource-intensive, ruining the fast, low-latency experience needed for high transaction throughput on the base layer.
- **Selective Immutability**
  Most users do *not* want every casual comment (e.g., "LOL") stored immutably forever. It's better to keep the on-chain layer for critical text, metadata, and important references.

Hence, pushing large files off-chain is both practical and efficient. This also helps to de-load the base layer allowing it to focus on storage only of critical information and data links that direct to off-chain information. The result is that the base layer can scale far beyond what was originally possible if everything had been stored only on the base layer.

18.2 How Off-Chain Incentives Work

With text on the base layer, you still need secure, censorship-resistant ways to store everything else. Think of it as **Layer-2** storage where off-chain, dedicated storage nodes maintain heavier files, but receive **on-chain incentives**. A widely discussed approach is a separate token-based system that pays operators for providing off-chain data availability.

1. **Users or Apps Want to Store Files**
   They create an on-chain contract specifying the data and how much they will pay to keep it available.
2. **Nodes Run Off-Chain Storage**
   These are community-run machines providing excess hard drive space or bandwidth.
3. **Proof of Storage or Access**
   The network randomly checks if the nodes still hold the data. If they prove it correctly by quickly delivering requested file segments they earn rewards.
4. **Layer-2 Tokenomics**
   An additional token can fund payouts for storage, encoding, or content delivery. This token's rules are anchored to the main chain but operate independently for heavy data needs.

18.3 Example: The SPK Network

One model for off-chain availability is the **SPK Network**, which stores large files (like videos) via a distributed set of nodes. There is:

- **A Core Incentive Token**
  Operators provide bandwidth and disk space for content. They are rewarded by user-created contracts, each specifying what files must remain available.
- **Validator Nodes**
  A light weight system of twenty community elected validators should be the route through which all content on the off chain storage system is uploaded. The Validators can then take the encoded chunks of data and hash their data footprints. Community storage nodes must download the files from these validators and hash the same data chunks to confirm receipt of the data.

The reason this works well is that it does not require all validators running nodes to process and store all files in the network, like a proof of work system would do. A Parameterised Coin Voting system (DPoS) for file storage is the optimum solution since it is lighter weight that PoW and, with 20 elected validators it can manage decentralised consensus governance whilst still being a trustless system which does not need to count only on the richest members of the community to run its most critical infrastructure; the content validator nodes.

- **Proof of Access**
  The network randomly pings community data storage nodes to confirm they can serve requested data. If they deliver the matching hashed chunks back to the validators quickly, this is confirmation that the storage node is storing what they say they are storing. As a result, they earn rewards from the allocated contract pool associated with the contract within which the file is stored.
- **Video Encoding & Streaming**
  In addition to raw storage, a system like SPK can incentivise video transcoding and live streaming servers, offloading the heaviest processing from the main chain.

Through these incentives, SPK aims to replace centralised video platforms' back-end (storage, streaming, encoding) with a decentralised, community-owned layer.

For further information on The SPK Network visit: https://spk.network/

18.4 Keeping the Base Layer Lightweight

Text is fundamental for an immutable record of governance, transactions, and high-level metadata. Everything else heavier or more data intensive such as video, large images, or software should be stored off-chain. By separating duties:

- **Layer 1**
  Stores text data (comments, references, IDs), plus the chain's consensus rules and transaction layer.
  - Remains fast, minimal, and non-"fat."
  - Uses no fees or very low fees, powered by a daily rewards pool of newly minted tokens.

- **Layer 2**
  Handles heavy storage with separate economic incentives.
  - Runs “proof of storage” or “proof of access” to verify hosting.
  - Nodes earn a specialized token.
  - Maintains partial immutability: if a node drops your file, it loses rewards and on chain reputation.

18.5 Why Separate Layers Matter

1. **Scalability**
   Dividing text-based consensus from heavy file hosting prevents the entire chain from bogging down.
2. **Targeted Security**
   Text on-chain enjoys the strongest guarantees (immutable, globally replicated). Multimedia off-chain can still be censorship-resistant but doesn’t force every blockchain node to store gigabytes of data.
3. **Flexible Costs**
   On-chain data is costly and must remain minimal. Off-chain nodes can set custom storage prices, allowing a market-based approach for different file sizes and retention durations.
4. **Endless Services**
   Beyond video, any large-scale process such as music hosting, 3D rendering, AI model storage and many more can be incentivized similarly. Community-run nodes provide resources and earn tokens for proven work.

Conclusion

- **Lightweight On-Chain Core**
  Text data and governance remain on a fee-less, Parameterised Coin Voting chain. This ensures immutable text based information and references, reliable transactions, and stable coin minting.
- **Off-Chain Data Availability**
  Parallel networks like SPK host non-text data under a separate token economy. Nodes prove accessibility of large files to get paid via the Proof of Access method (PoA). Users, content companies and content platforms create contracts for any multimedia content. As a result, individual community members can be paid for backing up this content.
- **Mutual Reinforcement**
  The main chain’s reputation and incentives ensure honest participation. Layer-2 nodes trust the base chain for governance, data permanence and data availability, while the base chain gains broader utility through off-chain hosting solutions.

This two-tier system (immutable text plus incentivized off-chain data) balances **scalability** with **censorship resistance**. It stores critical records on the main blockchain and offloads heavier or less crucial files to user-powered networks for back up. The result is a robust ecosystem where nodes can specialize, content remains online without centralised servers, and the core chain stays lean and can scale.

Chapter 19. Service Infrastructure Pools (SIP)

Paying the community instead of the exchanges

Introduction

A Service Infrastructure Pool (SIP) combines elements of a decentralised exchange (DEX) and a DAO. Normally, DEX trading fees go to a centralised operator's profit. In a SIP, those fees are pooled and can be voted on by token holders to fund infrastructure improvements or other community initiatives.

19.1 Basic Concept – Send Exchange Fees Back to the Community

Instead of letting a centralised exchange collect trading fees, a SIP aggregates them into one pool. Stakeholders then decide how to use those pooled funds. They might pay infrastructure operators, fund new features, or distribute incentives that benefit the broader network. This is often coupled with a way for the SIP to sell an autonomous product or service. The revenue of which goes directly into providing additional liquidity to the SIP account. This allows the SIP to grow over time, potentially to a point where the fees generated from token exchanges are able to fund all or most of the infrastructure that is operating on the wider network.

19.2 Example from SPK Network

In SPK Network, users can buy mining tokens (like LARYNX) to improve their share of mining rewards directly from the SIP account. Purchasing these tokens requires locking up dollars (HBD or similar) in a liquidity pool. The key points are:

- Buyers of tokens place funds into a SIP account.
- Those funds stay in the pool and can be used for community-driven initiatives.
- The mining tokens give owners more "mining" weight or resource priority.
- If attackers want control, they must buy these tokens from existing holders, effectively paying the community their required rate for taking over the governance, after which the original community will likely fork, if the attacker is deemed as non benevolent to the protocol.

This setup discourages hostile takeovers because any large purchase of mining tokens raises the token's price (benefiting existing holders), and the attacker's funds permanently bolster the ecosystem's liquidity.

19.3 Combining a DEX and a DAO

A typical DEX allows people to stake liquidity, earn fees, and withdraw profits. In a SIP, part of (or all) the funds remain in the pool rather than returning to individual stakers. The pool's growing liquidity produces trading fees, and those fees can be:

- Sent to infrastructure operators.
- Allocated to development teams.
- Distributed for marketing, user incentives, or emergencies.

By design, it is like a DAO controlling a permanent liquidity stash, with revenue streams continuously replenished by users buying service tokens (e.g., mining tokens which improve a users mining capabilities in the network).

19.4 Required Technology and Combining Ecosystem liquidity

As SIP's grow they can be combined as multi-sig liquidity and collateral providers, stored on the base layer. For additional security, they can employ a massive mutli-sig technology such as BLS signatures. This allows for a reduction in size of the signature storage required in each block and therefore accommodates 400 up to thousands of keyholders on the main multi-sig account (SIP) in the ecosystem. This means that much larger amounts of liquidity can be securely stored for various purposes by various parties on chain who seek increased security for their liquidity providers.

19.5 Self-Sustaining Ecosystem

Over time, more participants buying tokens for better mining efficiency drives more funds into the SIP. The liquidity pool gradually swells. As it does, it may earn enough in trading fees to:

- Pay for infrastructure without relying on external funding.
- Provide a safety net if outside market conditions weaken.
- Autonomously finance new ecosystem projects and expansions.

The end goal is an ownerless, decentralised “pot of liquidity” that pays for the chain’s operations and growth, acting like a shock absorber during market downturns.

19.6 Replacing centralised Exchanges

Centralised exchanges such as Binance or Coinbase collect trading fees for corporate profit. A SIP, by contrast, directs its fees and other revenue streams into an on-chain pool governed by community votes. Rather than benefiting a few large shareholders, these funds can:

- Reward node operators.
- Subsidize new projects or Dapps. - Remain inside the community, strengthening the protocol overall.

This model reclaims revenue streams that would otherwise flow into centralised parties.

Key Takeaways

- **Autonomous Purchases**
  When users buy mining or service tokens from the SIP, funds go into the SIP and never leave, creating a permanent, increasing liquidity reserve.
- **DAO-like Control**
  The community decides how to allocate SIP reserves, ensuring democratic management.
- **Stability and Growth**
  As more people seek the service tokens, the SIP grows, generating fees that can fund infrastructure or offset downturns.

- **Reduced Attack Vectors**

  A would be attacker must inject significant capital to gain leverage, thereby strengthening the ecosystem in the process.

Conclusion

Service Infrastructure Pools blend DeFi liquidity pooling with DAO governance to create sustainable, community owned revenue mechanisms. They transform trading fees into collective assets that keep infrastructure running and development funded, all without centralised exchange intermediaries.

Chapter 20. Open Source Makes IP Less Valuable

A new business model is to accumulate the governance token and give the rest away for free

Introduction

Open source development challenges the traditional value of intellectual property. In a blockchain ecosystem built on open source principles, code can be freely copied, iterated upon and improved by anyone. Instead of focusing on proprietary software or brand protection, the emphasis shifts to tokenizing a base layer protocol that gains value from community driven network effects.

20.1 Why Traditional IP Models Will Weaken

20.1.1 Copy and Iterate

In open source projects, anyone can copy the code and iterate upon it. This significantly reduces the power of patents and copyrights that typically protect software. Once the code is public, forks and variations can proliferate without legal barriers. It also vastly reduces the amount of work required to build a new digital project or product in cases where the original source code are used as the basis for that project.

20.1.2 No centralised Enforcement

Truly decentralised systems are resistant to lawsuits. You cannot sue an amorphous community of contributors or node operators, especially when many use pseudonymous identities. Traditional IP enforcement mechanisms lose their potency.

20.2 Accumulating the Base Token Instead of IP

20.2.1 Governance Rights Accumulation as the Business Model

Because open source leaves little “IP rent” to collect, builders accumulate governance or utility tokens in the underlying blockchain as a result of having received community votes for their valuable contributions to code building. As the ecosystem grows, the quality of products improves, a network effect takes hold in the user base, adoption increases, and the token’s value can rise.

20.2.2 Community Ownership

Projects no longer rely on proprietary lock in. Instead, they encourage developers to improve the code and create stronger network effects. Holding more of the base layer token gives influence and a direct stake in the ecosystem’s success, which incentivises further contributions from developers.

20.3 Abundance vs. Scarcity of IP

20.3.1 Abundant Code

In a fully open source environment, code is shared, and even brand elements can be replicated or remixed. This approach prioritizes expanding overall utility rather than controlling a limited pool of IP.

20.3.2 Power of The Network Effect

Instead of leveraging a single brand or patent, participants focus on building a strong community. The most valuable resource becomes the network of users, developers, and infrastructure operators all benefiting from a thriving token economy.

20.4 Brand and Community Tensions

20.4.1 Forking Logos and Names

In decentralised contexts, truly decentralised communities can mimic or adapt a project or brand's logo or name. Traditional lawsuits become impractical since there is no central entity to target. Attempts at enforcement can even backfire by uniting the community against the IP owner.

20.4.2 Brands Aligning with Their Community

Companies must adopt new ways to cooperate with decentralised user bases rather than trying to dominate them or see the data the generate as the sole property of the company to mine, sell and monetise. Real value lies in fostering community loyalty and participation, giving them skin in the value system via fair distribution of tokens / stake, not in clinging to trademarks or brand identities.

20.4.3 Stake for Resources

In a well designed, decentralised system, users or apps stake the token to gain network bandwidth. Developers build open source apps and receive tokens either by purchasing them on the market or earning them through community rewards for having done something valuable for the community itself.

20.4.4 Intrinsic Utility

A well designed, decentralised system offers censorship resistant text storage, fast and fee-less transactions, and stablecoin infrastructure. Its core is maintained by distributed contributors who share a common stake in the token of the community.

20.5 Suing a Distributed Community

20.5.1 Impossible Central Target

A fully decentralised network has no "headquarters" to subpoena. If there is no pre-mine, no foundation, and no single entity, lawsuits over IP infringement have no direct target.

20.5.2 Communities Undermining IP Laws

As a network becomes more censorship resistant and globally distributed, it becomes harder for IP owners to enforce claims. Communities operating worldwide with pseudonymous digital identities render legal pressures over trademarks and copyrights less effective.

Conclusion

- **Code Freedom Over IP**: Open source software weakens traditional IP claims. Anyone can copy and improve code without significant legal fear.
- **Token-Based Incentives**: Instead of profiting from patents, developers accumulate the base layer token, aligning them with long term ecosystem growth which in most cases incentivises further open source contributions from developers and other community members who want their existing stakes to grow in value.
- **Community as Strength**: Brands and logos can be forked in truly decentralised systems. The most influential brand is the one the community supports, not the one with the most lawyers.
- **No Central Point to Sue**: Fully decentralised projects lack a headquarters, owner, central figurehead or foundation. IP related lawsuits have no clear way to shut them down.
- **Focus on Network Effects**: Real value flows from community collaboration and user adoption. Open source accelerates ecosystem growth by inviting a broad range of contributors and forks.

When open source principles merge with decentralised governance, traditional IP loses its status as a profit centre. Economic rewards shift away from proprietary ownership and toward token staking in an ever-growing, cooperative network.

Chapter 21. Importance of Decentralised, Immutable Communities as Network States

Now Network States can Form

21.1 Defining Network States

A Network State is a globally distributed community that manages its own governance, has an internal economy, and cannot be easily shut down or censored by external forces. The idea is often associated with the concept of online nations that develop real world influence. Some may eventually purchase or acquire land and function with true sovereignty and a real world economy complete with trade deals and international agreements with other states. Achieving this requires:

- **Immutable ledger and governance**: A censorship-resistant blockchain or data layer upon which the community operates in the digital realm.
- **Decentralised ownership**: No single entity should control the chain, avoiding pre-mines, ICO's, or foundations.
- **Sustainable economy**: The community must be able to create and maintain its own token, Incentivizing contributions and causing buy demand for some sort of utility that increases proportionately to scaling, network effect and competition for demand for resources to interact with the communities base layer (as with the Resource Credit model described in previous chapters, See Chapter 7 – "Sustainable Economy & Decentralised Coin Distribution" for further information on creating sustainable economies with resource credit systems).

Unlike typical blockchain projects with ICO's or heavy centralisation, genuinely decentralised Network States distribute tokens fairly, making it impossible for any single party to dominate. This fosters a robust, self-sustaining digital community.

21.2 Power of Self-Sovereign Communities

When a community reaches critical mass, it can self-organize to:

- Communicate and collaborate without top-down control on an un-censorable text based, decentralised base layer.
- Offer real economic incentives for labour and contributions.
- Print its own token with no reliance on external permission.
- Protect members from censorship, as there is no centralised database to shut down.
- With an algorithmic stable coin on the base layer, the community can carry out trade in and conversion to stable value without needing an external DEX or CEX.

Such communities can become de facto nation states. Traditional governments rely on force or laws to secure currency demand, while these blockchain based communities rely on voluntary adoption and network incentives. Community members hold their stake because they earned it or purchased it off the open market, not because they were ordained it in a pre-mine. If they grow large enough, they can challenge or complement legacy financial and governance systems by making them more efficient and transparent.

21.3 Decentralised Token Distribution on Layer 2

Many Network States will likely form at the "layer 2" level, meaning they build on top of an existing censorship-resistant, neutral base chain. with the following characteristics:

- **Fair token distribution**: No large pre-mine, no venture capital in the "first ICO round," and no single dominating stakeholder.
- **Earning vs. pre-ordained**: Members earn tokens through valuable work or content creation, or buy them on the open market - they are not self gifted tokens at low prices in a pre sale or for "funding and development" of the project.
- **Self-sustaining model**: The token's utility (e.g., voting, access, on chain resource bandwidth access) creates ongoing demand with growth of transactions within the community.

Communities can thus issue tokens without creating a central point of failure. Over time, these tokens govern the community's own rules, curation and distribution mechanisms, and reward pools.

21.4 Sustainable Token Value and Staking Incentives

To foster lasting engagement:

- **Voluntary demand**: As more people want influence, reputation, or access to blockchain bandwidth, they buy or stake tokens, raising overall liquidity and reinforcing value.
- **Layer 2 Resource credit models**: Community members will have to stake both the Layer 1 governance token and the Layer 2 community token in order to obtain bandwidth or resources to operate in, post to and vote in the L2 community or Network State. As a network effect takes hold for the community, this will create demand for the token, driving its price up and making the token and community economy sustainable over time.
- **Stake for influence**: Members stake tokens to gain voting power, resource allocation, or other utilities (similar to how base layer staking controls network resources).
- **Reward for participation**: A daily rewards pool funded by newly minted tokens or other reward mechanisms ensure contributors receive tokens.

All of the above turns each community into its own mini economy, encouraging long term commitment rather than short term profit taking.

21.5 Liquidity Pools for Each Community

Instead of using a centralised exchange that extracts fees and can seize funds, each community maintains its own Layer 2, community specific decentralised liquidity pool for trading. Key benefits:

- **Fees return to the community**: Rather than paying centralised operators like Binance, trading fees feed back into community development and infrastructure operation.
- **Reduced attack vectors**: No custodial risk on centralised exchanges so tokens remain community owned.
- **Sustainable growth**: As liquidity pools deepen, more users participate which creates a virtuous cycle based on increasing liquidity and increasing confidence in the community and its economy.

Over time, these pools can become self sustaining, generating enough fees to fund infrastructure or act as shock absorbers during market downturns, subsidising trusted, but unprofitable infrastructure in times of a down turn in the market.

21.6 Community Self-Regulation of Content and Rewards

Because communities operate socially, they need to manage on-chain discussions and incentives:

- **Rewarding quality**: Users or apps vote on which posts, projects, or members deserve tokens.
- **Downvoting abuse**: Undesirable content can be downvoted or flagged, reducing its rewards or visibility.
- **Consensus-based rules**: The community sets thresholds for removal, tagging (e.g., NSFW), or moderating spam.

No single corporation is in control. Instead, collective rules, stake based voting, and front end policies govern how content is curated.

21.7 Content Gateways and Validators

On certain architectures (like an off-chain video storage layer), validators or gateways can decide which content is acceptable for the community. They are elected or chosen based on stake-weighted votes, so the community's values and nuances ultimately guide what gets through via elected content validators.

21.8 Stake-Weighted Tagging

Members with sufficient stake can force specific tags (e.g., NSFW, political, spoiler) onto content if they reach a voting threshold. This allows flexible, community-driven categorization without needing a central moderator.

21.9 Reward Disputes

If there is disagreement on how many rewards a piece of content deserves, or if someone has gamed the system, the community can downvote or re-allocate rewards. In advanced setups, a "jury" process might review disputes to decide whether to restore or remove tokens, or rally community support to re-upvote content that has been unfairly downvoted.

Conclusion

- **Self-Sovereign Network States**: Truly decentralised communities form online "nations" that can potentially buy land or exert real influence without centralised leaders or corporate backing.
- **Fair Distribution**: To remain censorship resistant, avoid pre-mines or ICO allocations. Community staking and fair issuance keep power spread out.

- **Sustainable Economies**: Internal tokens gain value through utility staked voting power, resource access, and liquidity pools that recycle fees back to the network.
- **Self-Governance of Content**: Community can set up effective content regulation systems on both Layer 2 Apps and Layer 1 content storage systems in order to prevent content that does not match the values of the community. The key is that one central entity cannot control censorship on chain.

Chapter 22. DAOs and Community Proposals for Self-Funding

Neutral funding removes compromise and maximises the neutrality of the tech

22.1 Decentralised and Neutral Funding

A major advantage of properly designed blockchain ecosystems is the ability to fund projects through truly decentralised, neutral mechanisms. Unlike traditional ventures or ICO's with centralised teams and venture capital, these models allow a community-owned treasury to fund ideas and community projects without a controlling entity or CEO. Community members vote on proposals using their stake, and once a proposal meets a threshold, funds are released on-chain to the developer or group that will perform the work.

In a truly neutral environment, there is no single legal entity, foundation, or board that dictates funding. Instead, participants stake their tokens for voting power, propose initiatives, and decide on projects that add value to the network. The key benefit is that funding does not come with the usual "strings attached" seen in centralised or venture-backed deals. Rather, it aligns community incentives toward shared goals.

22.2 What Is a DAO?

A Decentralised Autonomous Organization (DAO) is a community-governed treasury and decision-making structure on a blockchain. It generally has:

- **On-chain funds**: Often funded from newly minted tokens or fees.
- **Proposal system**: Projects request funding by submitting proposals.
- **Stake-weighted voting**: Token holders cast votes. If a proposal meets the required threshold, funds are released.

A genuinely decentralised DAO has no outside venture capital dictating decision makers. It has no single company or CEO that can override votes, and no foundation controlling funds. Instead, the community's stake decides how to allocate resources.

22.3 Decentralised vs. VC-Backed DAOs

Many DAOs appear decentralised but are, in reality, influenced or controlled by large venture capital allocations ordained or obtained far below market price at a pre-mine stage early on in the project, often before the tokens are traded on the open market. These VC's can concentrate voting power, leading to outcomes favourable to a few stakeholders rather than the entire network. Venture Capital firms also usually reside in "regulation friendly" jurisdictions, making them prone to regulatory pressure that can significantly shape funding decisions.

In contrast, a truly community-driven DAO has widely distributed tokens, no pre-mine, no ICO, and no single party holding a controlling majority stake. The ideal scenario and balance is where, even without the votes of the largest stakeholders, projects can still obtain funding via obtaining votes from the rest of the community. These are the rare DAOs that cannot be easily shut down, coerced, or dominated by external investors. Their funding decisions reflect actual community interests rather than extractive-driven agendas which do not necessarily serve the community.

22.4 Returning Value to DAOs

Because these DAO-funded projects do not have strings attached from corporate entities, it is crucial for the community to establish accountability:

- **Milestone-based releases**: Funds are released only after certain goals are achieved.
- **Monthly or phase payments**: Ongoing work (e.g., maintenance) is funded incrementally, with the community free to remove votes if progress stalls.
- **Open bidding**: The community can publish desired tasks, inviting multiple bids. Stakeholders then vote on the most competent developer with the fairest price.

The community expects projects to benefit the ecosystem long-term. A neutral DAO often funds tools or protocols that enhance network utility (for example, off-chain storage, social features, or scaling solutions). The team's reputation is on the line: if they fail to deliver, future proposals are unlikely to pass.

22.5 Example: The Hive Blockchain Decentralised Hive Fund (DAO) and SPK Network

On The Hive Blockchain (a text-based storage layer), the SPK Network received funding from Hive's decentralised proposal system to build off-chain media storage. SPK's work benefits Hive users who want to store large files (videos, images) beyond the scope of the base chain. In return, SPK gains community recognition and support but has no direct "contract" with a corporation. In return for this, the project dropped its mining tokens to the entirety of the Hive community in a claim drop. The users who claimed tokens are able to mine more efficiently in the network and therefore earn the network's governance token for providing infrastructure operation. Due to DAO funding, there was no need for a pre-mine or ICO to fund the project, and therefore the SPK Network has a highly neutral layer that protects the rights of users and their content storage.

The community can stop funding at any time if deliverables fall behind or if the project ceases to align with Hive's goals by un-voting the proposal and dropping its total votes below the community set threshold of votes required to receive funding.

This model shows how a community can sponsor critical infrastructure without relying on ICO's, venture capital, or centralised companies. It aligns incentives around expanding the chain's ecosystem while preserving user ownership and governance.

22.6 Alternatives to "No Strings Attached" Funding

A common concern with "free" funding is that teams could run off with the money. DAOs mitigate this by:

- **Clear scopes of work**: Publicly outline tasks and deliverables.
- **Reputation and trust**: Developers who leave projects incomplete damage their standing, making future funding unlikely.
- **Revocable votes**: If a project deviates from its stated goals, community members can un-vote their support, temporarily or permanently halting further payouts.

These checks protect communities from severe losses and ensure ongoing alignment. The outcome is a more transparent, flexible funding environment that encourages collaborative development.

22.7 Why Neutral DAO Funding Matters

- **Eliminates Venture Capital Control**: No massive early allocations or pressure to chase short-term profit.
- **Scales Through Collective Effort**: Communities that must fund and maintain the chain themselves learn to optimize and reduce bloat.
- **Resists Regulatory Capture**: Without a centralised owner or foundation, a decentralised treasury cannot easily be forced to censor or comply with unfavourable rules.
- **Protects Against "Exit liquidity" Behaviour**: Teams funded by neutral DAOs are less likely to dump tokens or pivot abruptly because they rely on continued community approval and can be dropped governance or mining tokens in exchange for DAO funding, excluding the need for bringing in Venture Capitalists whose values and reasons for being involved in the project may not align with those of the community.
- **Promotes True Decentralisation**: Everyone with stake can contribute ideas and vote, reflecting widespread consensus rather than corporate edicts.

Projects developed under this model become genuinely community-oriented. Their tokens have higher community trust because there is no hidden pre-mine or venture round waiting to sell into unsuspecting community members at higher prices. As a result, DAOs with a broad, participatory user base produce ecosystems that are more censorship-resistant, equitable, and sustainable in the long run.

22.8 DAOs are Always More Centralised than the Witness Pool

Community members that vote for Witnesses often do not also partake in DAO voting to fund projects. Fewer people vote in DAO proposals since new funding proposals are submitted on a regular bases and are more difficult therefore for the whole community to keep track of when compared to voting for Witnesses which evolves much more slowly over time. The result is that whale votes in DAO voting is more extreme than in Witness voting and DAOs can often seem more centralised than the Witness voting distribution. This is because the influence of one whale in the consensus Witness when voting along side a vast majority of the community seems less significant when compared to that same vote when compared to the fewer number of participants that vote in DAO funding proposals.

This may lead to accusations of DAOs being centralised as it is often the case that one whale can sway a community decision on whether or not something is voted above the voting threshold for funding.

There are two key things to remember here:

1) That the Witness voting remains decentralised when the voting tokens are well enough distributed that one whale cannot vote to manipulate and decide the top Witness pool such that your fundamental rights to transact and grow community on chain is no longer preserved. If one whale can vote in a super majority of the witnesses then the Witness voting mechanism is centralised and highly corruptible.

2) Should a situation arise whereby the voting threshold for funding is voted so high by the community that only whale can decide which proposals get funded and which don't, while this is not an ideal situation, it does not mean that the base chain is centralised.

Ideally there should not be a situation when only one member of the community can have a vote strong enough to elect proposals past the voting threshold for funding. Proposals should be able to be elected into funding without the vote of the largest voter on chain.

Times where situation 2) may benefit the chain is when:

a) the largest voter feels that a proposal is not legitimate and is an attack on the chain and that community members have been mislead into believing a proposal is genuine, when in fact it is an attempt to drain the DAOs funds and,

b) when a collective of users feel that the chain is spending from its DAO beyond its means to sustain such spending and so drastic measures are needed to increase the voting for funding threshold high enough that only the largest voter can put proposals into a position where they exceed the voting threshold for funding. The result is that spending from the DAO is vastly reduced.

Scenarios a) and b) are however highly controversial situations and should only be temporary if at all, until such a time as the attacking proposal is removed, or until spending is bought into control.

Should this situation continue past either of these points, then the community should find diplomatic ways to ensure that the largest voter on chain de-escalates and allows money to flow based on decentralised community decisions again.

Neither of these scenarios however mean that the blockchain itself is centralised. Only that there are extreme or edge case scenarios whereby one of the funding distribution mechanisms (the DAO) can potentially be decided by one user for a temporary period when it is justified. The community itself can however collectively influence the whale in question to de-escalate prematurely if there is enough social consensus against the action taken.

Chapter 23. A New Model for Startup Funding

A practical way to fund projects without compromising to early Venture Capital or other centralising forces

Introduction

Many blockchain projects raise funds through token sales (ICOs, pre-mines) or venture capital, leading to centralization and misaligned incentives between founders, investors, and the community. It should be noted that the following is just a suggested way to create more decentralized projects with fewer conflicts of interest and centralizing stakes, and there may be many other approaches.

A more decentralized alternative is to obtain funding from an existing demonstrably decentralized DAO community, airdrop "miner or governance tokens" to its community, and allow participants to earn governance tokens by running infrastructure or otherwise contributing. This approach avoids early, compromising venture capital, ensures a fair launch, and promotes true decentralization by reducing conflicts of interest and centralized control compared to traditional funding models that use pre-seeds, early investor stakes, pre-mines and ICO's.

23.1 DAO, Miner Tokens, and Fixed-Governance Supply

DAO Funding:

A community DAO (decentralised, with no single owner) can vote to fund your project over a set period. If you prove the project benefits that DAOs ecosystem, you receive an ongoing allocation. No venture capital or private deals are required.

Miner Tokens Instead of Pre-Mines:

Instead of distributing governance tokens directly, you drop a miner token to the DAOs community. Anyone claiming and staking these miner tokens can run infrastructure (storage nodes, validation nodes, etc.) to earn the system's governance token over time.

Controlled Supply and Inflation:

- **Build Phase:** Governance-token minting schedule is set to a minimum feasible amount in order to discourage massive speculative gains and over-rewarding of "early adopters".
- **Maturity Phase:** Once the system matures, the community members which have earned governance tokens by operating infrastructure (often at a loss during the build phase) can vote to raise the token minting schedule to normal levels, allowing wider participation and adoption during the maturity phase.
- **Sustainability Phase:** After several years and once the project is well established, having reached network effect, the new token minting may taper to a much lower, long-term, long tail sustainable rate.

Self-Funding Through the DAO:

The startup team relies on DAO proposals for funding while completing the initial build. Once the core is stable, the newly launched project can develop its own internal DAO over time, funded by a portion of its daily minted governance-tokens. The community, not a founder, then decides how ongoing maintenance or development is financed.

23.2 Liquidity and Value Through Miner Tokens

- **Autonomous Purchase:** Anyone wanting to run infrastructure (and thus earn governance tokens) must acquire miner tokens. This can be done by claiming an airdrop, receiving them from the DAO community, or buying from individuals who already have them.
- **Staking and Infrastructure:** Once staked, miner tokens grant mining efficiency. i.e. all other things equal, an infrastructure operator mining with the same equipment but staking more miner tokens than others, would earn a higher share of governance token rewards than their peers. This aligns incentives with participants who truly support the network with real infrastructure and have paid into the network by buying miner tokens.
- **Service Infrastructure Pools (SIP's):** A related model can create an autonomous liquidity pool for these miner tokens. When new infrastructure operators buy miner tokens, the funds remain in the pool, benefiting the community by creating self-sustaining liquidity for the ecosystem in exchange for the miner tokens it issues.

23.3 Starting a Decentralised Project

1. **Find a Neutral DAO:**

   Ideally, this DAO is widely distributed with no single controlling whale. Propose your project, outlining how it benefits that community. If funded, the community avoids pre-mines and having to do corporate deals.

2. **Drop Miner Tokens:**

   - **Purpose:** Dropping the main governance token to everyone can lead to poor incentives. Miner tokens let only those who truly want to participate (by running infrastructure or delegating) acquire the real governance token.
   - **Low Early New Token Minting:** Keep governance-token inflation minimal in the initial build phase. Early participants gain influence, but not an outsized supply.
   - **Ramp Up Later:** Once the technology is proven, the community can vote to increase token minting, letting new contributors earn tokens and preventing early insiders from dominating.

3. **No Founder Pre-Mines:**

   Since the DAO funds your work, you do not need to give yourself or your team a large initial stake. All token allocations occur through mining, staking, or DAO proposals. This eliminates the usual "team or founder tokens" problem and fosters broader trust.

4. **Distribute and Validate:**

   - Encourage many accounts to claim miner tokens.
   - Let them stake miner tokens or run infrastructure nodes to acquire governance tokens.
   - Monitor distribution: if a single account accumulates too much, initiate community-driven remedies early on in development to maintain a wide token distribution and decentralisation of the network.

23.4 Key Advantages

- **Fair, Low-Value Start:** By keeping token issuance under the radar at first, you avoid hype-driven pump-and-dumps. Tokens slowly gain value organically as the network utility grows instead of purely via speculative investments.
- **Aligned Incentives:** Those who run infrastructure or actively contribute earn governance power. There is no venture capital or early founder dump. Everyone starts from zero.
- **Voluntary Team Building:** Without a massive pre-mine for a small group, talented community members step up voluntarily. People who see long-term potential contribute, rather than working as employees of a central entity.
- **DAO-Based Accountability:** The community can stop funding if milestones are missed. It can monitor distribution, reject bad actors, and ensure the project remains neutral and widely owned.
- **Post-Launch DAO:** Eventually, the new network forms its own internal DAO. The startup team can propose further work be funded by this new DAY, but only receives funding if governance stakeholders of the new system approve. This sustains development without centralising ownership.

23.5 Example: SPK Network on the Hive Blockchain

- **Hive DAO Funding:** The Hive community voted to fund SPK Network, which aims to provide decentralised off-chain storage (video, large files).
- **Miner-Token Drop:** Hive users could claim SPK miner tokens. Those who believed in the project participated and ran infrastructure, while uninterested users simply ignored the claim drop.
- **Build Phase:** Newly minted Governance token amounts remained low at first while the project was built out, preventing an unfair early grab by early adopters. Community trust and decentralised ownership grew gradually.
- **Long-Term Vision:** Once stable and utility is demonstrated, SPK Network can create its own DAO. Ongoing funding decisions will again be subject to decentralised votes, not founder mandates.

This approach kept SPK from needing an ICO or a venture round. No founder gained a massive token allocation. In turn, the community remains motivated, the distribution is healthier, and the final platform is more censorship-resistant.

23.6 Best Practices and Takeaways

- **Avoid ICO's and Pre-Mines:** Receiving or directing tokens on day one will centralise the chain, making it susceptible to regulation, securities laws and corruption, as well as misaligning the incentives of the founders and the community
- **Find a neutral, decentralised DAO** Dropping value to such communities means that one central stakeholder or entity will not control the governance of the system you are building
- **Drop miner tokens to the DAO community:** Having to stake these tokens and provide a service in order to mine governance tokens, means only those who are interested in the

project and also provide genuine value to it will have influence over the governance of the new ecosystem being developed

- **Monitor for genuine decentralisation:** Once the miner tokens are dropped and governance tokens are being distributed, the system can be monitored for strong distribution of tokens, nodes and governance stakeholders. If this tends to centralisation, the community can take mitigating actions.
- **limiting influence of early adopters:** starting with a very small governance token inflation initially during the build phase, ramping up inflation once the system goes live and normal operation takes hold and finally moving to a limited long tail minting schedule after several years of operation allows the system to adequately reward its value creators while keeping fees low or at zero into the long term.

Chapter 24. Future Implications

How power is decentralised via tokenised, self-sovereign Network States in the future

Introduction

The future implications of systems being built that broadly follow the guidelines outlined in this book are detailed below. Decentralised communities and Network States that can be created by following the guidelines in this book secure Digital Rights for all and have profound implications for the future of humanity and its ability to secure its freedom in the digital and then, with the adoption and implementation of Network States, the real world.

24.1 Social Media Account Not Owned by Silicon Valley Companies, Digital Self-Sovereignty and Guaranteed Free Speech

Accounts on the immutable base layer cannot be deleted or suspended. As long as the network runs, these accounts and their followers remain intact. This gives individuals true ownership over their identities and speech, reducing the risk of being de-platformed. People can express themselves more freely, knowing their accounts will not disappear due to centralised decisions.

When the social accounts of community members exist on the base layer of such Web3 technology as outlined in this book, Web2 social media companies like Facebook, Instagram, Twitter, Google and others no longer control the keys to your account. They exist outside of the Web2 social platform's control. Social platforms become Layer 2 system that allow the Layer 1 accounts to log into them. In this way, the social media platforms cannot confiscate, manipulate or delete your social account any longer. Your social account exists on a neutral Layer 1 which has its own economy and self funding mechanisms, which is controlled by the community, not private companies. The same is true for your followers lists and the communities that you build; they all exist on Layer 1 and therefore cannot be deleted by any individual entity or Web2 tech company.

Content is served from the Layer 1 because the social platforms all tap into the same content database on Layer 1. This combined with the sovereignty of your social account now means that free speech and the right to express ideas within a community is already guaranteed for all people online who posses such Web3, DPoS social accounts, without the influence of a company or intermediary.

This also means that wherever you login with your Web3 Social account, you take your followers lists, account history, reputation, community, merits and achievements with you to each Web3 enabled platform you use.

24.2 No Longer Possible to Manipulate History

In addition to protecting speech, such networks preserve all interactions and historical events on-chain. Attempts to erase or rewrite the record are virtually impossible once multiple nodes independently store the information.

A key outcome of these decentralised systems is that history stored on-chain cannot be changed or erased. Once data is published, the record stays intact as long as the network operates. This makes it difficult for any authority to revise past events and ensures a permanent record of social, economic, and governance actions and data. Once existing Wikis and Encyclopedias begin using such technology to document present affairs, History will be preserved, protected by the community's super majority, elected consensus.

24.3 Impossible to Shut Down

By design, these networks are highly resilient. When governance and infrastructure are distributed among many participants with no central authority, there is no single point of failure. Even if an outside party tries to take over or attack the network, the original community can fork away and move to a new chain, leaving the attacker alone on the old chain. Ironically, attempted takeovers often enrich the original community, as hostile actors must buy large amounts of tokens on the open market.

24.4 Money Attacks Can Strengthen Communities

If a hostile entity purchases a significant share of tokens to dominate the network, they raise the token price in the process. Original holders can sell at higher values or fork to create a new chain, leaving the attacker with worthless tokens on the old fork. In this way, an economic attack can backfire, making the community wealthier, more united and more motivated, while the attacker ends up holding depreciated assets.

24.5 Community Holding Abusive Oligarchs to Account

These protocols also allow communities, a new, novel and tested way to deal with abusive large holders who fail to reinvest in the community or who harm the network. If a single individual accumulates an excessive share and exploits users, the community can collectively decide to fork, granting the abusive oligarch zero balance on the new chain. This mechanism avoids traditional violent revolutions by enabling digital secession from exploitative stakeholders.

24.6 Network State Communities and Governments

Over time, many believe governments will begin recognizing these decentralised, online "Network States." Some may cooperate, some will oppose and others may launch competing versions. Either way, communities that run their own economies, distribute governance rights, and store data on censorship-resistant chains could become akin to self-sovereign states, operating largely on voluntary participation rather than imposed authority.

24.7 Rebalancing of Power

Currently, a handful of national governments hold tremendous monetary power through fiat issuance. Soon, hundreds or even thousands of decentralised digital communities may issue their own currencies, manage their own governance, and command real economic influence. This diffusion of power could reshape global politics and economics.

24.8 Fee-less DeFi

In most existing DeFi (Decentralised Finance) systems, each transaction incurs gas or network fees. On high-traffic chains, these fees can be prohibitively expensive. By contrast, fee-less models allow users to stake tokens based on them possessing resource credits instead of paying a gas token for every transaction. This creates more inclusive finance where people can trade, lend, or provide liquidity without constant fees. Systems such as Honeycomb and VSC (Built on Layer 2 systems on The Hive Blockchain, for further information and definitions of these two systems see Annex I –

Glossary of Terms and Acronyms) are already developing fee-less DeFi and Smart Contract capabilities.

See the following links for further information on these systems:

- Honeycomb Layer 2 Smart Contracts: https://www.hivehoneycomb.com/
- VSC Layer 2 Smart Contracts: https://vsc.eco/

24.9 Competition with Traditional Models

Fee-based chains may struggle to serve a global user base for everyday transactions. As fee-less alternatives mature, they could challenge established DeFi ecosystems by significantly reducing barriers to entry and increasing user adoption.

Conclusion

Emerging blockchain architectures where communities store data, govern themselves, and issue tokens signal major shifts in how people will organize in future. They enable:

- **Immutable Records:** History and accounts cannot be altered or de-platformed.
- **Social Account Self-Sovereignty** Accounts are owned outside of Silicon Valley Web2 company control.
- **Free Speech** Text communication is stored publicly on a neutral consensus based Layer 1 which is almost impossible to shut down or modify without a community super majority fork for anomalous situations.
- **Autonomous Communities:** Groups can run their own decentralised infrastructure and economies without being shut down or regulated by centralised entities.
- **Resistance to Takeovers:** Hostile actors enrich original participants but rarely succeed in capturing the network.
- **Evolving Global Order:** Network States may coexist with or challenge traditional governments and financial systems. In some cases they will demonstrate how they can improve existing governmental system and provide them with renewed legitimacy.
- **Fee-less Finance:** Decentralised finance without high transaction costs can boost accessibility and everyday utility.

In short, these technologies are poised to disrupt power structures, incentivize more equitable governance models, and grant greater self-sovereignty to digitally native communities. The economic, political, and social implications are vast and still unfolding.

Chapter 25. Examples of Self-Funded Communities and Initiatives

Already, so much is being done in the physical world

25.1 Increased Security

Beyond the examples below there are countless others and such independently funded initiatives will only continue to grow. An important note is that where this technology continues to assist people with basic services and infrastructure where their governments failed to due to corruption or incompetence, any attempt to shut down or oppose such it will likely be met with resistance from local people who benefit from the benefits it provides. The result is that neutral blockchains that carry out such work, not only help local communities, but they increase the distribution of their own tokens by benevolent means, which indirectly strengthens the protocol and its security against hostile shut downs by governments.

It is difficult to attack or shut down a system that is legitimately helping people who were not previously served by their existing systems.

25.2 Ghana Borehole Projects

In Ghana, local groups have successfully utilized decentralised autonomous organizations (DAOs) to fund the construction of boreholes, providing clean water to communities lacking direct access. By submitting proposals and documenting their progress on-chain, they have secured community support and funding.

As of the date of publishing, the Ghana water borehole project has installed 21 water wells for villages that previously did not have access to fresh water.

See link for latest progress and evidence for all 21 boreholes installed: https://hive.blog/hive-176874/@mcsamm/progress-update-on-the-21st-hive-borehole-project

Key Points

- **Transparent DIRECT Funding:** Budgets and construction processes are documented on-chain, ensuring transparency without a facilitating charity accepting donations and taking a cut of the funds to cover its own operational costs. Funds are sent directly from the blockchain to local, trusted people who have built reputation on chain over time
- **Community Trust:** Successful projects build trust, enabling further funding for subsequent initiatives.
- **Real-World Impact:** Access to clean water improves health and daily life for thousands.

This approach bypasses traditional charitable institutions, which often have high administrative costs, by using on-chain reputation and proof-of-work content to ensure donations reach intended projects.

25.3 Ghana Health Checks

Building on the success of the Ghana borehole initiative, the same groups in Ghana have organized dental and health check-ups for remote villagers who do not have access to such services. Securing DAO funding and maintaining transparency through on-chain documentation, they provide free healthcare services to underserved communities.

See link for further details of this initiative: https://hive.blog/hive-176874/@hive.ghana/idhhbowu

Key Points

- **Healthcare Accessibility:** Offering free dental and health services to communities in need.
- **Reputation Growth:** Consistent project delivery fosters community support and enables larger-scale funding.

25.4 Venezuela: Street Acrobatics and Infrastructure

In Venezuela, groups have obtained funding for equipment, shows, and community-building efforts. They promote their activities through various channels, bringing attention to decentralised funding models.

Key Points

- **Grass-roots Development:** Small teams receive on-chain funding to purchase merchandise and organize events.
- **Local Empowerment:** Initiatives benefit individuals with limited economic opportunities.

25.5 Cuba and Mexico: Paying Utility Bills with Content Rewards

In parts of Cuba and Mexico, individuals create on-chain content to earn rewards, which they can convert into local currency or use to pay utility bills. This system is particularly impactful in regions with limited banking services or where remittances incur high fees and restrictions.

Key Points

- **Daily Necessities:** Users generate content, such as blog posts or community updates, to earn tokens.
- **Real Bills Paid:** Services exist to convert these tokens directly into utility payments, reducing reliance on traditional banks.

By circumventing conventional financial gatekeepers, these users demonstrate how decentralised currencies can provide tangible benefits in areas with restrictive or expensive financial systems.

25.6 Why It Matters

- **Improved Security** Providing grass roots, locally operated services and infrastructure where government was not able to increases token distribution, social image, local support and therefore security of the network.
- **Neutral, Decentralised Funding:** No single corporation controls the treasury; funds are allocated through community-approved proposals based on reputation and transparent reporting.
- **Direct Accountability:** All spending is documented through immutable on-chain posts, allowing donors or voters to see exactly how funds are utilized, reducing corruption and mismanagement.
- **Real-World Impact:** From building water wells to supplying medication and paying essential bills, on-chain funding models deliver concrete results in underserved regions.

- **Incentivized Community Participation:** Individuals who provide high-quality work and transparent reporting enhance their on chain reputation, attracting more votes and social trust for future initiatives.
- **Scalable Model:** These projects can inspire similar initiatives worldwide, with each region adapting decentralised tools to address local challenges.

Conclusion

These examples illustrate how self-funded, reputation-based blockchain communities can achieve what traditional charities and governments often struggle with: direct, efficient delivery of aid, physical infrastructure and services. Whether providing clean water in Ghana, supporting community initiatives in Venezuela, or assisting families in Cuba and Mexico with utility payments, on-chain funding brings transparency and accountability.

By eliminating intermediaries and enabling communities to vote directly on proposals, these projects build lasting trust and deliver genuine impact. In a world where many lack basic infrastructure or face restrictive financial systems, decentralised initiatives offer a promising glimpse into the potential of blockchain governance and funding in the future.

Annex I – Glossary of Terms and Acronyms

Definitions are from Leo Glossary:
https://ecency.com/post/@leoglossary/leoglossary-main-menu)

AMM - An automated market maker (AMM) is a type of decentralised exchange that allows users to trade digital assets automatically using liquidity pools instead of relying on traditional buyers and sellers

Block Producer - Block producers are incentivized to run software that generates blocks and maintains the network. On many chains, this entails ensuring the ledger is free from any errors, including double spend problems.

BLS Signatures - A BLS digital signature, also known as Boneh–Lynn–Shacham (BLS), is a cryptographic signature scheme which allows a user to verify that a signer is authentic where Multiple signatures generated under multiple public keys for multiple messages can be aggregated into a single signature, making the size of the signature far smaller than standard cryptographic signatures.

CEX - A centralised exchange (CEX) is an exchange that allows for the trading (or swapping) of assets yet is not decentralised. Most exchanges fit this criteria including those that handle stocks, commodities, or bonds. These, however, are rarely terms as CEX.

CFTC - The Commodity Futures Trading Commission (CFTC) is a U.S. government agency responsible for regulating the futures and options markets. The CFTC's mission is to protect market participants, promote open access to the markets, and foster economic efficiency, competitiveness, and stability.

DAO - A decentralised autonomous organization (DAO) is a business structure that is based upon the concept of decentralisation. This is in alignment with how many view the digital world. Essentially, a DAO is a digitally-native business that is built on the Internet. It is truly decentralised without traditional management structure. There is also an autonomous governance system in place

DeFi - Utilizing distributed ledger technology (DLT), DeFi eliminates the need for intermediaries such as banks, exchanges, or brokerage firms. All financial activity can occur utilizing applications built to facilitate what is needed. This is possible due to the use of smart contracts. Delegation

DEX - Decentralised Exchange (DEX) is a structure that is most commonly used with cryptocurrency. This contrast with centralised exchanges (CEX) which are centralised and are associated with a company.

DHF - An on-chain decentralised autonomous organization (DAO) that allows community members to submit proposals for projects that benefit the ecosystem. It is through this process that funding is allocated to proposals with members using stake weighted voting to select the projects that should be funded.

DPoS (PCV) - An alternative to the Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus mechanisms for blockchains. With PoS, there is no mining. Instead blocks are produced based upon the number of coins that are staked. Those who stake more coins will increase their chances of being chosen to validate new blocks.

DPoS takes this a step further since many who are staking the coins are not interested in being block producers. Under this mechanism, the responsibility is outsourced (delegated) to those who handle it.

HBD - The **Hive Backed Dollar (HBD)** is a stablecoin that is resident on the Hive blockchain. It is categorized as an algorithmic stablecoin) in that it does not keep a reserve like many other tokens in this category. Instead, each HBD is can be converted into $1 worth of HIVE

HODL - Hold On for Dear Life. This is a play on the idea of HOLD. It is a strategy for holding one's coins through volatile markets no matter what. Cryptocurrency can see some major pull-backs, hence the dear life part. When the crypto bear comes out, it can feel like one's world is coming to an end.

Honeycomb - Layer 2 software that builds a network of peers that use the Hive Blockchain to post and interpret transactions. This allows these peers to come to a consensus and elect peers to run tasks. Distributed computing, in this way allows for decentralised operation of a vast amount of potential applications, DeFi, and oracle services.

HP - Hive Power is the term given to a Hive coin state that is staked on the Hive blockchain. It is done through a process called powering up which switches liquid $HIVE into Hive Power, or HP. This is what gives people access to utilize the blockchain through Resource Credits. Thus, we can consider Hive Power to be an access token for the network and to write to the database.

ICO - This is a spin on Initial Public Offering (IPO) in the equity markets. An ICO is the selling of a token in exchange for fiat currency, Bitcoin, or other altcoins in the early phase of a project in order to fund development. However, this often results in people investing in scams without realising. It also creates a centralising force in the project as many regulatable Venture Capital firms or entities become holders at artificially low prices compared to what normal users have access to later on in the project

IPFS - The Inter-Planetary File System (IPFS) is a protocol, hypermedia and file sharing peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace connecting IPFS hosts.

KYC - The Know Your Customer (KYC) rules are requirements placed upon financial institutions by governments to combat money laundering and terrorism. Basically it necessitates the institutions to know their customers by obtaining such identification where the government can determine all of an individual's activities.

Within the cryptocurrency realm, this often applies to centralised exchanges. The design is to remove anonymity from the system in case of wrongdoing according to the different governments.

Layer 1 – Or the Base Layer is the basis for immutability. Here is where decentralization takes place due to the node system. It also includes block time, the consensus mechanism deployed, programming languages, and rules pertaining to the network's core operations.

Layer 2 - The second layer (or Layer 2) refers to the secondary layer or protocol that is build on top of a blockchain. These are designed to enhance the scaling of the ecosystem far above what can occur at the base layer. Blockchains tend to be limited in the number of transactions they can process. There are also memory concerns since individuals nodes have limitations

Network State - The Network-State is in contrast to the nation-state. Here we have a governance system that is based upon where one is geographically born. That is how citizenship is established. The rules of the land are based upon where one is physically. In comparison, the network-state is dependent within which digital ecosystem one is located. This is paralleling the idea of nations and networks.

NFT - Non Fungible Tokens are unique since they cannot be replaced with something else. Each NFT is tied to a different set of data. This contrasts with Bitcoin where each coin is essentially the same

NOSTR is an open protocol for decentralised message transmission, with the intention to be able to resist internet censorship while maintaining session integrity. "NOSTR" can also be translated as "our" or "ours" from Latin

Pre-Mine - A pre-mine is the act of mining or creating coins or tokens before the cryptocurrency is released to the public. This is an activity that was very common for both blockchains and secondary projects.

The pre-mine is usually a way the founders pay themselves. During the initial coin offering days, many were giving themselves healthy chunks, an amount they typically dumped on the market. This led to price collapses, leaving the investors with near worthless assets. Many scams and centralised projects pretending to be decentralised operate by using pre-mines.

PoB (ISHD) - Incentivized Stakeholder Distribution, or Proof of Brain (PoB) is a token distribution method whereby a daily rewards pool of tokens is minted and is distributed to users in a blockchain ecosystem for creating valuable content and receiving votes from other token stakeholders. Rewards from the pool are distributed to both stakeholders for voting and users for creating content. The more stake that votes for the content, the more of the daily reward pool the content and the voters receive relative to other content in the ecosystem.

PoS (UPCV) - A blockchain consensus mechanism which requires the staking (locking up) of coins to earn a chance of adding new blocks. The chances of becoming a validator increase the more coins one stakes.
The method should also be referred to as Un-Parametered Coin Voting (UPCV) since consensus is set by stakeholders voting with their coins and the biggest stake holder has the biggest influence on the governance of the chain, hence there are no parameters to prevent a “rich get richer” scenario or to incorporate any social nuance of the community into the governance system.

PoW (IV) - Proof-of-Work (PoW) is a blockchain consensus mechanism that is used to validate blocks of information that are attached to each other. This data structure creates ledgers of transactions utilizing distributed ledger technology.

This system should also be referred to as Infrastructure Voting, since the community recognises the longest chain when forks split the consensus. The longest chain is normally formed only by the chain which has been able to deploy the most infrastructure and thereby the most computing power to secure the consensus. Eventually infrastructure operation becomes expensive and resource intensive, making it economically viable only to those who have the money to invest in large amounts of expensive equipment.

Power Down - The opposite of Power Up – As a security mechanism, this should take several weeks in order to dis-incentivise centralised exchanges holding custodial stake from powering up to attempt to control the consensus of a decentralised community, by voting against the interests of community members, using their own custodial stakes which are stored on the exchange against them.

Power Up - This is when one converts a governance token (such as $HIVE) to the staked for governance version of the token (such as Hive Power). Powering up increases one's voting power for both governance issues along with distribution of the daily reward pool. The amount of Resource Credits one has available increases as Powered Up tokens increases.

SEC - An independent federal regulatory agency that is tasked with the oversight of the securities markets. One of the main goals is to protect investors from predatory and criminal activity.

Smart Contract - A smart contract is a self executing agreement between two parties. Both the action of buyer and sellers are determined by the code that is in the contract. There are no external

entities that are involved in the transactions. Smart contracts are tied to blockchains. This are a vital part of Decentralised Finance since there is no need for any third party involvement

SPK - The governance token of the SPK Network; An off-chain, decentralised, incentivised Peer to Peer: Storage, Encoding and Content Delivery Network

Staking - This is generally the process of holding coins or tokens in a wallet to support a particular blockchain or application. People typically do this to support network operations in return, typically, for some type of reward. Depending upon the system, there might be time commitment as well as a certain period to un-stake.

Staking is viewed as a greater level of commitment than simply holding the cryptocurrency in liquid form.

Sybil Attack - A Sybil attack is a type of cybersecurity threat where a single entity creates multiple fake identities to gain control over a network, often undermining its integrity and security. This can lead to issues like manipulating votes or transactions within decentralized systems, such as blockchain networks

VSC - Virtual Smart Chain: a Layer 2 smart contract system for cross chain interoperability powered by ZK-proofs and economically secured wrapping protocols

Witnesses - are elected into their position on DPoS chains by stake weighted voting from community votes. They, like Block Producers are incentivized to run software that generates blocks and maintains the network. On many chains, this entails ensuring the ledger is free from any errors, including double spend problems. On DPoS chains they also run the social consensus software such as voting, rewards and distribution mechanisms, set interest rates and act as manual oracles for price feeds.

ZK Proof - ZK-proofs work, essentially by allowing someone to prove that they have access to information without actually showing that information to the party asking for proof - they are great for scaling as they can finalise proofs on the Layer 1 chain without having to compute heavy transaction data on it. They are also provide transaction privacy

What if your community could run its own economy, speak freely online without fear of censorship, and build systems that no government or corporation could shut down? The Digital Community Manifesto is a guide to doing exactly that.

This book isn't about hype coins or crypto trading. It's about how people can come together to build digital spaces that are fair, transparent, and truly owned by the community itself. The authors draw from their own battle hardened experience, having been involved in one of the only successful social community blockchain forks, a rare project that actually stayed decentralized after fighting off a corporate takeover. They break down and systematically lay out how to build systems that resist control and empower people.

You'll learn what decentralization really means beyond the buzzword. You'll see why most blockchains today aren't actually free or neutral, and how they've been designed to serve early investors or founders instead of users. The book unpacks how to avoid those traps and offers practical tools for creating new, censorship resistant communities from the ground up.

It covers:

How to launch a community without needing VCs, pre-mines, or companies

How to design zero-fee, scalable systems that anyone can access

How to build real economic value through community participation, not investor speculation

How to fund infrastructure and public goods with DAOs instead of relying on outside VC money

Why game theory, reputation, and social trust are critical for long-term survival

What it takes to evolve from a group chat into a self-governing digital Network State

Whether you're building a platform, leading a community, or just want to understand how digital freedom is actually created and protected, this book lays it all out. It's technical, but not cold. It's opinionated, but grounded in real-world examples. And more than anything, it's a challenge: to stop waiting for better systems and start building them.

If you've ever felt that the internet should belong to its users, not to Big Tech or centralized gatekeepers, this is your blueprint

Value 4 Value Donation

If you feel this work have given you value, please return some via donation of proportional value to the following:

Donate **Lightning** to:
networkstate@sats.v4v.app

Donate **HBD** to:
@networkstate
(Scan with Hive Keychain Scanner)