Tonomy Gov OS Technical Whitepaper

Governance Operating System for Ecosystems of Trust

v1.2

By the Tonomy Foundation

Executive Summary

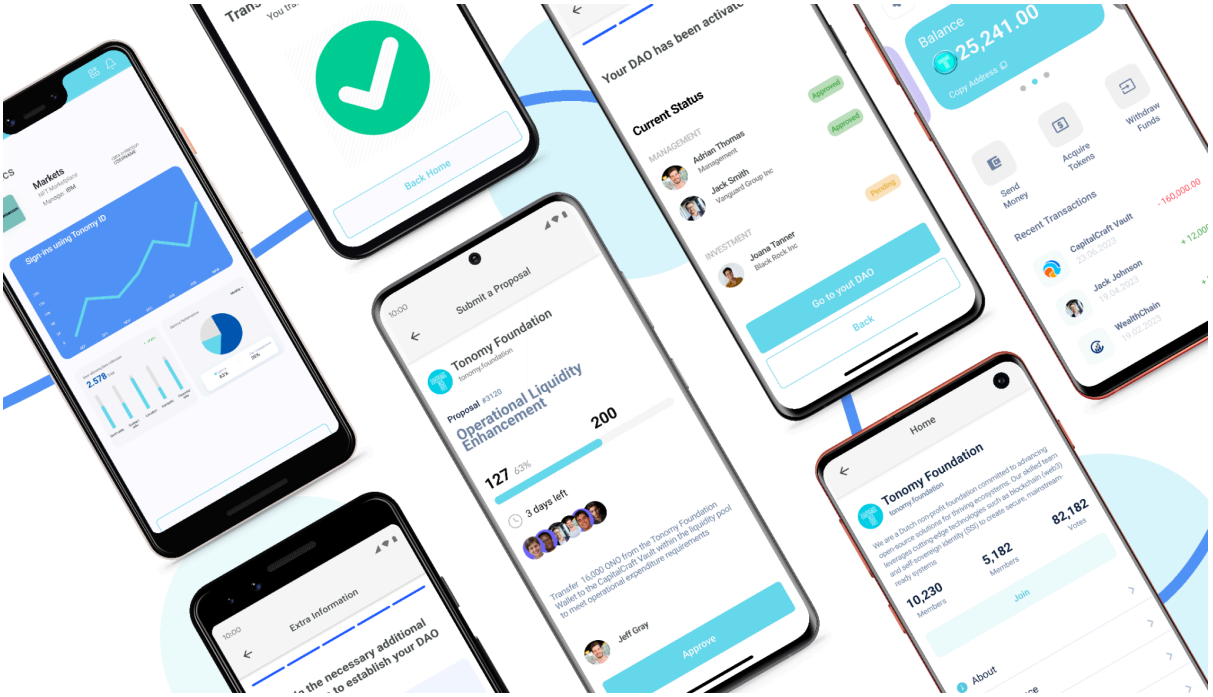
Tonomy Gov OS is a groundbreaking governance operating system, meticulously crafted to establish trust in various ecosystems, including governmental, enterprise, and public commons governance. This innovative platform adeptly handles the governance of complex multi-party ecosystems such as social welfare, healthcare, large enterprises, infrastructure, state nations, land territories, AI systems, cryptocurrencies, and global environmental commons management. Key features include:

- **Modular, Configurable Governance:** The network features a highly customisable system for governance, identity, and economics. Its modular design allows for tailored solutions to meet diverse requirements, ensuring adaptable and effective governance in various environments.
- **High-Performance Consensus Algorithm:** Tonomy utilises a scalable aBFT consensus algorithm with a 0.5s latency, capable of handling 10,000 transactions per second. This high performance is crucial for supporting large-scale, efficient, and secure transactions within the network. This can be further increased to support an infinite number of transactions per second with the implementation of sharding in the future.
- **Artificial Intelligence Enhancement:** AI is ethically integrated into the network to streamline governance, developer and administrative tasks. This reduces operational friction and improves usability, making governance more efficient and user-friendly.
- **Zero Knowledge, Privacy and Compliance-Centric:** The network's identity management system prioritises privacy and compliance, employing a zero-knowledge architecture and advanced cryptography. This architecture eliminates the need for databases to store personal information, thereby enhancing cybersecurity and ensuring compliance with privacy regulations. It also embodies the first true implementation of fully self-sovereign Identity adhering to and exceeding industry standards.
- **No-Code Platform:** The network's no-code features significantly enhance its scalability and mainstream usability. These no-code applications empower developers to launch blockchain-ready apps in minutes rather than weeks, making the platform accessible to a broad audience and streamlining the development process. For the first time, dApp developers are also able to manage users & their privileges, enabling a regulation-ready infrastructure & the elimination of bad actors.

In essence, Tonomy represents a significant advancement in digital governance. Integrating state-of-the-art technologies offers a robust, scalable, and user-friendly governance operating system, ready to transform how digital ecosystems operate and interact on a global scale. While offering all of the benefits of traditional blockchain networks, a Tonomy network introduces a set of advancements that enable the mainstream adoption of distributed ledger technology while exceeding the capabilities of predecessor networks.

The Tonomy Foundation will use this the Tonomy Gov OS software suite to launch Tonomy, the first global decentralised governance network. This network aims to provide a trusted global governance system to power Internet users with better autonomy and privacy while providing Internet application providers with better facilities for user security, team management and cooperation. Tonomy will introduce the global currency TONO, which is a

payment system between individuals and DAOs. The strategy, governance and economic system for this network are outlined in the [Tonomy Virtual Nation Whitepaper](#).



Contents

Impact Statement

Before the initiation of this project, the Tonomy Foundation deemed it imperative to establish both internally and externally the feasibility and sufficiency of its expertise in developing the technologies delineated in this White Paper. This objective has constituted a principal focus of the Foundation over the past eighteen months.

One of the most important and intricate components of Tonomy is its identity system. The Foundation has successfully developed Tonomy ID, a comprehensive and production operational system. This system encompasses a fully non-custodial wallet capable of signing data, including smart contract transactions and W3C Verifiable Credentials and DIDComm messages. It facilitates the storage and sharing of private data. Remarkably, Tonomy ID maintains stringent security measures while offering an experience akin to mainstream Web2 interfaces. This product, having recently been introduced to the market, is garnering favourable responses from our clientele. Try using Tonomy ID here.

In this venture, the Tonomy Foundation has significantly contributed to the World Wide Web Consortium (W3C) decentralised Identity ecosystem. Through collaboration with the W3C Credentials Community Group and the decentralised Identity Foundation, the Foundation has substantially developed the did-jwt and did-jwt-vc, facilitating multi-party and delegated signatures. These technologies, the most utilised libraries in DID technologies with an upward trend of 40,000 weekly downloads, are poised for widespread adoption within the EU digital identity wallet framework and various national identity programs. These developments utilise the W3C CCG standard, co-authored by Tonomy founder Jack Tanner, which introduces the "Conditional Proofs" which extends the Decentralised Identifier standard enabling multi-party and delegated signatures. Further details can be found at W3C CCG Conditional Proofs standard.

Additionally, the Tonomy Foundation has been instrumental in establishing the Telos Network, serving as one of its launching nodes. This engagement has provided critical insights into the core consensus model, which will be substantially modified to forge a democratic-enabled blockchain. Our research and development in governance have demonstrated the adaptability of the core protocol in supporting diverse governance models, including democratic, proof of share, proof of stake, and direct or representative frameworks. More information can be found at EOSIO Governance Contracts.

The Tonomy Participate project, a proof of concept delivered for the city of The Hague as a participatory budgeting tool, has been another significant achievement. This project secured the second prize at the Odyssee hackathon, followed by engagement from the Hague government.

In conclusion, our team possesses the requisite technical expertise and the operational capability to implement and develop the technologies specified in this White Paper.

Overview

Tonomy is a software suite that can deploy digital governance on any ecosystem. Tonomy does this by including critical out-of-the-box components necessary for digital governance. These enable the management of identity, organisations and institutions including governance systems and software applications. The modular approach can create various and upgradeable models for the governance of ecosystems of trust, such as democratic, proof of stake, representative, direct or hybrid models.

Tonomy heralds a paradigm shift in **digital governance architectures**, meticulously engineered to instil trust across a spectrum of ecosystems, inclusive of governmental, enterprise, industry, and communal governance domains. This pioneering system adeptly orchestrates governance processes within intricate multi-stakeholder ecosystems, addressing sectors ranging from social welfare and healthcare to large-scale corporate entities, infrastructural initiatives, national territories, artificial intelligence frameworks, cryptocurrency mechanisms, and comprehensive global environmental stewardship.

Central to Tonomy is a digital ecosystem, distinct in its ability to foster autonomous user engagement, team collaboration, and the development of revolutionary applications **devoid of reliance on centralised third-party services or data repositories**.

At the core of its operational model, Tonomy encompasses five pivotal actors: individuals with unique identities, decentralised autonomous organisations (DAOs) constituting multiparty entities, a specialised DAO for ecosystem governance, applications providing standard functionalities, and network infrastructure services, including blockchain nodes.

The network employs a diverse array of scalable, low/no trust technologies to construct a decentralised service network, powering a comprehensive application ecosystem. This infrastructure facilitates a suite of standardized, user-centric applications, encapsulating:

- **Tonomy ID:** A self-sovereign identity, data and web3 wallet facilitating single sign-on across Web2 & Web3 applications, whilst also enabling digital eiDAS compliant signatures, sharing of W3C Verifiable Credentials & sovereign data storage.
- **Tonomy DAO:** A platform enabling collaborative formation & democratic administration of new legal entities for joint management of apps, data, funds, policies and much more.
- **Tonomy Gov+:** A platform for sustainable ecosystem governance encompassing policy management, network infrastructure, operations, arbitration, funds management.
- **Tonomy Bankless:** A tool for seamless financial management, micropayments & connection of different Web2 & Web3 payment rails, incorporating advanced features such as subscription models, AML adherence and threshold settings.
- **Tonomy Build:** A no-code platform for managing network infrastructure, including applications, validator nodes, and servers, smart contract creation, user management & much more powered by Artificial Intelligence

Tonomy's architecture is underpinned by a **modular software approach**, offering high configurability to meet diverse requirements of complex ecosystems, whilst avoiding the

need for L2 networks and rollups which constitute a series of usability and security risks. This is achieved through:

- A **flexible identity management** system employing multi-key technologies and Self-Sovereign Identity principles for private, secure, and interoperable identities.
- A **modular governance** system integrating various consensus algorithms and governance models, including traditional direct and representative democracy, alongside innovative stake-based and liquid democracy systems.
- A **versatile economic system** enabling advanced resource allocation configurations, denial of service security methods, and currency token management tools.

Beneath its interface, the network integrates a multitude of system services to deliver a unique user experience in a decentralised and secure manner. This is facilitated by a multilayer system comprising:

- A **scalable blockchain network** acting as the core execution layer for critical ecosystem components such as identity, governance, and economics, utilising an advanced aBFT consensus algorithm capable of handling substantial transaction volumes.
- Support services enabling peer-to-peer communication, identity verification, secure data and identity recovery, all leveraging decentralised Identifiers (DIDs).

Tonomy's **zero-knowledge architecture** for identities and DAOs obviates the need for trust or storage of personal information, addressing significant cybersecurity risks and data compliance challenges inherent in current internet architectures. The system's identity and key management framework and a design-driven approach enhance user accessibility and usability.

Advanced cryptographic techniques, such as **zero-knowledge proofs**, are employed for selective data disclosure and on-chain proofs, fostering provable and private systems and facilitating enterprise adoption by ensuring compliance with data privacy regulations such as GDPR.

Integrating **artificial intelligence** within DAO and ecosystem governance processes provides concise summaries of technical proposals and discussions, aiding in managing new proposals from diverse perspectives in an opt-in ethical way.

User safety within the ecosystem is enhanced through features like DAO and identity anonymised accountability, transparent governance, and an arbitration system that allows for the issuance of warrants under specific conditions for governance and administrative functions.

Tonomy offers developers an engaging experience through the **no-code network infrastructure** developer console, enabling easy onboarding, user retention, and efficient management of applications and network infrastructure.

Cryptocurrency comparison:
Tonomy facilitates the creation of decentralised, public currencies. Unlike Ethereum and

most cryptocurrencies, Tonomy provides out-of-the-box no-code tools for autonomous governance and administration of cryptocurrency operations, such as developer grants, improvement proposals, and policy and standard updates. Its mainstream-ready application suite provides an immediate web2-like experience for using currencies as well as governance and operation without compromising on web3 fundamentals like autonomy and decentralisation.

State-nation comparison:
When applied to state-nation governance, Tonomy enables the digital foundation for sovereign-state institutions, including ministries and sub-departments, to manage legislative, judicial, and executive functions. This approach contrasts with existing state-nation systems by providing a digital platform that allows for the rapid adaptation and expansion of policies and governance structures, responding more effectively to citizens' needs. The advanced cryptography and distributed network systems enable state nations to manage their cyber security needs without worries of citizen fraud, data breaches or foreign digital attacks.

Tonomy and TONOCurrency

This white paper outlines the software suite in which Tonomy creates a modular Governance Operating System for Ecosystems of Trust. These can be adapted and configured for various use cases requiring complex governance and multi-party interactions.

The community including Tonomy Foundation and partners will use this framework to launch the first global decentralised governance network called Tonomy. This network aims to provide a trusted global governance system to power internet users with better autonomy and privacy while providing application providers with better facilities for user security, team management and cooperation. Tonomy will introduce the global currency LEOS, which is used as a payment system between individuals and DAOs. The network has a long-term vision of fostering better global political and environmental governance.

Read the Tonomy - Governance & Strategy document for details of this Tonomy powered network.

Features

For Users

Self-Sovereign Identity Management

Tonomy ID empowers users with full autonomy over their digital identities, enabling seamless interaction with various entities within the network, including people, DAOs, and applications. This system eschews third-party identity providers, offering a democratised approach that caters to all technical skill levels.

Zero Knowledge Privacy-Preserving Autonomous Control

The design paradigm of Tonomy prioritises user privacy. By vesting data control in the hands of users and employing advanced cryptographic techniques such as zero-knowledge proofs, the network guarantees privacy and consent without reliance on third-party custodians.

Decentralised Identity Verification

The network facilitates private and anonymous identity verification processes. Personal verification proofs are stored locally on users' devices, not on central servers, enhancing privacy and trustworthiness across the network. KYC costs for businesses integrating with Tonomy ID are reduced 100-fold as users verify their identity once and can prove their status anywhere, as many times as needed.

Seamless UX with Advanced Web 4.0 Security Features

Tonomy enables users to execute digital eiDAS compliant qualified electronic signatures (QES) and smart contract transactions within the app environment, leveraging multi-factor authentication, multi-party approvals, hardware signature proofs to bolster security. This enables a military and banking-grade infrastructure that adheres to the highest industry standards.

Simplified Financial Transactions and Account Management

Tonomy Bankless offers a user-friendly financial interface akin to modern neo-banking systems. It allows for simplified payments, receipt management, and advanced account management, blending hot and cold wallet features while hiding cryptographic complexities. The network's low transaction fees also make it an ideal rail for micropayments and small-value transactions.

Robust Governance and Identity Access Management (IAM) for DAOs

Tonomy DAO offers flexible and comprehensive governance templates and IAM structures, supporting diverse organisational models. It enables efficient management of permissions and roles, enhancing operational security and efficiency whilst paving the road for entities that aim for high levels of compliance.

Arbitration System for Privacy-Preserving Safety and Conflict Resolution

The network features a comprehensive arbitration system that ensures privacy while providing safety and conflict resolution mechanisms. This system is crucial for maintaining a secure and compliant environment, enabling the resolution of disputes and the protection of user data. Justice should be delivered digitally in the 21st century and an environment of accountability is established through a mix of privacy-preserving identity, arbitration and governance features.

Transparent and Participatory Ecosystem Governance

The network's governance and administration system is open and accessible, fostering democratic participation in policy and rule-making. This transparency ensures

accountability and sustainable evolution of the ecosystem. Tonomy is the first blockchain suite with an inbuilt network governance platform.

AI-Assisted Decision-Making and Policy Formulation

The network leverages artificial intelligence to aid in creating clear and comprehensive governance proposals and policies, enhancing decision-making quality and regulatory compliance. AI is also used to intelligently analyse the network & social sentiment to create improvement proposals for the network.

Streamlined Network Infrastructure Management

Tonomy offers a no-code application development and management platform, facilitating rapid deployment and integration of decentralised applications for anyone, regardless of their technical skill set.

For Infrastructure Operators

High-Performance On-Chain Consensus and Scalability

The network achieves significant throughput (15,000 transactions per second) with low latency (0.5 seconds), utilising advanced consensus algorithms like aBFT and HotStuff, enabling efficient on-chain application performance.

Modular and Adaptive Transaction Fee System

The network employs a flexible and modular approach to transaction fees, allowing for customisable models that cater to diverse needs within the ecosystem. The core network employs fixed-dollar fees, enabling predictable expenses for businesses that deploy applications on Tonomy-powered networks.

On-Chain Consensus Model for Modular Governance

Tonomy implements an on-chain consensus model, facilitating a dynamic and adaptive governance structure of the technical infrastructure. This model allows the network to evolve its governance policies in response to its participants' changing needs and consensus.

Eco-Friendly and Upgradeable Cryptographic Framework

The network's use of optimised server technologies and efficient consensus algorithms minimises its environmental footprint. Its cryptographic infrastructure is designed to be upgradeable, ensuring readiness for future advancements. The Tonomy Foundation also commits to purchasing carbon credits in the future to make the network carbon-negative.

Enhanced Data Privacy and Interoperability

Employing decentralised identifiers (DIDs), the network ensures private and verifiable off-chain data, enhancing interoperability across the internet and other blockchain systems.

Multi-Language Smart Contract Support Including EVM

The network supports the creation of on-chain smart contracts in multiple programming languages and execution in WASM smart contracts or through the Ethereum Virtual Machine

(EVM), offering developers flexibility and choice based on use-case requirements and team expertise.

EVM and DeFi Compatibility

Ensuring compatibility with Ethereum Virtual Machine (EVM) and decentralised finance (DeFi) protocols, Tonomy is poised to integrate with existing DeFi ecosystems. This compatibility facilitates liquidity and interoperability, broadening the network's appeal and utility within the broader blockchain landscape.

Data Privacy Compliance

The network's architecture ensures compliance with global personal data privacy regulations such as GDPR, CCPA, and CCRA to facilitate enterprise and government adoption. This compliance is intrinsic to the system's design, making it a viable and trustworthy option for enterprise and government applications, ensuring cybersecurity and privacy.

For Ecosystem Operators

User-Centric Design for Mainstream Adoption

Tonomy adopts a human-centric approach, prioritising intuitive user experiences and seamless integration of cryptographic technologies, mirroring familiar Web2 standards while leveraging advanced Web3 innovations.

Integrated Suite of Standardized Tools

Contrasting with the fragmented nature of many cryptocurrency ecosystems, Tonomy provides an integrated, user-friendly suite of standardised out-of-the-box tools. This cohesive ecosystem enhances the user experience, reducing complexity and confusion for novice and experienced users.

Self-Regulation and Enhanced User Safety

Tonomy’s self-regulation mechanism, underpinned by its robust identity and governance systems, allows applications and the ecosystem to enforce policies and network rules autonomously. This approach diverges from traditional, unregulated cryptocurrencies, establishing a secure and politically resilient environment.

Modular Governance System for Ecosystem and DAOs

Tonomy introduces a flexible governance framework, enabling customisable governance models for both the ecosystem at large and individual DAOs. This modular system accommodates a range of governance styles, from democratic to share-based, supporting diverse organisational needs and facilitating effective self-governance.

Modular System Architecture with White Label Capabilities

The network's architecture is modular, allowing for tailored configurations in various sectors. Its white-labelling capability makes it adaptable to diverse ecosystems, enhancing trust and adoption rates.

Open Source Development Ecosystem

All software within Tonomy adheres to the Apache 2.0 license, encouraging community collaboration and bolstering security and privacy. This also assists in government adoption to prevent vendor lock-in.

Solution

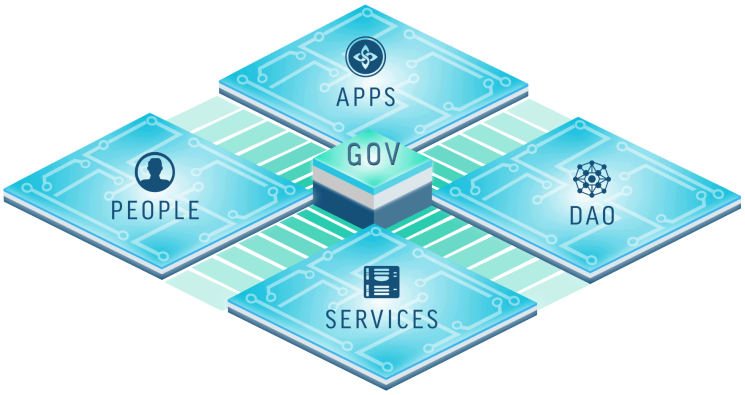


Figure 1: Network Actors

Actors

Tonomy ecosystems comprise diverse actors, each playing a crucial role in the network's functionality and governance. These actors include individuals, decentralised Autonomous Organizations (DAOs), the Governance unit (GOV), applications (Apps), and services. Below is a detailed exposition of each actor within the network.

Individuals

Individuals are the primary users of a Tonomy network. Each person engages with the system through a unique digital identity, which serves as a gateway to access the broader ecosystem. This digital identity is a critical component, ensuring secure and personalised interaction within the network.

Decentralised Autonomous Organizations (DAOs)

DAOs represent collectives of individuals, varying from companies and NGOs to government departments and state governments. These entities collaborate towards shared objectives within agreed governance frameworks. DAOs may be structured as open or closed teams. Furthermore, they are pivotal in managing the network's infrastructure, including blockchain nodes and communication services. Tonomy is the first network that enables democratic voting within DAOs due to its advanced identity capabilities.

Governance (GOV)

The Gov acts as the administrative body for the network's ecosystem. It is a specialised DAO with additional explicit responsibilities for overseeing network rules, security, and operational management. The Gov sets network fees, and incentives and ensures that DAOs managing the network infrastructure adhere to set expectations. The Gov DAO manages a pool of the native currency which may be present in the network (such as an ecosystem fund), and it’s distribution within the governance system or to contributors or other DAOs.

Applications (Apps)

Apps are software programs that facilitate interaction for users, DAOs, and the Gov DAO. The network features five core Apps — Tonomy ID, DAO, GOV, PAY, and Developer Console — which form the foundation for enabling ecosystem features. DAOs also have the

autonomy to develop their Apps, ranging from existing Web2 SaaS applications to fully decentralised applications utilising the network's unique architecture and smart contracts.

Services
Services in Tonomy refer to specific server operations run by DAOs that support the network infrastructure. The operational policies and management of these services are determined by the Gov DAO.

Architecture Overview

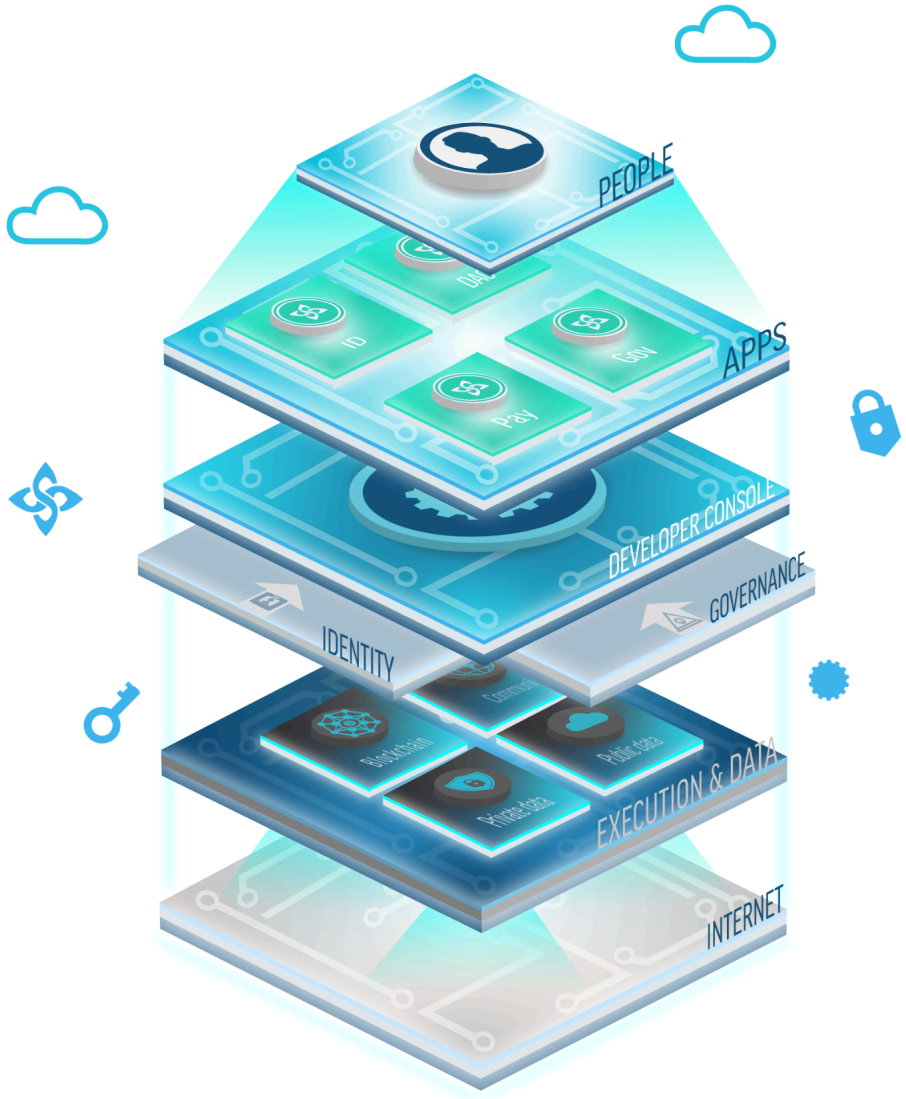


Figure 2: Architecture Layers

Execution and Data Layer
At the foundational level, the network is built upon the Internet protocol, encompassing an execution and data layer. This layer is responsible for storing both private (secured via zero-knowledge architecture) and public data. The network's infrastructure operators cannot access private data, ensuring confidentiality for individuals and DAOs. The consensus engine within this layer acts as a unifying source of truth in the peer-to-peer network, facilitating data consistency and integral services such as peer-to-peer communication, identity verification, and recovery.

Identity Layer
The identity layer operates as an intermediary between the execution applications and the core services. It is pivotal in representing the identities of individuals and DAOs within the system.

Governance Layer
The governance layer provides mechanisms for policy and ecosystem configuration decision-making. It is a versatile platform where various economic, governance, and system tools can be configured and upgraded. This adaptability makes Tonomy suitable for diverse applications in government, enterprise, public communities, and large-scale community environments.

Core Applications
The ecosystem provides standardised core applications to facilitate the formation and operation of citizen and DAO interactions. These applications include Tonomy ID, DAO, Gov, Pay, and Developer Console. They offer a mainstream-ready interface, enabling no-code, Web2-like interactions within the ecosystem and other applications.

DAO-Managed Applications
DAOs can create and manage their applications within the marketplace. This feature caters to Web2 and Web3 applications, encompassing various domains like decentralised finance, gaming, social networking, and e-commerce.

Application Layer
Individuals interact within the ecosystem primarily through applications. These applications provide a user interface that allows safe and trustless interaction, shielding users from the technical complexities of the underlying layers.

Applications Layer

The Application Layer of Tonomy networks comprises both the Tonomy Core Applications and those developed by DAOs. This document elucidates the quintet of Tonomy Core Applications, delineating their objectives and functionalities. Collectively, these foundational applications empower entrepreneurs and developers to expedite the creation of innovative use cases with unprecedented efficiency.

This facilitation is primarily attributed to the diminution of developmental intricacy and the mitigation of associated risks. This is actualised through several strategies:

- Provision of comprehensive solutions for identity, team Identity and Access Management (IAM), governance, and payment systems. These solutions are designed to accommodate 99.9% of potential use cases.
- Offering these solutions in formats amenable to developers, notably through enabling access to blockchain functionalities via application interfaces. This obviates the necessity for developers to engage directly in smart contract creation or blockchain interactions.
- Endowing developers with a "no-code" experience, permitting facile customization of identity, IAM, and governance aspects within their systems. This flexibility allows for adaptations in response to evolving requirements.
- Ensuring a streamlined and intuitive onboarding process for users. This approach ensures the security inherent in web3 technologies while maintaining a user experience akin to web2 standards. Additionally, it offers users an ongoing, straightforward interface to navigate and manage the diverse applications within a Tonomy ecosystem.

Web3 comparison:
Currently, web3 developers are compelled to undertake the complex process of navigating identity, multi-party management and governance in the new web3 paradigm, often requiring learning new programming languages and paradigms. Users faced a technically daunting and complex experience, struggling with novel technical paradigms and a disjointed onboarding and application ecosystem. Tonomy eradicates the time-intensive and high-risk tasks inherent in initiating new projects for developers and users by offering a clean no-code application system anyone can use to create well managed apps, and onboard users and in a simple familiar, albeit significantly more secure manner.

Tonomy now enables application developers to conceive and execute a plethora of use cases that were previously unfeasible. These use cases can be categorized broadly into two segments:

- Web2 applications that can leverage the substantial cybersecurity advantages of web3 technology and make data breaches a thing of a past with passwordless identity.
- Web3 applications that were previously too arduous or cumbersome to develop and use become both consumer and developer friendly.

These categories span multiple industries, with examples including:

- Governance: Tools for policy creation and budgetary participation.
- Supply Chain and Logistics: Systems benefiting from transparent tracking and tracing, alongside flexible governance mechanisms.
- decentralised Finance (DeFi): Transparent operations and governance in financial systems.
- Healthcare: Enhanced privacy and portability of data facilitated by Tonomy ID.
- Gaming: Advanced web3 asset proofs and control mechanisms for in-game collectibles.
- eCommerce: Augmented security through the use of Tonomy ID's sovereign storage vault.

- Software as a Service (SaaS) Platforms: Improved public and inaccessible sovereign single sign-on capabilities.

Tonomy, thus, presents a paradigm shift in application development, significantly enhancing the feasibility and scope of various use cases across diverse sectors.

Tonomy ID

Identity serves as the foundational and terminal interface for individuals within digital ecosystems.

Tonomy ID is an advanced wallet compatible with both Web2 and Web3 frameworks, encompassing all requisite identity functionalities for user engagement with digital systems. This system facilitates user access to both Tonomy Core Applications and broader market applications, enabling secure and sovereign digital signatures and data exchange.

Users are granted full technical autonomy, maintaining complete control over their data and authorizations. This concept is commonly referred to as self-sovereign identity or a non-custodial wallet. Unique authorisation secrets, such as private keys derived from phrases, PIN codes, and biometric data, are stored solely on the user's device, eschewing database storage. Likewise, personal data is exclusively retained on the user's personal device. This architecture significantly enhances security by mitigating the risk of centralised hacking attempts, a paramount concern for users and corporations when selecting identity service providers.

In contrast to Web2 identity services like those offered by Microsoft or Okta, the Tonomy architecture eschews the storage of any user authorisation secrets or data in databases, thereby offering substantial cybersecurity advantages. Unlike existing Web3 wallets and self-sovereign identity (SSI) wallets, Tonomy ID combines the merits of being fully non-custodial with a user interface sufficiently intuitive for individuals accustomed to mainstream platforms such as Google.[1]

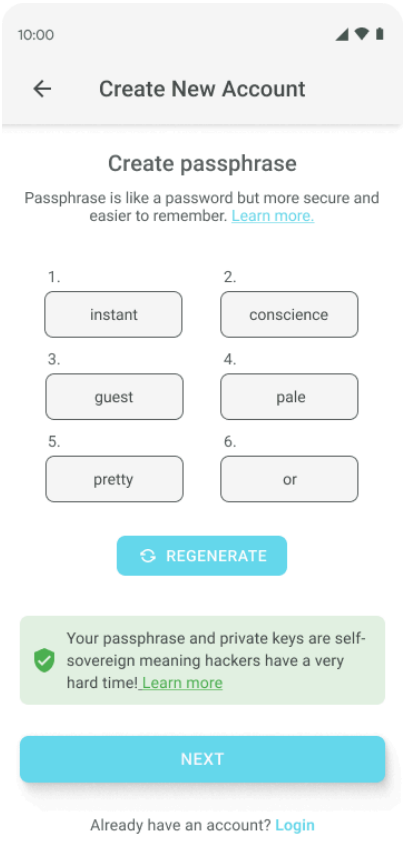


Figure 3: Siz-word mnemonic passphrase

Accounts and Onboarding

Account creation within the Tonomy ecosystem is primarily facilitated through the cross-platform mobile application via Tonomy ID. Users select a private username during this process and are assigned a random, unique, and publicly accessible anonymous user ID.

Users are provided with a cryptographically secure six-word mnemonic passphrase for account recovery and security. This passphrase is a randomly generated and easily memorable string and is passed through the secure argon2 key generation algorithm to create an ASIC-resistant, robust security. The algorithm would take every computer working together over 10,000 years to break a single key.

Resource Allocation and Transaction Fee Management

In the context of system security and protection against denial of service attacks, the identity administration portal of Tonomy incorporates a configurable resource allocation model. This model offers a selection of templates with diverse configurations to cater to various use cases, ranging from government entities to community groups, for efficient identity management.

The resource allocation model operates in the following exemplary manners:

- Central Allocation: The identity administration module possesses the discretion to allocate resources to users as deemed appropriate.
- decentralised and Equitable Allocation: All users receive equal resource allocations (e.g., 5 daily transactions) contingent upon complete verification.
- User-Directed Allocation: Users are initially provided equal allocations, with the option to acquire additional resource packages via the system's native currency.

This approach simplifies complex infrastructural aspects, enhancing accessibility for mainstream users. Requiring users to engage directly with blockchain or other intricate technical infrastructures on a per-transaction basis may result in user disengagement due to its complexity. The flexibility to revert to a cost-free account highlights the Tonomy's dedication to universal accessibility.

Social Login via Multi-Party Computation

For application processes not demanding elevated security measures, the system will support social login functionalities to streamline user onboarding for low-security applications.

The safeguarding of unique authentication secrets for this login mechanism is achieved through multi-party computation. In this framework, the user retains one key, while the social login service holds another, which is utilised to facilitate social login. Both keys are essential for the login process, ensuring the user maintains full control over their authorisation credentials[2].

Passwordless Single Sign-On

Tonomy enables users to access any affiliated Web2 or Web3 applications seamlessly. The sign-in process, analogous to Google Sign-In but employing QR codes, bridges desktop websites with mobile devices, establishing the mobile device as the primary authentication authority.

The passwordless single sign-on mechanism eliminates the need for users to input their passphrases for each website login. Instead, it utilises QR codes and URL redirections for swift and user-friendly authentication.

A distinctive aspect of the single sign-on process is the generation and authorisation of an application-specific private key. During the login procedure, a private key is randomly generated on the user's device within the currently used application. For instance, a unique key is created in the local storage of the user's browser tab on airbnb.com. Upon consenting to the login, this key is authorised to sign data on behalf of the user, with its scope limited to the application being accessed[3]. This key is subsequently employed for authorisation purposes from the application to Tonomy ID and in digital signature functionalities.

Google SSO comparison:
This feature resembles Google Sign-In, yet operates independently of Google's involvement, allowing users to authenticate directly from their phone to the application without intermediary involvement.

MetaMask comparison:
This method parallels the Web3 login experience via Metamask, focusing on user-friendliness by avoiding exposure to complex cryptographic details. It also facilitates in-app digital signatures, significantly enhancing user engagement and retention. Using scoped application keys within the multi-key account system elevates the usability of Tonomy ID, distinguishing it markedly from Metamask's single-account, single-key framework.

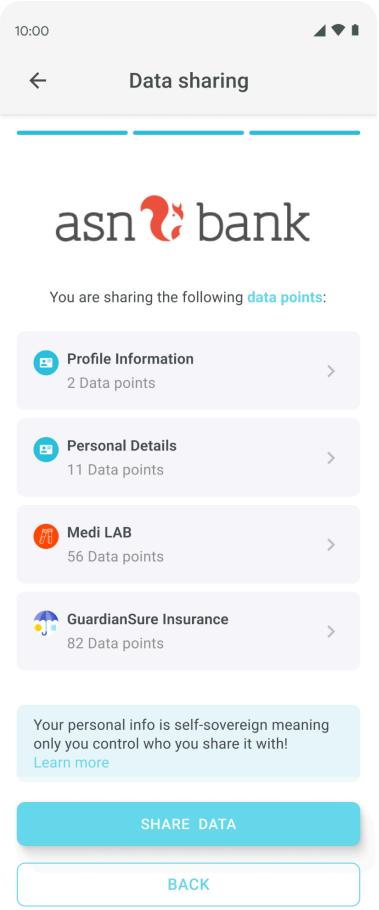


Figure 4: Data Sharing

Data Sharing and Consent:

Data stored in the sovereign storage vault can be utilised and downloaded by the applications in which it was originally created. Additionally, users can share data between applications. This is executed via a fully consensual process, allowing users to review the data being shared, its intended use, and the receiving parties. Since user data is stored on their device, there is a technical guarantee of their consent to any data sharing.

This functionality enables the transfer of portable and private data across the internet, facilitating a rich data experience across applications while preserving a seamless user experience. This capability addresses the current limitations of the internet due to technical data silos and the challenges posed by data privacy regulations. Tonomy ID heralds an era of Data Internet without compromising data privacy.

Sovereign Storage Vault

Application developers are empowered to store user-generated data within the confines of the user's device, as opposed to relying on a private database vulnerable to cyber-attacks or a public data system like IPFS, which compromises user privacy.

Healthcare example:
Consider the scenario in a healthcare application where a user's medical record, once generated, is transferred and stored in the user’s sovereign storage vault. This data is exclusively tied to the generating application, with read and write permissions limited to said application. Subsequently, other applications may access the data stored in the vault, subject to user consent for read privileges. For instance, an insurance application may request access to medical records, enabling the user to submit claims.

This paradigm of user-controlled, centralised yet fully autonomous data storage markedly enhances data security and portability across the internet. It results in diminished security risks for companies, elevated user trust, and a more enriched data interaction due to the facilitated, risk-reduced storage of personal information across diverse applications.

Conceptually, this feature is akin to having all personal certificates, diplomas, event tickets, employment contracts, and more stored digitally and verifiably within one's mobile device rather than in a remote database.

Private Identity Verification

During application sign-in procedures, users might encounter a request for identity verification to authenticate the congruence of their identity with the provided data. This is an elective part of the login process, determined by the application developer.
Various identity verification mechanism exists controled through the identity administration portal, which is in turn controlled through the governance system. Tonomy ID provides newer decentralised identity verification mechanisms utilising off-chain social graphs and ergonomics and backwards compatible identity document verification (KYC-like) flows with enhanced capabilities.

During an identity document verification flow, the verification proof is retained in the sovereign storage vault instead of being stored in a database, thereby preserving its confidentiality and reusability. This approach sustains user trust while reducing the long-term costs associated with identity verification.

For instance, numerous financial applications necessitate this process for regulatory compliance, whereas contemporary Web3 decentralised finance applications might forego this, permitting anonymous logins. These apps leverage the de-anonymization governance feature to ensure user accountability without necessitating personal information from each user.

Netverify comparison:
This feature could be compared to Netverify (utilised by Airbnb), with the distinction that post-verification, identity data, including the verification proof, resides solely on the user's device, enabling repeated use without additional verification costs.

Account Guarantee

The Tonomy ecosystem assures that users will maintain access to at least one account. This is facilitated through the private identity verification process. This guarantee is crucial, considering that certain governance features within the system allow for the partial or complete freezing/disabling of fake or compromised accounts. The identity verification protocol ensures that even individuals who violate the rules by creating fake accounts will always have one unfrozen account, thus ensuring uninterrupted network access. Such accounts may bear warnings to discourage such conduct, but access remains unfettered.

This feature ensures universal accessibility for every user while still maintaining the ability to self-regulate detrimental behavior.[4]

Digital Signature Mechanism

Tonomy ID integrates a sophisticated digital signature mechanism using fully non-custodial keys. This system accommodates diverse data formats, security protocols, and proof types to cater to a comprehensive spectrum of use cases.

DocuSign comparison:

The digital signature capability in Tonomy ID is analogous to a highly advanced and secure version of DocuSign but has considerably broader applicability. It facilitates the signing of a wide array of entities, from documents to transactions, employing customisable flows that can be adapted to various use cases and user preferences regarding security and usability.

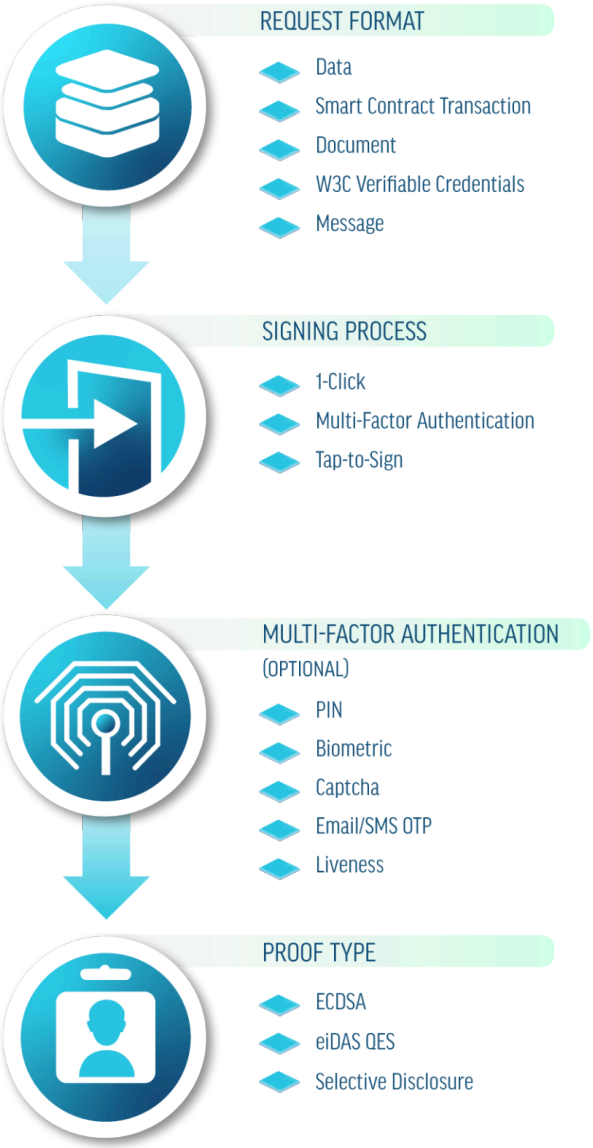


Figure 5: Digital Signature Process

The signature process is subject to the discretion of the application developer, who decides on the following parameters based on the application's specific needs:

- **Request Format:** This involves choosing the format of the data requiring a signature, ranging from raw data, W3C verifiable credentials, standard documents (e.g., PDFs), smart contract transactions, to simple messages.
- **Signing Process:** This determines the flow and security-usability balance of the signature. Options include in-app signing (generated during Single Sign-On, ideal for games or low-security transactions), multifactor authentication (for higher security, involving additional authentication like PINs or biometrics), and smart NFT technology (for offline or non-phone digital signatures using NFT-smart cards or hardware security wallets).
- **Multi-Factor Authentication:** If enabled, users undergo additional steps based on the requested challenges, each offering varying security guarantees. For instance, a PIN challenge provides a "proof of knowledge," whereas a biometric challenge offers a "proof of person."
- **Proof Type:** Developers can select from various digital signature proof types. The default is Elliptic Curve Digital Signatures (ECDSA), with options for an eiDAS Qualified Electronic Signature (QES) for EU-recognized signatures or Selective Disclosure Proofs for enhanced data privacy.

Crucially, the private keys used in these digital signatures remain under the user's control, ensuring maximal security and privacy for users and applications.

For further details, please refer to the Digital Signatures section of the Tonomy ID White Paper.

Peer-to-Peer Messaging

Leveraging the same private keys and digital signatures, Tonomy ID facilitates peer-to-peer messaging within and across various applications. This is achieved by implementing the new W3C standard DIDComm, a transport-agnostic, highly standardised, and interoperable private messaging protocol.

DIDComm Messaging represents a sophisticated method for individuals, institutions, and IoT entities to engage through machine-readable messages, underpinned by the security and privacy features of decentralised identifiers (DIDs). It is compatible across various transport mediums, including HTTP, Bluetooth, and websockets.

DIDComm also incorporates Onion routing for messages, significantly enhancing user privacy.

WhatsApp comparison:
This feature offers end-to-end encrypted messaging capabilities comparable to applications like WhatsApp, with the added flexibility of functioning across different applications and having enhanced security and governance.

Private Reputation System

Within the Tonomy ID ecosystem, identities can accumulate and be accountable for private ratings from other users, striking a balance between privacy and accountability. These private reputation systems can undergo audits via the governance's arbitration system through appropriate warrants.[5]

Account Recovery

Tonomy ID utilises a secure 6-word passphrase as the primary authentication method for its mobile app. To address situations where users forget or lose this passphrase, Tonomy ID offers several non-custodial recovery mechanisms, ensuring autonomous control over user accounts:

- Social Recovery: Users can designate trusted contacts to assist in account recovery collectively.
- Hardware Recovery: Pre-authorized devices like secure hardware wallets or NFC-enabled smartcards can be used for recovery.
- Security Questions: Utilizing advanced cryptographic techniques, users can recover accounts by correctly answering pre-selected personal questions.
- Partially-Custodial Identity Verification: An identity verification process through governance services allows temporary access to a user's sovereign storage vault for identity confirmation.

The recovery process includes a mandatory timeout period, varying based on the security level of the chosen recovery method.

Additionally, Tonomy ID offers optional plug-ins for various custodial recovery techniques, enhancing its suitability for enterprise use.

For more information, please see the relevant sections in the Tonomy ID White Paper.

Identity Administration Portal

The Identity Administration Portal facilitates the configuration of various features and settings integral to Tonomy ID. Key aspects that can be adjusted include:

- Identity Verification Methods: Establishing protocols for identity authentication.
- Resource Allocation Models: Defining parameters such as daily transaction limits per user.
- Security Policies: Implementing security measures for single sign-on and digital signatures, including considerations for mandatory multifactor authentication.
- Private Reputation Systems: Guidelines for activating and regulating private reputation mechanisms.
- Account Recovery Options: Selection of available mechanisms for account recovery.

This portal plays a crucial role in setting ecosystem-wide identity access policies. It enables administrators to:

- Specify policies governing user admission to the ecosystem.
- Administer account-related actions such as account freezing and issuance of access warrants.Establish identity systems ranging from closed systems (e.g., invite-only for enterprise employees) to open, public, permissionless networks.

Through the portal, individual identities within the ecosystem can be managed, including the ability to freeze accounts or de-anonymize identities under specific warrants.

The identity system's configuration is accessible via a user-friendly, no-code platform. Depending on the governance system in place, configurations may be determined by authorised entities (e.g., a department of identity employees) or through multi-party governance proposals.

Tonomy DAO

Tonomy DAO represents a paradigm shift in organisational management, facilitating the formation and autonomous governance of various collective entities such as companies, foundations, communities, associations, and commons. This platform maintains autonomy and control over governance, data, funds, and operations, negating the requirement for external service providers.

Within Tonomy, governance is administered through the Tonomy DAO system, embodying a decentralised control model.

Tonomy DAO integrates advanced Identity and Access Management (IAM) mechanisms, supporting diverse member entities from individuals to other DAOs. Its architecture, characterised by low-latency transactions and versatile IAM configurations, enables a broad spectrum of governance structures. This makes Tonomy DAO a versatile platform for mainstream organisational management, straddling high-security Web2 and high-usability Web3 applications across various sectors.

DAOs, functioning as public entities, maintain visible profiles, yet member identities are safeguarded through anonymised account IDs. Membership entails automatic access to other members' information, aligned with the established privacy policy. This aspect of Tonomy DAO is critical, underpinning the decentralised control of multi-party sovereign entities on the Internet.[6]

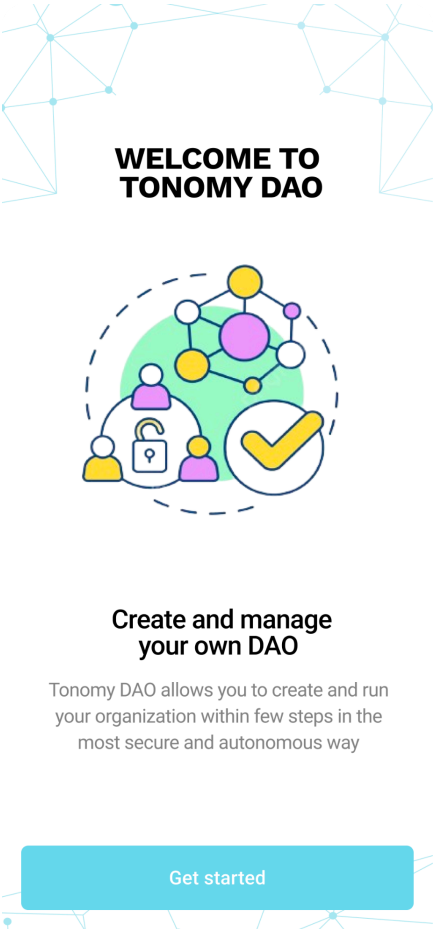


Figure 6: Create a DAO

Incorporation Process

Creating a DAO within a Tonomy network is a streamlined process. Prospective founders select key attributes such as name, description, liability model, categories, and governance structure. Post-creation, members are onboarded, and governance frameworks or DAO profiles are modifiable.

The chosen liability model, categories, and governance structure are integral in defining the regulatory framework of the entity, facilitated by the platform's self-regulating governance capabilities.

Governance Templates and Models

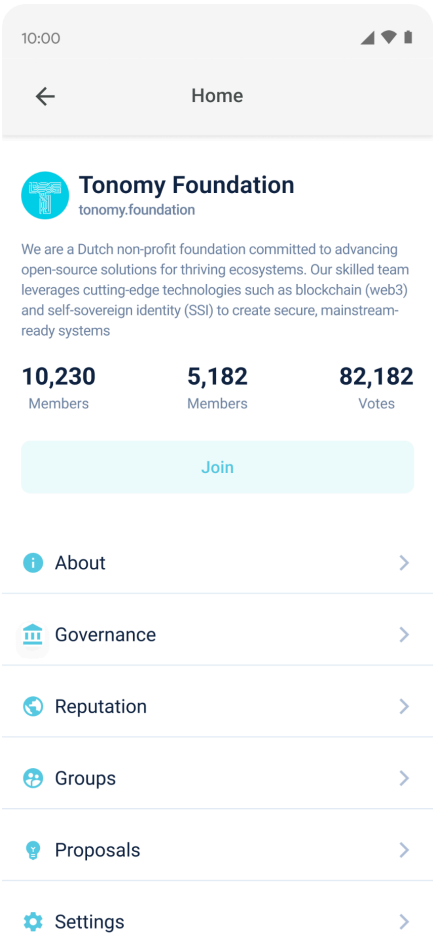


Figure 7: DAO Profile

Tonomy DAO offers an array of foundational governance templates, enabling diverse voting privileges:

- Democratic: Equitable voting rights for verified members.
- Share/Token-Based: Votes are weighted by token holdings, managed through Tonomy Bankless.
- Sole-Proprietor: Tailored for individual enterprises with centralised decision-making.

Decision-making models within Tonomy DAO vary, including:

- Federated: Governance by a self-selected executive group.
- Representative: Indirect voting through trusted representatives.
- Direct: Direct voting on decisions by all members.
- Liquid: A nuanced approach combining direct and representative voting, allowing members to delegate voting power in specialised areas.

These models cater to a wide range of entities, from government departments, and profit-driven companies to self-managed communities, demonstrating Tonomy DAO's adaptability and innovation in organisational governance[7].

Identity Access Management (IAM)

IAM is crucial in managing DAO members and their authorisation levels. As DAOs expand, they can:

- Form multiple groups akin to departments, each with defined responsibilities, permissions, and security policies.
- Configure access rights which control the way members join and leave these groups. These can be configured to allow open access or invite only.
- Configure security policies for the group that control the requirements for digital signatures to authorise the documents or transactions for which the group is responsible.
- Assign members to these groups, granting them corresponding rights.

For example, a finance group might have specific responsibilities, permissions up to a certain transaction limit in Tonomy Bankless, and security policies requiring multifactor authentication for authorisations.[8]

Sovereign Storage Vault

DAOs utilise sovereign storage vaults for private data storage, similar to Tonomy ID but adapted for multiparty use. These vaults are permissioned based on group assignment, with parent groups having access to child group data, supported by multiparty encryption.

Google Drive comparison:
The Sovereign Storage Vault for DAOs is like having a Google Drive available to employees, except that the data stored in the vault is not visible to any third parties. This is a significant privacy improvement for people and companies and a significant cyber security and compliance improvement for ecosystem operators.

Multi-party Proposals

Figure 7: DAO Profile

DAOs govern through multi-party proposals, encompassing:

- Documents - Creating or modifying the documents. For example, this can be used to create, sign and execute articles of association for a company. Or it could be used To sign an employee agreement between the employee and their new manager.
- Policy - Creating or modifying company policies and agreements. For example, this can create new security policies for groups or expectations for new employees regarding holidays.
- Funds - Sending money to suppliers or for other expenses. This is particularly useful for high-value transfers to have multiple-party authorisation. It can also create and configure new multi-party funds accounts and Tonomy Bankless.
- Governance - The top-level owners and governance structure used within the DAO can also be upgraded. This leverages the upgradable accounts and governance features of the underlying structure. This allows DAOs to remain agile and flexible.

Proposals impact the proposing group and its subordinates, ensuring higher-level security integrity.

Voting Mechanisms

The network accommodates multiple voting mechanisms to meet distinct privacy and security requirements:

- **Public and decentralised On-Chain Voting:** Offers supreme security and transparency to users.

- **Private On-Chain Voting:** Employs advanced cryptography, balancing high security with user scalability and long-term cryptographic reliability.
- **Private Off-Chain Voting:** Utilizes cryptography with low-trust vote custodians, providing scalable private voting but with reduced security assurances.

Different voting strategies are also offered in modules. These can be configured at the policy proposal level or applied to all policies based on whether there is the option to vote on one policy at a time or between a selection of options:

Voting strategies for single policy voting:

- **Binary Choice:** Typically, voters are presented with a yes/no or approve/reject option for the proposal.
- **Quorum Requirements:** A minimum number of participants (quorum) may be required for the vote to be valid. This can be based on total membership or only active participants.
- **Counting Absences:** Depending on the rules, absentees may be counted as implicit approvals, rejections, or not counted at all.

Voting strategies for multi-option policies:

- **Multiple Candidates/Options:** Voters select from more than two options, which could be candidates, policies, or proposals.
- **Voting Systems:** Can use a variety of methods like first-past-the-post, preferential (ranked-choice) voting, proportional representation, etc.
- **Majority or Plurality:** Depending on the system, the winner may need a majority (more than 50%) or simply a plurality (the most votes).
- **Budget Based:** Users are allocated a budget which they can spend on proposals which each have been assigned a cost.
- **Sequential Elimination:** In some methods like instant-runoff voting, options with the fewest votes are eliminated in rounds until a winner emerges.

Artificial Inteligence Enhanced Proposal

During the creation of new policies and proposals, artificial intelligence creates suggestions For enhancements in the language and content, using the existing policies as well as its connection to the discussion and communication forums for context. Uses creating the proposals are always able to opt-in to suggestions, to ensure Verification and ethical use of AI generated content.

This feature helps proposal writers ensure they have captured the main perspectives including thinking about pros and cons. The artificial intelligence algorithms help summarise existing discussions and perspectives from them, and provides convenient links to these discussions for verification.

Public and Private Reputation

DAOs maintain both public reputations and private ratings, subject to audit through the governance's arbitration system under specific warrants.

Billing and Insights

DAOs, as entities, incur costs. The Billing and Insights portal offers insights into expenses and member analytics, aiding in efficient management.

DAO Administration Portal

This interface allows for the configuration of Tonomy DAO features, including:

- DAO incorporation requirements.
- Resource allocation models per DAO.
- Group-specific security policies.
- Reputation system management.

Like the identity system, DAO configurations are accessible through a no-code platform. They are subject to the prevailing governance system, potentially managed by authorised individuals or through multi-party governance proposals.

Tonomy Bankless

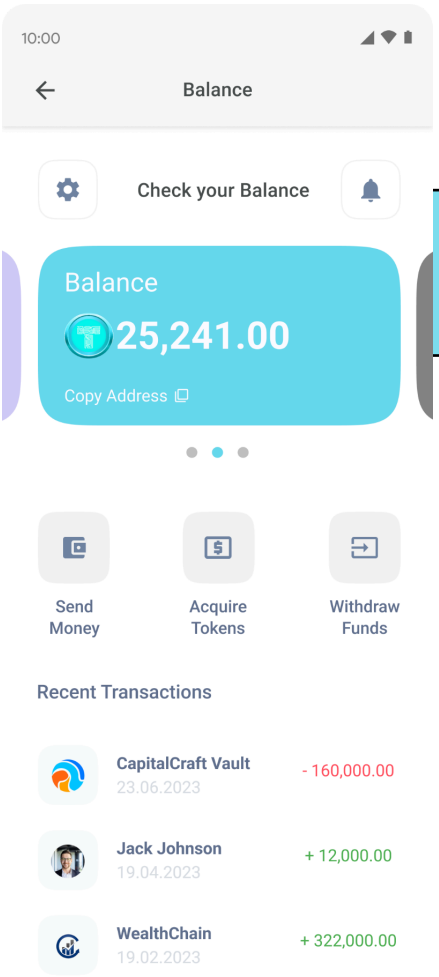


Figure 8: Tonomy Bankless

Tonomy Bankless represents a sophisticated, decentralised platform for payment processing and financial resource management. This platform facilitates secure and autonomous financial transactions and management for individual users and DAOs.

Neo-bank comparison:
The functionality is designed to simulate that of contemporary neo-banks like Revolut or N26; however are devoid of a centralised technical backend.

Primarily, Tonomy Bankless is accessible to both individuals and DAOs, featuring an array of functionalities tailored for multiparty financial management. While individual users predominantly access the platform's services at no cost, DAOs engage with the platform on a paid basis, utilising its advanced banking infrastructure.

The platform's design emphasises user empowerment in terms of control and ownership, with a user experience mirroring that of Web2 applications. Integration with Web2 companies is streamlined through the use of simple JavaScript SDKs, bypassing the complexity of coding token contracts.

Payment Processing

Core to Tonomy Bankless is its ability to process transactions using the system currency. Users execute payments via QR code scans by inputting usernames or selecting from pre-used contacts. Integrating with the Tonomy ID sovereign security vault enhances long-term transaction security, ensuring that contact information remains protected and is not centralised, in line with Tonomy's privacy principles.

Advanced Payment Options

Tonomy Bankless supports diverse payment modalities including escrow payments, where the system currency is temporally secured, facilitating smart services and other Web3 applications. It also accommodates recurring subscription payments, a feature extensively employed by SaaS platforms and for billing DAOs for network services.

SWIFT/SEPA comparison:
In this way, Tonomy Bankless matches and extends additional functionality while still retaining backwards compatibility with modern payment networks like SWIFT and SEPA.

Ethereum/Solana comparison:
Other cryptocurrencies often have features such as subscriptions or escrow built in as second-layer features, requiring users to use a second token or application creating a confusing experience. Tonomy Bankless considers these features primary and is configurable in the native currency token.

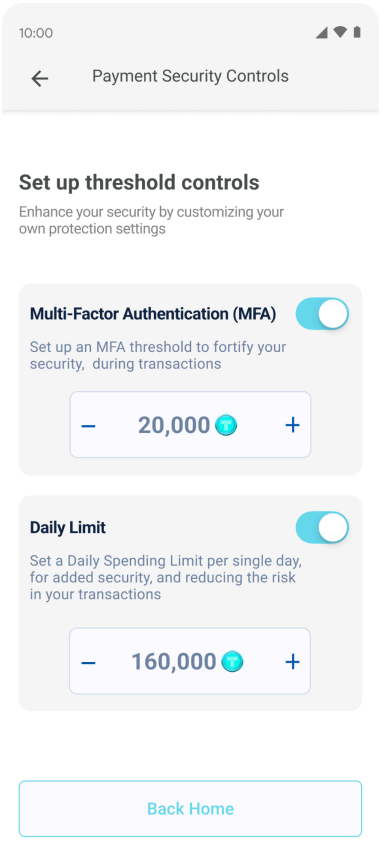


Figure 9: Payment Security

Account Management and Automated Budgeting

The platform allows users and DAOs to segment their funds into distinct accounts based on specific requirements. This feature includes creating tiered security systems within DAO's groups for effective funds management. Additionally, automated budgeting capabilities enable the strategic allocation of funds across accounts according to preset parameters.

Enhanced Payment Security

Tonomy Bankless introduces granular security controls for transactions. These include threshold limits with attached security policies, enabling varying degrees of authentication based on transaction amounts. Such controls are customisable at the account level, with DAO groups controlling applicable security measures for their respective accounts. For example, users or DAOs can introduce a minimum threshold for payments after which multifactor authentication is required. DAOs may do the same but introduce a minimum threshold after which multi-party authentication is required.

Ethereum/Solana comparison:
Unlike other cryptocurrencies that work on a 1 key per account system, Tonomy Bankless is easily able to allow users to flexibly manage large and small amounts of tokens in cold/hot wallet flows based on their needs while staying fully non-custodial

Transaction Receipts

The platform supports the generation of private, standardised receipts for each transaction, facilitating automatic insights reporting and, where applicable, transaction taxation. These receipts are cryptographically linked to their respective transactions, enhancing the integrity and traceability of financial records.

Asset Management

Beyond conventional currency, Tonomy Bankless extends its management capabilities to other digital assets such as tokens, NFTs, and collectables. This feature caters to a diverse user base, including investors and gamers, while maintaining a user-friendly interface focused on primary system currency transactions.

Analytics and Insights

In line with neo-bank standards, Tonomy Bankless offers comprehensive analytics and insights regarding account usage and payment activities. This is augmented by the platform's capability to process private receipts, providing detailed financial data.

Currency Management Panel

The platform encompasses advanced privacy management tools, including zero-knowledge proofs and ring signature privacy features, which users can configure according to their preferences. Furthermore, the currency administration panel facilitates the management and customisation of currency features, such as inflation rates and administrative controls. This is particularly pertinent for entities managing currencies like CBDCs, stablecoins, or decentralised cryptocurrencies, offering a modular, customisable approach to currency administration.

Tonomy Gov+

Tonomy Gov+ adopts a no-code paradigm, employing swift and adaptable foundational systems that ensure cryptographic integrity. This ensures that the governance framework is autonomous, accessible, and adept at fostering sound, well-integrated decisions within a self-regulatory ecosystem.

The foundational Tonomy technologies offer a modular toolkit, enabling a Tonomy network to select and modify its governance framework as needed. This adaptability is crucial for scaling the governance structure and features as the network expands. Additionally, it is vital for other networks to utilise the white label feature to create new networks, allowing them to harness and tailor this technology to their specific use cases.

The ecosystem governance institution within the networkIs a special DAO. Most of the legislative features (who and how are decisions made) are controlled through the existing Tonomy DAO features. It is through Tonomy DAO that a democratic or proof of stake network are configured, or a representative or a direct voting system are employed.

The ecosystem governance DAO has several additional specific features outlined in this section of the White Paper.

Multi-DAO DAO

Due to the complexities of government and multi-stakeholder ecosystems, in some cases the governance of the ecosystem will be split across several governance DAOs. For example this could, for example be a main DAO for the parliment, and other DAOs for ministries. Within each DAO, different security groups can be created as well. With the ability to create different DAOs and groups within them, complex governance ecosystems can form to meet their needs using these two simple abstractions in Tonomy. This also allows simple ecosystems to grow and evolve to be more complex over time with ease.

Treasury

The ecosystem governance DAO Is responsible for managing the policies, income and expenses of the native currency. This is done through the treasury currency account available in Tonomy Bankless.

There are two different types of fund management:

- **Automated:** Network policies Provide the fees and other expenses paid by network participants to access Network services. These fees go into a collective pool. The network policies also specify the incentives paid to the network operators. These Payment collection distributions Coded into the protocol level And are fully Automated and low-trust. The policies themselves are configured through the policy manager in the governance DAO.
- **Manual:** Ecosystems made used to create their own treasury pools which they manually manage. This gives them greater flexibility to use funds without needing to make policy changes for every payment system. For example this could be used to create a ecosystem fund generated from investors to pay development of apps, or for a fund to pay for a user support system (not one of the default network services).

Discussion and Communication

An integral part of decision-making requires discussion and deliberation in complex ecosystems. Tonomy provides an intuitive discussion forum as well as a more casual communication platform through which this is facilitated. Built into the discussion forum is the ability for non-binding votes and sentiment collection. This is done using the same anonymous voting technologies from Tonomy DAO, such as preference voting or binary voting. In this way, group perspectives can be collected and integrated into proposals to create the best proposals possible before they go for final decision-making voting.

EIP Comparison:
The Ethereum Improvement Proposal (EIP) is an important part of the Ethereum governance process and has been widely adopted across many open-source projects. The Policy Management platform in Tonomy encapsulates a similar level of features but is more general and can apply to alignment on policies and standards not specifically related to digital infrastructure. For example, it can govern healthcare policy in a state-nation ecosystem or the payment process and KYC requirements in an enterprise ecosystem.

Artificial Intelligence Enhanced Discussions

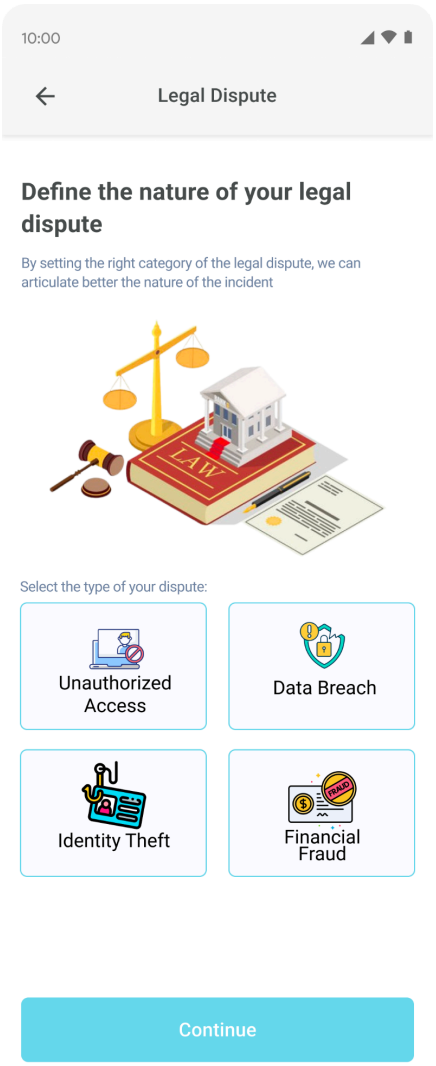


Figure 10: Legal Dispute

Integrated into the discussion and communication platforms is a artificial intelligence bot that helps navigate and guide new and experienced users through complex policy and technical discussions. It provides up-to-date summaries of the discussions, pros and cons and active analysis of the current sentiments based on votes, reactions and the discussions. In further assists in suggesting proposals and counterproposals when relevant to facilitate direct and practical progression of discussions. The bot is also able to quickly identify when proposals may violate the existing policies and provide quick links for verification from participants.

This provides a higher level of accessibility discussions amongst its participants and helps facilitate moderation and progression of the discussion in a practical way. To manage ethical use of AI, these features are optional, and users always need to opt-in to accept AI suggestions.

Network Infrastructure Administration and Monitoring

The organized registration of network Infrastructure service providers and the monitoring of their infrastructure performance and availability is an important part of the governance oversight. Here, the status and monitoring of different infrastructure providers can be easily viewed and checked. Alerts system are built in place to alert relevant groups when system infrastructure has issues.

Because this is a highly technical art of the system, it is likely that complex ecosystems will delegate authority to a separate governance DAO (a commission) to facilitate this oversight. The complexity of this could also be handled successfully using more hybrid governance models like liquid democracy. Each ecosystem will decide how to handle this technical oversight.

This portal facilitates an understanding of technical capacity and growth and enables the configuration of network settings, incentive structures, and service fees, further detailed in the Tokenomics model section.

Ecosystem and Governance Configuration

Each core application within the network features an administration panel, allowing for the customisation of network settings. For instance, Tonomy ID permits setting minimum security policies for single sign-on logins, while Tonomy DAO allows configuration of incorporation

data requirements. Governance DAO settings, including voting policies and communication platforms, are also configurable through this system.

Arbitration Platform

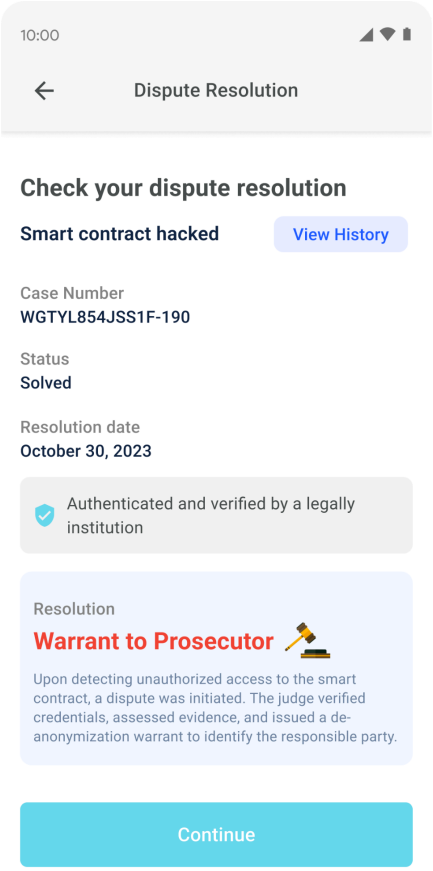


Figure 11: Dispute Resolution

Tonomy will incorporate an arbitration platform to facilitate dispute resolution among ecosystem participants, leveraging the policy system. This platform will evolve from a basic structure to a more complex system, accommodating various arbitration methods such as judges, juries, and public and private adjudication.

Arbitration Proof Verification

The arbitration process will heavily utilise verifiable data using W3C Verifiable Credentials from Tonomy ID digital signatures to streamline dispute resolution, reducing legal friction. Privacy-preserving functionalities, like selective disclosure, will enable public court cases without compromising private information.

Ecosystem Warrants

The system will encompass several vital functions to uphold self-regulation specific to the Tonomy:

- **Warrant Issuance:** Upon providing concrete proof of a security or protocol breach, a prosecutor may obtain a warrant for de-anonymizing identities, applicable in cases involving malicious actors or non-compliant entities.
- **Account Freezing/Unfreezing:** Proof of identity policy volioation (e.g. each person may only have one identity) can lead to the freezing of accounts, this exists to reinforce the identity verification protocol.
- **Imposition of Fines:** Evidence of policy violations not automatically enforced by software can lead to fines for individuals, DAOs, or the governance administration.

In all scenarios, digital evidence must be presented within a network-based arbitration system, where decisions are made following the network's policy interpretations.

Artificial Inteligence Assisted Policy Interpretation

During arbitration cases, artificial intelligence algorithms help provide a summary and links to the relevant ecosystem policies that may apply to the situation. This can then be used by the prosecutor, defendants, judges, juries and more to facilitate a more efficient and accessible conversation that will result in a well rounded and faster resolution. This significantly reduces costs and facilitates greater understanding and participation in the legal system.

Tonomy Build

Tonomy Build is a sophisticated platform designed to facilitate developers in the streamlined setup and management of network infrastructure and applications. This no-code interface offers structured guidance, enabling app developers and infrastructure providers to seamlessly register, administer, and regulate their applications and services within the ecosystem.

Google Developer Console and Web3 comparison:
Tonomy Build platform offers a nuanced and user-friendly approach, greatly mitigating operational risks for developers and entrepreneurs engaged in ecosystem activities. Its conceptual framework is akin to the Google Play Console, which provides developers with the tools to manage Google resources or implement Single Sign-On (SSO) with their applications. In Web3, the prevalence of such intuitive, no-code development platforms is limited, often necessitating developers to navigate through extensive documentation and employ command-line inputs or Software Development Kits (SDKs) for system implementation and management.

Tonomy Build is enhanced with built-in analytics and advanced security features, positioning it as a more innovative and less risky option than other platforms. In the spirit of transparency, most information about applications and network infrastructure managed through the console is publicly accessible, barring data sensitive to privacy and security. While the general public holds read-only privileges, developers and infrastructure providers retain comprehensive control over the configuration and management of their respective products and services.

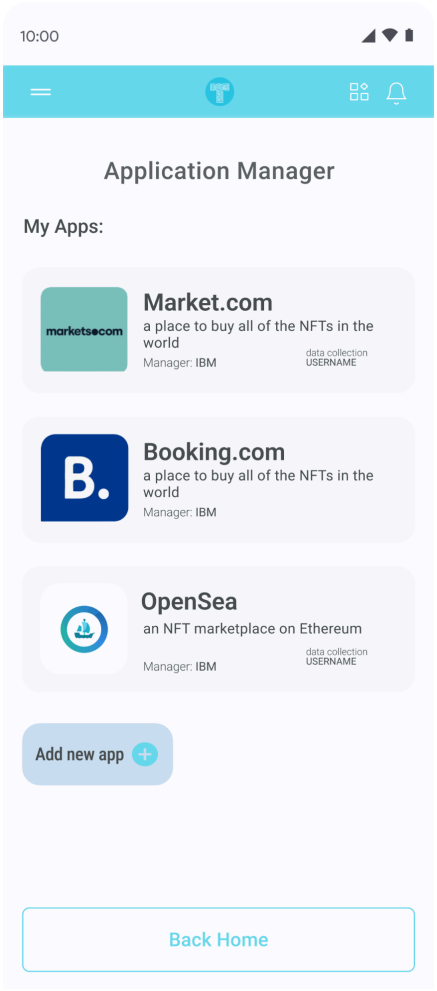


Figure 12: App Manager

Billing within Tonomy Build is bifurcated into two distinct categories:

- Applications and services offered by DAOs to the other network participants, where fees are levied based on infrastructure utilisation.
- Services provided by DAOs to run the core infrastucture of Tonomy networks, which are free of charge, with compensation managed through the network's policy, governance, and administration systems.

Application Manager

Application developers can register, administer, and remove applications from the private app market. This section allows for configuring requisite security policies for logins, such as the option of social login, varying multifactor authentication procedures, or different levels of identity verification. Developers can also specify the user data required from the sovereign storage vault upon login, such as names or data from other applications. Additionally, settings regarding login privacy, including permissions for blockchain transaction signing, are configurable here.

Customer Identity Management

Application owners are empowered to manage and oversee users accessing their applications. This feature facilitates control in alignment with the application's terms and conditions or privacy policy.

Application Services Manager

This section allows for the addition of auxiliary services to different applications. These services encompass:

- Registration of public keys for authorising digital signatures from the application system.
- Deployment and updating of smart contracts.
- DNS verification processes.

Artificial Inteligence Guidance and Education

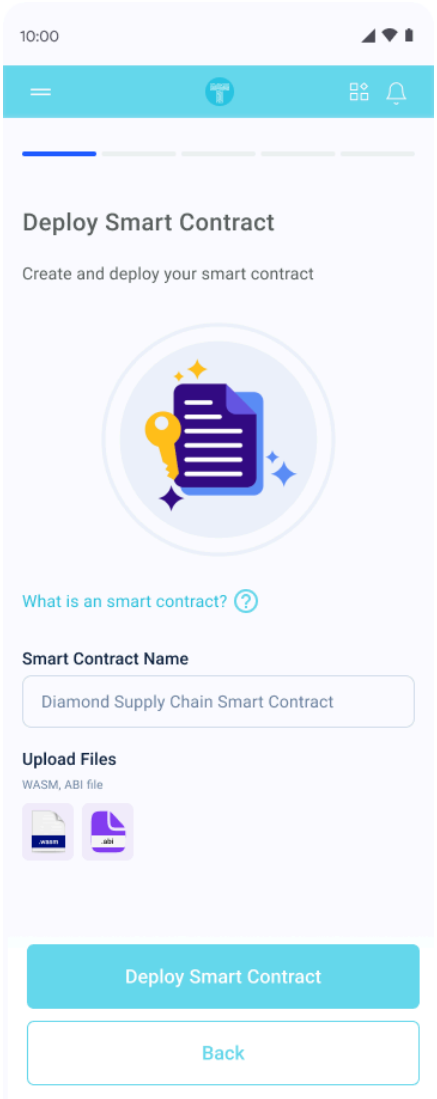


Figure 13: Smart Contract Deployer

To navigate the various configurations and functions available for technical participants of the ecosystem, artificial intelligence chat bots are available. These allow developers to ask questions and get answers on how to do things. The chat bots are connected to a helpdesk wiki, as well as the ecosystems policy system. This allows convenient and easy access in a cost-efficient way. By connecting to the ecosystem policy system, developers can also easily be aware of any policies that may affect the way they are configuring applications and infrastructure services.

Network Services

DAOs aspiring to offer services to the network, such as validated nodes, DIDComm nodes, or other services referenced in the Execution and Data Layer section of this document, can register, manage, and deregister their services here. This feature simplifies service management and ensures accountability and oversight over network services. Services are categorised and configurable based on type (e.g., validator nodes can adjust stakes, and identity verification bridges can manage signing keys).

Analytics/Insights

A comprehensive array of analytics and insights is available to service providers and application services, offering deep visibility into service performance and user engagement.

Developers Administration Portal

The Developers Administration Portal facilitates the configuration of overarching ecosystem infrastructure settings. Capabilities include:

- Enabling or disabling smart contract deployments or upgrades.
- Activating or deactivating various registerable services.
- Establishing minimum requirements for registration and configuring security policies, such as multifactor authentication or identity verification.
- Configuring fees and fee models for services, including application or public key registration.

Identity Layer

Tonomy's identity layer provides a sophisticated mechanism for account identification, utilising either anonymised, randomly generated account names or privately selected usernames. This framework is integral to the functioning of identities, DAOs, and applications within the ecosystem. It capitalises on blockchain technology as a singular,

verifiable source of truth, storing cryptographic data that underpins client-side controlled identities engaging in peer-to-peer interactions.

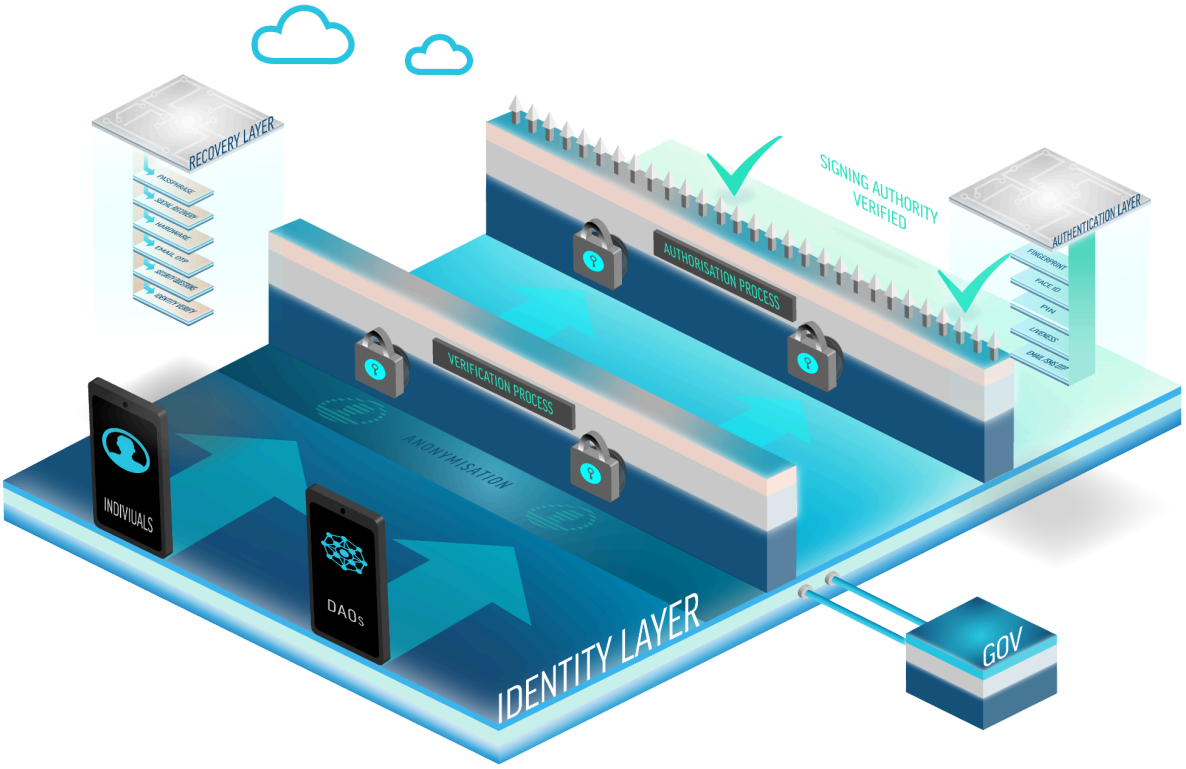


Figure 14: Identity Layer

General Account and Key Structure

Tonomy features a meticulously constructed account and key management system anchored in the robust account functionalities of the Tonomy Blockchain. Embracing a modular design philosophy, this system ensures comprehensive, consistent, and accurate operational processes.

Cryptocurrency/Ethereum comparison:
Distinct from conventional currencies, Tonomy accounts utilise an abstraction framework permitting the management of multiple, nested, and named keys in a versatile manner. This structure is extensively employed to foster a user-friendly experience in the application layer. In contrast, traditional cryptographic approaches often adhere to a one-account, one-key model, which imposes constraints on identity management and user experience, occasionally leading users to adopt less secure workarounds.

Role-Based Permission Management

Tonomy incorporates an advanced role-based permission management system, facilitating granular control over operations and linking authority to specific entities or collectives. This system transcends basic signature-verification models, enabling more refined and adaptable operation authorisation. For example, an organisation can allocate varying access levels to different team members, ensuring that operations are confined to their respective authority levels.

This separation from the business logic of applications standardises authentication and permission management, catalysing the development of universal tools for permissions management, performance optimisation, and security enhancement.

Hierarchical Authority Structure

In a Tonomy network, each account is controlled by a hierarchically arranged combination of other accounts and private keys. This structure, mirroring real-world permission systems, supports multi-user control and augments security. For instance, a corporate account might be regulated by combining the CEO's key and a collective of executive keys, maintaining balanced and secure operational control.

Named Permission Levels

Accounts within Tonomy can establish various named permission levels, each inheriting from higher-tier permissions. These levels encompass threshold multi-signature checks and combine keys and named delegations to other accounts. A user, for example, could establish a "Friend" permission level, permitting friends to execute specific operations on their account.

Permission Mapping

The network facilitates the mapping between contract operations and designated permission levels. This feature allows account holders to dictate which operations are executable by particular permission groups. A user might, for instance, link their social media activities to a "Friend" permission group, authorising friends to post on their behalf while maintaining traceability and accountability.

Evaluating Permissions

When initiating an operation, Tonomy employs a multi-tiered process to evaluate permissions. It scrutinises specific permission mappings related to the operation, verifying signing authority through a threshold multi-signature process. The system escalates through parent permissions if direct permission is not met, ensuring an exhaustive and secure validation procedure.

Flexible Account Types

Exploiting its hierarchical permission and key structure, a Tonomy network supports the creation of varied account types. This versatility is conducive to tailoring accounts for individuals, DAOs, applications, and potential new entities like AI bots or IoT devices. The system's adaptability positions it to evolve alongside emerging technologies and user requirements.

Individuals

The permission structure for individual accounts in a Tonomy network is hierarchically organised as follows:

- ➔ Recovery Layer: This topmost layer consists of keys linked to the user's configured recovery mechanisms. These could be account delegations to trusted contacts for social recovery, keys derived from secret questions or hardware devices.
  - ◆ Passphrase: The primary account access key, generated using the secure Argon2 key derivation algorithm from a set of six randomly chosen, easily memorable words.
  - ◆ Biometrics: A securely generated key uniquely associated with the user's biometric challenge.
  - ◆ PIN: A securely generated key uniquely associated with the user's PIN challenge.
  - ◆ Liveness: An account delegation to the identity verification bridge enabling liveness checks.
  - ◆ Email and SMS OTP: An account delegation to the accounts service, facilitating email and SMS one-time password (OTP) verification.
  - ◆ Local: A securely generated key without an associated challenge, utilised for peer-to-peer messaging and challenge-less signatures.

On iOS and Android devices, all these private keys are stored within a secure hardware enclave.

As detailed in the respective section, a private key is randomly generated in the browser's storage during the single sign-on process. Upon user consent for login, the corresponding public key is added to the blockchain as a separate permission, defining the security scope of the key and its application-specific associations.

Decentralised Autonomous Organizations (DAOs)

The permission structure for DAOs encompasses:

- ➔ Owners: This top layer includes delegations to individuals and other DAOs owning the entity. In democratic entities, each delegation is equally weighted. In share-based entities, delegations are weighted according to share ownership.

Below the owner level, three default groups (see Identity Access Management) are created:

- ◆ Contributors/Members: Representing all DAO contributors, not limited to owners.
- ◆ Developers: Entrusted with managing developer infrastructure via Tonomy Build
- ◆ Finance: Responsible for managing payments through Tonomy Bankless.

DAOs possess the flexibility to establish new groups, representing various internal departments or units, each with distinct permissions and responsibilities.[9]

Decentralised Identifiers (DIDs)

In Tonomy, all entities, including individuals, DAOs, applications, and smart contracts, are assigned decentralised Identifiers (DIDs). These entities can use DID infrastructure, such as W3C Verifiable Credentials and DIDComm. These mechanisms operate transparently across the network, underpinning verifiable private data and communications.

Verification Process

Identity verification occurs during application login and is funded by the application. This process ensures that each individual maintains only one account within the network. In cases where multiple accounts are detected, the additional accounts may be frozen, but one account will always remain active for the user. Verification operates as a modular plug-in that applications can select during deployment. At launch, a set of standard verification mechanisms will be implemented.

Governance Layer

The white paper delineates the requisite governance layers using the trias politica model while acknowledging the applicability of other models to this governance system. The model comprises three components:

- **Legislative Layer:** Tasked with formulating and upholding the policies/rules/regulations governing the ecosystem. These rules oversee the infrastructure, such as validator nodes and identity systems for people, DAOs, application rules, financial aspects like inflation rates, etc. The process and authority for policy-making form part of these modules.
- **Executive Layer:** Responsible for implementing and maintaining the policies. This encompasses the operation and upkeep of software and infrastructure, including remuneration for developers, administrators, lawyers, and payments to infrastructure node operators. Policies under ecosystem governance are executed within these features, adhering to Elinor Ostrom's principles of effective policy implementation.
- **Judicial Layer:** Charged with interpreting policies in dispute scenarios. This involves an arbitration system capable of enacting positive reinforcements or sanctions to uphold policies in compliance with arbitration standards.

The flexible and modular approach using DAOs and groups allows the governance system to separate these three powers into separate groups of actors.

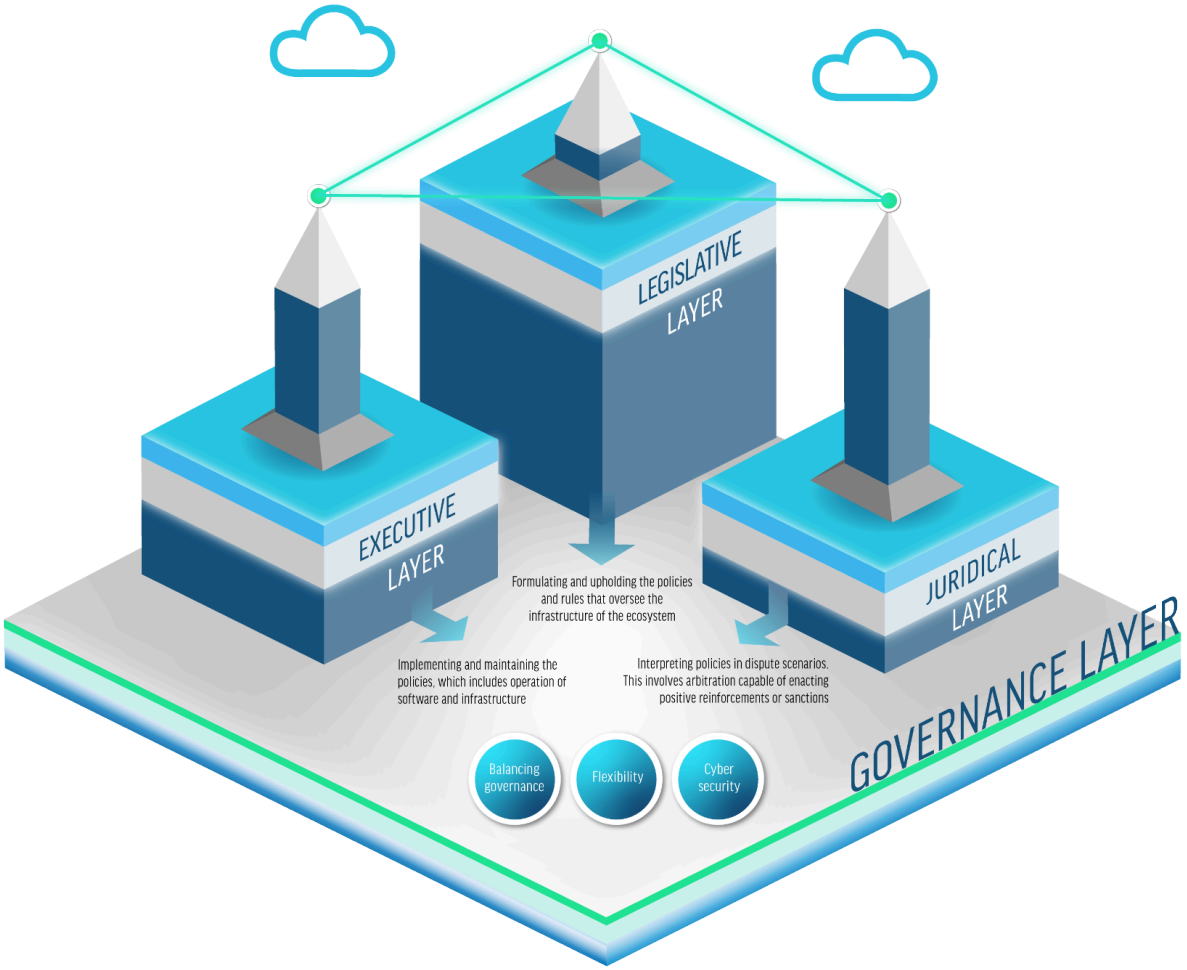


Figure 15: Governance Layer

State-Nation Governance comparison:
Traditional governance models heavily favour state-nation power. In contrast, Tonomy's technologies offer flexibility for governments to balance governance power between state-nation and lower governmental levels, promoting adaptability and versatility.

Cryptocurrency/Cardano Comparison:
Unlike most cryptocurrencies that rely on singular, financially incentivised governance models (proof of stake or similar), Tonomy supports both financial incentive models and truly democratic approaches (one person, one vote). It also advocates for a modular and upgradable governance framework, accommodating ecosystem evolution and growth.

In addition, all or most of the governance and administration decisions and configuration must be done by developers still using developer tools. In Tonomy Gov+, the no-code platform allows non-developers to easily participate in decisions and execution of core ecosystem and DAO management.

Legislative Layer

The Tonomy DAO platform is endowed with sophisticated governance mechanisms at its zenith, providing comprehensive control over ecosystem governance. These intrinsic capabilities enable a variety of democratic and equity-based voting systems, encompassing direct, representative, or liquid democratic frameworks. This structure forms the cornerstone for collective policy development and regulation within the ecosystem, thereby metamorphosing it into an expansive, integrated Decentralized Autonomous Organization (DAO).

The Modular Programmable Consensus Algorithm, intrinsic to the blockchain architecture, empowers Tonomy with the ability to support programmable and modifiable governance structures (e.g. democratic). This flexibility allows for the implementation of various legislative models, such as democratic systems, at the protocol level.

Executive Layer

The execution of governance functions within the system is partially automated.

The network's fee and incentive scheme operates on full automation, ensuring protocol-level enforcement. This approach minimizes trust requirements and reduces financial impediments in the network's high-priority economic framework.

Additional executive functions are facilitated through discussion forums and communication platforms, or via Tonomy's core applications. For instance, manual disbursements from the Treasury to contributors are conducted using the Tonomy Bankless application.

Estonia comparison:
Estonia has conclusively fortified themselves as a leading digital ecosystem provider.[10] Their digital infrastructure leads policy-making and has shown to significantly reduce friction.

Tonomy provides the core services of identity, chamber of commerce, government and finance, however it does this in a way where no infrastructure provider is in total control of any of these core systems. Equally importantly, no ecosystem members personal data is stored in a government database as seen in Estonia. Both these features significantly enhance the cyber security edges of the ecosystem as a whole as well as bolster privacy and trust for Tonomy ecosystem members.

Judicial Layer

The arbitration platform is pivotal in interpreting and applying approved ecosystem policies, utilizing evidence to deliver verdicts and enforce said policies. Judicial authority is granted privileged capabilities, including the issuance of de-anonymized warrants or fines, to safeguard the ecosystem's users. These exclusive judicial powers are detailed in the Warrants section.

Ecosystem participants can utilize this framework to enforce various ecosystem policies, including contractual agreements, subject to the specific policy configurations of the respective ecosystem.

Execution and Data Layer

The execution layer comprises an array of data consistency, consensus, and storage services, meticulously architected to satisfy the exigencies of identity, governance, and application strata. These services are tailored for high throughput and high availability within distributed architectures, emphasising minimal to no reliance on the trustworthiness of technical service operators. This objective is attained through an amalgamation of advanced cryptographic techniques and distributed systems computing methodologies.

Central to the execution layer is the **blockchain network**. It is a pivotal distributed execution framework, endowing the network with robust identity, DAO, and governance functionalities. Additionally, it provides a versatile distributed programming interface conducive to developing decentralised applications in private market sectors. The blockchain's role extends to being the unequivocal source of truth, guaranteeing uniformity and consistency across the service ecosystem. Predominantly, it facilitates authentication via decentralised Identifiers and orchestrates ordering services to maintain data coherence.

The data storage dimension is bifurcated into two distinct services:

- **Private Data Storage:** This service is dedicated to housing data that remains confidential and unseen within the ecosystem. It adheres strictly to data regulation norms and is specifically engineered to securely store private, personal, and organisational data. Primarily, it supports backup and recovery processes for data housed in the sovereign storage of Tonomy ID and Tonomy DAO.
- **Public Data Storage:** This service is earmarked for storing data that is openly accessible across the ecosystem. Employed exclusively when personal information is not implicated, it ensures adherence to data privacy regulations. Its primary use includes creating public profile information for DAOs and configuring application settings, such as security policies.

Furthermore, the network incorporates a **communication service** facilitating peer-to-peer private data transfer among various identities. The **identity verification bridge** is an instrumental service enabling third-party identity verification providers to integrate their verification proofs into the network. Additionally, a **key recovery service** is in place to offer a low-trust mechanism for backing up and restoring encryption keys utilised in the sovereign storage vault, thereby supporting comprehensive data backup during account recovery processes.

All services in the Tonomy Execution and Data Layer use the standardised decentralised Identifiers as the primary means for authentication and cryptography. Using the W3C standards supports compatibility and compliance with government and enterprise solutions while adhering to the required strict privacy and security requirements.

The execution and data layer services are partially underpinned by existing, proven technologies that meet the specified technical requirements. Concurrently, developing

proprietary new software is undertaken to bridge any gaps. The Tonomy Foundation's commitment to these technologies is not inflexible; adaptations may be made in response to emergent superior technologies or evolving requirements emanating from the application, identity, and governance layers.

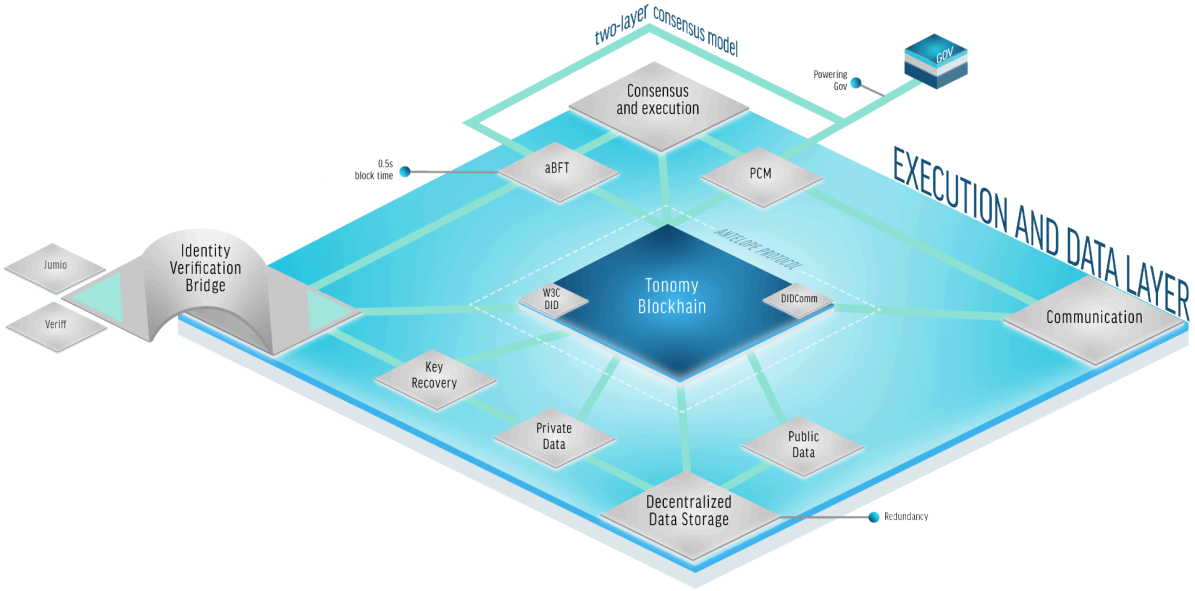


Figure 16: Execution and Data Layer

Blockchain

The Tonomy Blockchain, with its advanced features and adaptations of the Antelope protocol, aligns seamlessly with the multifaceted requirements of businesses, enterprises, and governmental entities. At its core, Tonomy offers a robust, scalable, and secure infrastructure that is crucial for these sectors, ensuring the ability to handle high volumes of transactions with efficiency and reliability. This is particularly vital for enterprises and government entities that deal with large-scale data and transaction processing.[11]

The Tonomy Blockchain exemplifies a paradigm of adaptation and enhancement in the blockchain domain. The core protocol of Antelope is being customised through on-chain programmable governance features, enabling the tailoring of network attributes to meet specific requirements of diverse ecosystems. This is achieved by leveraging modular components and configurable on-chain settings, thus providing a foundation for a wide range of applications, including governance and participation systems, employee identity for enterprise, decentralised finance (DeFi), supply chain management, non-fungible tokens (NFTs), and gaming platforms.

Tonomy Blockchain will adapt and extend the core Antelope protocol by using the on-chain programmable governance features to tailor networks to the individual needs of the ecosystem. This will be done using modular components and configurable on-chain settings.

Antelope, supported by some of the most usable networks such as WAX, Telos, UX Network and EOS is renowned for its role in underpinning some of the most agile, secure, and user-friendly Web3 products and services, managing millions of transactions daily. The WAX

network alone has hosted over 13B transactions, more than 10 times that on the Binance chain.[12] The protocol's emphasis on vertical scalability is evident in its capability to process up to 10,000 transactions per second before implementing sharding techniques.

Antelope Protocol

The decision to base the Tonomy Blockchain on the Antelope protocol is grounded in a comprehensive evaluation of Antelope's distinctive features, each of which aligns with the strategic objectives of Tonomy in building a robust, scalable, and user-centric blockchain ecosystem.

Modular Account Abstraction

Antelope's modular account structure is a key differentiator. This feature allows for the customisation of account types and permissions, catering to diverse user needs. This modular approach provides the flexibility necessary for Tonomy to implement nuanced access controls and identity management systems, a crucial aspect for DAOs and individual users.

Scalable Transaction Throughput

The protocol's capability to handle 10,000 transactions per second (tps) before sharding is a testament to its scalability. This high throughput is vital for Tonomy Blockchain, as it ensures that the network can accommodate a large volume of transactions without sacrificing speed or efficiency, a critical requirement for applications ranging from micro-transactions in DeFi to high-frequency trading systems.

Capability to Scale to 1 Billion Accounts

The ability to scale to 1 billion accounts is a significant feature that underscores Antelope's capacity to support many users. This scalability is essential for Tonomy's vision to create a blockchain network that is not only powerful but also inclusive, catering to a global user base.

Low Latency with Rapid Finality

Antelope's low latency, characterised by 0.5-second blocks with 4-second finality, ensures quick transaction confirmation times. This is crucial for Tonomy Blockchain's aim to provide a seamless and efficient user experience, particularly for applications requiring real-time interactions, such as gaming or live auctions.

Modular Programmable Consensus Algorithm

The Antelope consensus algorithm exhibits remarkable flexibility, crucial for the implementation of diverse governance models within the Tonomy Blockchain. This flexibility is instrumental in facilitating the development of custom governance structures for distinct Decentralized Autonomous Organizations (DAOs) and community-driven initiatives. It significantly contributes to the promotion of a more democratic and decentralized decision-making framework.

This enhanced adaptability is achieved through a dual consensus layer model, comprising:

- **Native Consensus Layer:** This primary layer is integral to the block confirmation process, ensuring each block's finality (irreversibility) through an asynchronous

Byzantine Fault Tolerant (aBFT) methodology. The native consensus layer is responsible for determining the finality of blocks, which are received and synchronized among elected producers. It operates on a schedule proposed by the political consensus layer, utilizing this schedule to authenticate blocks signed by the designated producer. For Byzantine fault tolerance, it employs a dual-phase block confirmation mechanism, wherein a two-thirds supermajority of producers from the current scheduled set are required to confirm each block twice. The initial confirmation phase designates a Last Irreversible Block (LIB). The subsequent phase ratifies the proposed LIB as final, rendering the block irreversible. This layer also plays a pivotal role in signaling potential changes in the producer schedule at the onset of each scheduling round.

- **Political Consensus Layer:** This secondary layer is pivotal in determining the producer schedule for participation in the native consensus. The configuration of this layer is executed programmatically via on-chain smart contracts. Consequently, the political consensus model can be diversified in numerous ways, including democratic, proof of stake, proof of share models, or any other programmable structure on the blockchain.

This two-tiered consensus model underscores the Tonomy Blockchain's commitment to a versatile and adaptable governance system, catering to the specific needs of various DAOs and fostering a more inclusive and decentralized decision-making ecosystem.

Flexible Programmable Transaction Fee Model

Antelope’s transaction fee model, which can be programmed and adjusted, allows Tonomy to optimise costs for users and developers. This flexibility is essential for maintaining a competitive edge in the blockchain space, where transaction fees can be a significant barrier to adoption.

Upgradable Webassembly Smart Contracts

The support for upgradable WASM smart contracts, particularly in a widely-used language like C++, GoLang, Python and Rust, enhances the robustness and longevity of applications built on the Tonomy Blockchain. This feature allows for continuous improvement and adaptation of smart contracts, aligning with Tonomy’s commitment to innovation and future-proofing its ecosystem.

EVM Support

The support for Ethereum Virtual Machine (EVM) makes Antelope highly compatible with a vast array of existing Ethereum-based applications and developer tools. This compatibility is crucial for Tonomy in facilitating easy migration and interoperability with the broader blockchain ecosystem.

Sustainable Footprint

Antelope’s design considerations for environmental sustainability resonate with Tonomy’s commitment to eco-friendly technology solutions. This aspect is increasingly important for both users and developers who are environmentally conscious.

Extended Features

The Tonomy Blockchain, utilising the Antelope protocol as its foundational framework, is poised to introduce several pivotal extensions to the protocol's existing features. These enhancements are meticulously designed to elevate the blockchain network's efficiency, security, and adaptability. The areas of extension include:

Modular Governance and Consensus Systems

The Antelope protocol employs a two-layer consensus model: a) Layer 1 - Native Consensus Model (aBFT) and b) Layer 2 Programable Consensus Model (PCM). Tonomy Blockchain aims to further develop this model by creating more sophisticated modular consensus systems on top of the programmable consensus layer. This advancement will enable a more dynamic and responsive governance structure tailored to the specific needs of various applications and use cases within the Tonomy ecosystem.

Manageable Transaction Fee and Resource Management

Antelope's platform allows for programmatic resource management and a flexible business model, enabling applications to adopt various models like a freemium model for executing transactions. In addition to these features, Tonomy Blockchain intends to refine the transaction fee and resource management system, making it more manageable and user-friendly. This will likely involve optimising the allocation and utilisation of key resources such as RAM, CPU, and Network (NET) bandwidth, all of which are integral components of the Antelope-based blockchain system.

Standardised Identity Account Structures

While the document does not provide specific details on standardised identity account structures, the Tonomy Blockchain is expected to build upon Antelope's comprehensive permission system. This system allows for creating custom permission schemata, enabling the development of permissioned applications atop a flexible infrastructure. Standardised identity account structures would further streamline and unify the approach to identity management across the Tonomy Blockchain, enhancing security and ease of use.

Account Delegations and Multi-Signature Permissions for DAOs

The Antelope platform's comprehensive permission system supports splitting the authority required to modify a smart contract across multiple accounts, each with varying levels of authority. Leveraging this capability, Tonomy Blockchain plans to strongly utilise account delegations and multi-signature permissions to create DAOs that are highly secure and user-friendly. This approach will likely involve devising intricate permission and delegation mechanisms that ensure robust security while maintaining operational efficiency and flexibility.

Tonomy Blockchain

The integration of the Antelope protocol within the Tonomy Blockchain represents a strategic alignment of advanced blockchain capabilities with the specific functional needs of a diverse and evolving digital ecosystem. Here, we delve into the depth of how Tonomy Blockchain will utilise the Antelope protocol:

Single Source of Truth for Infrastructure Services

The Antelope protocol will act as a foundational ledger, providing a reliable and immutable record of transactions and interactions across the Tonomy ecosystem. This will ensure consistency and reliability in data across all infrastructure services.

By serving as the central reference point, the protocol will streamline integration with various services like smart contract execution, data storage, and network communication, ensuring that all components operate with a synchronised and accurate dataset.

Single Source of Truth for Authentication

The blockchain will store public keys and hashes, enabling the secure verification of authentication and off-chain data. This feature is crucial for maintaining data integrity and transactions that originate outside the blockchain but require validation and incorporation within the ecosystem.

Identity Management, decentralised Identifiers, IAM, and CIAM

decentralised Identity (DIDs): Tonomy will leverage Antelope's capabilities to facilitate creating and managing decentralised identities (DIDs). This approach enhances user privacy and control over personal data.

Integrated Access Management (IAM): The protocol will enable a robust framework for managing access to network resources, ensuring that only authorised users can perform specific actions based on their identity and role.

Customer Identity and Access Management (CIAM): CIAM capabilities will allow Tonomy Blockchain to manage customer identities, preferences, and consent, delivering a seamless and secure user experience.

Token Management

Antelope's token management capabilities will be utilised to create and manage various tokens within the Tonomy ecosystem. This includes utility tokens, governance tokens, and others, with features like transferability, divisibility, and programmability

The system will support privacy-centric tokens, facilitating anonymous transactions with the ability to comply with regulatory requirements through controlled de-anonymization mechanisms.

Governance

DAO Governance: The protocol will underpin the governance mechanisms for DAOs within Tonomy, allowing for democratic decision-making and stake-based governance models.

Flexible and Programmable Governance: With Antelope's modular programmable consensus algorithm, Tonomy Blockchain can implement various governance and system management models. This flexibility ensures that governance structures can evolve with the needs of the community and ecosystem.

Communication

In Tonomy's advanced communication infrastructure, the adoption and enhancement of DIDComm features play a pivotal role. This sophisticated communication service integrates a WebSocket DIDComm transport, ensuring secure, private, and interoperable messaging capabilities across the Internet. This system is particularly notable for its high latency, privacy, security and reliability.

The Tonomy Communication Infrastructure, with its integration and extension of DIDComm features, is exceptionally well-aligned with the stringent and multifaceted requirements of businesses, enterprises, and government entities. Firstly, the infrastructure's emphasis on secure and private messaging resonates strongly with the critical need for data confidentiality and integrity in these sectors. The use of WebSocket DIDComm transport ensures that communications are secure and adhere to globally recognised standards, a key consideration for organisations operating in regulated environments.[13]

The infrastructure's commitment to privacy and security is paramount for businesses and enterprises, particularly those dealing with sensitive customer data or proprietary information. The fully managed keys feature simplifies the complexity of cryptographic security, allowing enterprises to benefit from high-level security protocols without needing in-depth technical expertise. This aspect is crucial for businesses that prioritise data protection but may not have the resources to manage complex security systems.

In the context of government entities, the infrastructure’s interoperability across different identity systems is a vital feature. It allows seamless communication and data exchange across various departments and agencies, many of which may use different systems and protocols. This interoperability is essential for efficient governance and service delivery.

DIDComm

The decision to employ DIDComm as the foundational technology for the Tonomy Communication Infrastructure is underpinned by many considerations, all of which align with the overarching objectives of security, privacy, interoperability, and user sovereignty.

- **Global Standardization:** DIDComm's recognition and support by the World Wide Web Consortium (W3C) positions it as a contemporary global standard, offering a reliable and universally accepted framework for digital communication.[14]
- **Self-Sovereign Identity Support:** DIDComm's architecture inherently supports self-sovereign and autonomous identity management,[15] a cornerstone in our commitment to empowering users with control over their digital identities.
- **Interoperability Across Identity Systems:** DIDComm demonstrates remarkable interoperability, functioning seamlessly with various identity systems, including web applications, Bitcoin accounts, and emerging identity frameworks. This flexibility is crucial for a network aspiring to widespread application and integration.
- **Transport Agnosticism:** As highlighted in the document, DIDComm is transport-agnostic, capable of operating over a range of protocols including HTTPS, WebSockets, Bluetooth, URLs, QR Codes and more. This adaptability ensures that communication remains uninterrupted and efficient, regardless of the underlying transport mechanism.

- **Advanced Privacy and Security Features:** DIDComm strongly emphasises preserving the integrity of messages and the authenticity of senders, employing state-of-the-art cryptographic techniques. It also offers features like onion routing, enhancing privacy by preventing unauthorised parties from discerning communication details.

Tonomy Communicate, by incorporating DIDComm, takes a significant leap in optimising the potential of decentralised communication, particularly through implementing fully managed and sovereign keys. This enhancement represents a critical innovation in the realm of secure and autonomous digital communications, aligning with the overarching goals of the Tonomy to prioritise user sovereignty and security.

Communication in Tonomy Networks

Communication will be employed in various facets of Tonomy networks:

- **Device-to-Device Communication:** Facilitating secure messaging between a user's multiple devices, such as a phone and desktop.
- **User-to-User Interaction:** Enabling encrypted messaging between users, akin to a secure messaging app.
- **User-to-Application Communication:** Allowing users to transmit verification information and other data to applications securely.
- **User and DAO Interactions:** Providing a secure channel for users to communicate with DAOs for activities like sending invoices.

Private Data

The private data layer within the Tonomy ecosystem represents a groundbreaking approach to managing sensitive information in digital environments. This layer is meticulously designed to cater to the specific needs of businesses, enterprises, and governmental entities, ensuring the confidentiality and integrity of their data. The layer offers a secure, decentralised framework for data management and operations by leveraging advanced encryption technologies and self-sovereign identity principles.

In a business and governmental context, the private data layer provides a robust platform for handling confidential data, including personal information, trade secrets, and sensitive governmental records. It ensures compliance with various data protection regulations, such as GDPR, while offering a flexible and secure data storage and access solution.

The Tonomy ecosystem extends the concept of private data by using fully managed self-sovereign keys. This innovative approach enables entities to maintain complete control over their data, ensuring that the data owner's policies govern access and encryption and not by third-party service providers.

Client-Side Encryption

Client-side encryption in the Tonomy ecosystem ensures that data is encrypted at the user's device before it is transmitted or stored on any server. This method employs advanced cryptographic algorithms to secure data. Even during transit or at rest, the data remains

encrypted, thus safeguarding it from potential vulnerabilities in the transmission channels or storage systems.

DID Authentication

Decentralised Identifiers (DIDs) are a cutting-edge solution for authentication in the Tonomy ecosystem. DIDs allow users to prove their identity without relying on centralised authorities. This decentralised approach not only enhances security but also provides users with greater control over their personal information. It mitigates risks associated with centralised identity repositories.

Advanced Encryption with Indexing and Search

This feature is a breakthrough in handling encrypted data. The Tonomy ecosystem uses specialised algorithms that allow for the indexing and searching of encrypted data without ever decrypting it. This capability means users can perform efficient searches and access operations on their encrypted data without compromising its security, a vital feature for businesses that require both security and efficiency.

Recovery of the Sovereign Storage Vault

The recovery mechanism for the sovereign storage vault addresses scenarios where a user might lose access to their device or forget their passphrase. The Tonomy ecosystem implements a secure recovery process that involves multiple layers of authentication and can include biometric verification, multi-factor authentication, and trusted recovery contacts. This process ensures that users can regain access to their data without exposing it to external vulnerabilities.

Warrants

Data access warrants can be claimed by proving that there has been some form of identity fraud or security or policy breach. In this case, prosecutors who go through the process of presenting proof and being approved can receive a data access warrant. This will allow the prosecutor to request data from another user's account, as well as retrieve a set of encryption keys they will be able to use to decrypt the data and inspect it for their security purpose.

Public Data

The Public Data Layer of Tonomy is a sophisticated digital architecture designed to generate and manage public data within the Tonomy ecosystem. This layer serves as a pivotal component for many users, including businesses, enterprises, and governments, by facilitating the creation of public profiles for DAOs and providing essential configuration data for applications. These functionalities are crucial during user login and interactions, ensuring a seamless and efficient user experience.

This layer is adept at handling public data, encompassing information that must be accessible across the Tonomy ecosystem. This includes but is not limited to, public profiles of DAOs and configuration details of various applications essential for user interaction. The Public Data Layer thus stands as a cornerstone in Tonomy, empowering a range of

stakeholders by providing them with the necessary tools and information for effective decision-making and operations.

A key innovation of the Public Data Layer lies in its approach to extending the concept of data ownership. Utilising fully managed self-sovereign keys, this layer introduces a paradigm shift in how data ownership is created and verified. By implementing self-sovereign key management, the layer enhances data ownership and security, allowing users complete control over their information.

DID Authentication and Encryption

The Public Data Layer employs decentralised Identifier (DID) technology for robust authentication and encryption. This feature ensures that each user's identity is securely verified and their data is encrypted, providing a high level of security and privacy. The use of DIDs in the Public Data Layer signifies a commitment to maintaining a secure and trustworthy environment within Tonomy.

Flexible Modular Data Structures and Searching

Flexibility are at the core of the Public Data Layer's design. It supports modular data structures, enabling users to tailor the data architecture to meet their specific needs. This modularity extends to the layer's search capabilities, offering a versatile and user-friendly search experience that can handle complex queries efficiently.

Supports Data Streaming and Storage Model

The layer is equipped with a sophisticated data streaming and storage model. It can handle both event- and state-based storage, allowing users to choose the model that best fits their requirements. This feature is particularly beneficial for applications requiring real-time data streaming or maintaining a historical record of data changes.

Indexing and Fast Querying

Efficient data retrieval is a critical aspect of the Public Data Layer. It supports advanced indexing mechanisms, enabling fast and efficient querying of the stored data. This feature is essential for applications that require quick access to large volumes of data and for users who need to make timely decisions based on the retrieved information.

High decentralisation and Availability

The Public Data Layer is highly decentralised, ensuring that the data is stored across multiple nodes in the network. This decentralisation enhances the layer's resilience and reliability. Moreover, the layer is designed to be highly available, ensuring that users can access the data they need whenever needed, without significant downtime or interruptions.

Key Recovery

The Tonomy Key Recovery service is a proprietary technology created to allow accounts to solve only recover their encrypted software and data balls in case they lose/forget their primary recovery phrase.

Key recovery is just one part of the account recovery step. Before the encryption key is recovered, the user must first recover their authentication keys. This is covered in the Tonomy ID app in multiple ways.after the authentication key is recovered, this can be used to request that the encryption key be recovered.

Encryption key recovery with Shamir's Secret Sharing

The encryption key is a private key c created using random entropy on the user's device when they create an account or log in. This key cannot be used to authenticate the user to any service and cannot be used to move funds of tokens or modify any on-chain or off-chain assets or data. The encryption key is only used to encrypt and decrypt data on the client side from the sovereign storage vault backup service. In this way, the security of the user is protected even if the key recovery service network acts maliciously in consensus (very unlikely as many entities need to conspire and lie in synchronised secret).

The recovery protocol uses Shamir's secret sharing to split the encryption key into multiple shards on the user's device and send each show to a different service provider. Service providers use the user's DID and authentication (a different key) to verify the request comes from the correct account and then save the data. If the user loses their encryption key, they must go through account recovery to recover their authentication and then can request that the encryption key be recent to them.

De-anonymization with Warrants

The Tonomy governance system allows for warrants to be issued that allow prosecutors to get access to a user's personal information. This is only used in the cases where the prosecutor can provide sufficient evidence to show a safety concern by checking the user's personal information.

Key Recovery service providers, by default, will only accept requests for key shards from the user to whom they belong. The exception is when a warrant is used and provided, granting the request access to the key. This can then go on to be used with the same warrants to access, retrieve, and decrypt the user's personal information.

There are long-term plans to research and develop a system where these key shards are not stored on services (servers) but instead shared amongst many of the user's contacts. Tonomy Foundation is researching the use of trusted execution environments for additional security.

Identity Verification Bridge

The identity verification bridge service is used to bridge existing third-party service providers like Jumio or Veriff onto the network and provide reusability of verified identities.

These service providers bridge an identity verification request from the network to the third-party service. Once verification is complete, they wrap the proof provided by the third-party service in a W3C verifiable credential, which is then returned to the user. The user, due to the nature of verifiable credentials, is then able to freely use this as proof of their identity and reuse this over and over.

The identity verification bridge does not store identity data. The third-party service provider may retain data for their maximum retention period after which the data will only exist on the user's device.

Tokenomics and Security Framework

The tokenomics architecture within the Tonomy is strategically designed to ensure optimal **allocation and utilisation of system resources**. It simultaneously aims to incentivise resource availability and **prevent the overuse of resources** that could lead to denial-of-service attacks. The inner details of the resource allocation model are designed to stay hidden from users under normal operating circumstances, such that they should only manifest to a user that is trying to attack the system to prevent it, or when a user needs to add priority to their transaction to ensure execution.

This segment delves into the incentives associated with network infrastructure and the payment mechanisms that support these incentives. The network may necessitate additional fiscal considerations for compensating governing council members and other key contributors in governance services, such as judges and prosecutors within the arbitration system, which are handled through the governance Treasury feature based on ecosystem preferences. As these are not infrastructure critical features, ecosystem fund allocations such as governance and arbitration incentives are not part of the security framework.

The tokenomics system also serves as a streamlined and user-friendly payment mechanism, facilitating transactions between users, DAOs, and within the governance infrastructure. Its modular and configurable nature allows tailored monitoring and adaptation to meet specific ecosystem requirements.

The Tonomy - TONOTokenomics document outlines the specific tokenomics model to be implemented in the forthcoming Tonomy civilization launch through the TONOcurrency. Alternative network configurations may adopt different models.

Tokenomics Roles

The Tonomy network encompasses a diverse range of roles, each integral to its ecosystem's functionality and security:

- **People:** These are individuals actively participating in the network, engaging in transactions, governance, commercial and community interactions.
- **DAOs:** Collaborative legal entities formed by network participants, taking various legal forms like businesses and communities, and playing a vital role in decision-making and resource allocation.
- **Apps:** Software applications used for governance, commercial, and non-profit activities, facilitating operations and interactions within the Tonomy ecosystem.
- **Services:** Servers operating essential system services like blockchain nodes and identity verification, crucial for the network's stability and reliability.
- **Gov:** Specialized DAOs or groups of DAOs responsible for ecosystem governance, maintaining the system's balance and fairness.

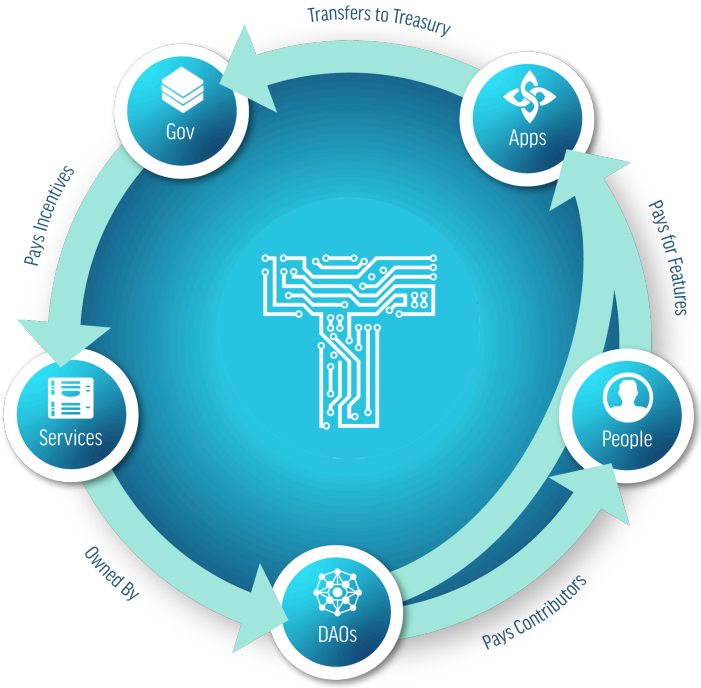


Figure 17: Tonomy Network Roles

Each role is pivotal to Tonomy's robustness and adaptability, contributing to its sustained growth and security.

Tokenomics Model

Figure 17 illustrates the flow of payments of the Tonomy native currency between the various roles in the network. These are:

- **Services** provide the digital infrastructure, including servers and other necessary elements for network operation.
- **Services** are automatically paid through the **Gov** treasury on the basis of the incentive structure of the network
- This treasury is funded from the payment of features through **Apps** by **People** and **DAOs**.
- Features offer both free and paid access, with **People** generally having some level of free-tier resource access based on identity verification, while **DAOs** pay for all feature usage.
- Services are owned by **DAOs** which are run by **People**. Gov is also a DAO.

In this way, a circular economy is generated. The accounting system underlying this facilitates the guaranteed availability of the network and insurers bad actors and not undermine the system.

This model is used to analyse the tokenomics of the system which are sound when both the following two conditions are met:

- **Economics:** when the payments into the Gov treasury are equal to the incentives out of the treasury.
- **Security:** when all underlying resources provided by each infrastructure service are guaranteed to always be available.

The model does not take into account additional optional features the ecosystems may decide to use the Tonomy native currency for such as incentives for contributors to the governance system or for use as legal barter for goods and services between DAOs and People, as these do not effect the security model.

Security of Core Network Resources

In the Tonomy system, each **Service** provides a set of digital infrastructure and exposes a **Core Network Resources** (CNR) accounting system used to account for the use of this resource. This is crucial to maintaining security and ensuring constant availability.

CNRs are completely hidden from most users. People will indirectly access these resources by purchasing them through monthly subscriptions or accessing network features through Apps. Only developers of apps need to worry about understanding CNRs. Developers will be able to purchase additional RAM for Apps, or expand their DAOs sovereign data vault through Tonomy Build.

Table 1 shows an overview of each Service and it's CNR that it offers.

Service	Core Network Resource (Units)	Description	Used by
Blockchain	RAM (bytes)	Data stored in smart contracts used by governance and core apps as well as DAO-owned apps. Such as account information, public keys, balances or more.	Apps, Services
	NET/CPU (priority unit)	Ability to send transactions within the network. Limited by the processing capacity of the blockchain network.	Identities, DAOs
Private Data	Private Data (Gb)	Data stored in the sovereign storage vault	Identities, DAOs
Public Data	Private Data (Gb)	Public data stored for public profiles	DAOs, Apps, Services
Comms	Messages (msg/s)	Messages sent between entities in the network	All
Key Recovery	Keys (bytes)	Shards of keys stored on the recovery notes	Identities
Identity Verification Bridge	Verifications (verifications)	Identity verification requests done through third-party identity verification services	Apps

Table 1: Core Network Resources

Each service handles the management of their resources differently. Each service also handles the data redundancy differently. By implementing an accounting system for each resource for each account in the network, Services can then easily create limits to ensure that network resources are guaranteed to always be available.

Paid Network Features

Fes are levied for accessing various features. The fee structure is diverse, covering a range of features. Table 1 Shows the network-based services and an example of the fee structure for those features.

For individuals

App	Service	Cost per month	Price unit
Tonomy ID	Pro account	Ø IdPro	per person

For DAOs

App	Service	Cost per month	Price unit
Tonomy ID	ID verification	Ø IdVerif	per verification
	Private data storage	Ø IdSovStorage	per Gb
	P2P Messages	Ø IdMessage	per 1M messages
Tonomy DAO	Pro account	Ø DaoPro	per company
	Incorporation	Ø DaoIncorp	per company
	Seat per person	Ø 1DaoSeat	per person
	Public data storage	Ø DaoSovStorage	per Gb
Tonomy Bankless	Escrow payments	Ø PayEscr	per transaction
	Payment authorizations	Ø PayAuth	per transaction
	Pro with advanced analytics	Ø PayPro	per company
Tonomy Build	App deploy	Ø DevApp	per app
	Smart contract deploy	Ø DevContract	per contract
	On-chain keys	Ø DevKey	per key
	Pro with advanced analytics	Ø DevPro	per company

Table 2: Example fees for network services

The fee model is flexible and can be adjusted based on the payment rates, units, or the period over which services are consumed (daily, monthly, etc.).

Service Incentives for Network Operators

All of the execution and data layer services are incentived within the ecosystem depending on it’s role and expenses.

Each Service has different pay rates based on their services using the following formular:

*Pay = PayBase + StakingRewardsFlag * (Staked Native Tokens / Total Staked Native Tokens) * StakePool + Expenses*

PayBase = base incentive
StakingRewardsFlag = Flag to turn off or on staking-based rewards
StakePool = Daily pool to be split based on stakes
*Expenses = Other operational expenses***

** Expenses are based on CNRs that are not already considered in the PayBase such as data stored for Public Data, or verifications for the Identity Verification Bridges.

Tokenomics Governance

The financial equilibrium of a Tonomy network is maintained using protocol enforced accounting using rules maintained by the governance system. The equilibrium is achieved when the combined fees from features equals the incentives paid to network operators.

Tonomy Build facilitates the configuration of these incentives. Pay rates for various server infrastructure services are based on factors like staked native tokens, operational expenses, and a daily funding pool from the Treasury.

The network incentives configuration panel also allows for the specification of the maximum number of nodes eligible for service registration, balancing the need for minimal service provision with equitable fee distribution among operators.

It is through the governance system that underlying prices and fee structures are monitored and updated through proposals. This core responsibility of the governance DAO ensures the network can grow and adapt to the network's needs which keeping the networks infrastructure layer secure and accessible.

References

1. Tom, Barbereau., Balázs, Bodó. (2023). Beyond financial regulation of crypto-asset wallet software: In search of secondary liability. Computer Law & Security Review, 49:105829-105829. doi: 10.1016/j.clsr.2023.105829
2. Team, P. (2023, October 23). Secure Multi-Party Computation (MPC): A Deep Dive. Panther Protocol Blog. https://blog.pantherprotocol.io/a-deep-dive-into-secure-multi-party-computation-mpc/
3. MacDonald. R (2022, August 19). Blockchain and passwordless authentication: Mitigating future cyberattacks with blockchain enabled. CIO AXIS. https://www.cioaxis.com/hottopics/security/blockchain-and-passwordless-authentication-mitigating-future-cyberattacks-with-blockchain-enabled-passwordless-authentication
4. Smit, A. (2020). Identity Reboot: Reimagining Data Privacy for the 21st Century. MintBit Ltd
5. Omar Hasan, Lionel Brunie, and Elisa Bertino. 2022. Privacy-Preserving Reputation Systems Based on Blockchain and Other Cryptographic Building Blocks: A Survey. ACM Comput. Surv. 55, 2, Article 32 (February 2023), 37 pages. https://doi.org/10.1145/3490236
6. Guskow Cardoso, A. (2023). Decentralized Autonomous Organizations - DAOs: the Convergence of Technology, Law, Governance, and Behavioral Economics. MIT Computational Law Report. Retrieved from https://law.mit.edu/pub/decentralizedautonomousorganizations
7. Schiener, D. (2018, June 20). Liquid Democracy: True democracy for the 21st century. Medium. https://medium.com/organizer-sandbox/liquid-democracy-true-democracy-for-the-21st-century
8. Moffat, S. (2021). Consumer Identity & Access Management: Design Fundamentals. Independently published
9. Law, A. W., Clinical Professor of Law at Benjamin N. Cardozo School of. (2021). The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges. Stanford Journal of Blockchain Law & Policy. Retrieved from https://stanford-jblp.pubpub.org/pub/rise-of-daos
10. Nyman-Metcalf, K. and Repytskyi, T. (2016). Exporting Good Governance Via e-Governance:
11. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 14(11), 341.
12. DappRadar. (2024). Top Blockchains - DappRadar. Retrieved from https://dappradar.com/rankings/chains?sort=transactionCount&order=desc&range=all"
13. Yildiz, H., Küpper, A., Thatmann, D., Göndör, S., & Herbke, P. (2022, August 8). A Tutorial on the Interoperability of Self-sovereign Identities. arXiv:2208.04692 [cs.SE]. Retrieved from https://arxiv.org/abs/2208.04692
14. Reed D, Sporny M, Longley D, Allen C, Grant R, Sabadello M, Holt J (2021) Decentralized identifiers (dids) v1.0: Core architecture, data model, and representations. https://www.w3.org/TR/did-core/, Accessed 25 May 2021
15. Enge, A., Satybaldy, A., & Nowostawski, M. (2022). An offline mobile access control system based on self-sovereign identity standards. Computer Networks, 219, 109434.