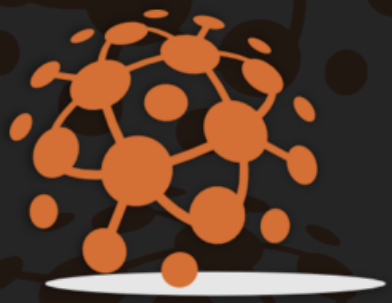
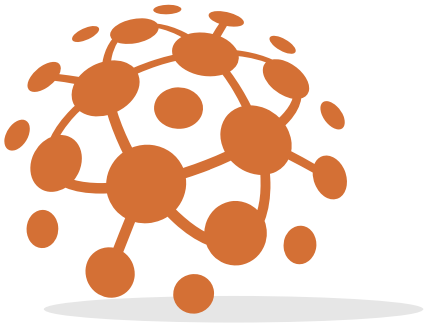
Litepaper



Privaceum®



Privaceum®

Table of Contents

Introduction

Privacy has eroded because traditional web 2.0 models set up individuals and companies in opposition to one another in a winner-takes-all scenario. Attempts at a solution have fixated on outmoded notice-and-consent paradigms and on individuals in isolation having privacy, disregarding the context in which privacy is relevant.

True privacy is contextual and collaborative. Privaceum recognizes that, in web3, we have the opportunity to coordinate incentives, governance, and transparency using a more powerful conceptual model that allows privacy to emerge from a network of trusted relationships.

Privaceum enables a decentralized, open-source privacy infrastructure on the blockchain. Our participant-governed, decentralized ecosystem provides a way for individuals and devices to communicate, interpret, and act in concert with one another's privacy expectations.

WHERE PRIVACY LIVES ON WEB3

At Privaceum, our vision is to create a privacy trust protocol that lets privacy be possible again using the power of web3. The blockchain is a key part of this vision. Using the blockchain, we can standardize the delivery and processing of privacy preferences, mediate conflicts between groups and individuals based on contextual norms, and monitor device compliance—all without reducing the usefulness of these devices for their intended purposes.

We believe that realigning data and privacy control with individual privacy expectations will bring a new level of interoperability and trust between people and organizations that care about privacy, re-energize the privacy conversation and, ultimately, imbue the Technosphere with a means of understanding and communicating human values across many domains.

THE PRIVACEUM BLOCKCHAIN

The foundation of the Privaceum protocol is a layer-1 blockchain developed in Rust using the Parity Substrate suite of tools. Current launch plans are to deploy as a parachain on the Polkadot network.

However, Privaceum goes further in its integration with Polkadot: it actually uses the DOT token rather than its own protocol token.

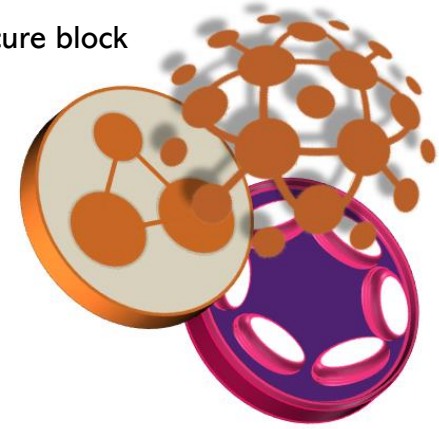
Using DOT for value exchanges between participants allows Privaceum to focus on its core mission—privacy—instead of on the tokenomics of its own protocol token. Participants can obtain DOT tokens using already existing mechanisms and use them seamlessly for Privaceum activities. They get the financial security of DOT's overall stability and widespread adoption.

DOT is only one part of our groundbreaking atokenomic model, discussed extensively later, in which we challenge and surpass the airdrop and other common methods that protocols use to encourage participation and healthy decentralized governance.

Privaceum is an "atokenomic" protocol powered by DOT on the Polkadot network

Being a member of the Polkadot network gives Privaceum several important advantages:

- Cross-chain composability across the entire Polkadot network, allowing Privaceum's primitives to be used in concert with other chains.
- Control of gas fees for transaction execution and storage affords Privaceum with complete flexibility to incentivize the right parties.
- Access to a large network of ready integration partners and BUIDLers with expertise.
- Ability to enable smart contract support so that integrators can add new capabilities safely and easily.
- Access to the existing Polkadot validator network for secure block authorship and consensus.
- Forkless upgradeability.



Privacy Awareness Network Identity Token

The Privacy Awareness Network Identity token (PANID) has a unique design that combines aspects of "soulbound" tokens (SBTs), which are non-transferably attached to an identity, with innovative NFT functionality such as configurability and composability. It is one of Privaceum protocol's fundamental units that function as chain primitives.

Different individuals have different privacy needs and expectations. One purpose of PANIDs is to define the boundaries of an identity's privacy expectations in a way that is reactive to changes in context, location, group, role, and other attributes.

Every PANID codifies an identity's privacy expectation "rule base." That rule base is itself made of composable, reusable privacy ruleset NFTs. This architecture enables the rule base to be accessible via the blockchain and readable by entities that want to understand an individual's privacy preferences across the web, blockchain/web3, robot, IoT, and wearable environments.

Privacy expectations organized in this way are not synonymous with identity, but are an important aspect of identity because they define how a person wants others to see or not see them in different roles and contexts.

The PANID primitive also contains additional aspects which enable integrators to extend PANID functionality by attaching new attributes, and even entirely new classes of attributes. This empowers integrators to build solutions for a range of related problems, such as identity, data marketplaces, personalization, inbound/outbound content control, and reputation.

RULESET NFTS (PANRS)

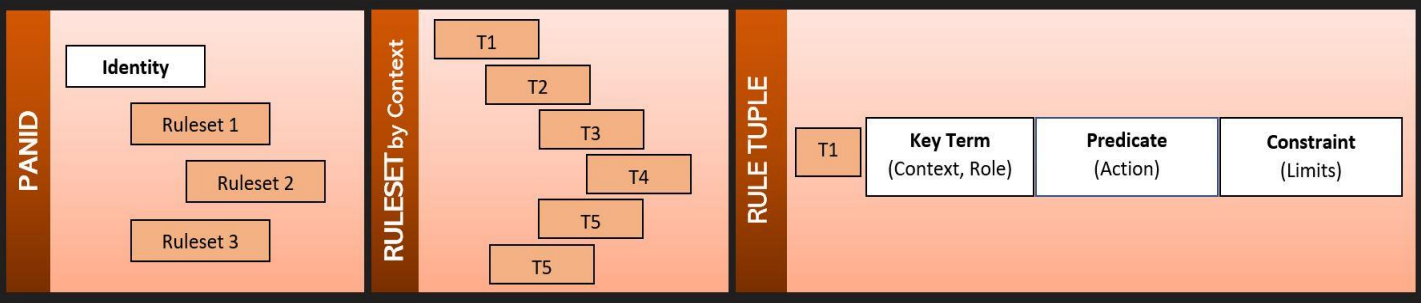
In Privaceum, we formulate privacy expectations so that they can be represented as “privacy rule tuples” describing the constraints we expect to be placed on a device’s behaviors in a given context and role. The sum total of our individual privacy tuples defines our “privacy identity”.

In most cases, a user’s context (derivable from where they are) and role (derivable from what they are) suggests or requires certain privacy constraints. Some constraints are dictated by law (e.g. health privacy laws such as HIPAA), others by rationality or cultural expectations. However, everyone doesn’t need, or want, to set up the rule tuples for these constraints themselves.

The Privaceum protocol is designed so that rule tuples are packaged into reusable units called "privacy rulesets" that define standardized groups of rule tuples for a context, role, or scenario.

The non-fungible token (NFT) framework, with a few extensions, maps quite well to a design for creating and sharing these privacy rulesets. In fact, in Privaceum, each of these rulesets is a type of NFT we call the PANRS NFT. The privacy identity token (PANID) either owns or holds a “use license” to one or more privacy ruleset NFTs.

Reusability of rule tuple collections as tokenized rulesets is beneficial not only in user convenience. It is also blockchain-efficient in terms of storage demands and gas fees — instead of the same rule tuple being stored multiple times, it can be stored once by the ruleset designer and “used” by multiple privacy identities. Updatability is also straightforward when new laws or norms demand that constraints for a context be modified.



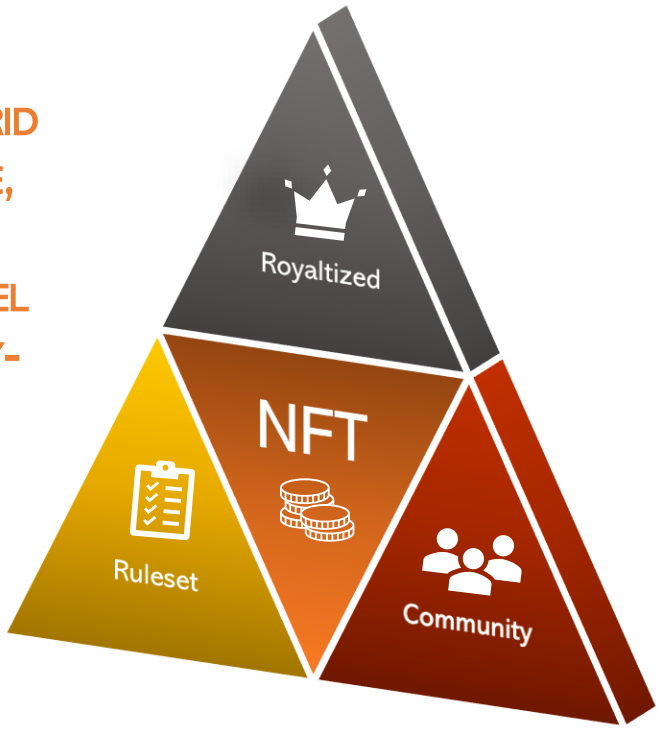
Privacy Ruleset Marketplace

The reusable, composable nature of a privacy ruleset means that ownership and responsibility for design and maintenance are separated from mere use. Since a builder of a ruleset is different from its users, keeping the parties aligned implies an incentive-based economic relationship.

Privaceum includes both royalty and governance models in the design for privacy ruleset NFTs. Each PANRS can have its own royalty model by which its builders are compensated when a privacy identity uses the PANRS as part of its privacy expectation definition in its PANID. Each PANRS can also have its own community-adaptive governance body by which a collective of individuals or entities forming a DAO can govern the design of its rule tuples.

Qualified third-party entities are able to form DAOs that set up rulesets with collections of rule tuples pertaining to one or more contexts and roles. These rulesets are then made available in a marketplace where PANID-holders can freely choose the rulesets used to define their privacy identities.

A ruleset token is a hybrid NFT that is composable, reusable, and has a royalty-paying use model paired with a community-adaptive governance mechanism



Privaceum has published and presented extensively on these topics. To explore further, have a look at Privaceum's Research Articles and Digitize Your Privacy with NFTs.

The Daoonomy

A fundamental idea behind Privaceum is that privacy is contextual. But, delineating the boundaries of context and collaborating to define the robust notion of context and related concepts necessary for a functional, practical privacy system is challenging in a blockchain.

We believe our Daoonomy is the key to solving these challenges. The daoonomy enables individuals and groups to work together to construct the schema and contextual hierarchies for privacy scenarios that are responsive to users' needs. The daoonomy is a universal way of thinking about the structure of shared concepts, values, and other taxa that allows them to be used by other systems as composable building blocks.

The daoonomy is made up of individual daoonomy sets, each of which hierarchically defines groups of related taxa. For example, the context hierarchy is a daoonomy set in Privaceum which defines functional or geographic location or situational boundaries. The role and predicate terms that round out the definition of a privacy tuple are also daoonomy sets.

To encourage sharing and collaboration, each daoonomy set can be created and adaptively governed by its own community. Each daoonomy set can also independently define economic incentives whereby the governing community is rewarded in proportion to the set's usefulness.

A Universe of DAOs

We built the Daoonomy for privacy, but its applicability is much more far-reaching. By structuring information so that it is reusable, composable, royaltizable, and governable by its own community, Privaceum enables a powerful new way of thinking about curating and sharing trusted information.

New Forms of Community

The Daoonomy can be a source of independently governed and adaptive shared concepts, values, and parameters that encourages entirely new models of community to grow. For instance, community-adaptive games in the metaverse might be developed in which the fundamental operational parameters change based on a player's chosen pathway in a daoonomy set defined by a community external to the game's developers.

New Ways to Reward Information Sharing

In fundamental contrast to the ways most markets reward information flows—by exploiting information arbitrage, or the difference between what different parties know—Privaceum's daoonomy rewards information flows that are shared, public, and useful. To the extent that communities create and share taxonomies of information that are useful to others, they are rewarded in direct proportion to their usefulness to the protocol.

New Uses for Shared Truth and Values

Autonomous agents such as ChatGPT/Bing run the risk of acting outside the boundaries of human value and human control. Many believe these agents constitute an existential risk to human life unless they are trained to understand and prioritize human values.

The Daoonomy can be an educational source for AI-bots operating on the blockchain and serve as a foundation for more generalized artificial intelligences in other systems. Individual sets governed by actual DAOs in an open and decentralized way can form the guiding concepts for how we want AIs to act on our behalf. An open, collectively-curated daoonomy set will communicate far better information about human normative behaviors and what humans truly value than the opaque processes by which AIs like ChatGPT are trained by their developers.

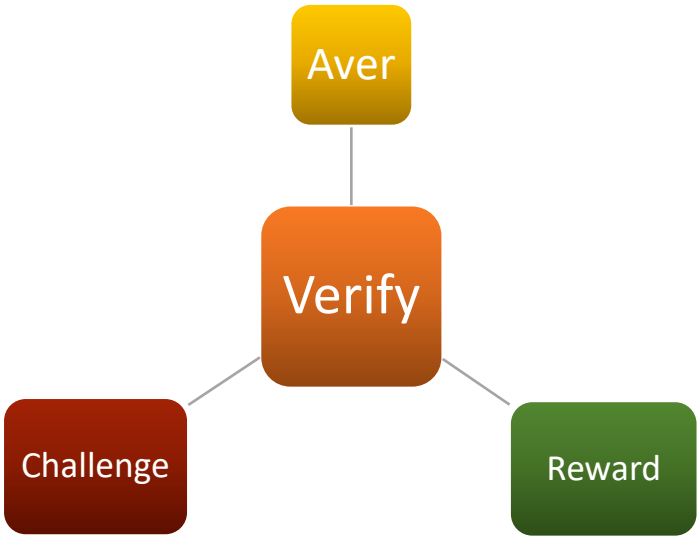
AVERIFY

We've described the protocol's methods of delineating and sharing a person's privacy preferences. But, as people familiar with the ways of Web 2.0 companies, how do we verify that a device or service is putting our preferences ahead of its own interests?

Privaceum's **Averify** ensures that a person's expressed privacy preferences are being respected by devices and services. With Averify, a privacy-impacting device "avers" (states "firmly and strongly that something is true") that it is acting in accordance with our privacy preferences when it collects and shares our data by submitting a package of confirmatory data with each privacy interaction.

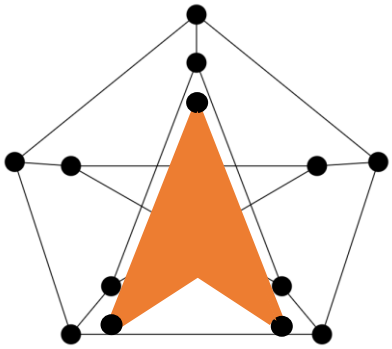
An independent auditor node will "verify" that this data package indeed confirms the adherence to the privacy preferences and convey a result. In addition, a challenger can call on the protocol to assess the accuracy of this result. The protocol incentivizes the good behavior of confirmatory data providers and auditors using a system of rewards, bond slashing, and corrections.

On a technical level, Privaceum aligns device and service behavioral control with human expectations; but, at a different level, we are cultivating the trust between technology and people that emerges when things continually act in the way they are expected to act.



Partial Knowledge Verification (PKV)

Averify is essentially an economy or marketplace in which entities can share data that proves a desired behavior was in accord with expectations. In Averify, the collaborating parties do not need to know one another's identity or have deep knowledge of one another's internal mechanics. But, with "partial knowledge" of the inputs and the end state of the data provider, it is possible for an auditor to assess whether the data provider acted within bounds. Outcomes over time may be used by others to evaluate the quality or reputation of data providers, as well as to reward, deter, or align the objectives of actors in a trust network.



On the surface, PKV resembles zero-knowledge proofs (ZKP), since an auditor only requires a subset of what the provider knows; however, PKV is focused on proving that outcomes or behaviors are acceptable within a flexible operational range rather than on proving a statement is true or known to the provider. It also requires the submission of confirmation data by the provider, which is by its nature more sophisticated, complex, less rigorously defined, and more dynamic than ZKP assertions.

In addition to privacy, the Averify functionality is applicable to a wide range of challenges in fields such as software validity, shipping and logistics, and proving assets, reserves, and deposits in various kinds of financial/defi instruments—basically any area in which one party needs to trust specific behaviors of another party. Privaceum's Averify is architected so that providers, auditors and the virtual models they use to verify data, the format of confirmation data packages, and the dApps which others use to understand provider quality are self-definable by the entities using them. This opens up the possibility for sophisticated verification markets and services to develop on Privaceum.

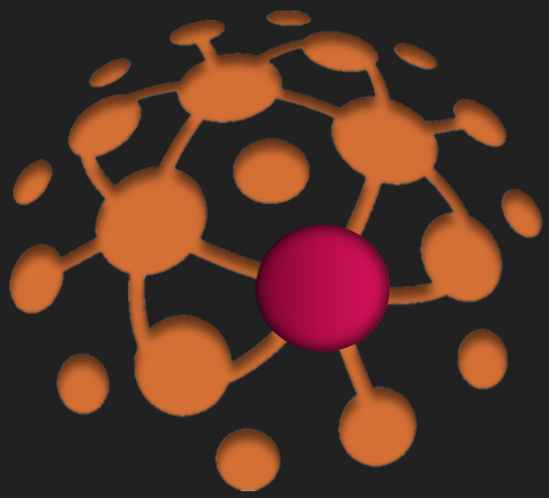
Privaceum's Atokenomics

Our “no token” protocol is a feature, not a bug.

Despite questions about whether every protocol needs its own token, almost all protocols launch with one. We took a different approach. For activities that require value transfers for gas, storage, or other fees, Privaceum uses the Polkadot network's master token, DOT. Using DOT for value exchanges between participants allows Privaceum to focus on its core mission—privacy—instead of on the tokenomics of a protocol token.

Users can obtain DOT tokens via already existing mechanisms and are afforded easy interoperability with the rest of the Polkadot network. Users spend and hold real DOT while our protocol grows, isolating them from the volatility of homegrown token economics schemes and speculators. Since the whole point of a layer-0 chain is that we all grow and benefit together, using DOT also makes the whole Polkadot network of chains more valuable, stronger, and more resilient.

A healthy protocol needs a way to encourage participants to do useful things, such as build and share privacy rulesets. Instead of an inflationary and inscrutable tokenomics scheme, our concept of "atokenomics" makes the fundamental driver of value on the network the usefulness of an entity's contribution rather than the quantity of a protocol token held. We measure the overall usefulness of participant activities with our Activity Impact Matrix (AIM).

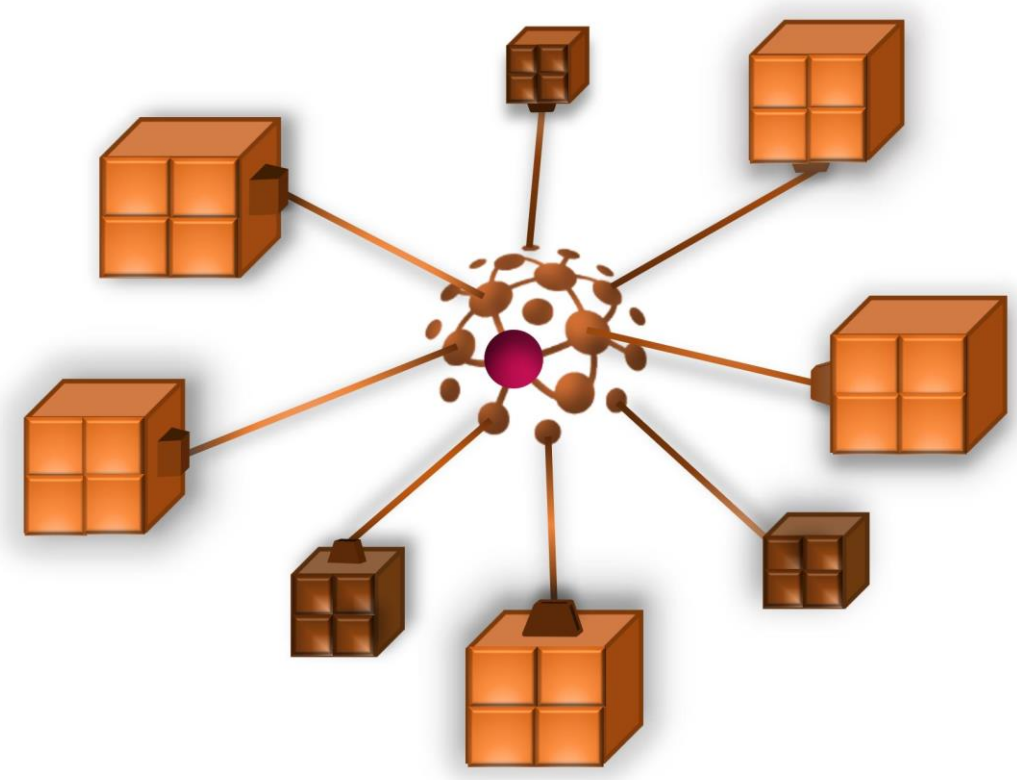


Participation and the Activity Impact Matrix

The Activity Impact Matrix (AIM) reflects the depth, complexity, and usefulness of a participant's activities on Privaceum. Every activity that any protocol participant does on the network improves or reduces their AIM, depending on whether the activity is positive or negative to the health of the network.

The AIM is intrinsic to understanding a participant's standing on the chain rather than just being an arbitrary computed number. The AIM is termed a "matrix" because it contains more than a single numeric measurement. Each individual AIM includes attributes that describe the momentum, diffusion, cohesion, and cumulative quantity of the participant's protocol activities--rather like a physical system has measurements that describe its temperature, volume, and density. The AIM also includes participant-specific weighting and conversion factors, as well as parameters for equations that describe how the various measurements translate into powers the individual has on the network (e.g., for governance or treasury share).

Attributes of the AIM can be used as a publicly accessible indicator of a participant's value to the chain. The AIM also has a real impact to both the participant's power on the protocol and to the participant's earned share of the chain treasury. This tangibly incentivizes participants to behave in ways that support the common goals of the chain.



Participation Means a Share of the Rewards

When you build something useful, more transaction and protocol fees are gathered in DOT from those using it, increasing the supply of DOT in the treasury. In Privaceum, everyone participating is entitled to capture value proportional to their own efforts to support the protocol. Factors in the Activity Impact Matrix (AIM) translate to a share of Privaceum's DOT treasury at the "participation valuation epoch" (PVE), which occurs a certain number of blocks after the participant first accrues certain AIM measurement minimums.

After their PVE, a participant becomes entitled to their earned share of the DOT in the treasury. This share is known as the earned treasury value (ETV), which is computed using the treasury exchange rate formula (PTX). The PTX considers the relation of the participant's AIM to all other participant AIMs, the amount of time the participant has been contributing, the quantity of available DOT in the treasury, and other scaling parameters.

HODLing and "Staking without Staking"

Although ETV can be taken as DOT at any time after the PVE, participants are encouraged in several ways to "HODL" their ETV rather than immediately withdraw it as DOT. In the first place, any withdrawals the participant makes into DOT are drawdowns of ETV against the current PTX. Since a key factor in the PTX is the length of time the participant has been contributing, withdrawing a portion of ETV earlier would sacrifice a more favorable PTX later. Second, as the size of the treasury grows, the participant is entitled to more DOT per AIM factor. Third, the participant's ETV can be spent for their own on-chain activities at a higher exchange rate than the withdrawal rate.

This model represents a new way of encouraging long-term participant engagement that avoids many of the pitfalls of airdrops and passive token staking.

Participants Are in Control

Privaceum protocol participants, all of whom collectively govern the chain, decide on the PVE block time and the AIM factors required for the PVE to begin countdown. They also decide on the modeling parameters that determine how the PTX converts AIM factors into ETVs. The amount of actual DOT held in the protocol treasury for earned participant shares is transparent to all participants at all times.

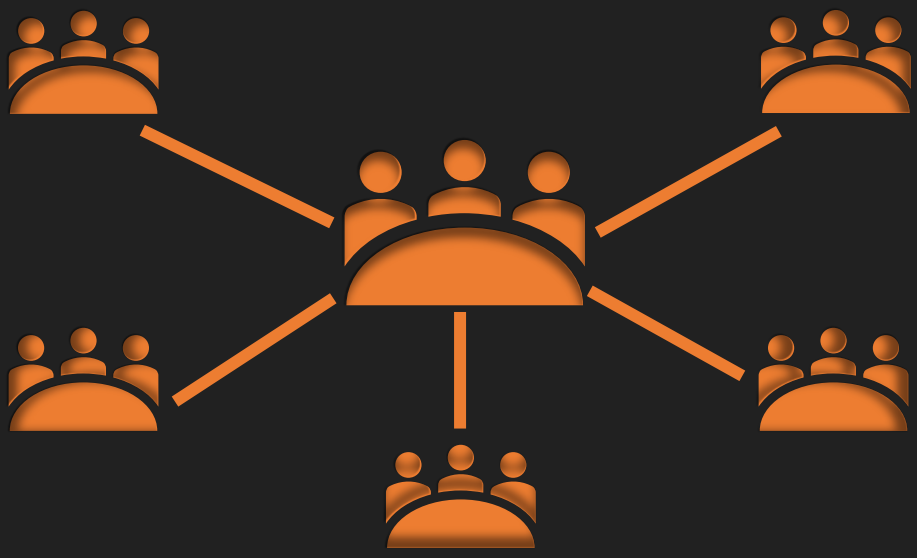
GOVERNANCE

Privaceum's participation model encourages better governance by entrusting the power to enact change to the people and entities whose activities are most supportive of the protocol.

Vote-per-token models of governance cause numerous issues that have to be fixed with other mechanisms. For example, governance power favors the largest token holders, who may have entirely different motivations than the long-term health of the protocol. Further, in a token-based governance system, a token-holder can diminish their governance power by actually spending token on the protocol. This opposing dynamic de-incentivizes a token-holder's participation in the protocol in order to preserve their holding/governance power.

In Privaceum, by contrast, the factors in the Activity Impact Matrix that determine the earned share of the treasury are conceptually separate from those determining governance power. The power of a participant to influence governance does not decrease simply because the participant takes a portion of their accrued ETV from the treasury.

This model fosters the formation of a true DAO by placing the greatest share of influence over the protocol in the hands of the highest quality participants.

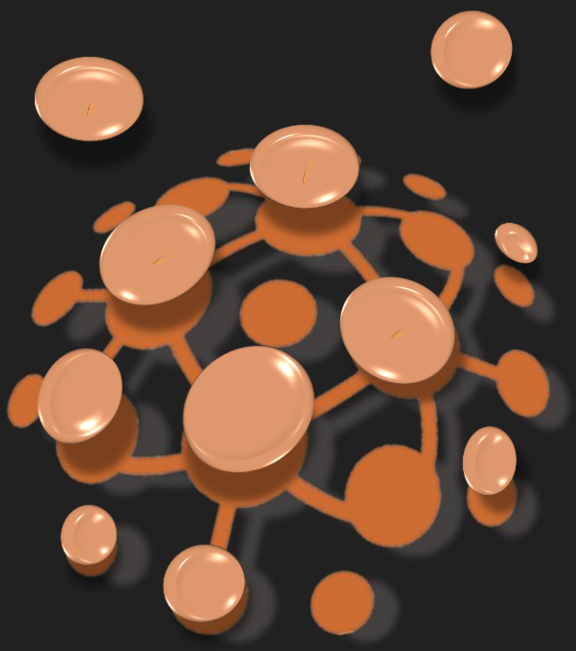


Integrators are Integral

The Privaceum protocol provides the architecture and a rich set of built-in primitives to solve privacy-related problems. To summarize, complex hierarchies of terms, such as the context daoonomy set, can be built and governed by their own DAOs. A sharing marketplace for rulesets describes how privacy can be delineated discretely, flexibly, and reusably. Identity primitives, as well as tools for verification of complex data sets, are built in. The atokenomic model of Privaceum encourages and rewards participation in the chain by the right types of actors.

Atop this infrastructure, Privaceum provides a rich model that encourages BUIDLers to use our tools for creating new capabilities that are both essential and tangential to the privacy domain. Opportunities and revenue models for participation and deep integration exist on many levels, ranging from defining contextual privacy rulesets and daoonomy sets, to operating an Averify auditor node, to building bespoke dApp experiences for specific Privaceum participant audiences, to integrating via the protocol's smart contract tools to create entire new categories of services that utilize our privacy-related primitives.

Keep reading to explore just a few ways to participate and integrate with Privaceum—but the ways are limited only by your imagination!



Collaborative Creation

A privacy protocol needs a nuanced understanding of the contexts, roles, actions, constraints, and parameters that describe privacy. Our royalty and participation model encourages a variety of participants to engage in a collaborative effort to define those aspects. For example:

- Create a daoonomy set
- Propose changes to a daoonomy set
- Vote on proposed changes to a daoonomy set
- Create an attribute extension to an existing daoonomy set
- Create a privacy ruleset that describes privacy tuples for specific contexts or user groups
- Share a privacy ruleset to the ruleset marketplace for others to use
- Join a shared ruleset's DAO governance body to propose and/or vote on changes to a ruleset

Decentralized dApp Ecosystem

Privaceum does not have a centralized frontend dApp. It instead incentivizes integrators to develop and deploy their own customized dApps to serve different privacy end-user vertical markets, support the needs of different participant capabilities within the protocol (e.g., auditor node management), and support seamless integration with other blockchains or Polkadot parachains.

This model encourages a robust level of buy-in within the developer community, optimizes the protocol for resilience, and provides avenues for engaging many different user bases.

Averifiers

Privaceum encourages good behaviors on the part of participants at all levels in the protocol. One way it does this is by engaging participants in a "partial knowledge verification" exchange that affords a participant the opportunity to claim, then enlists an auditor to confirm, that the claimant is acting as expected.

There is a revenue model in Privaceum supporting each of the following roles and activities:

- Devices/services who submit confirmatory data proving their responsible use of privacy expectations and agreeing to post a bond staking their good behavior
- Auditors who review the confirmatory data and assess whether it passes or fails
- Challengers who demand a second audit to review the first audit
- Integrators who define action/constraint models that different types of devices and services can use to control their systems in accord with users' privacy expectations
- Integrators who define verification models that auditors can plug into auditor nodes to assess different types of confirmatory data packages

Unchain Privaceum

Privaceum includes smart contract features that allow developer-integrators to build entirely new capabilities leveraging the building blocks of the chain.

Some integration opportunities for new features and capabilities include:

Data Sharing Marketplaces

Privaceum's foundational technology facilitates robust control over the data gathering capabilities of devices and services. Integrators can build on this foundation of privacy preference primitives to create a decentralized data-sharing marketplace that re-orients the rewards for shared personal and behavioral data back to the end-user.

Preference Systems

Privacy preferences are subsets of a more general category of preferences users may want to communicate across a range of domains. The PANID's attribute primitives can be used to build a robust and flexible preference system that communicates with other systems in specific contexts. For example, your dietary preferences or restrictions might be automatically communicated in a restaurant, or investment management parameters might be communicated to Defi trading bots that execute your investment strategies.

Identity Solutions

Control over personal privacy preferences is a necessary, but not sufficient, aspect of a comprehensive identity solution. The soulbound PANID token and its related flexible attribute primitives can be used as a foundation for a more general identity solution that incorporates built-in privacy.

Negotiation Protocols for Privacy Ruleset Conflict Resolution

Multiple privacy identities with conflicting preferences may sometimes be present in the same context at the same time. Various models could be developed for resolving such conflicts through consensus, negotiation, or value alignment. For example, one type of model could be based on value questions, another could be based on Activity Impact Matrix factor increases for cooperation and compromise, and another could be based purely on remuneration exchanges between conflicting users.

Activity Impact Matrix Extensions

The Activity Impact Matrix on Privaceum is a highly-developed and nuanced metric of a chain participant's reputation on a complex, functioning chain. Integrators might develop extensions that allow oracleized access to this key metric, or combine this metric with other data, to be used by other systems both within and outside the web3 ecosystem. For example, another protocol might utilize a user's Privaceum Activity Impact Matrix to assist in evaluating their governance proposals or determining their voting power.

Financial Product Integration

Defi protocols on Polkadot or other chain networks could integrate with Privaceum to allow participants to leverage their unused ETV in financial transactions or instruments, such as loans, without withdrawing the ETV into DOT. Or, another protocol could use the Activity Impact Matrix to evaluate creditworthiness for loans or access to grants from foundations such as Gitcoin and the Polkadot Treasury.

Context-Defined Datasets

Privaceum has an elaborate set of tools for distinctly defining particular contexts. Integrators could use context primitives in innovative ways. For example, what if we could assign subsets of private data to be shared according to the context we're in? When a device or system that needs certain data detects our presence (using a smartphone dApp or a wearable hardware device), the dApp could automatically share only the data appropriate to that context. Access to the data sets would expire when presence in the context ceases.

Status

Privaceum's core technologies are founded on several years of academic research into privacy architectures. This research has been presented at academic conferences around the world.

Privaceum also holds six U.S. patents on various aspects of the technology:

- U.S. Patent No. 11,423,174, issued August 23, 2022
- U.S. Patent No. 10,831,925, issued November 10, 2020
- U.S. Patent No. 10,831,924, issued November 10, 2020
- U.S. Patent No. 10,579,825, issued March 3, 2020
- U.S. Patent No. 10,521,604, issued December 31, 2019
- U.S. Patent No. 10,452,863, issued October 22, 2019

Initial explorations into the use of the blockchain as a foundational technology for solving privacy problems were conducted in conjunction with the Ethereum network. We implemented a working model of the architecture as Ethereum smart contracts, dApps, and code modules in which many core concepts were shaped.

Recognizing that there are certain limitations to using Ethereum smart contracts for an architecture with the complexity of Privaceum's, we have been developing our Substrate chain as a stealth project for the past nine months. Core modules such as the PANID primitive, Daoonomy, privacy rulesets and marketplace, Averify, and governance modules are at or near code-complete.

TEAM

Kevin L. Miller

FOUNDER, CEO

An attorney, author, inventor, researcher, Microsoft veteran, and entrepreneur, Kevin has over 25 years of experience in software engineering/architecture and development management.

His work with Microsoft in the late 1990s helped address key scalability and state management problems in web and data services, experiences he shared in his book *Professional NT Services* (Wiley/Wrox 1998). The book became a standard reference text for the implementation of highly scalable multi-tiered systems.

After leaving Microsoft and co-founding several successful technology startups, Kevin became interested in the impact of technological advances on law, policy, legal automation, and human rights. He obtained a J.D. and has practiced IP, data privacy, and startup law for several years. He has written widely about surveillance and predictive policing, the privacy impacts of new technologies, algorithmic accountability and fairness, and legal and ethical issues in cyberwar. Kevin's original research on privacy architectures converged with his interest in blockchain to form the foundational ideas for Privaceum.

Kevin is a registered patent attorney with a B.A. in Philosophy and Computer Science, an MBA, and a J.D. from the University of Florida; he is a Microsoft Certified Solutions Developer and is a Consensys Certified Blockchain Developer. He also holds seven patents in blockchain technologies.

Victoria J. Miller

FOUNDER, COO

Over the last 15 years, Victoria has co-founded several technology startups. She has also served as strategic advisor to several other technology startups, lending her creative vision, strategic and tactical business planning, and project management skills.

Starting her career in healthcare management, she played a key role in helping create one of the most innovative healthcare initiatives in the country in Arizona and assisted with expansion efforts in other states. Victoria moved into project management in the insurance industry, spearheading a major workflow redesign initiative that aligned new technologies with improving processes and communication across multiple departments and external agencies.

An inventor, entrepreneur, and seasoned technology management professional, Victoria is passionate about blockchain, privacy, and creative, forward-looking solutions to society's hardest problems. She holds a patent applying blockchain technologies to road safety systems.

Victoria brings a wealth of operations, marketing, and project management experience to Privaceum. A Brit by birth, she has lived in seven countries and speaks German and English. She has a Master's in Organizational Management.

Contact

It takes all of us working together to save privacy. If you are interested in joining the Privaceum network to promote privacy or partnering with us as a developer/integrator or investor, we'd love to hear from you!

Learn more on the Privaceum Website

Or email us at: **info@privaceum.com**

Follow Privaceum on:

Twitter

LinkedIn

Medium