PRüF is a blockchain based system for the tokenization, provenance, and management of real-world or virtual assets.

The PRüF ecosystem consists of the PRüF contract infrastructure, PRüF users, and PRüF nodes.

The PRüF contract infrastructure is centered around a tightly integrated network of upgradeable contracts. The core of this structure is the primary storage contract, which integrates specific business logic associated with secure asset management. Closely tied to this are the AC_Manager, Escrow_Manager, and Verify contracts, all of which also hold additional local data. Although these contracts hold critical data, they are still upgradable using a “replicate on read” migration pattern. This is made possible using our contract name resolution system, which allows contracts to be “hot-swapped” in place without interrupting service.

All other business logic and asset control contracts plug into these systems and are trivially upgradeable, as they are stateless.

PRüF users are, of course, the users of the PRüF system. They may be individuals or organizations seeking to establish secure, private provenance and control of assets. Users access the PRüF infrastructure from any internet-connected device, and can manage, transfer, or modify their assets through the PRüF node of their choice.

PRüF nodes define and serve as portals for “asset classes”, or types of things. Users for each type of object being tokenized benefit from a customized experience tailored to the specific asset type and region. In response to these variations, PRüF node operators customize their web portal design, node name, classification nomenclature, and revenue structure to reflect the needs and desires of the communities they serve.

Most node operators serve customized versions of our white-label portal, run custom server applications, or deploy apps to the device ecosystems that they serve. Node operators earn

PRüF tokens through fees for service, direct advertising revenue, or sales from in-portal commerce. Some Node operators representing larger brands may opt to provide the node free to their customers to increase customer engagement and brand education opportunities.

As a Minimum Viable Product/demo solution for node operators just starting out, PRüF provides unbranded access through our basic portal and app deployments.

For fee-for-service operators, PRüF provides a “try before you buy” model. After minting by burning PRüF, a new node token (PRFN) is configured with a 51/49% revenue split with the PRüF foundation. By upgrading a node with PRüF tokens, a node can reach a 90/10% revenue share model. Funds from revenue shares provide funding to the PRüF foundation for ongoing development and innovation in the PRüF ecosystem, benefiting users and node operators alike. By encouraging investment in Node tokens, PRüF incentivizes node operators to build effective service models and offer a pleasant user experience catered to user’s needs within their market niche. This helps to encourage responsible operators that seek to provide valuable services while discouraging “spammy” nodes or bad actors by ensuring node operators have something at stake. Since Node tokens can be renamed and retain their revenue sharing percentage if transferred, node tokens represent a tangible asset that gains value with the popularity and brand presence of the node.

Since PRüF does not store personally identifiable information by default and all information stored is publicly available, data cannot be “hacked” or legally coerced from the PRüF system. In some cases, a user may desire a record to be easily verifiable or even publicly visible. In these cases, PRüF can provide this. In other cases, users may require absolute secrecy, while maintaining trustable verifiability. In this case, a strong arbitrary length passphrase can be included, making an item or identity mathematically impossible to link to any record in the PRüF system without the passphrase, even if identity information is known. For most users, private identity with transparent item encoding provides the ideal balance of security and utility.

PRüF is designed to work effectively for both decentralized and custodial asset management.

For most applications, a fully decentralized implementation where users maintain token custody and direct control in their own cryptographic wallet offers the ideal combination of privacy, security, autonomy, and freedom. There are some cases, however, where a managed custodial solution desirable.

Strong cases for custodial implementations may be found where there is an existing trust infrastructure such as governmental systems of asset provenance, where legal standing is established as stemming from registration with an extant governing body. Another similar application exists where a managing entity utilizes an asset token as a contractual instrument, or where a trusted custodial entity is desirable for reasons of continuity, physical security, etc.

In these cases, PRüF can easily be used by, or alongside, existing state systems, reinforcing or augmenting extant social infrastructure. PrüF accommodates this need through custodial contracts, where the governing contract holds the token representing the asset. In this case, ultimate provenance is determined through the cryptographic hash stored in the token itself, rather than the wallet that holds the token. Entities which are authorized to manipulate a class of assets can authenticate owners using a private and secure method that conserves privacy while facilitating supervised provenance. Using custodial asset classes with the PRüF protocol, an owner can demonstrate provenance without the need to involve any third party. Even if an asset is tokenized in a custodial asset class, it is mathematically impractical for anyone (including custodians) to enumerate or correlate ownership without the full cooperation and knowledge of the owner.

Whether fully distributed or supervised by a node operator, the PRüF protocol, when properly used, offers robust protection against malicious actors either with or without state backing.

The PRüF contract infrastructure is operated using a variety of tokens.

PRUF

The (fungible) PRüF utility token (PRUF) is used primarily as “gas” for tokenizing, modifying, and transferring assets. In addition to fueling functions on the network, it serves as an incentive mechanism for PRüF node operators and network users, as well as the sole medium for acquiring and upgrading PRüF nodes. PRüF may also be used to offset Ethereum gas costs in future expansions of the ecosystem.

PRFN

The (nonfungible) PRüF node token (PRFN) acts as a control key for operating PRüF nodes. Holders of a PRFN token have the ability to operate a PRüF node, which acts as a portal for users to interact with the PRüF system. The PRFN token allows node operators to access their controls for pricing, naming, and addresses to receive PRUF tokens collected for services provided by the node.

PRAT

The (nonfungible – nonstandard) PRüF asset token (PRAT) is the tokenized representation of assets held in the PRüF system. PRAT tokens are the blockchain representation of assets and are interacted with by the PRüF infrastructure to facilitate the secure, private control and transfer of assets, in both real and virtual spaces. PRAT tokens are held by users in noncustodial asset classes or held in custodial contracts for managed asset classes. The transfer of PRAT tokens is controlled by the underlying PRüF contract infrastructure and may be restricted by contract operations for certain functions such as escrows or when reported as lost or stolen by the token holder.

PRID

The (nonfungible – nonstandard) PRüF ID token (PRID) acts as a certificate, indicating that the holder has been identity verified by PRüF or a trusted third party or system. PRID tokens do not contain personally identifiable information, but are unique and derived from a verified personal or automation identity. In this way, PRID tokens represent a unique identity certificate, reducing the incentive and opportunity for malicious actors among users and systems trusted with the tokenization of assets. PRID tokens are nontransferable and are permanently associated with the address to which they are issued. If a PRID token is to be moved to a new address, it must be burned and reissued by a trusted entity.

In general, only the PRUF and PRFN tokens are meant to be managed by standard token handlers, though the PRAT token is transferrable by token holders as a normal ERC721 token as long as it is not locked by an escrow contract or by the token holder.

The core PrüF protocol tracks 10 critical data points for each asset in the system.

1: The cryptographic hash for the item itself (idxHash)
2: The cryptographic hash for the rights holder (rgtHash)
3: The status of the asset record—transferrable, nontransferable, etc.
4: The number of times, if any, that a record has been edited (only applies to certain asset classes that may have administrative oversight)
5: the asset class that the asset is inscribed in
6,7: A decrement-only counter, and its starting point. This is used to track consumables or remaining service life, for instance.
9: An updatable pointer to an optional IPFS file, typically A JSON data structure including pointers to media, information, and files. ****descriptions, photos, other
9: An immutable pointer to an optional IPFS file, typically A JSON data structure including pointers to media, information, and files. This might typically be used for certifications of authenticity, valuations, documentation, and other persistent information.
10: The number of times that the asset has been transferred.

How PRüF works, a walkthrough:

The first step to onboard an asset into PRüF is tokenization. This is accomplished either by a manufacturer or certifying entity, ensuring that fakes or after-hours production are easily identified, or by an individual or organization wishing to onboard their own assets.

The process of tokenization begins by identifying the uniquely identifiable features of the asset. This usually consists of the manufacturer, model, and serial number of the item along with any other specific features unique to the class of asset being tokenized.

Once identified, this information is entered into a PRüF portal (the web interface for a PRüF node). If the asset is to be kept hidden (secret) on the PRüF platform, a passphrase or secret key may be included with this information.

It is important to note that using the PRüF protocol, this information remains local to the terminal being used (web browser, app, etc) and is not transmitted over the internet or stored in PRüF. This information is used locally to create a strong cryptographic hash through multiple cryptographic hashing operations. In this process, the original information is lost to entropy, so it is mathematically impossible to recreate the original information from the resulting hash. The hash resulting from processing the asset data is called the idxHash.

Once the idxHash has been created, another hash is made from data supplied by the user for the purpose of owner identification. This might be a company name and license number, an individual name and ID number, biometric data, or any other externally verifiable information that can be used by an owner to uniquely differentiate themselves. This data should include a strong passphrase known only to the owner. This new hash is called the “raw” rgtHash.

Once the idxHash and the raw rgtHash have been created, they are hashed together to form the full rgtHash. This is important because, without this step, it would be possible to scrape the blockchain and compile a list of rgtHashes and the assets they correspond to, a potential metadata attack on user privacy.

With the rgtHash hashed with the idxHash, an attacker would have to have a user’s full identity information, all of the item’s detailed information (manufacturer, model, serial, and item passphrase, if used), as well as the passphrase used to encode the user’s identity. In other words, they could not find out anything they did not already know and would be extremely unlikely to be able to even definitively correlate an item to a user without the user's full cooperation.

Once the full rgtHash and the idxHash have been created, these hashes are transmitted to a blockchain node. At no time is any of the data used to make the hashes transmitted or stored. Once the hashes are sent, the PRüF contract infrastructure creates a database record and a modified ERC721 token using the idxHash as the token ID. This token is created either in the user's wallet or in a custodial contract, depending on whether the item was tokenized in a custodial or noncustodial asset class. Additional information including a consumable counter, additional description data, and changeable file attachments can be made at this time. In additional steps, immutable file attachments or notes can be made, as well as updates to any description or media files attached to the asset.

At this point, an optional label can be printed to attach to the item, using any label compatible printer. The label contains a QR code for instant, effortless, and cost free lookup of the item in the PRüF system. It should be noted that looking up an item on PRüF requires either the QR code, the idxHash, or the full item information including manufacturer, model, serial, or any other information used when the original idxHash was created. Looking up an item on PRüF does not reveal any information about the owner. Only the owner can verify their ownership of an item.

Once the tokenization process is complete, the tokenized item can then be manipulated using the PrüF contract infrastructure. A user can mark an asset as non-transferrable, transferrable, transferred, discardable, discarded, lost, stolen, or any other custom status. Assets can be transferred between users, transferred out of the system, used in escrows, and manipulated using custom business logic for any definable process. The PRüF provenance system is flexible, robust, customizable, and upgradable to meet both present and future asset management needs.

PRüF assets that have not been made “stealth” are easily retrieved from the blockchain using our app or website. In this way, it can be instantly verified if someone presenting an item for sale is the registered owner, for example. If an item is lost or stolen, the owner can mark that in the PRüF system, so that anyone looking up an item will see that status. An item in a store can be scanned to verify that it is authentic and unregistered (unused). Used items can have their authenticity verified through PRüF as well, as only items listed by a manufacturer or official verifying vendor will be listed in that manufacturer's or vendor's asset class.

By securing provenance and creating verifiable trust, PRüF enables secure and private ownership, facilitates private commerce, works to disincentivize theft and counterfeiting, and empowers individuals with cryptographically secure, privacy-first tools to secure their belongings.

In addition to these already built capabilities, PRüF is forging important partnerships and crafting new tools to create a local-first global marketplace that emphasizes P2P trade and small businesses, backed with deep global distribution chains.

The PRüF contract infrastructure manages asset provenance and business logic, facilitating the private and secure management and transfer of assets.

The basic PRüF protocol provides functionality for ownership verification, authenticity verification, and the direct or mediated transfer of assets. Additional PRüF protocols such as PRüF-Boomerang, and PRüF-Recycle further extend functionality for PRüF tokenized assets.

Although PRüF was designed specifically for privately and securely managing the provenance of physical items, PRüF tokenized assets can also include virtual items such as legal contracts, token wallets, other asset tokens, access keys, licenses, or other documents. By linking with the global, decentralized Interplanetary File System (IPFS) PRüF enabled assets can be connected to a wide variety of transient or immutable data objects, including photos, media, documents, software, and more.

For asset ownership, PRüF allows an asset holder to authenticate that they are the legitimate holder of the asset. This can be done either by confirming their possession of the token in their wallet, or for additional verification, showing that they can reproduce the item’s rgtHash using their (in-person verifiable) identity information.

For third-party provenance certification, PRüF facilitates the storage of immutable media on the Interplanetary File System (IPFS). This media may contain a digital copy of certification by a recognized certifying agency, which itself may refer to a unique PRüF certificate which can be traced to the certifying agency on-chain, linking back to the asset in question, creating a verifiable circle of trust. A simpler implementation of this, optimized for manufacturers, tokenizes the asset itself in a certified Asset Class, creating inherently verifiable provenance for the asset. (see PIP, below)

PRüF supports the secure transfer of assets. In secure-transfer, a receiver or buyer first verifies the ownership of the asset by the provider or seller. The seller first proves ownership by demonstrating that they can reproduce the items unique rgtHash, either off chain or on. In this scenario, the buyer uses their verifying application, so that the seller cannot falsify the rgtHash match unless the buyers application is compromised. In neither case is the personally identifiable information transmitted. A completely trustless variation of this can also be utilized without trusting any device-side software, but some non-identifying intermediary hash information is inherently made visible on-chain, so that the rgtHash is permanently “burned” and cannot be safely reused. After such a verification, an asset will require transfer or modification of the rgtHash to be once again verifiable in this way.

With PRüF it is also simple to arrange supervised transfers, known in the PRüF systems loosely as “escrows”. PRüF escrows are contracts that specify the terms of a transfer, a holding lock, or other asset manipulations. They can be controlled by time, payment transfer, on-chain oracles, or authorized controlling addresses. In a simple example, an asset is held as collateral, pending the release by a controlling entity or a specified passage of time. During this “escrow period” the asset cannot be modified or transferred. PRüF escrows can be written for nearly any set of conditions that can be monitored on or off chain.

PRüF incentivises the responsible discarding of still usable objects through the “Recycle” protocol. With PRüF-Recycle, a user who discards an item receives PRüF tokens when someone re-homes the item in the PRüF ecosystem. This encourages users to give away still-useful items instead of throwing them in the trash.

If a PRüF tokenized item is lost or stolen, the owner can change it’s status to reflect that in PRüF. This alerts potential buyers that the item being presented is not owned by the seller, and can also be used by the owner to provide an incentive for a finder to ensure the safe return of a lost or stolen item. In this way, by making them difficult to sell and enabling a return bounty, PRüF-Boomerang disincentivizes theft and helps lost items find their way home. PRüF-Boomerang ecosystem partners can further facilitate the return of items, collecting bounties and providing delivery services.

The PRüF infrastructure is infinitely Extensible

Due to the versatile nature of the PRüF infrastructure, custom smart-contract plugins can be written and permissioned for specific asset classes that perform specialized business logic for almost any application.

An example of this extensibility can be found in the PIP (Product Initiation Protocol) contract, which enables manufacturers to tokenize goods at a low per item cost. These tokenized items are authenticateable prior to full registration on the PRüF system, allowing the authenticity of the item to be verified prior to purchase. Once the item is purchased, it is then registered by the buyer in the manufacturers PRüF portal. PRüF PIP provides a turnkey, low cost system to eliminate brand piracy.

Another example of the unlimited extensibility of the PRüF infrastructure is the PRüF-Verify protocol. With PRüF-Verify, a single PRüF asset holds a list of serial numbers (or other PRüF assets) in a “wallet”. The master token acts as a key, enabling the holder to check assets into or out of the wallet. The PRüF-Verify protocol is designed to be used to counteract counterfeiting of serialized fungibles, and to affordably track the holding and disposition of this kind of asset for entities that handle significant volumes of serialized assets in a single class.

PRüF provides turnkey solutions at common pain points
for users, manufacturers, and resellers.

Buyers want to buy genuine products from legitimate sellers. PRüF enables lifetime verification of authenticity, provable provenance, and simple systems for transferring ownership or managing assets that add value for users. Even a garage sale can get added value from PRüF, establishing the legitimacy of ownership and the verifiable authenticity of items for sale.

Sellers and manufacturers want to be able to distinguish themselves from brand counterfeits. PRüF gives buyers and sellers peace of mind, creating an unforgeable certificate of authenticity on the blockchain that customers can easily verify with any internet-connected device. Counterfeit certificates are technically infeasible to create, and if a genuine one is copied, the fake will be detected after the first one is verified by a customer. PrüF delivers a low-cost turnkey solution to end brand piracy.

In addition to these solutions, the PRüF ecosystem provides opportunities for increased customer engagement, leading to additional or repeat purchases and increased brand loyalty.

Strong potential exists for integration with e-commerce retailers and marketplaces through the proposed MarketSpace ecosystem, effortlessly connecting small retailers and individuals through a local-first global marketplace, backed up by deep supply chains to turn the world into an expansive physical showroom. Larger vendors could benefit from increased sales opportunities as well as long-tail customer engagement, providing additional opportunities for up-selling, accessory sales, and repeat purchases.

The PRüF ecosystem consists primarily of the PRüF blockchain-based provenance system, combined with business unit partnerships with PRüF-Node operators. PRüF-Node operators would use in-house software or customized versions of our open source web template to create a portal to the PRüF back-end, custom-tailored to their customer base and product line(s). Operating a PRüF-Node could provide revenue directly through service fees paid by end-users, advertising, or sales of tailored products and services for the specific market niche.

For larger businesses, Operating a PRüF-Node will increase brand engagement, provide an opportunity for product education, and bring customers into contact with promotions, new products, and other revenue-generating interactions.