PRüF

A blockchain based asset tokenization ecosystem

TABLE OF CONTENTS

Imagine a world without counterfeit goods and brand piracy.

PRüF makes it instant, free, and easy for buyers to verify the authenticity of their purchase before they buy.

Counterfeit goods confuse buyers, cost sales, and erode brand value. Unfortunately, many sales channels (especially online) are not incentivized to care. PRüF provides pre and post-sale verified authenticity with Trust-enabled assets. With trust-enabled, consumers can verify the authenticity of goods before purchasing in both primary and secondary markets, protecting brand integrity, product value, and customer confidence.

Theft, counterfeiting, and fraud levy an illegitimate shadow-tax on society. It is estimated that by 2022, economic losses from counterfeit goods and cash may reach over a trillion dollars in value extracted from local economies. As with most systemic costs, this burden is carried disproportionately by those who can least afford to bear it.

Beyond falsified goods, as many as one in 40 currency notes are estimated to be counterfeit in some major western economies. Cash businesses lose billions annually to cash theft and fraud. These burdens amount to significant friction losses in legitimate economies by criminal actors, and the situation can be much worse in the developing world.

YOU WORK HARD FOR WHAT YOU OWN.

Imagine a world where theft or seizure was less lucrative and where possessions and assets were provably and privately yours with a title on the blockchain. Imagine a world where lost or stolen items or even cash would have little resale value unless returned, and where lost items could come home on their own.

Imagine effortless commerce, where selling something was as easy as marking it “for sale” in your wallet - Where finding a private or commercial seller for something you saw or liked in the wild was as easy as choosing “for sale near me” from a menu. Imagine purchasing a one of a kind item through the window of a closed local boutique and having the item show up later at your door. Imagine effortlessly and costlessly enabling local and global e-commerce for every “mom-and-pop” store, democratizing front door access to the marketplace.

Imagine a world with PRüF.

Existing systems facilitate the resale of stolen goods and incentivise theft.

Buyers or resellers of used goods are often put in the awkward and difficult position of trying to decide if an item they wish to buy was legitimately obtained by the person selling it.

PRüF Secure-Transfer allows a buyer to be sure that the person in front of them is the actual owner of an item being offered as collateral or for sale. Using Secure-Transfer protects both the buyer and seller by documenting the release of rights to the item, as well as the (optional) immediate transfer of rights on the blockchain to the buyer. PRüF Private-Provenance makes it very difficult to sell a stolen or lost item because a free cursory search on any PRüF portal can indicate that the item was reported as lost stolen by the owner.

If an item is lost or stolen, PRüF gives you options.

If a PRüF trust-enabled asset goes missing, it can be optionally linked with a mechanism for a reward if returned. Assets can be tagged with return information, facilitating securely contacting the rights holder*. PRüF trust-enabled assets are difficult to sell if stolen because checking if an item is lost or stolen is easy, fast, and free from any web-enabled device. It will become part of reasonable due diligence by dealers, pawnshops, or private buyers to support PRüF trust-enabled assets.

Even if found, lost or stolen items are often not be returned to the owner.

Without adequate documentation of ownership, even in cases of theft where the item has been located, the possessor is usually assumed to be the owner unless additional proof is available. PRüF private-provenance allows a rights holder to prove the legitimacy of their claim, tracing the possession of the item back to a specific point in time or the original sale, irrefutably.

'Registration' as it is known today can erode privacy and creates ancillary risks from private or government entities. PRüF *private-provenance* eliminates this risk, even for the most sensitive of assets.

PRüF private-provenance allows records to be stored such that ONLY the true owner can prove ownership. When using the private-provenance feature, Names or identifying information cannot be looked up in the system, cross-referenced, or tracked. Additionally, items cannot be looked up in the PRüF protocol without the actual item serial number. For additional privacy, a secret can also be included in the item record, creating a stealth listing, so that only the holder of the secret can look up the item at all.

Tokenized Real-world Assets

Acting as a "title" to everyday goods, PRüF tokenized assets allow the protections of title to extend to all of your valuables. PRüF private-provenance allows rights holders to securely hold, transfer, sell and collateralize their possessions without opening their lives to scrutiny.

In addition to everyday items, collectibles, heirlooms, and capital goods under personal ownership, PRüF tokenized assets open up a multitude of options for discreet and protected asset ownership. In this model, major assets would be held and managed by a holding company. The executive advantages of ownership are controlled by the token without the attendant risk exposure. Assets benefitting from this management model range from real properties, boats, aircraft, and vehicles, to fixed fungible assets, such as a safe deposit box of financial instruments.

A truly democratized, local-first global maketSpace with PRüF

PRüF enabled tokenized assets are linkable to automatically generated or customized item profiles. These profiles can include manufacturer-provided information for mass-produced items, or artisan profiles and introductions for handcrafted goods. Each PRüF enabled item bears a unique identifier, that can be (optionally) tied to this profile.

For mass-produced goods, the item profile would likely include model number or series, documentation or manuals, instructional materials, feature demonstrations, etc. For artisanal goods, the profile could link back to the artist, other work she has available, a Wikipedia page, or other information. In any case, this "PRüF tag" can be represented on a QR code or an NFC chip that can then be attached to or placed alongside the item as a sticker, tag, or label—or even built into the item in the case of RFID.

PRüF enabled tokenized assets align perfectly as an opportunity for partnering with marketplace integrators to create a local-first global marketplace. Such an integrator would have the opportunity of blending existing industry-scale supply chains with a local marketplace of pre-owned and artisanal items, leveraging the advantages of proximity marketing with deep supply and distribution backing. By leveraging this model, online-only retailers effectively convert the world into their showroom. With effortless point of exposure shopping and deep brand integration possibilities, we expect this opportunity to be an attractive option for e-commerce at scale.

PRüF marketSpace vision

By scanning a PRüF data tag (or even just looking at it, with AR glasses), any data that the owner may have chosen to make public can be displayed. By default, generic manufacturer data would be shown, but If the owner does not wish the tag to link to anything, something like “private” might be displayed instead. If the item is for sale, price and sale information will be displayed along with the item info, giving the viewer the option to immediately enter into a purchase escrow to reserve the item if that option has been made available by the seller.

In this way, with only cheap (pennies for 100) to print QR codes, any seller or private individual can effortlessly “list” their items on a global marketplace with a strong local-first aspect. When examining an item, a potential buyer could search “similar items near me” for example, and local listings for similar or identical items could be provided as options, backed up by listings from major suppliers and distributors. For the system to maximize throughput, local listings would be given top visibility so that users would be incentivized to provide “advertising” by displaying and listing their items in the system. This alignment of incentives allows for the integration of a local-first marketplace with global reach and deep supply chains.

Counterfeit products made up 5-7% of world trade in 2013, and it hasn't gotten any easier to protect your brand. ***PRüF can help.***

Counterfeit goods confuse consumers, cost sales, and erode brand value.

Unfortunately, many sales channels are not incentivized to care.

With PRüF trust-enabled assets, it's never been easier or more cost-effective to protect customers from fakes. With an individual asset ID for each genuine product, a quick scan with the PRüF app verifies that the item is genuine and the ID unused. If a brand pirate tries to make asset ID's, they will show up as fake. If they try to reuse a real number, it will show up as already used (and therefore unregisterable) after the first customer registers that ID on the platform. PRüF trust-enabled[3] adds value and a premium nuance to products, while reducing the threat of brand theft with nominal infrastructure investment and a nominal unit cost.

In the store, your customer can scan the PRüF trust-enabled tag or label with their phone. Since the item being verified is real, it will show up as "Genuine, unowned". After purchase, your customer can open the sealed certificate included with the item, and enter the number inside using our app or your website. The item is then registered as "owned", and the customer may then register themselves as the owner. For nontrivial items, the customer then enjoys all of the protections of a PRüF trust-enabled asset.

For online sales, the vendor can include the PRüF trust-enabled tag of the specific item purchased as an image on the invoice before shipping. Clicking through, the customer will get verification of authenticity, mark the item as owned, and can be brought to a product anticipation section of the brand's website. This will provide an opportunity for additional customer education, brand promotion, social media generation, and additional sales opportunities. After receiving their purchase, the customer can open the sealed certificate and enter the

number inside using our app or the brand's website. The item is then registered as "owned", and the customer may then register themselves as the owner of their new PRüF trust-enabled asset.

After the sale, onboarding, registration, and subsequent verification of the authenticity of the item can generate valuable insights for the brand, and help onboard 2nd or later party owners, bringing them to the brand's website, offering additional information, offering service contracts or upgrades, or enabling other valuable customer interactions.

PRüF can offer all of this as a very low barrier turnkey solution, or can provide manufacturers or vendors the tools to fully integrate authenticity verification into their online presence with no blockchain development required. PrüF is so easy and affordable to implement that it makes blockchain enabling products as accessible to Individual creators as it is to fortune 500 companies.

Counterfeit currency, fraud, and cash theft are global problems. PrüF can help.

Beyond falsified goods, as many as one in 40 currency notes are estimated to be counterfeit in some major western economies. This amounts to significant friction losses in legitimate economies by criminal actors, and the situation can be much worse in the developing world. PrüF verify can track larger denomination currency notes on the blockchain, so that serial numbers on bills can be scanned (at no cost) at the point of sale by vendors, with a smartphone by individuals, or at any point in the supply chain by banks, mints, and reserves. If a bill being scanned is marked as "held" by some other entity such as a bank, store, or other cash business, it can be considered questionable and returned to the bearer or more closely examined. If there is a question about the validity of a note, it can be referred to a bank or other appropriate agency for further inspection.

All of this can be done with privacy and anonymity provided by the PrüF verify protocol, keeping cash "cash".

Currency "locking" with PrüF *verify* can disincentivize theft for cash businesses.

Robbery and theft are common pain points for nearly all-cash businesses. Using PrüF verify, a business that uses cash could run each bill through an inexpensive scanner, automatically verifying each bill and marking it as "held" by the business. As part of the deposit process, bills would be scanned out of inventory and accepted into the inventory of the bank taking the deposit. For high-risk locations, cash drawers or overhead camera systems could be adapted to scan high-value bills in or out automatically.

Bills held by the bank then would be scanned out to individuals or businesses, so that all bills under the control of a bank or transport company would be similarly protected from robbery or other loss to malicious actors.

Each step of the way, all bills are accounted for, and any missing bills could be made very difficult to use, marked as stolen by a trusted entity, rendering theft or robbery nearly pointless for a very small cost. Aligning incentives against malicious actors makes dollars and sense, and private and public insurances will be quick to recognize these advantages.

Theft, counterfeiting, and fraud levy an illegitimate shadow tax on societies. The PrüF verify protocol enables pervasive counterfeit detection and theft prevention by aligning incentives within an economy and reducing friction losses caused by malicious actors. This in turn lowers insurance costs, security infrastructure costs, enforcement costs, and a host of other zero return inefficiencies that result from these malignant expenditures. Using the PrüF verify protocol can improve outcomes in disadvantaged economic sectors by making cash safer, more secure, and less costly. Lower costs mean lowering the barrier to entry for entrepreneurs, translating to improved growth, less crime, and healthier economies, benefiting all of us.

Technical Overview: PRüF is a blockchain based system for the tokenization, provenance, and management of real-world and 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 is 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. PRATs 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. PRATs are held by users in noncustodial asset classes or held in custodial contracts for managed asset classes. The transfer of PRATs 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) by a PRID token holding entity or person. 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 expandability 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 expands into diverse markets through the effort of PRüF-Node operators. PRüF-Node operators 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 provides 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 increases brand engagement, provides an opportunity for product education, and brings customers into contact with promotions, new products, and other revenue-generating interactions.

PRüF is more than a product, SAAS, or a blockchain company.

PRüF was designed from the ground up as an ecosystem and is designed to be upgradeable, scalable, persistent, and eventually to operate autonomously without oversight.

The core values exemplified by PRüF are:

Data Sovereignty - you should be in control of your data and how it is used. PRüF does not collect sensitive data from its users. Whenever personally-identifying information is required, it will be used for computations on the users own computer, and only the irreversible hashes made from that data will be stored on the blockchain.

Safety - PRüF systems are engineered so that they will not inadvertently or intentionally compromise the security, privacy, or agency of users. PRüF will protect the privacy of its users by collecting the minimum information required to provide the desired service, and clearly informing users of actions that may put their privacy, security, or agency at risk.

Personal Agency - PRüF strives to increase the freedom of its users from the external application of coercive force, whether financial, physical, or social.

Sustainability - As a blockchain-based service, PRüF is designed to stand the test of time. The PRüF protocol is engineered to be flexible, upgradeable, modular, and persistent. PRüF will seek opportunities to incentivize activities that enhance the sustainable uses of PRüF, its applications, and the natural environment in which we all share.

Do No Harm - The developers of PRüF are committed to building a tool that has a positive impact on society. Many of the design decisions built into the PRüF protocol are designed to facilitate the positive uses of PRüF and discourage bad actors. The PrüF ethos is our commitment to ensuring that PRüF will not be used to deprive others of their rights, freedom, or property.

Since PRüF does not hold any sensitive data, PRüF cannot be forced to divulge customer records, names, or information about their assets. Our customer's secrets are protected by entropy and mathematics, not passwords, locks, and doors.

PRüF, as a smart contract infrastructure, can continue to operate indefinitely without maintenance, oversight, or external control. It is designed to eventually be completely autonomous. Payments are handled autonomously, on-chain, as are all critical data functions. Some enhanced functionality utilizes IPFS, so this functionality might become unavailable if the core system were abandoned, but the main functionality would continue, unimpeded.

The actors within the PRüF ecosystem are the PRüF foundation, Independent business units (Node operators), the developer community, and, of course, PRüF asset rights holders. After the initial launch and beta phase testing, PRüF will be fully open-sourced and community development opened up. On-chain governance will be implemented as the project moves forward from the beta testing benchmark.

A limited number of Asset Class (PRFN) utility tokens will be distributed.

Asset Class business unit (Node) operators will be able to set and collect fees from asset management services, transfers, tokenizations, and value-added services desired by the customers they serve. Pricing for these services may vary widely, from negligible for basic services for common goods, on up to significant fees for bespoke management and legal support in more complex high-value asset management scenarios.

With no smart contract development required and simple, open-source templates using the popular REACT web framework, each node represents a turnkey backend solution with only minimal customization required to be a PRüF portal service provider.

Each PRüF-Node token is minted in a root class: for example, ‘bicycles in Pakistan’ might be one AC, minted in the root class ‘global bicycles’, while ‘bicycles in the USA’ is another node, in the same root. Asset rights holders

can move between nodes that they are qualified to be in by ownership, geography, or other factors, but any non-secret asset can be looked up globally on the system to discover its status.

PRüF will start with a few hand-picked PRüF-Node partners in just a few of the most critical, pain point filled asset classifications. Using our web3 templates and the PRüF smart contract infrastructure, each partner will build out their web presence as a PRüF-Node operator.

As each type and region of node being operated will face unique challenges and customer needs, this ecosystem approach provides for a marketplace of ideas and methods, encouraging innovation while maintaining an unfragmented system of decentralized asset provenance. Maintaining a cohesive universal repository for all providers allows everyone to benefit from network effects and protects the PRüF ecosystem from the potentially negative trust effects of multiplicity. Providing a ready-for-customization deployment with prebuilt infrastructure gives PRüF and PRüF partners a strong first-mover advantage in every potential market segment.

There is an incentive built into PRüF to encourage re-sharing of still-useful discarded items, by incentivizing the donation of a disused asset with a rebate on initial inscription costs. Recycling of assets in the PRüF ecosystem encourages the re-homing of items in the real world, reducing waste, environmental footprint, and atmospheric carbon production.

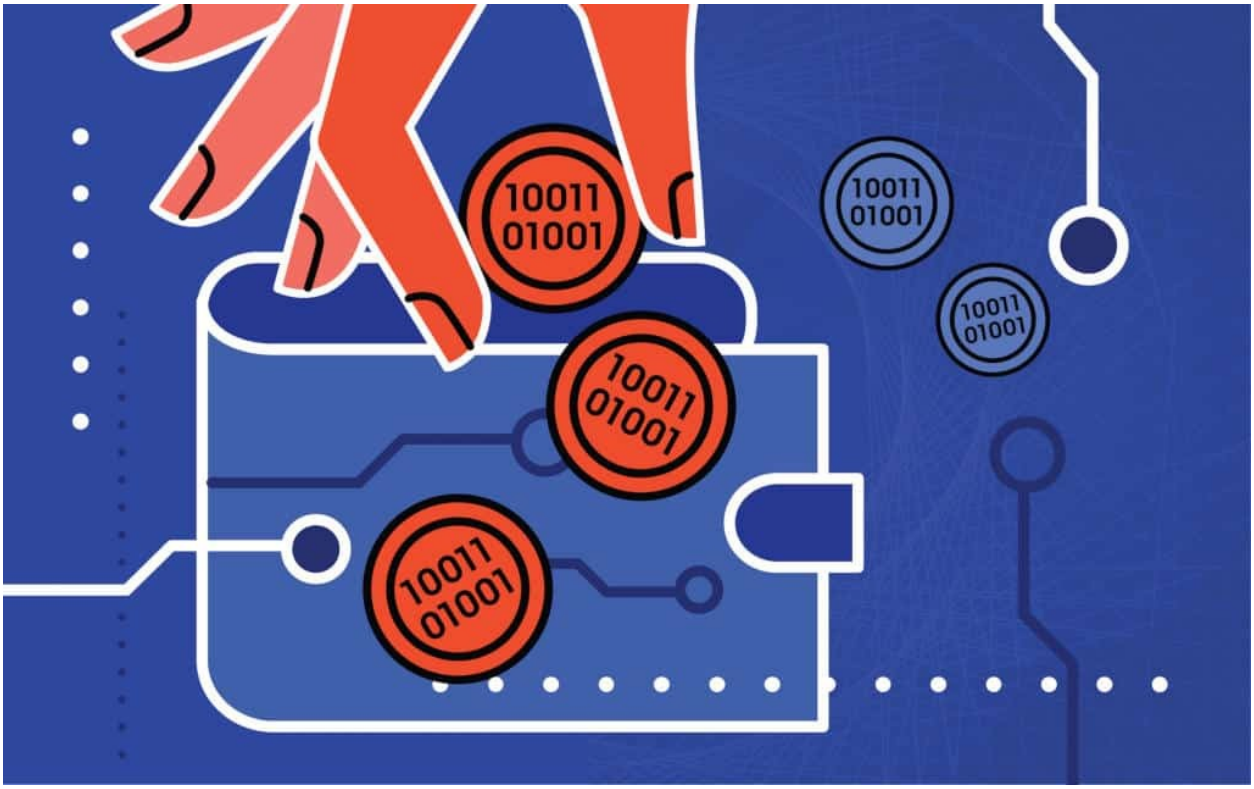
The PrüF contract infrastructure is modular, upgradeable, and security-forward. PrüF data manipulation and storage functions are handled by contracts that can only be written to by other trusted PrüF contracts. Edge interfaces are handled on a once-removed basis so that all interactions with data are constrained to expected and acceptable parameters, even if an external contract could be manipulated into an unanticipated state. Payable surfaces are limited to a safe-withdraw payment function which implements a pull-payment pattern. Function calls in PrüF contracts are unidirectional, with no stateful calls into previously called contracts or functions within a transaction, and the checks-effects-interactions pattern is universally implemented.

With flexible, extensible architecture, simple, powerful tools, and turnkey integration, PrüF brings the empowerment and advantages of the blockchain to a variety of B2B and consumer-facing applications without any blockchain programming or infrastructure rollout.

** This feature is not trustless and may compromise secrecy for sensitive users. In the case of lost asset recovery, this information would only optionally be provided by the rights holder in order to facilitate the recovery of their lost item. Items marked stolen or lost, but without contact information, would still compromise the resale of an asset, reducing the incentive for theft. This feature is not inherently trustless. If used, it could potentially make user information provided in this step vulnerable to official coercion or data breach. Users should decide if these risks are outweighed by the benefits in each case.*

*** For especially sensitive applications, the name and ID can be replaced with a surrogate, alias, or a cryptographic token, enabling perfect anonymity.*

**** Although basic PrüF verify verification is trivial to deploy to the public with minimal risk, Private party use of PrüF verify "hold" or "locking" functions would have to be carefully and ethically deployed because of an inherent risk of data misuse. The PrüF team will not implement "PrüF verify personal" unless we are satisfied that we have created a protocol framework that protects the interests of users.*



PrüF Token Integrations and tokenomics

In its most basic form, PrüF uses two types of non-fungible tokens for data management and control. Asset class nodes are controlled by holders of a corresponding asset class node token (PRFN) that acts as an authorization key to enable them to change pricing and payment parameters of their asset class. Assets themselves are represented by asset NFT's (PRAT)—each one corresponding to an asset on PrüF.

The PrüF protocol also supports special-purpose satellite contracts that may be configured to control additional token systems of fungible or nonfungible tokens. These tokens may represent digital assets, in-game currency, tokenized representations of actual currency for anti-counterfeit applications, or other applications where specialized control of a token system may be required.

In addition to this core functionality, PrüF uses the PrüF utility token (PrüF), a fungible ERC20 token which helps to scale and secure the economic growth of the platform. Designed primarily to align the incentives of the dev team and to incentivize community development of the platform, PrüF will function as "gas" for fee based operations, and under the "services discount model" on the B2B side. In addition to this, PrüF is burned in the minting of PRFN asset class nodes.

Fees for use of the PrüF infrastructure are chosen by asset class operators. They are set by the asset class (AC) token holder for the asset class that they own and operate in the PrüF ecosystem. By default, fees are split

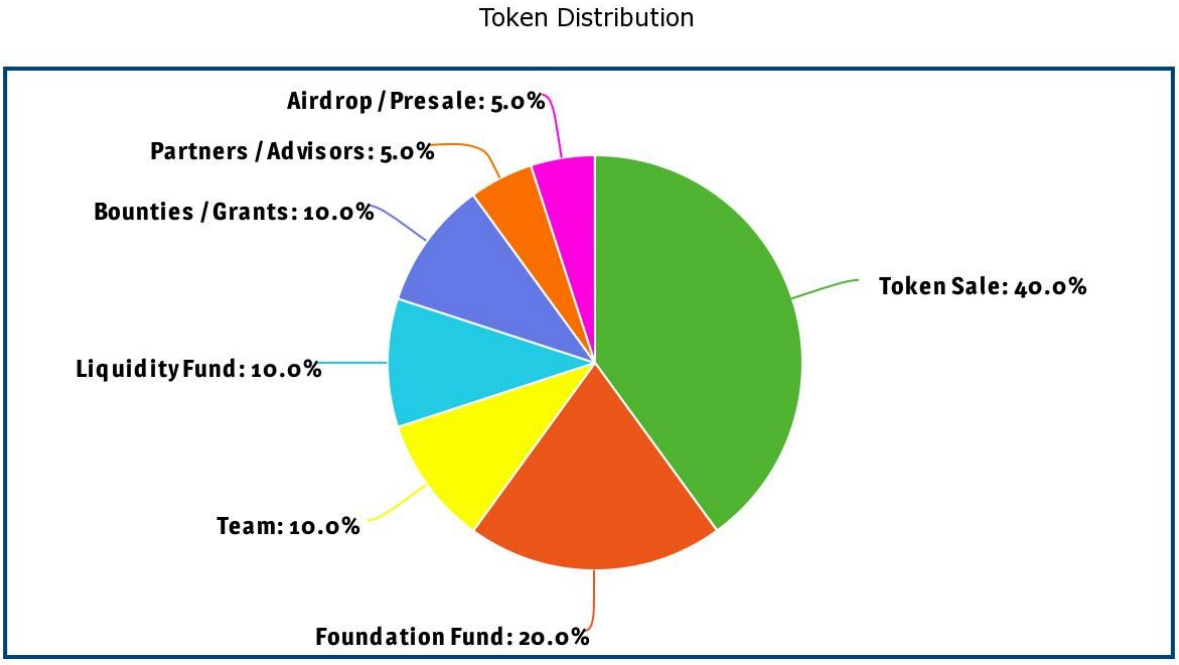
49/51 between PrüF and the AC token holder, respectively. Using PrüF tokens, PRFN token holders can increase their earnings percentage to 90 percent, depending on the amount of PrüF that they spend.

After an initial buildout, PRFN node tokens will be distributed on a schedule controlled by the PrüF foundation at an algorithmically generated unit cost. The cost will scale exponentially with the number of node tokens sold, up to the maximum number of asset classes (tentatively numbered at 4 billion). PrüF Tokens exchanged for PRFN tokens will be burned, increasing token scarcity and allowing the influx of new tokens without affecting the economics of the platform.

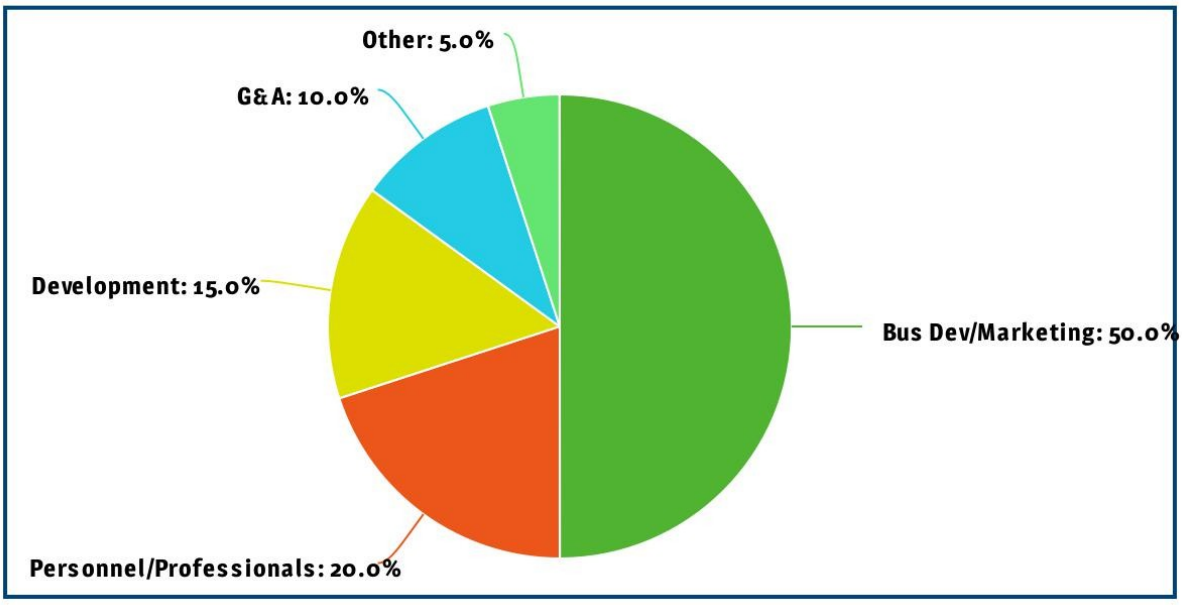
PrüF Token Roadmap

The following tokenomic roadmap is a rough draft and serves only to elucidate our overall conceptual plan for the PrüF utility token. We will consult a qualified economist prior to formulating a final plan because we are blockchain developers, not economists.

Up to 4 billion PrüF will be initially minted. Initial disbursement of 80 million will be by an opt-in airdrop. The dev team will retain 800 million PrüF which will be trickle-unlocked over 4 years, ensuring that they are incentivized to produce the best possible product. The PrüF foundation will be founded with an endowment of 800 million PrüF, and an additional 400 million PrüF will be retained by the PrüF foundation for bounties, incentives, and community development. Initial founding investors and advisors will receive 200 million PrüF. 1.6 billion PrüF will be distributed in a pre-launch token sale, and 400 million will be held as a reserve to balance the economic model in case of critical scarcity. The amount to enable an asset class for 90% revenue capture will initially be 120,000 PrüF.

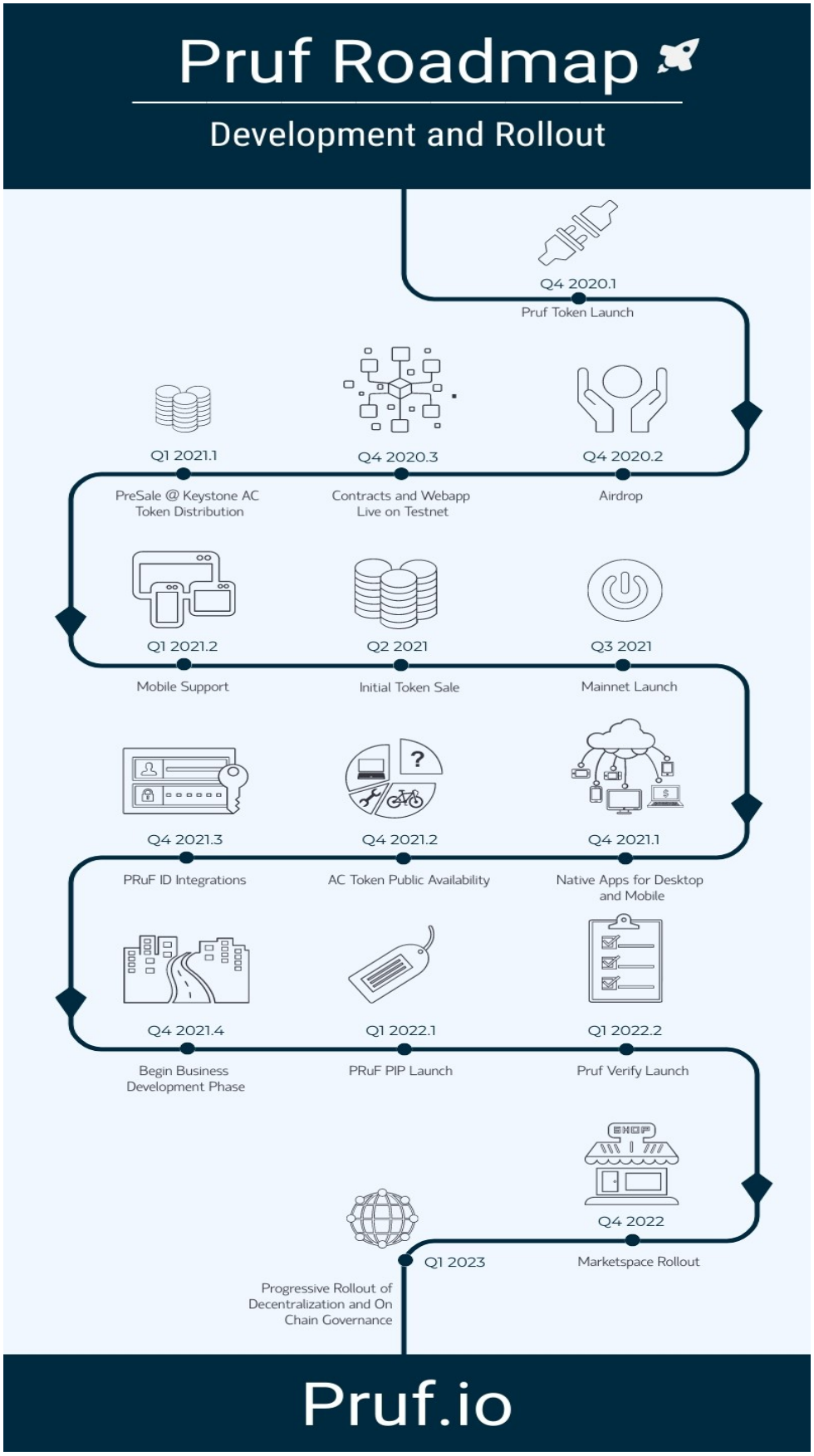


Foundation Fund Token Distribution



If the available supply of unburned tokens drops below 100 million PrüF and no more liquidity buffer tokens are held by the foundation, more tokens may be minted and airdropped (replacing burned ones) to avoid a critical liquidity crisis.

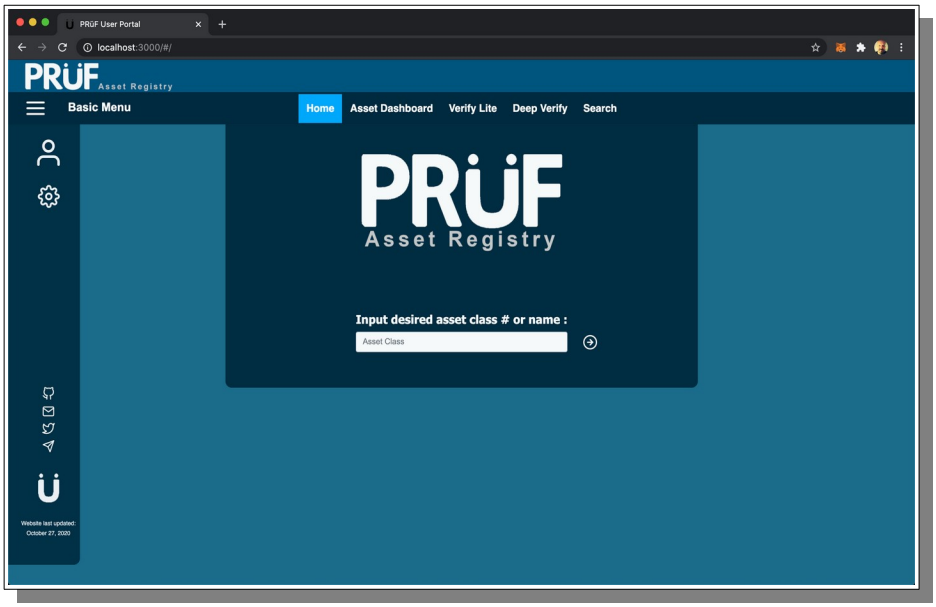
The PrüF team may also implement a private security token that acts as a key to unlock a percentage of the internal earnings from the PrüF infrastructure based on token holdings. This would be a private, non-fungible asset that would be held by PrüF team members and the PrüF foundation. It would serve as a long term fractional holding in PrüF earnings, providing ongoing funding for the PrüF foundation and helping to align the team incentives toward long term growth and profitability for PrüF node partners.


Pruf Roadmap
Development and Rollout
Q4 2020.1
Pruf Token Launch
Q1 2021.1
PreSale @ Keystone AC Token Distribution
Q4 2020.3
Contracts and Webapp Live on Testnet
Q4 2020.2
Airdrop
Q1 2021.2
Mobile Support
Q2 2021
Initial Token Sale
Q3 2021
Mainnet Launch
Q4 2021.3
PRuF ID Integrations
Q4 2021.2
AC Token Public Availability
Q4 2021.1
Native Apps for Desktop and Mobile
Q4 2021.4
Begin Business Development Phase
Q1 2022.1
PRuF PIP Launch
Q1 2022.2
Pruf Verify Launch
Q4 2022
Marketspace Rollout
Q1 2023
Progressive Rollout of Decentralization and On Chain Governance
Pruf.io

The PrüF team Progress So Far

At this time, all of the core PrüF contracts are nearing pre-alpha and are undergoing extensive automated and manual testing. The tests will be published along with the code as we grow out of stealth mode. The contracts are fully operational and implement all of the core blockchain functions of PrüF private-provenance, trust-enabled, boomerang, marketSpace, and more. PrüF currently implements our sample web3 interface deployed using React.js.

All core PrüF features have been finalized, and modular methods of adding future features have been implemented. Contract upgrades and data migrations have been gamed out and all necessary features implemented to support upgrades, bug fixes, and expansions on a live system. In addition to core features, satellite example contracts for custodial and non-custodial escrows have been implemented, and many more transaction handlers are planned for pre-release development including Release on delivery escrows, Asset-backed loans, PrüF verify, and others. Because of the PrüF protocol infrastructure underlying these satellite contracts, development is greatly simplified and highly standardized with feature-rich, secure functions available to the satellite business logic from the core infrastructure.



By helping to align the incentives in everyday commerce, PrüF can reduce frictions and improve security without the need for additional enforcement or state-sponsored coercive force. PrüF private-provenance and PrüF trust-enabled assets enhance the value and utility of the existing infrastructure of things while maintaining user privacy and data sovereignty.

Key Takeaways

- PrüF *Private-Provenance* secures a user's rights to their possessions.
- PrüF *Boomerang* helps to recover lost or stolen items.
- PrüF *marketSpace* enables and facilitates P2P and Industry scale commerce.
- PrüF *Trust-Enabled* reduces brand risks from counterfeit goods and enhances brand interactions.
- PrüF *Verify* disincentivizes theft and fraud
- PrüF can improve economic efficiencies in a broad range of domains