PRüF

A blockchain based asset tokenization ecosystem

TABLE OF CONTENTS

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 they were returned to their owner, 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, eschewing market giants for diversity, and truly democratizing front door access to the marketplace.

Imagine a world with PRüF.

It can be difficult for private buyers or resellers to be sure if an item being sold is genuinely owned by the seller.

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

PRüF *Secure-Transfer* allows a buyer to be ensure that the person in front of them is the actual owner of an item being sold. Using *Secure-Transfer* also protects the buyer 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* reduces the incentive for property theft, as stolen items can be marked as stolen or lost once their absence is noted by the rights holder. This makes it very difficult to sell the stolen or lost item, because a free cursory search on any PRüF portal will indicate that item is lost or reported stolen.

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

If a PRüF *trust-enabled* asset goes missing, it can be marked by the rights holder as being lost or stolen, and optionally linked with a mechanism for a reward if returned (and 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. It will become part of reasonable due diligence by dealers, pawn shops, or private buyers to support PRüF *trust-enabled* assets.

The rights holder to a lost or stolen item can register return instructions with a PRüF *boomerang* return service provider*. The lost or stolen status and the reward will then be visible for anyone checking the provenance of the item after finding it, or before purchasing it from someone else. This would make stolen items very difficult to sell (except perhaps for a fraction of the reward money in certain circles). In any case, the resale value would be lowered substantially, and thieves or finders would be required to expose their identities to claim any reward.

Alternatively, a rights holder could set a price on the item. A finder could then pay that price, on-chain, and have the asset ownership transferred to them through an escrow contract on the PRüF platform.

Any special terms of recovery can be made available on the items PRüF listing, so that the owner can tailor the conditions of return for the best possible outcome.

You could, of course, also choose to do nothing, discard the item, or mark it as transferred in cases where that was the best outcome.

‘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.

With PRüF *private-provenance,* sensitive information is not actually stored at all. A cryptographic derivative “shadow” of the original data is stored, but it is impossible to recreate the original data from this shadow, because the original information is destroyed. Sensitive information is not only encrypted, it is simply not stored at all.

A rights holder of a PRüF *trust-enabled* asset can easily prove ownership by demonstrating that their name**, ID**, and secret creates the same key as was stored previously. Only this specific combination of information, known only to the rights holder, can produce this key.

Often, even if found, lost or stolen items will 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.

Tokenized Real-world Assets

Acting as a “title” to everyday goods, PRüF enabled tokenized assets allow the protections of title to extend to all of your personal 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 enabled 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, without risk exposure, could be controlled by the token. This could range from real properties, boats, aircraft, and vehicles, to fixed fungible assets, such as a safe deposit box of gold coins.

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 hand crafted goods. Each PRüF enabled item bears a unique identifier, that can be (optionally) tied to this profile.

For mass produced goods, this information 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 link can be represented on a QR code or an NFC tag 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. The PRüF data tag indicates that there may be information available about the item, and that it will be very difficult to sell (or use in some cases) if stolen.

PRüF enabled tokenized assets align perfectly as an opportunity for partnering with a marketplace integrator, 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. 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.

What this might look like

By scanning a PRüF data tag (or even just looking at it, with AR glasses) data that the owner may have chosen to make public can be displayed. 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 that is not for sale, 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 incentivised 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 pre-established distribution 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 incentivised to care.

With PRüF *trust-enabled* assets, its never been easier or more cost effective to protect your customers from fakes. With an individual asset ID for each genuine product, a quick scan 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 used after the first customer registers that number on the platform. PRüF *trust-enabled*[3] adds value and a premium nuance to your product, while reducing the threat of brand theft at a nominal unit cost, and with very little technology or equipment investment.

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 prior to shipping. Clicking through, your customer will get verification of authenticity, mark the item as owned, and can be brought to a product anticipation section of your 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, your customer can open the sealed certificate 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 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 your brand, and help onboard 2nd or later party owners, bringing them to your website and giving your brand an opportunity to impress again, offer service contracts or upgrades, or enable other valuable customer interactions.

PRüF can offer all of this as a very low barrier turnkey solution, or can give you the tools to fully integrate authenticity verification into your online presence with no blockchain development required. PrüF is so easy and affordable to implement that it makes blockchain enabling your product as accessible to Individual creators as it is to fortune 500 brands. For appropriate projects, we can partner with your team to create a bespoke PrüF solution for your brand’s asset provenance needs.

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 the appropriate agency for further inspection.

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

Potentially, even private parties could use PrüF to secure their holdings. If a bill “held” in your wallet is stolen, it can be marked as stolen in PrüF *verify* and be made much harder to pass to someone else. When you wish to spend your bill, just scan it out of your wallet, marking it spent, and the accepting party will see that it is clean and safe to accept. Commodification of AR via smart glasses and related technology will streamline this process—bills with questionable provenance or known counterfeits could simply show up as red in an augmented reality display as device sensors read and look up the serial number in real time.***

Passing fake or stolen money just got a lot harder, and avoiding getting stuck with a counterfeit or stolen note just became easier than ever.

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 means lowering the barrier to entry for entrepreneurs, translating to improved growth, less crime, and healthier economies, benefiting all of us.

An afternoon with PrüF

The day is clear, with a warm sun lighting the shopfronts on the opposite side of the street. In the comfortable shade on the lower side, Anne walks casually down the sidewalk, enjoying a light breeze as she walks into small street-front gallery. Her eye is attracted to a contemporary scene rendered in deeply textured oils, and her glasses paint the small PrüF enabled QR code on the frame's corner a fluorescent green. As she briefly stares at the dotted symbol, an image of the artist's bio superimposes itself onto the lower right quarter of the frame along with a brief video as he coyly discusses the inspiration of his work. Mildly annoyed, she silences the video with a gesture and other information about the piece dominates the viewport. The painting is for sale (big surprise there, she muses) and the price is listed at 700. Impasto. That's the word she was looking for. That kind of painting is 'impasto'.

Being a little over her budget for retro-art paintings, she browses around a bit more before lazily drifting back out to the street. Looks like that wall above the sofa is staying blank for now. Walking further down, she happens upon an open air exhibition with some pleasant but unoriginal work—more of the same-old-same, with even a still life of fruit (who would buy that?) on display. She does a double take before looking back at a tranquil oriental-style river scene, comfortingly unremarkable yet possessing a certain serenity that she enjoys.

Pleasantly surprised when a very reasonable price appears along with no annoying video, she imagines that this is probably the thousandth time that the faceless artist has painted that scene, identical yet lovingly original in each of its iterations. Exactly what she was looking for, a mood but not a conversation piece.

Quickly purchasing the item with a swipe of her hand, she passes the delivery information to the merchant with her electronic payment, pending delivery. She watches as the price is replaced in the AR view with “purchased, delivery with escrow”. A small sound and buzz emanates from the sellers pocket, and he takes an ancient iPhone out and reviews the purchase. Her eyes warm, savoring the picturesque scene of the wrinkled man squinting at the screen in his hand. He smiles, pleasant if slightly practiced, at Anne and dips his head, reaching over to the brown paper roll as he begins to package the painting for travel. She smiles back, wondering if he doesn't speak Portuguese, or if maybe he just pretends not to—something that she feels she could relate to if she were in his shoes. Later this afternoon, she will receive the painting at her flat. when she does, she will confirm the receipt and the escrow funds will be released to the seller. She wonders if she should put an outrageous price on the painting now, just in case someone really wants it… but no. Too tacky. She hates when she goes to someones house and *everything* is for sale.

Almost tripping on her waistcoat, she bumps gently into an adorable magenta scooter parked along the street. Oh, wow, its a Tespa! She has seen these new ones around quite a bit these days, but she hasn't taken the time to see one up close and personal yet. With a battery that would last her a week of daily use and an advanced maneuvering assistant, these cute little vehicles are all the hotness for style, economy, and safety in a commuter bike. Curious, she focuses briefly on the umlaut in the center of the ID sticker, but the words “privately owned” are all that is displayed. With a subtle flicking gesture, a context menu of “for sale near you” zooms into view hovering over the sticker. There are two within a kilometer, but looking at the prices, she sighs and selects “notify me of new listings under 6235”, a preset she uses that provides her with notifications for 75% or less of the relevant price.

Making her way towards her favorite spot at the park, near that one street vendor with the empenadas from heaven (or is it really heaven, with all its wicked temptation?). Bending to sit at her favorite bench, she muses about whether or not she should put a reward on her “phone” as she feels the coldness of the bench soaking up through her coat. She “lost” it yesterday, but she’s starting to think maybe it was lifted from her pocket? Not that she really needs it anyway, but being kind of old fashioned (but *definitely* not a hipster, she told herself reassuringly), she still carried one. There was something just a little more *real* about looking at words on a screen instead of reading them floating in mid air.

Anne thought to herself that maybe she should let that habit go anyway. No one from her generation (or her mother’s) or really, hardly anyone except wrinkled old men and anachronists – used phones, but she decided to set 19.9997 as the reward instead That would cover the network fees to an even 20. She went into the myStuff app (she still used MyStuff, even though

the interface was a little dated, and there were much more modern PrüF wallets) and selected her phone with a subtle pinching motion, flicking it up onto the center of her view. She quickly changed the status of the sleek rectangle to “lost’, and enabled a “reward if returned” flag.

Chastising herself for being careless, she cringed over her embarrassment in thinking someone had taken it. No one did that anymore, except out of pure malice. What would you do with a stolen thing anyway? No one will buy it, unless you can somehow change the serial numbers - and even then, an unlisted, used item? Pretty suspicious. I guess you might be able to sell the parts, but at that point, who would bother?

Birds chirped overhead, (at least Anne was pretty sure they were real birds) as she watched two children playing what seemed to be a game of tag around a grassy mound. Wistfully drifting between thoughts, she was startled when a voice came from just beside her. It was Martim. He was a little late, of course, but she expected that.

“Oh, hi, I was just wondering where you were!” she said. (she wasn’t, but she wanted him to think she was) “You owe me 20.” smiled Martim. “What?” “Just kidding. You left this relic at my house yesterday, thought you might want it…” with a sudden recollection, a playfully feigned puzzlement was written across her brow. Martim continued: “I saw you put a reward on it… you really are a luddite, you know that?” “Oh thanks..” she said, mildly amused at herself and rising to her feet—Martim wasn't wrong, really. As they walked together towards the river, a tourist gondola was sliding silently by on the other side. They paused, near the riverbank, at the faux-rust stained railing. Taking in the scene, a moment of silence ensued as the boat passed, a sun worn older gentleman adjusting his glasses at the bow of the narrow craft. As if on que, they turned toward each other as the beautifully painted transom of the boat came into view. Looking away to the river, Martim said, with a hint of a smile, “forget the twenty, you can buy us a pizza”.

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, scaleable, persistent, and to eventually 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 incentivise

behaviors 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 customers 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 PRüF ecosystem will consist of the PRüF foundation, Independent business units (Asset Class operators), the developer community, and, of course, PRüF asset rights holders. After initial launch and beta phase testing, PRüF will be fully open sourced and community development opened to all.

A large but ultimately limited number of Asset Class utility tokens will be distributed.

Asset Class business unit operators will be able to set and collect fees from asset management services, transfers, inscriptions, 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 Asset Class Token represents a turnkey backend solution with minimal front end customization requirement to be a PRüF service provider in a given asset class. Asset Class Tokens are like a key, used to control the pricing, payment, contract authorization, and namespace for their Asset Class, so that searches and lookups of their particular focus will lead to their online presence and customer interface.

Each Asset Class (AC) 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 AC, in the same root. Asset rights holders can move between AC's 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 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 an Asset Class Token holder.

As each type and region of asset will face unique challenges and customer needs, this ecosystem approach provides 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 (after all, if this one says stolen, and this one says you are the owner…who should I trust?). Providing a ready-for-customization deployment with prebuilt infrastructure gives PRüF and PRüF partners a strong first mover advantage in every potential market segment.

All assets are represented by lightly augmented ERC20 compliant tokens. In some asset classes, operators will mint new asset tokens into the controlling contract. This (custodial) model is ideal when an asset class must be supervised by trusted agents. In this model, agents provide a necessary or convenience enhancing trust function. In other asset classes, asset tokens will be minted to the customers wallet, under their full control. (non-custodial). Customers may move their asset between qualifying custodial and non-custodial asset classes within the same root asset class. The use of this dual model allows accommodation of the wide variety of needs that may be encountered in such a diverse global market.

In the event that a customer loses control of their Asset token, it may optionally be recoverable by the use of a predetermined secret, re-minted into a new wallet under their control. This feature is still experimental, but we expect to make it an option to customers to reduce the otherwise brittle nature of dealing with the blockchain. Online wallets and other token securing mechanisms will doubtlessly be made available by 3rd parties as the ecosystem grows.

In the PRüF ecosystem, an asset can be marked as nontransferable, transferrable, in escrow, discarded (recyclable), transferred, lost, stolen, and other statuses. This status is available quickly, freely, and securely anywhere internet access is possible. These statuses govern the mobility and mutability of the asset record, and inform potential buyers, sellers, and owners of assets as to the current status of asset provenance and ownership.

There is an incentive built into PRüF to encourage re-sharing of still-useful discarded items, by incentivising 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 one 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.

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

1: The cryptographically derived "shadow" for the item itself

2: The cryptographically derived "shadow" for the rights holder

3: The status of the asset record, transferrable, nontransferable, etc.

4: Then 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 could be 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.

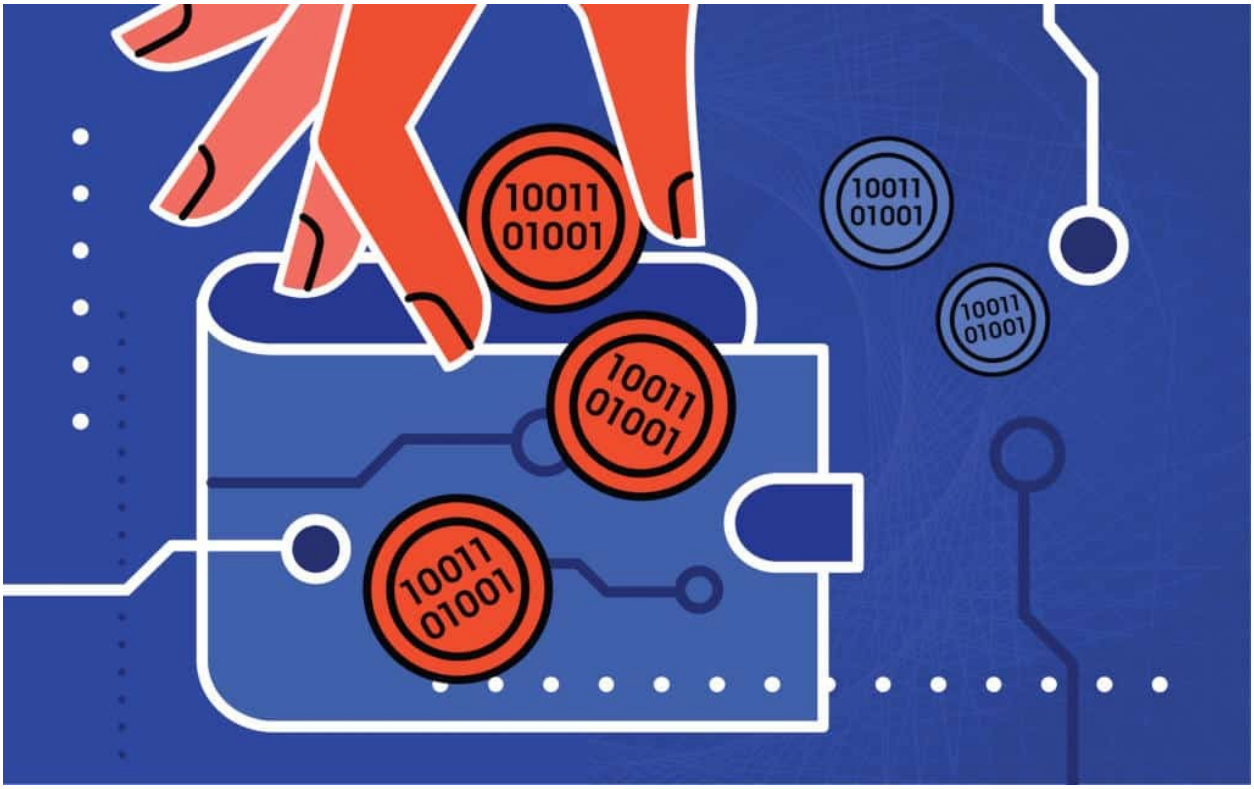
In addition to these 10 data points, additional data is stored on chain as needed to accomplish other use case specific business logic. Authorized modular contracts handle such ancillary functions, and connect to the core PrüF infrastructure through an intermediary interface manger contract. These contracts can be written for a

variety of general or very specific use cases, and may include auctions, contests, various kinds of structured sales, escrows, asset collateralized loans, surety bonds, or other instruments.

For lightweight, low granular value applications, PrüF utilizes a much lighter footprint model which can have the same, or even expanded functionality by leveraging IPFS as a primary storage medium. This can minimize blockchain related expenses and allow for zero marginal cost operation for less critical asset classes.

Manufacturers can create, in bulk, “light assets” which are preregistered on the blockchain at a very low cost, facilitation onboarding of new items and providing an opportunity for enhanced customer interactions, including customer education and brand awareness, service agreements, warranty registration and service, technical support, additional sales opportunities, etc.

With flexible, extensible architecture 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, and with a simple set of tools that enable positive transactional asset control on a variety of scales.



PrüF Token Integrations and tokenomics

In its most basic form, PrüF uses two types of non-fungible tokens. Asset classes are controlled by holders of a corresponding asset class token 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 token NFT's - each one corresponding to an asset on PrüF.

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

In addition to this core functionality, the PrüF team will implement **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 under the "services discount model" on the B2B side, as well as the only way to mint new asset class tokens.

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 70/30 between PrüF and the AC token holder, respectively. By freezing **PrüF** tokens in the address that they

hold their AC token in (180 days?), AC token holders can increase their earnings percentage to 90 percent, depending on the amount of **PrüF** that they hold.

After an initial buildout, AC 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 AC tokens sold, up to the maximum number of asset classes (tentatively numbered at 100k). **PrüF** Tokens exchanged for AC tokens will be burned, increasing scarcity and allowing the influx of new tokens without damaging the economics of the platform.

* *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 individual case.*

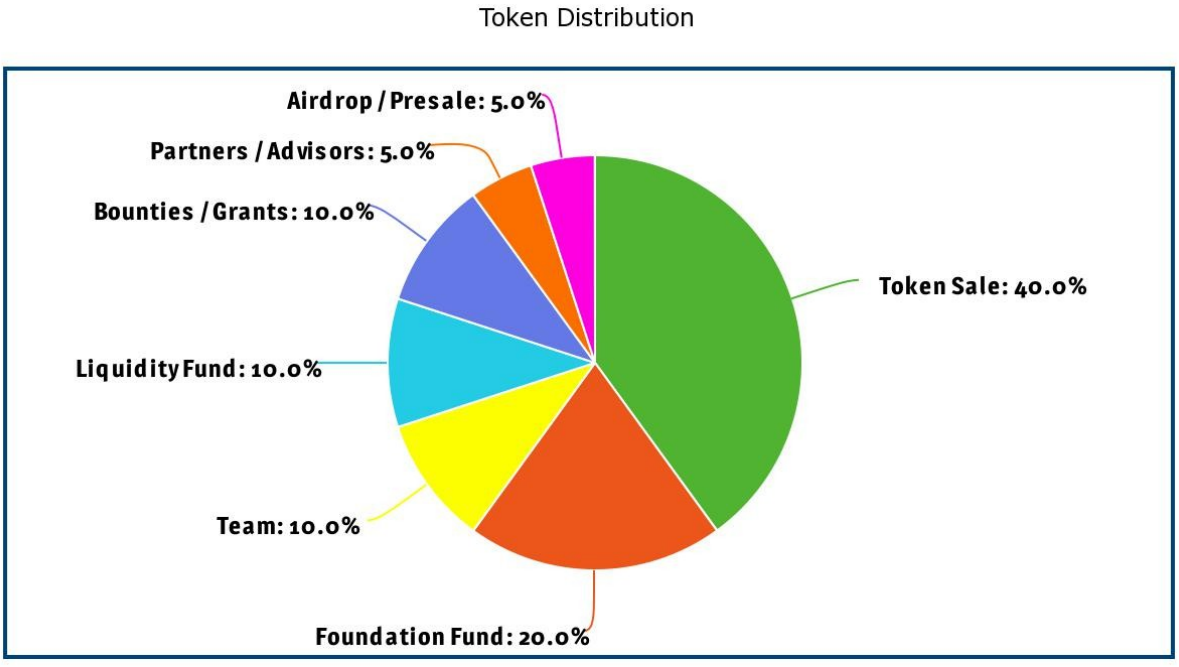
** *For especially sensitive applications, the name and ID can be replaced with a surrogate, alias or a cryptographic token, enabling perfect anonymity.*

*** 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.

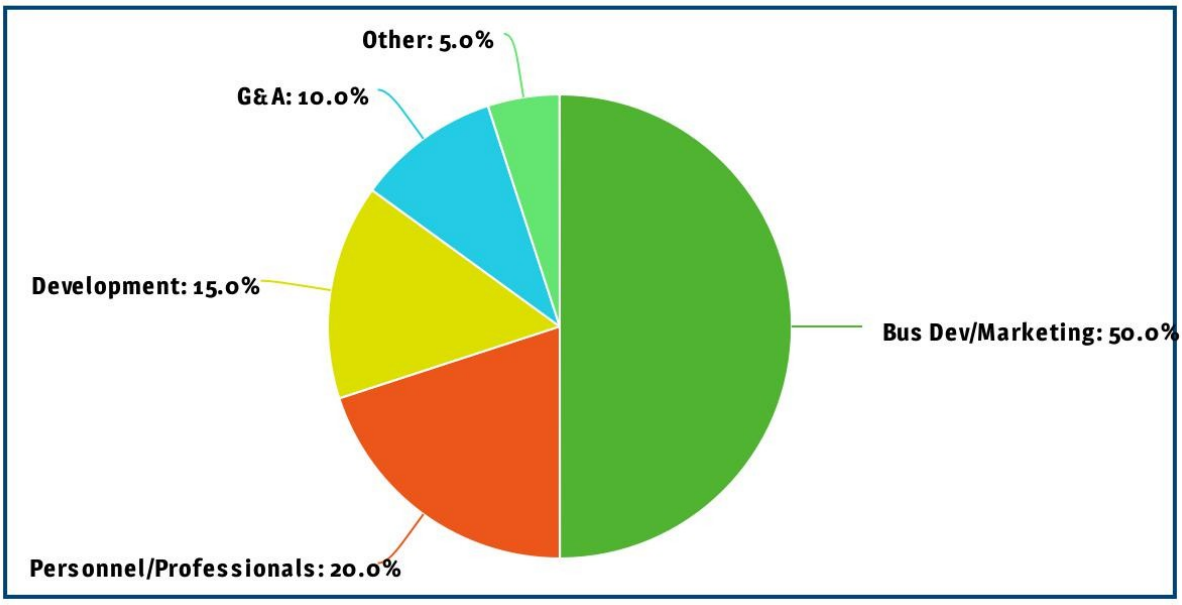
PrüF Token Roadmap

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 incentivised 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 100,000 **PrüF**.

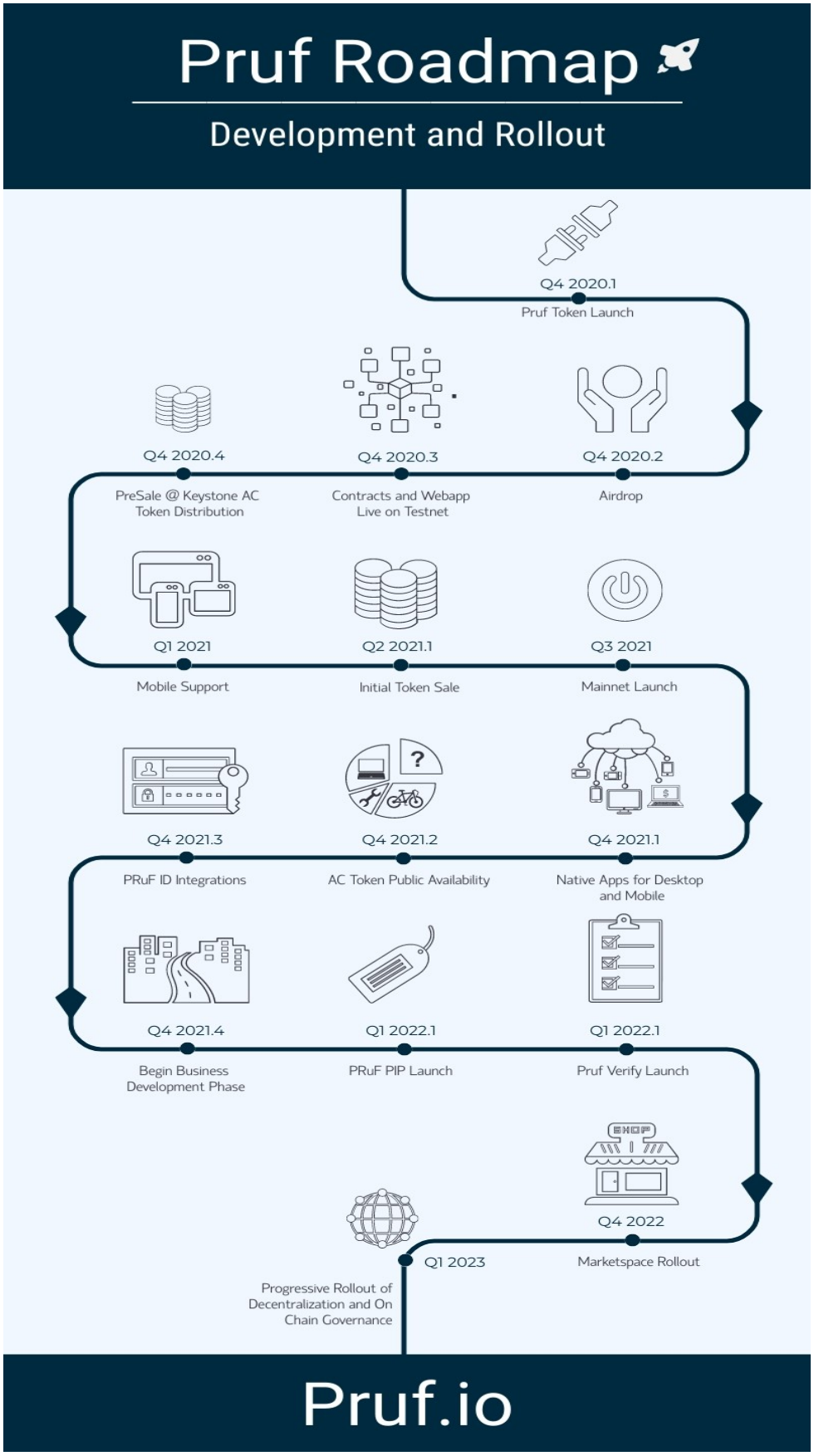


Foundation Fund Token Distribution



If 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 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, nonfungible 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 AC token partners.


Pruf Roadmap
Development and Rollout
Q4 2020.1
Pruf Token Launch
Q4 2020.4
PreSale @ Keystone AC Token Distribution
Q4 2020.3
Contracts and Webapp Live on Testnet
Q4 2020.2
Airdrop
Q1 2021
Mobile Support
Q2 2021.1
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 2022.1
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 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 in 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.

Conclusion

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 asset*s enhance the value and utility of the existing infrastructure of things while maintaining user privacy and data sovereignty.

Key Takeaways

- PrüF *Private-Provenance* secures users 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