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 your possessions were provably and privately yours, with a title on the blockchain. Imagine a world where lost or stolen items would have little resale value unless they were returned to their owner, and where lost items came home on their own.

Today, people have no way of proving that most of their valuables and personal assets are actually theirs. An original bill of sale is usually sufficient in these cases, but is often lost or unavailable if an item is gifted or privately purchased from a third party. In the absence of clear and compelling testimony or documentation to the contrary, the person in actual custodial possession of an asset is often presumed to be the rightful owner, even when they are not..

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

PRüF *Secure Transfer*[2] allows a buyer to be completely sure that the person in front of them is the actual owner of the item being sold. Using *Secure Transfer*[2] also protects the buyer, by recording the release of rights of the item by the seller as well as the (optional) immediate transfer of rights on the blockchain to the buyer.

If a PRüF *trust enabled*[3] 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*[3] assets would be 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.

In some cases, "Registration" can erode privacy and creates ancillary risks from private or government entities. PRüF *Private Provenance* eliminates this risk, even for them most sensitive of assets.

PRüF *Private Provenance*[1] allows records to be stored in such a way that ONLY the owner can prove ownership. When using the *Private Provenance*[1] feature, Names cannot be looked up in the system, cross referenced, or tracked. Additionally, items cannot be looked up in PRüF without the actual item serial number,

and for additional privacy, a secret can be included in the item record so that only the holder of the secret can look up the item at all.

With PRüF *Private Provenance[1], sensitive information is not actually stored at all.* A cryptographic derivative key of the original data is stored, but it is impossible to recreate the original data from this key, because the original information is destroyed. Sensitive information is not just encrypted, it is simply not stored in the first place.

A rights holder of a PRüF *trust enabled[3]* asset can easily prove provenance 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.

Even if recovered by the police, stolen items will often not be returned to the owner without acceptable documentation of ownership. Even in cases of a reported theft where the item has been located, the possessor is usually assumed to be the owner unless additional proof is available.

PRüF *Private Provenance[1]* 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.

PRüF *Private Provenance[1]* even reduces the incentive for theft, because stolen items can be marked as stolen or lost after their absence is noted by the rights holder. This makes it difficult to sell the stolen or lost item, because a free, quick, cursory search on any PRüF portal will indicate the item is lost or reported stolen.

The rights holder then has several options:

- They can do nothing.
- They can offer a reward for the return of the item, and register the return instructions with a return service provider. The stolen status and the reward will then be visible for anyone checking the provenance of the item before purchasing it, for example. This would make stolen items very difficult to sell, except 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.

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 (especially online channels) are not incentivised to care.

With PRüF *trust enabled*^{3} 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 with our 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 assetID with their phone. If it is real, it will show up as "Genuine, unowned". After 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. For nontrivial items, the customer then enjoys all of the protections of a PRüF *trust enabled*^{3} asset.

For online sales, the vendor can provide the asset ID of the actual item prior to shipping. Clicking through, your customer will get verification of authenticity, 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. For nontrivial items, the customer then enjoys all of the protections of a PRüF *trust enabled*^{3} 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.

Counterfeit currency is a global problem.

Beyond fake goods, as many as one in 40 currency notes are estimated to be counterfeit in some major western economies. This amounts to a significant "tax" on legitimate economies by criminal actors, and the situation can be much worse in the developing world. PrüF can track large bill currency 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, 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, 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 protocol. If a bill marked as "held" in your wallet is stolen, it can be marked as stolen in PRüF and be much harder to pass to someone else. When you wish to spend your bill, just scan it and mark it spent, and the accepting party will see that it is clean and safe to accept. Passing fake or stolen money just got a lot harder, and avoiding getting stuck with a counterfeit or note a lot easier.

PRüF can offer all of this as a very low cost, turnkey solution, or can give you the tools to fully integrate authenticity verification into your online presence, no blockchain development required. Our product is 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 blockchain solution for your asset provenance needs.

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

PRüF was designed from the ground up as an ecosystem, and is designed to be upgradeable, persistent, and to survive transfer to a foundation or even core abandonment.

The core values that PRüF is built to exemplify 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 – To the extent possible, PRüF systems will be built in such a way that they do not inadvertently or intentionally compromise the security, privacy, or agency of the user. PRüF will protect the privacy of its users by collecting the minimum information required to provide the desired service, and informing users of actions that may put their privacy, security, or agency at risk.
- Personal Agency - However practical, PRüF will aim to increase the freedom of the user from the external application of coercive force, whether financial, physical, or social.
- Sustainability - As a blockchain based service, PRüF aims 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 environment in which we all must live.
- 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, while not making PRüF a useful tool for fraud, theft, or coercion. Any tool can be misused, but the PrüF ethos seeks to minimize the usefulness of PRüF to deprive others of their rights, freedom, or property.

As 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, logistical, 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.

- The cryptographically derived “shadow” for the rights holder
- The status of the asset record, transferrable, nontransferable, etc.
- Then number of times, if any, that a record has been edited (only applies to certain asset classes that may have administrative oversight)
- the asset class that the asset is inscribed in
- A decrement only counter, and its starting point. This could be used to track consumables or remaining service life, for instance.
- An updatable pointer to an optional IPFS file, typically A json data structure including pointers to media, information, and files. ****descriptions, photos, other
- 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.
- 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, "naked assets" which are preregistered on the blockchain at a very low cost, facilitation onboarding of new items and providing an opportunity for post-sale customer interactions, including service contracts, 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.

The following tokenomic roadmap is a rough draft, and serves only to elucidate our overall conceptual plan for PrüF tokenomics. We will bring in a qualified economic advisor prior to formulating a final plan, because we are blockchain developers, not economists.

*"Up to 1 billion **PrüF** will be initially minted. Initial disbursement of ten million will be by an opt-in airdrop, with the next 90 million airdropped in subsequent promotional airdrops over the following years for maximum effect. The dev team will retain 300 million **PrüF** which will be trickle-unlocked over 5 years, ensuring that they are incentivised to produce the best possible product. An additional 200 million **PrüF** will be retained by*

the PrüF foundation for bounties, incentives, and community development. 200 million will be slated for further promotion, and 200 million will be held as a reserve to balance the economic model in case of critical scarcity. The hold amount to enable an asset class for 90% revenue capture will initially be 100,000 ***PrüF****.*

If available supply of unburned tokens drops below 11 million ***PrüF*** *and no more liquidity buffer tokens are held by the foundation, more tokens may be minted to avoid a critical liquidity crisis."*

Or, something like that.

We 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 as a long term fractional holding in PrüF earnings.

DAY IN THE LIFE marketplace

- QR
  - ART EXAMPLE
    - art gallery
    - gateway game
    - IPFS details
    - pricing, medium, details, history,etc
  - put items up for sale
    - yard sale
  - scan code brings up markeptplace
  - can be pruchased
    - partnering
      - ebayish
    - nearby items for sale

**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 a subpoena 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.*

PRODUCT/SERVICE/METHODOLOGY

Describe the methods and demographics you used to obtain your data. Why did you choose the research tactics you implemented? How will this strategy inform on the topic you're covering?

KEY FINDINGS

Key Findings #1

Research and argument

[To replace a photo with your own, just delete it and then, on the Insert tab, click Picture.]

Key Findings #2

Research and argument

Key Findings #3

Research and argument

Visual Data

Insert any data tables/charts/graphs/infographics etc.

CONCLUSION

Time to wrap it up. What is your conclusion? How would you synthesize all the information into something even the busiest CEO wants to read? What are the key takeaways? How does your product/service/methodology uniquely address the issues raised by your study?

Key Takeaways

- Takeaway #1
- Takeaway #2
- Takeaway #3