

# PRÜF

A blockchain based asset  
tokenization ecosystem

## TABLE OF CONTENTS

Concept	3
PRÜF MarketSpace for a local-first global market	6
PRÜF Verified – brand trust, anti-counterfeiting, and theft deterrence	7
PRÜF for creators	10
Technical overview	12
The PRÜF ecosystem and core values	22
PRÜF tokenomics	25
Community Governance	27
State of the project	29
Key takeaways	30
Roadmap	31

# PRÜF that it's real.

Proof that it's yours: feature-rich tokenized real-world and virtual assets.

PRÜF is a blockchain-based protocol for creating and managing **digital and physical assets**. Whether holding digital media or acting as a "title" to everyday goods or virtual property, PRÜF tokenized assets allow rights holders to hold securely, transfer, sell and collateralize their possessions without opening their lives to scrutiny. **Data and media stored using the PRÜF protocol doesn't depend on servers or centralized services.** The protocol provides options for low-cost permanent blockchain storage, creating timeless and durable assets with **no maintenance overhead, ever.**



PRÜF enables developers, individuals, and teams to issue media-rich, customized NFTs for projects from digital art to real estate without writing a single line of blockchain code.

With features like on-chain permanent media storage, self-contained presentation context, branding, and verifiable provenance, **PRÜF is the decentralized low or no-code solution** for brands and artists to tokenize and create verifiably authentic assets on the blockchain. PRÜF assets are designed for permanence, offering an **exceptional value proposition to end users.**

PRÜF makes NFTs what they should have been from the start – brandable, secure, private, permanent, functional, and self-contained. Many current NFT digital assets from major **platforms will become dead internet links** when their website goes down. In contrast, PRÜF based NFT, even a game or application – can be stored entirely on the blockchain – continuing to work long after the creator has forgotten any thought of paying server bills to keep it running.

Whether used by artists or manufacturers, PRÜF fights fraud and counterfeits – protecting brand integrity by verifying authenticity and provenance. The PRÜF protocol provides enterprises and creators with their own **unique blockchain minting identity**, empowering brands to quickly create digital or physical assets exclusively **tied to their online trade and media presence**.

As a decentralized **protocol instead of a platform**, PRÜF enables brands and creators to manage their blockchain presence and provide a curated customer experience with feature-rich, tokenized digital and physical offerings. Luxury brands don't have to worry about ending up next to a trading card, and artists can be sure their art will be presented as they wish. With PRÜF, **creating a personalized marketplace or exhibit is easier than ever**, and smaller projects can leverage an ecosystem of existing portals and markets.

## **Imagine a world without counterfeit goods and brand piracy.**

PRÜF makes it **instant, free, and easy** for buyers to verify the authenticity of items before they buy – **no download required**.

Counterfeit and fraudulent 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 PRÜF, 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.

## You work hard for what you own.

Imagine a world where theft or seizure was less lucrative, and possessions and assets were **provably and privately yours** with a title on the blockchain – a world where lost or stolen items or even cash would have little 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 – and finding a private or commercial seller for something you see is as easy as choosing "for sale near me". Imagine purchasing a one-of-a-kind item through the window of a closed local boutique and having the article show up later at your door – effortlessly and costlessly enabling **local and global e-commerce for every "mom-and-pop" store** by democratizing front door access to the marketplace.

**...Imagine a world with PRÜF.**

## Existing systems facilitate the resale of stolen and counterfeit goods.

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

PRÜF Secure-Transfer allows a buyer to **be sure the person in front of them is the actual owner** of an item offered for sale. Secure-Transfer protects both the buyer and seller by documenting the release of ownership, with the option to transfer rights to the buyer on the blockchain. **PRÜF makes selling stolen property more difficult than ever.** A free cursory search on any PRÜF portal can indicate that the owner reported the item as lost or stolen, reducing value and options for would-be thieves.

## If an item is missing, PRÜF gives you options.

If a PRÜF 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 from any web-enabled device is easy, fast, and free**. Dealers, shops, or private buyers will adopt PRÜF Trust-Enabled assets as part of reasonable due diligence.

**'Registration' as it is known today can erode privacy and create ancillary risks from private or government entities. PRÜF eliminates this risk, even for sensitive assets.**

PRÜF Private-Provenance allows records to be stored such that ONLY the valid owner can prove ownership. When using Private-Provenance, 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 only the secret-holder can see the item at all.

In addition to everyday items, digital art, and capital goods under personal ownership, PRÜF tokenized assets enable discreet and protected arms-length control options.

## A truly democratized, local-first global MarketSpace with PRÜF

PRÜF tagged items can be scanned to find other identical items for sale, either by local businesses, private parties, or e-commerce giants. **Instant discovery** and seeing-is-believing confidence – **the world is the showroom.**

## PRÜF MarketSpace vision

By scanning a PRÜF data tag (or even just looking at it, with Augmented Reality), any data 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, a placeholder might be displayed instead. Likewise, if the item is for sale, price and sale information will be displayed along with any special 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, **any seller or private individual can effortlessly "list" their items on a global marketplace** with a robust local-first aspect. When examining an object, a potential buyer could search "similar items near me," for example, and local listings for similar or identical items could be shown as options, backed up by listings from major suppliers and distributors. In addition, local listings would be given top visibility, so users would be incentivized to provide "advertising" by displaying and listing their

items in the system. This alignment of incentives allows for integrating a **local-first marketplace with global reach and deep supply backing**.

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.

PRÜF enabled tokenized assets align perfectly as an **opportunity for partnering with marketplace integrators**. Such an integrator could blend existing industry-scale supply chains with a local marketplace of pre-owned and artisanal items, combining the advantages of proximity marketing with deep supply and distribution backing. By leveraging this model, **online-only retailers effectively convert the world into their physical showroom**. More prominent vendors benefit from increased sales opportunities as well as long-tail customer engagement, while local vendors and individuals benefit from proximity marketing. With effortless point of exposure shopping and profound brand integration possibilities, we expect this opportunity to be an attractive option for e-commerce at scale.

### **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 has 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 any smartphone camera verifies that the item is genuine** and the ID unused. If a brand pirate tries to falsify asset IDs, they will show up as fake. If they try to reuse an actual ID from a legitimate product, it will show up as already used (and therefore not registrable) after the first customer registers that ID on the platform. PRÜF Trust-



Enabled adds value and a premium nuance to products while **reducing the threat of brand theft with little infrastructure investment and a nominal unit cost.**

After the sale, onboarding, registration, and subsequent verification of the item's authenticity generates valuable insights for the brand through customer interactions. The protocol facilitates onboarding second-party owners, bringing them to the brand's website, offering additional information, and offering service contracts or upgrades – all value generating interactions.

### **PRÜF delivers a low-cost, turnkey solution to end brand piracy.**

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.

PRÜF can provide manufacturers or vendors with 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 nontechnical, individual creators as it is to Fortune 500 companies.

### **PRÜF Verify can disincentivize theft for cash businesses.**

Robbery and theft are **common pain points for nearly all cash businesses.** Using PRÜF Verify, a company 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 bank's inventory. For high-risk locations, cash drawers or overhead camera systems could automatically scan high-value bills in or out. **Any cash theft would result in stealing "marked" bills,** tied to the robbery or theft, making use fraught with risk.

Bills held by the bank would be scanned out of inventory 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 minimal

cost. Aligning incentives against malicious actors makes dollars and sense, and private and public insurances will be quick to recognize these advantages.

## 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 another entity such as a bank, store, or other trusted 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".

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 resulting 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 us all.

## PRÜF enables creators.



Many potential NFT based projects are launching with web developers with little to no blockchain experience, facing a steep developer onramp for developing secure blockchain applications.

While PRÜF was initially conceived as a global solution for **private and secure asset management**, the protocol built to achieve that goal is almost universally ideal for all kinds of tokenization scenarios and includes a wide variety of built-in features that **make implementing an NFT based project more accessible and extensible than ever before**.

PRÜF makes NFTs what they should have been from the start – branded, secure, private, durable, functional, and self-contained.

NFTs created or wrapped in PRÜF have built-in features for metadata, file or multimedia storage on-chain or on IPFS, business logic for accepting payments in multiple fungible tokens and cryptocurrencies, escrow and loan contracts, controls on transferability, and a host of other immutable and mutable characteristics and features. PRÜF NFT assets can even contain a **built-in presentation context stored on-chain**. These assets may require **no web servers or support infrastructure** -- and can even include client-side JavaScript integration so that a game or collectible series can remain playable long after the company supporting it no longer exists.

## Up and running in minutes instead of months.

With a few minutes of configuration in the ACNode manager portal, teams can launch their NFT within our thoroughly tested and audited contract network, eliminating expensive and time-consuming contract development and audits.

Developers can deploy NFT dApps by incorporating PRÜF Node.js libraries into their websites or adapting our sample react template. Using the tooling we provide, developers can design the features, look, and feel desired for their project in a fraction of the time required for ground-up development. Using the ACNode management portal, developers can deploy their token, defining their data schemas and customizing the scope of the business logic that will apply to their token—all **without writing a single line of contract code**.

The resulting **standards-compliant token** is deployed within a recognized universal NFT network on the blockchain, with a contract-origin pedigree making them instantly **recognizable, tradeable, and interoperable** with other major platforms.

Each ACNode (token minting authority) can define a unique name for their NFT, automatically preventing others from using their label and related namespaces in the system. This creates valuable branding IP for developers. The ACNode token itself also represents a tangible asset that can **help make projects more fundable**.

Tokens created with PRÜF can be made **automatically monetizable**, requiring payment to the ACNode holder (token founder or delegated address) for operations such as the modifications of mutable characteristics, status changes, or transfers. Costs for **revenue-generating events** can be set individually and range from no cost to whatever price a developer chooses.

All NFT assets produced using the PRÜF protocol are standards compliant to ERC-721 and fundamentally interoperable, though they vary widely in added content and functionality. In addition, PRÜF assets can be viewed and interacted with within a shared infrastructure, enabling a diversity of markets, trading platforms, and galleries that work with compliant NFTs inside and outside the PRÜF ecosystem.

The PRÜF protocol solves data permanence, branding, and authenticity in the blockchain tokenization space.



### Technical Overview:

The PRÜF ecosystem consists of the PRÜF contract infrastructure, PRÜF users, and PRÜF nodes. The PRÜF protocol operates from a tightly integrated network of upgradeable contracts. The core of this structure is the primary storage contract, which integrates sparse business logic associated with secure asset management. Closely tied to this are the Node manager, Escrow manager, and Verify contracts -- all of which also hold additional local data. Although these contracts curate critical data, they are still upgradable using a "replicate-on-read" migration pattern. For protocol updates, contracts can be "hot-swapped" in place without interrupting service, using our contract name resolution system.

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

The users of the PRÜF system are individuals or organizations seeking to establish secure, private provenance and control of physical or digital 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. Each kind of object being tokenized benefits from a customized experience tailored to the specific asset type and region. 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 of their users. Node operators earn PRÜF tokens through fees for service, direct advertising revenue, or sales from in-portal commerce. Some Node

operators representing more prominent brands may opt to make their systems free to their customers to increase engagement and brand education opportunities.

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

By requiring **token-burn to mint Node tokens**, PRüF incentivizes Node operators to build effective service models and offer a pleasant user experience catered to users' needs within their market niche. By ensuring Node operators have something at stake, PRüF encourages responsible operators who seek to provide valuable services while discouraging "spammy" nodes or bad actors. Since Node tokens can be renamed and retain their utility if transferred, **Node tokens represent a tangible asset** that gains value with the popularity and brand presence of the Node.

For fee-for-service operators, PRüF captures a fraction of generated revenues. Funds from revenue shares are divided between stakers on that Node and provide funding to the PRüF foundation for **ongoing development and innovation in the PRüF ecosystem**.

Since PRüF does not store personally identifiable information by default and all data 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, which PRüF can allow. In other cases, users may require absolute secrecy while maintaining trustable verifiability. In this case, a robust arbitrary length passphrase "salt" can be added, 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 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 in conjunction 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 registration 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 holding 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 decentralized or supervised by a Node operator, the PRÜF protocol, when properly used, offers **robust protection against malicious actors of any scale**.

## **The PRÜF contract infrastructure uses 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.

**PRND** - The PRÜF Node token (PRND) acts as a control key for operating PRÜF nodes. Holders of a PRND token have the ability to operate a PRÜF Node, which acts as a portal for users to interact with the PRÜF system. The PRND 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 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.

In general, only the PRUF and PRND 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.

## How PRÜF works, a walkthrough:

The first step to onboard an asset into PRÜF is tokenization. Tokenization is accomplished either by a content creator, manufacturer, certifying entity, or an individual or organization that wishes to onboard their own physical or digital assets.

The process of tokenization begins by identifying the uniquely identifiable features of the asset. This may consist of the manufacturer, model, and serial number of the item, along with any other class-specific features. For example, in the case of Digital-content NFTs, the class will be tied to the specific brand, artist, or agency.

Once identified, this information is entered into a PRÜF portal (the web interface for a PRÜF Node) by an ACNode (PRND) holder or in unrestricted asset classes, a credentialed entity or person. If the asset is made hidden (secret) on the PRÜF platform, this information may include a passphrase or secret key.

It is important to note that information remains local to the terminal (web browser, app, etc.) in this process and is not transmitted over the internet or stored in PRÜF. Instead, this information is used locally to create a robust cryptographic hash through multiple cryptographic hashing operations. The original data is lost to entropy in this process, so it is mathematically impossible to recreate the original information from the resulting hash, known as the idxHash.

Once the idxHash has been created, another hash is made from data supplied by the user for owner identification. For example, a user might provide a company name and license number, an individual name and ID number, biometric data, or other verifiable information that an owner can use to differentiate themselves uniquely.\*\* 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. Without this critical step, it would be possible to scrape the blockchain and compile a list of rgtHashes and the assets they correspond to in a potential metadata attack on user privacy.

With the rgtHash hashed with the idxHash, an attacker would need a user's complete identity information and all 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.

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

If the item is physical, a QR label could be printed to attach to the item using any label compatible printer, for instant, effortless, and cost-free lookup of the item in the PRÜF system. It should be noted that looking up an article on PRÜF requires either the computed idxHash, or the complete item information, including manufacturer, model, serial, or any other (including potentially secret) information used when the original idxHash was created. Looking up an item on PRÜF does not reveal any information about the owner, and only the owner can verify their ownership of a properly configured item.

Once the tokenization process is complete, the item can 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, moved 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 "stealthy" are easily retrieved from the blockchain using our app or website. If the listing were made "stealthy" by including a secret in the item data, that secret would have to be known to look it up. In this way, it can be instantly verified if someone presenting an item for sale is the registered owner. If an item is lost or stolen, the owner can mark that in the PRÜF system, so anyone looking up an article will see that status. A shopper can scan an item in a store 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 safe, 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 core PRÜF protocol tracks 9 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, a record has been edited (only applies to certain asset classes that may have administrative oversight).
- 5: The asset class, or Node, that the asset is minted in.
- 6: A decrement-only counter, and its starting point. This is used to track consumables or remaining service life, for instance.
- 7: An updatable pointer to content addressable storage (CAS), typically A JSON file including pointers to media, information, and files, also stored as CAS either on chain or off. (descriptions, photos, etc.\*\*\*).
- 8: An immutable pointer to content addressable storage (CAS), typically A JSON file including pointers to media, information, and files also stored as CAS either on chain or off. This might typically be used for certifications of authenticity, valuations, documentation, and other persistent information.
- 9: The number of times an asset has been transferred.

**The PRÜF protocol manages asset provenance and business logic, facilitating the private and secure management and transfer of assets.**

The basic PRÜF protocol provides functionality for authenticity and ownership verification as well as the direct or mediated transfer of assets. Additional PRÜF "escrow" protocols such as PRÜF-Recycle further extend functionality for PRÜF tokenized assets.

Although PRÜF was explicitly designed for privately and securely managing the provenance of physical items, PRÜF tokenized assets can also include virtual items such as NFT media content, legal contracts, token wallets, other asset tokens, access keys, licenses, or other documents. Images, media, documents, software, or data of nearly any kind can be **stored permanently and without ongoing costs with PRÜF**. For content-based NFTs, the minting Node provides a touchpoint for ensuring that tokens are **authentic and authorized**. Combining verifiable authenticity and self-hosting media with permanent on-chain storage, the PRÜF protocol presents an **exceptional value proposition for tokenized media offerings**.

## **PRÜF supports secure in-person transfer of assets.**

In secure-transfer, a receiver or buyer verifies the ownership of the asset by the provider or seller. The seller first **proves ownership** by demonstrating they can reproduce the item's 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 buyer's 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. In this case, 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 verification, an asset will require transfer or modification of the rgtHash to be once again verifiable in this way.

## The PRÜF infrastructure is infinitely extensible.

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. As a simple example, an asset can be 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.

Using this escrow system, PRÜF incentivizes the responsible discarding of still functional 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 things instead of throwing them in the trash.

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

For example, the PIP (Product Initiation Protocol) contract enables manufacturers to authenticate goods at a low per-item cost. Once the item is purchased, it is then registered by the buyer in the manufacturer's PRÜF portal. Thus, PRÜF PIP provides a turnkey, low marginal 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 "container". The master token acts as a key, enabling the holder to check assets in or out of the container. The PRÜF-Verify protocol counteracts theft or counterfeiting of serialized fungibles for entities that handle significant volumes of serialized holdings in a single class.

**PRÜF provides turnkey solutions at common pain points for NFT issuers, users, manufacturers, and resellers.**

Buyers want to buy genuine products from legitimate sellers. PRÜF enables lifetime verification of authenticity and provable provenance while providing simple systems for transferring ownership or managing assets, adding value for users. Even a yard sale can gain added value from PRÜF, establishing the legitimacy of ownership and the verifiable authenticity of items for sale. PRÜF effortlessly opens up global e-commerce to small businesses – no signup, no barriers, no fees.

For content-based NFTs, using Node keys (PRND) as a requirement for token minting in PRÜF not only protects token buyers, it also protects content creators and minters. The protocol protects Node holders by **securing their unique space within the ecosystem and preventing their brands from interference from bad-faith actors**. In addition, the PRÜF community governance DAO can quickly deal with dishonest actors within the system, clearly marking fraudulent tokens.

The PRÜF protocol solves data permanence, branding, and authenticity in the asset tokenization space. DAO managed, with built-in commerce and curated brand experiences, PRÜF offers a trusted, no-code solution for brands and creators to bring permanent NFT assets to a multi-chain, distributed ecosystem. The PRÜF protocol makes tokenization what it always should have been : Verifiably authentic, permanent, decentralized, and blockchain agnostic.

## The PRÜF ecosystem

PRÜF is more than a product, SAAS, or blockchain company. PRÜF is designed from the ground up as an ecosystem – upgradeable, scalable, persistent, and will eventually operate autonomously with the PRÜF DAO.

### Our core values for PRÜF:



**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 user's computer. Only the irreversible hashes made from that data will be stored on the blockchain.

**Safety:** PRÜF systems are engineered so they will not inadvertently or intentionally compromise users' security, privacy, or agency. 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 we all share.

**Do No Harm:** The developers of PRÜF are committed to building a tool that positively impacts society. As a result, 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 PRÜF will not be used to deprive others of their rights, freedom, or property.

### Secure and extensible by design:

Since PRÜF does not hold any sensitive data, PRÜF cannot be forced to divulge customer records, names, or information about their assets. Users' 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, governed by the PRÜF DAO. Payments are handled autonomously and on-chain, as are all critical data functions.

The actors within the PRÜF ecosystem are the PRÜF foundation / DAO, 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 will open. On-chain governance will be implemented as the project moves forward from the beta testing benchmark.

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 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 needed 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 Node, 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 they are qualified to be in by ownership, geography, or other factors. Still, 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 their web presence as a PRÜF-Node operator.

As each type and region of Node 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 source of truth for all providers allows everyone to benefit from network effects and protects the PRÜF ecosystem from the potentially adverse 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 assets in the PRÜF ecosystem promotes the re-homing of things in the real world, reducing waste, environmental footprint, and atmospheric carbon production.

The PRÜF protocol infrastructure is modular, upgradeable, and security-forward. PRÜF data manipulation and storage functions are handled by contracts that only connect to other trusted contracts. Edge interfaces are handled on a once-removed basis. 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.

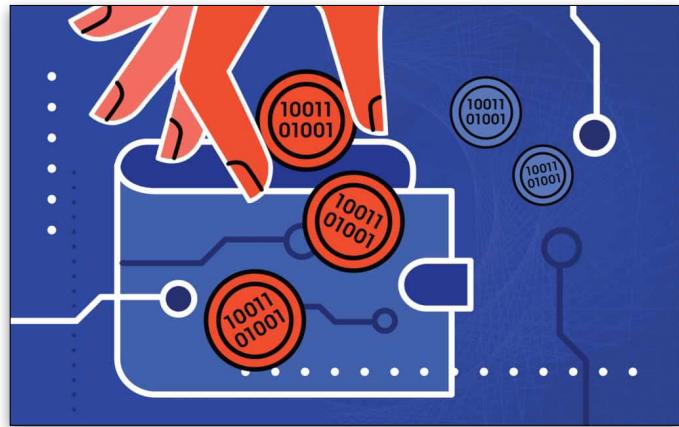
\* This feature is not trustless and may compromise secrecy for sensitive users. In the case of lost asset recovery, this information would only optionally be provided by the rights-holder to facilitate the recovery of their lost item. Items marked stolen or lost but without contact information would 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 we have created a protocol framework that protects the interests of users and stakeholders.

## 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 Node token (PRND) that acts as an authorization key to enable them to change the pricing and payment parameters of their Node. Assets themselves are represented by asset NFTs (PRAT), each 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 non-fungible 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 that helps scale and secure the economic growth of the platform. Designed primarily to align development incentives and community governance of the protocol, PRÜF will function as "gas" for fee-based operations and under the "services discount model" on the B2B side.

PRÜF is burned in the minting of PRND Nodes, and PRÜF holders can stake on nodes. Token holder rewards for staking will be determined by Node revenues, distributed among the Node stakeholders.

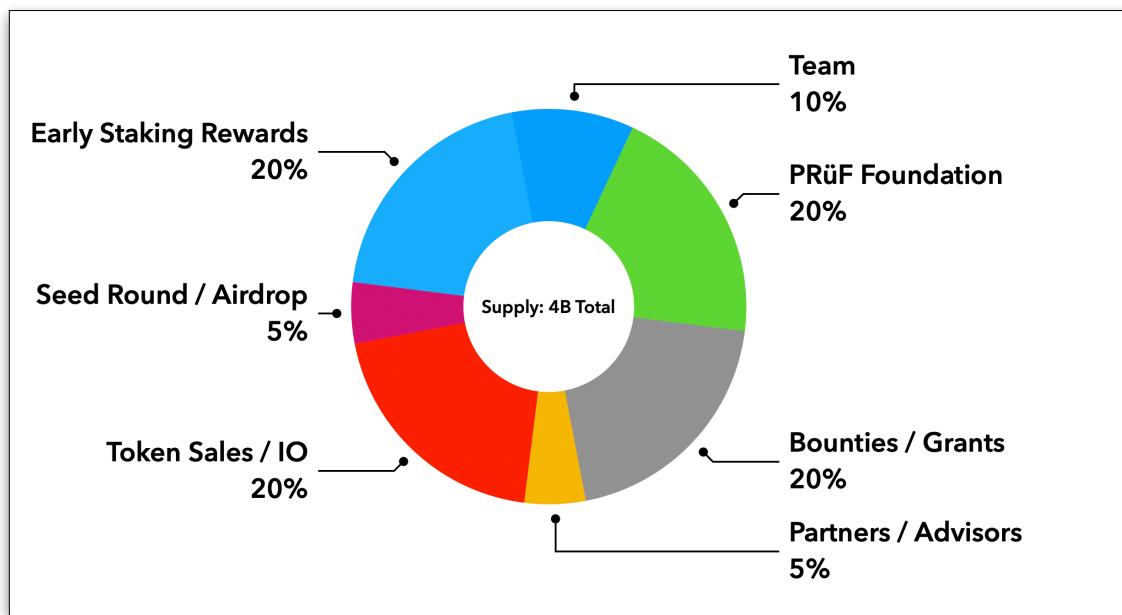
Nodes are the customer-facing endpoints of the PRÜF infrastructure and generate revenue based on monetized services and business logic provided by the Node operator (PRND token holder).

Under the current plan, 50% of Node revenue goes to the Node operator. Of the remaining 50%, A fixed 37.5% is divided among stakers on the Node. The remaining 12.5% is diverted to the PRÜF Foundation to pay for ongoing development, bug bounties, and platform marketing. In the event of

surplus revenue, the PRÜF foundation will burn or redistribute these tokens as additional staking or Node rewards.

Node operators choose fees for the use of their PRÜF infrastructure. They are set by the asset class Node (PRND) holder for the Nodes they own and operate in the PRÜF ecosystem. By default, fees are split 12.5/37.5/50 between PRÜF stakers, and the Node token holder, respectively.

After an initial buildout, PRND Node tokens will be distributed on a schedule controlled by the PRÜF foundation at a nominal 200,000 PRÜF per Node (the price may be adjusted). Half of all PRÜF Tokens exchanged for PRND tokens will be burned, increasing token scarcity and allowing the influx of new tokens without affecting the economics of the platform, while the other half will be used to incentivize node buildout and promotion through "mentor/referrer" bounties and other programs.



## PRÜF Token Roadmap

Up to 4 billion PRÜF will be minted. Initial distribution of up to ü80 million will be by an opt-in airdrop and token sale. The dev team will retain ü400 million, unlocked over four years in four equal blocks, ensuring the team is incentivized to produce the best possible product.

The PRÜF foundation will be founded with an endowment of ü800 million, and an additional ü800 million will be managed by the PRÜF Foundation for bounties, incentives, and community development. The bounty and development fund will be used for community expansion (marketing, PR, etc.) or direct payment of development, bug, or social bounties. This combined pool will be unlocked over ten years, at (up to) ü160,000,000 per year beginning in 2022. Any tokens unused from the annual disbursement will be burned each year for the first five years and then either burned or saved for further development for the final five years based on decisions of the DAO.

Initial founding investors, contributors, and advisors will receive up to 200 million PRÜF total, with all significant (over ü10,000,000) holders subject to a four-year progressive token unlock schedule, 1/4 per year as with the founders.

Four hundred million PRÜF will be distributed in pre-launch offerings and ongoing sales, and 400 million will be placed in a staking incentive fund which will be used to reward early stakers on the network, helping to stabilize token value.

Aside from this, 400 million PRÜF will be held as a reserve to balance the economic model in case of critical token scarcity, which could damage the ecosystem's growth. If the need for this fund is deemed unlikely by the foundation or the DAO, these tokens will be burned.

The amount to mint an ACNode will initially be 200,000 PRÜF, half of which is burned with every ACNode minted.

## PRÜF Community Governance

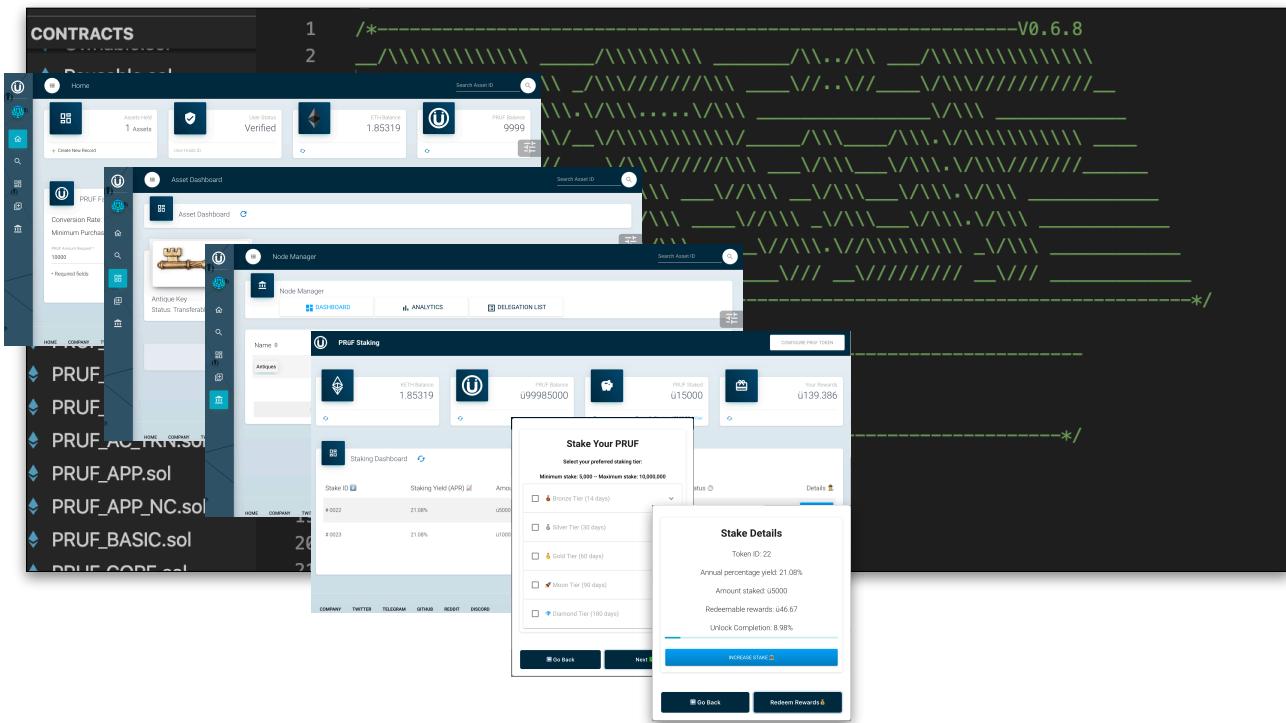
With staking open for all Nodes (PRND authorized endpoints for the PRÜF ecosystem), unbiased holders will flock to the most profitable – but not over-staked – nodes to stake on. The amount of stakers is balanced by diluting the stake revenue pool by stakers, reaching an equilibrium based on the opportunity cost of staking.



Nodes will be given voting weight in community governance based on the number of staked tokens delegated to their Node. This incentivizes economically motivated management of the PRÜF DAO. The PRÜF Foundation will work with the community-based DAO to ensure that the needs and rights of good-faith actors are prioritized on the protocol while ensuring a vibrant and prosperous ecosystem. For governance, any utility token holder will be able to propose a resolution. A resolution must meet a quorum of support by Node holders to be brought to a vote. This would typically be achieved by out-of-band advocacy to Node operator communities. After crossing the threshold quorum to trigger a vote, a resolution must gain 51% (or more, which may be established in the proposal) of the support of a quorum of Node holders. Quorum sizes may be increased (but not diminished) within the proposal framework. Nodes that participate in the vote will receive an incentive drawn from global Node earnings.

Resolutions will be limited to one per 6 epochs and will be lifted from the table in the order of the quorum size. Resolutions that fail to make a vote within 12 epochs will be postponed indefinitely and must be revived through a new quorum of support. Mechanisms to prevent unwanted vote concentration and limit other potential perverse incentives are currently being developed, and will likely be patterned after successful solutions.

Along with offering token holders a source of passive income, Node staking is expected to bring a vibrant guidance mechanism to the PRÜF community, empowering token holders and Node operators alike to steer the platform to prosperity and dynamic growth.



## Progress so far

All of the core PRÜF contracts are in beta and are undergoing extensive automated and manual testing. The contracts are fully operational and implement all 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, and we have produced a Node.js bundle and API documentation to make accessing the PRÜF ABI easier than ever.

We have completed a successful seed round. We have deployed the utility token, and early opportunity staking is live on the Ethereum network and polygon POS.

All core PRÜF features have been finalized, and modular methods of adding future features are in place. 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. Many more transaction handlers are planned for pre-release development, including release on delivery escrows, asset-backed loans, PRÜF Verify, etc. Because of the PRÜF protocol infrastructure underlying these satellite contracts, development is greatly simplified and standardized with feature-rich, secure functions available to the satellite business logic from the core infrastructure.

## Key Takeaways:

### PRÜF aligns 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.

### PRÜF creates

PRÜF empowers artists and innovators with a low-to-no code pathway to easily and simply create NFTs or tokenized assets verifiably tied to their brand. With features like nonperishable storage, branding, presentation control, and verifiable provenance, PRÜF enabled physical and digital assets are what NFTs should have been all along.

#### For Users:

- 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.

#### For Creators:

- PRÜF Private-Provenance secures a user's rights to their possessions.
- PRÜF legitimizes NFTs. Brandable, secure, private, durable, functional, and self-contained.
- PRÜF offers a turnkey, low-to-no-code solution for creators to monetize their content, without giving up control of their branding and presentation.
- PRÜF protects customers from fakes, aids in discovery and customer onboarding—all without having to be a web3 expert or writing a single line of blockchain code.

#### For Enterprise:

- PRÜF-Verify protects against theft, counterfeits, and fraud.
- PRÜF enables brands to manage their blockchain presence, controlling their image and presentation.
- PRÜF NFTs enable a curated experience, with feature-rich, tokenized digital and physical offerings.
- PRÜF can improve economic efficiencies in a broad range of domains.

# PRÜF ROADMAP

PRÜF THAT IT'S GENUINE. PROOF THAT IT'S YOURS.

