LOX WHITEPAPER

v2

LOX Network

The Global Smartphone Crime Problem

Since Apple introduced the iPhone in 2007, our lives are increasingly condensed into these small, handheld devices and have become central to everything we do. Smartphones are the ultimate do-it-all device. Everything from navigation, health monitoring, socializing, banking, payments, shopping and entertainment are all accomplished with two thumbs and a bit of dexterity.

According to a Pew Research Center report, more than an estimated “… five billion people have mobile devices …” and Statista reports that “… the number of smartphone subscriptions worldwide today surpasses six billion and is forecast to further grow by several hundred million.”

As smartphone ownership nears equaling the world’s population, smartphone crime is also on its own meteoric rise. Authorities in some countries are reporting up to 80-percent increases in smartphone theft, creating what U.S. authorities are calling a smartphone theft pandemic. A telecommunications expert estimated to Financial Times that the industry is suffering a loss of nearly $17 billion annually in insurance payouts alone.

Cell phone carriers do operate blacklists tagging smartphones that have been reported lost or stolen using the device’s unique International Mobile Equipment Identity number, better known as the IMEI. While this often does effectively prevent the stolen device from being used within the country it was stolen, it may not be effective at all should the phone be shipped to another country. A quick Google search reveals more than 646,000 results on tutorials and third-party services to bypass the block for easy activation in nearly any country. This is made possible for one simple fact: wireless carrier blacklists don't interoperate with each other. It’s a massive blindspot that enables phone theft to proliferate in a globalized world.

The smartphone theft pandemic

A $30 billion smartphone theft pandemic is, ironically, being enabled by the phone providers' own strategies designed to prevent the issue. Unfortunately, the blacklisting systems designed to stop this criminal industry often operates in silos restricted by country and network. This generally means wireless carriers' programs do not work together to assist one another, leaving massive gaps for stolen devices to go undetected.

The phone companies are, quite understandably, locked in deep competition with one another. This pushes each of them to adopt their own standards when possible, including which radio signal to use (GSM or CDMA), along with dozens of other modular choices. However, when it comes to identifying smartphones, wireless carriers have adopted one global standard — the IMEI number.

Every cell phone device is assigned a unique IMEI, giving individuals, carriers, law enforcement, and insurance companies a way to track down stolen phones, or, at the very least, place them on a blacklist.

IMEI Blacklists Aren't Widely Adopted

IMEI numbers are, theoretically, great for flagging or tracking stolen phones. Unfortunately, the centralization and separation of IMEI blacklists operated by carriers have produced several problems.

Amongst them are:

1. IMEI blacklists are geographically restricted by country;
2. Some wireless carriers respect certain blacklists, while others don't, creating inconsistency;
3. IMEI blacklists are often proprietarily held, making it difficult for law enforcement, insurance companies, or individuals to access and use blacklist data.

This isn't all to say that attempts to create a universal IMEI blacklist haven't been made. GSMA, a mobile network industry group, created the GSMA Global IMEI Blacklist. Owing to the breadth of it's globe-spanning member networks, GSMA has had limited success, bringing 110 carrier networks under the same blacklist standard.

Centralized Blacklists Give Special Interest Groups Too Much Power

However, centralized, interest-driven groups like GSMA exclude networks that don't align with their industry efforts, driving both large and small operators away.

Additionally, the centralized nature of industry groups like GSMA leads to a concentration of power wherein their blacklist is subject to influence. Finally, centralized attempts at creating blacklist standards give operators and government regulators great pause when deciding who should be in charge of creating such standards in the first place.

Despite the actuation of blacklists within specific geographic regions, the ongoing lack of a cohesive global blacklist means tainted phones need only cross a border before being operational again.

As such, the incredible amounts of red tape have led to the creation of an international black market for stolen smartphones that gets more valuable by the day.

At LOX Network, we're proud to develop the world's first fully decentralized security network

Designed to target and dismantle the global phone theft industry with a decentralized blacklist empowering the individual to report phone thefts.

The core concept of an IMEI blacklist is sound, but the execution of such blacklists by centralized parties is not. When Satoshi Nakamoto first described decentralized ledger technology in the Bitcoin Whitepaper, it became clear that the technology for eliminating the stolen device trade had arrived.

A Decentralised IMEI Blacklist Benefits Everyone

Using a dual NFT proof-of-ownership model to ensure control across multiple devices, LOX Network puts the power of device ownership in the hands of owners — not wireless carriers.

Just as anyone can build using open blockchain protocols such as Ethereum, Solana, and Polkadot, developers, carriers, law enforcement, insurance agencies, and private individuals can create applications using the LOX Network decentralized blacklist API integration and also accessible via the LOX mobile app and the forthcoming Lostorstolen.io web-based app giving everyone access device status information.

The LOX standard is especially crucial in today's market given that the market for unlocked phones is skyrocketing around the world. In the U.S. alone, a 22-percent increase in unlocked device sales was reported in the first quarter of 2019.

Unite the World's Wireless Infrastructure

The $30 billion illicit phone trade is a global problem requiring a network agnostic, public, universal blacklist.

By lowering the barrier to reporting and blacklisting a stolen phone, LOX Network provides the first truly crowdsourced solution for combating device theft no matter where it occurs.

Keeping the blacklist publicly accessible by default (as an inherent quality of public blockchains) makes it impossible to hide a phone's IMEI status, and enables marketplaces, whether centralized or decentralized, to securely sell devices with good standing.

A network and geolocation agnostic blacklist provide interoperable infrastructure for the emerging decentralized marketplace niche.

LOX Network

LOX Network is a hybrid blockchain being built with Hyperledger fabric to record transactions to the XRP Ledger and interoperate with Flare Network for Turing Completeness using the Ethereum Virtual Machine, or EVM. The LOX Network is where SmartNFT, our NFT platform, and SmartLOX, the mobile security application reside.

The native currency, LOX, powers LOX Network. The token is used to pay transaction fees when interacting or executing contracts via LOX Network.

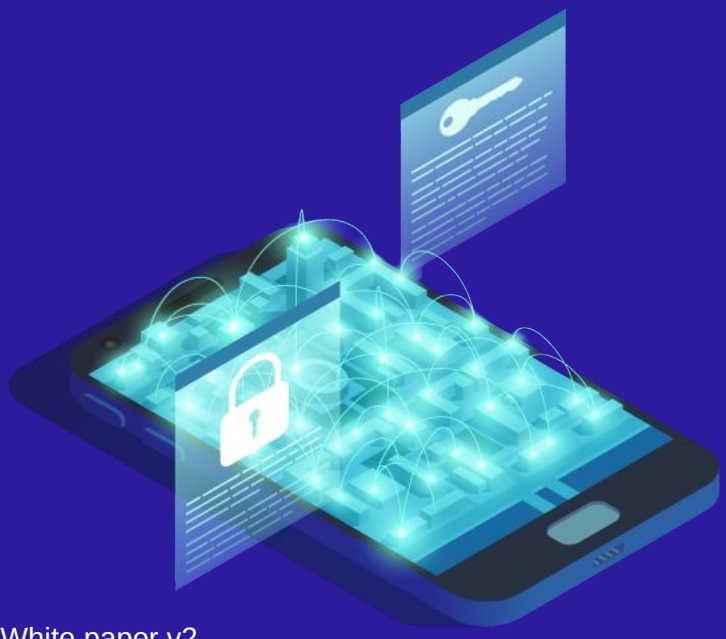
The first two applications to be built by the team at LOX Network are SmartNFT, an NFT platform where users can mint digital representations of themselves and their devices among other uses, and SmartLOX, the mobile security application.

The SmartNFT platform works just like any other NFT marketplace. Here, the user creates a digital representation of themselves and their devices in a QR-coded NFT, including name, email address, and additional pertinent information.

Once the user NFT is created, The user can mint a digital representation of their device, including its make, model, IMEI number and other identifying information.

The SmartLOX mobile security app uses LOX Network to identify and bridge a users' profile NFT stored on the mobile application and a device NFT stored on the SmartNFT platform to pair them together, creating the proof-of-ownership bond backed up by the XRP Ledger’s decentralized transaction records.

Using the power of Flare Network and the speed, reliability, cost efficiency, and, most importantly, the decentralization of the XRP Ledger, any actions recorded by LOX Network are verifiable on public XRP Ledger scanners such as XRPScan or Bithomp, creating verifiable, irrefutable documentation and immutable proof-of-ownership



LOX Mobile App

The LOX Security App (SmartLOX) enables users to manage the security, whereabouts, and ownership rights of multiple devices accessing LOX Network's proof-of-ownership system. Proof-of-ownership whitelists device owners on allotted devices, thereby excluding non-whitelisted users and detecting instances of theft.

With the LOX Security App suite, users can:

- Check the security status of a device
- Remote lock a device
- Remote backup a device
- Remote locate a device
- Block and blacklist a device
- Forward proof of ownership to a new users
- Offer rewards for recovery of lost/stolen devices
- Secure rewards for finding lost devices
- Secure rewards for returning lost devices to owner

While the LOX Security App's initial rollout is limited to smartphone devices, upcoming development milestones will see the addition of any network-connected devices such as smartwatches and laptops along with other high-value items such as e-bikes.

LOX Security Tagging

LOX blacklisting technology primarily relies on IMEI, serial numbers, and IP address tracking for identifying, locating, and locking lost or stolen network-connected devices.

However, not all items that are prone to theft contain network connectivity or identifying data. Additionally, in most instances, when a smartphone or other high-value item is stolen, the owner rightfully wants to do more than blacklist it — they want to retrieve it, if possible.

Blockchains have proven immensely useful in combatting fake, non-genuine goods in the retail world. By tagging and tracing retails goods through the entire duration of their production and lifecycles, blockchain-backed platforms have proven that decentralized ledger technology simply works for track and trace usecases.

LOX Network is a distributed network built for securitizing your possessions, which is why we're currently developing LOX Nano Security Tagging — an invisible method for tagging and tracing items using Microdot Technology.

By tagging your valuables with Microdots, then registering them on the LOX Network, your undisputed ownership of an item is publicly claimable. If that item is ever lost or stolen, it can easily be tracked, and your unique Microdot-based LOX Security Tag identifies it as yours.

LOX Network API

The LOX Network captures the unmet need for a global blacklist that unites wireless carriers and device owners. As such, LOX Network data is immensely valuable for a long list of wireless ecosystem participants:

Anyone, including the entities mentioned above, can quickly and securely receive LOX Network data using the LOX API. Additionally, as blockchains continue being adopted by incoming services, smart contracts will become a standardized part of tech stacks the world over.

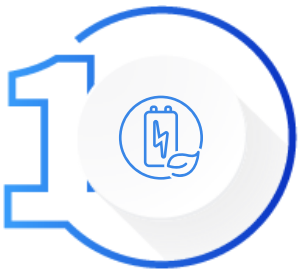
The LOX Network API is designed to account for this, and is connectable to smart contracts using a simple oracle intermediary.

LOX Token

The LOX token is a utility token acting as the native currency of the LOX Network.

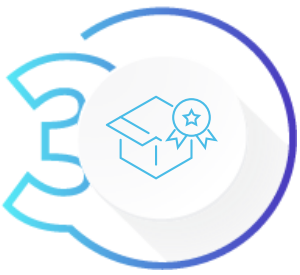
LOX Token Utility

Central to the LOX Network mission is recovering devices through global data sharing. $LOX has three functions in a reward structure to incentivize our mission success.



Device owners can create bounties paid in $LOX for the recovery of lost or stolen devices.

Users who find a lost device and return it to their rightful owners receive a reward paid in $LOX.



Users who find a blacklisted device with no apparent owner receive a reward paid in $LOX.

(The value of the rewards paid in scenarios 2 and 3 are subject to community governance votes.)

Payment

Accessing LOX Network services requires $LOX — in the initial phase, no other currency will be accepted as payment. In a later phase, we plan to integrate front-end payments using BTC, ETH, XRP, and other currencies that are then summarily swapped for $LOX.

Token Burn

In the first phase, $LOX tokens used to pay for network products and services will be burned at the beginning of the next financial quarter. As such, each fiscal year will contain four token burns preceded by a report on the financials of the previous quarter.

To balance token burn and token emission, a governance vote before the mainnet launch will take place amongst SmartNFT and SmartLOX token holders to decide:

- Token burn program duration
- Yearly token emission rate

Governance

All network rules, standards, mechanisms, and direction are transparently laid out, organized, and enacted by the LOX Foundation, a Decentralized Autonomous Organization (DAO).

To participate in the LOX Foundation for proposing, voting, and passing governance decisions, one needs only to hold SmartNFT or SmartLOX tokens in their wallet. Both tokens enable the holder to participate in all governance Issues dictating the platform’s future direction.

Proposing Referenda

To propose an issue to the LOX Council, an amount of SmarNFT or SmartLOX is staked by the proposer. Any subsequent token holders can then choose to support the referenda by stake-pledging an amount of tokens equal to the original amount.

Once the issue has received enough collateral to be made an official governance matter, it's held to a council-wide vote wherein the result is protocol-binding.

Stake-pledging

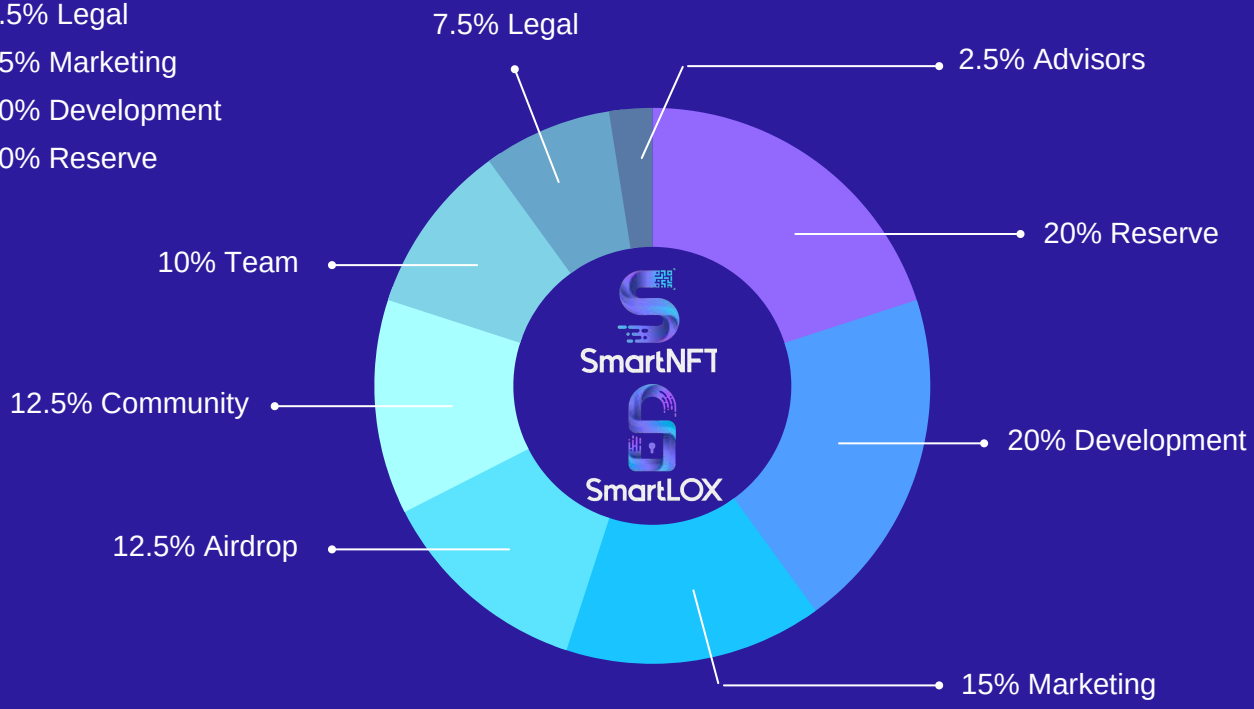
All token holders are entitled to one vote per SmartNFT or SmartLOX token held. However, some may choose to consolidate voting power to control the network's direction by becoming “whales,” or individuals with large wallets with the intent to control smaller wallets.

To avoid this scenario, we've included a stake-pledging function that empowers smaller wallets with greater voting power. Small wallets (>1% total) can stake their tokens to their vote for a period of up to 30 days. The longer the stake-pledge, the greater the weight their vote carries, allowing smaller wallets the means of influencing governance decisions on a larger scale by signalling commitment.

SmartNFT & SmartLOX

Share the same tokenomics structure

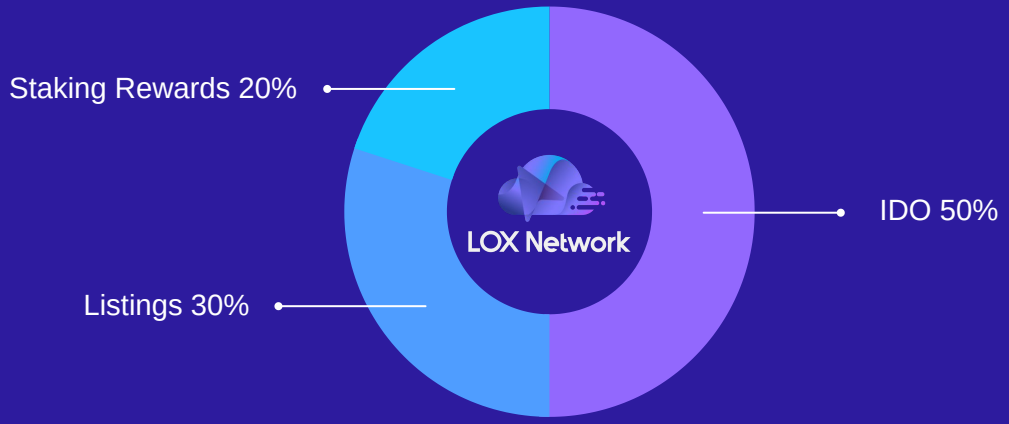
- Max supply is 1 billion tokens
- 12.5% Airdrop
- 12.5% Community
- 10% Team
- 2.5% Advisors
- 7.5% Legal
- 15% Marketing
- 20% Development
- 20% Reserve



LOX Network Token

Share the same tokenomics structure

- Max supply is 1 billion tokens
- IDO 50%
- Listings 30%
- Staking Rewards 20%
- Any remaining tokens from the IDO will go towards LoxDAO reserve



SmartNFT

SmartNFT is an NFT platform built on the hybrid LOX Network blockchain and houses all users' and devices' QR-coded NFT representations. The SmartLOX mobile security app references the NFT representations to verify and bind the mobile device to a user. The token, SmartNFT, is an XRPL token that governs the NFT platform.

SmartNFT was the first of the ecosystems' three XRPL tokens launched on Aug. 28, 2021, and distributed via airdrops. The SmartNFT token is used for the governance of the SmartNFT platform and used to purchase artwork to pair with the user or device profiles. Additionally, it can be staked to earn LOX tokens.

Issuer Address:	rf8dxyFrYWEcUQAM7QXdbbtcRPzjvoQybK
HEX ID:	536d6172744e4654000000000000000000000000
Limit:	100,000,000

https://t.co/g7jEOro0gw

SmartLOX

SmartLOX is the mobile security app built on the LOX Network hybrid blockchain. SmartLOX references the SmartNFT platform to identify and bridge a users' and a devices' QR-coded NFT creating a proof-of-ownership bond that irrefutably determines you, the user, is the rightful owner of a specific device.

SmartLOX was the second of the ecosystems' three XRPL tokens to launch on Sept. 5, 2021, via a snapshot of all SmartNFT holders and distributed via further airdrops. The SmartLOX token is used for the governance of the SmartLOX mobile application and to purchase in-app services. SmartLOX can also be staked to earn LOX tokens.

Issuer Address:	rBdZkMKuPnzYVVkyL2DrQKV3DsYt5PPVRh
HEX ID:	536D6172744C4F5800000000000000000000000
Limit:	100,000,000

https://t.co/kv7HlxuxLF

LOX

LOX is the native currency of the hybrid LOX Network blockchain and is the payment mechanism for all LOX Network actions. LOX Network will use Flare Network for Turing Completeness using the EVM and record transactions on the XRPL. The SmartNFT platform and SmartLOX mobile security application are both products of LOX Technology Limited and will be built on top of LOX Network.

LOX is the third of the ecosystem's three XRPL tokens on Sept. 10, 2021, via an IDO on the XRPL decentralized exchange.

Issuer Address:	rLLJvh6bwj2eTYwzLL484AW6EyH4rdZqWZ
Token currency code:	LOX
Limit:	1,000,000,000

https://t.co/6yUgGGMvBW

NOTE

XRP Toolkit permits Currency Code to be letters if the currency is no greater than 3 characters. Hex ID is only required for tokens with more than 3 characters

Roadmap

LOX Network launched in the 3rd quarter of 2020 as an Ethereum project. As the project was in development, Ethereum's gas fees began to become uneconomical for LOX's intended use of microtransactions.

Imagine paying a nominal fee to use LOX Network and be faced with insurmountable gas to pay for the transaction.

Q3 - 2020

- Lox Network Project launched
- Use case research & development
- Whitepaper v0.1

Q4 - 2020

- Commercial Implications researched
- Tokenomics v0.1
- Core Team Building
- Whitepaper v1.0

Q1 - 2021

- loxcoin.io goes live Ethereum gas prices make LOX unviable on the Ethereum blockchain
- Covid restriction slows progress

Q2 - 2021

- Alternative blockchain solutions researched
- lostorstolen.co.uk testing begins (web version of app)
- Whitepaper v1.2

Q3 - 2021

- XRPL selected as blockchain of choice
- LOX Network relaunch on XRPL (LOX)
- Inception of SmartNFT
- SmartLOX is born

Following Ethereum's London hard fork, our team observed the gas fee issue was not going to resolve quickly enough and LOX Network began its transition to the XRPL in the 3rd quarter of 2021.

LOX Network will take advantage of the XRPL's proven speed, reliability and efficiency with essentially no transaction fees. This updated roadmap focuses on the new goals and estimated times of completion.

Q4 - 2021

- Community building
- Development team selected
- Mobile Application MVP (Internal)
- Whitepaper v2

Q1 - 2022

- Technical paper v1
- Consumer Adoption
- Commercial partnerships
- Mobile Application Alpha release (closed Internal)

Q2- 2022

- Commercial Adoption
- Main-Net Launch (pending Flare)
- Mobile application Beta release (closed public)

Q3 - 2022

- Mobile application Gold release (final public)
- lostorstolen.co.uk final release (web version of app)
- Nano Tagging introduced (microdot technology)

Q4 - 2022

- LoxDAO goes live
- Giv token is launched
- Further development and partnerships

Q1 2023

- New features introduced (Phase 2) smartwatches, laptops and other high value goods prone to theft