offshift

WHITEPAPER V2

The World's First Private Derivatives Platform

PIONEERING #PRIFI

TABLE OF CONTENTS

- **Abstract** 3
- **Introduction - The Crypto-Space in 2021: Trendlines & Pain Points** 4
- **Value Proposition: Offshift** 6
  - _ **zkAssets:** Private, On-chain Synthetics for Anonymous Ownership 7
  - _ **Asset Diversity:** Crypto, Fiat, Commodities, and Anything with a Price Feed - All on One Platform, All Private 7
  - _ **Stress-Free Exchange:** 1:1 Collateral, Zero Slippage, Zero Margin Calls, Zero Liquidations, & Zero Liquidity Risk 8
  - _ **Cross-Chain Strategy:** Prioritizing Interoperability & Reducing Costs to Users 8
  - _ **Rug-Pull-Proof DeFi:** Hardcoding Integrity into Offshift 9
- **Platform Tokenomics: Utility & Incentives** 9
  - _ Shifting with our Burn-and-Mint Mechanism 10
  - _ Bridge Fees 11
  - _ Chainlink's Oracle Network 11
  - _ Zero-Knowledge (zk) Proofs 12
  - _ Staking Rewards 12
- **Fundraising & Token Metrics** 13
  - _ Capital Raise 13
  - _ Token Allocations 13
  - _ High-Integrity Tokenomic Measures 14
  - _ Token Emission Schedule 16
- **Development Roadmap** 17
- **Long-Term Vision: A Privacy-Centric DeFi Ecosystem** 18
- **Resources** 18
- **Disclosure Note** 19

ABSTRACT

Barely more than a decade into its existence, the landscape of cryptocurrency is already well distanced from its origins as an obscure hub for experimental ventures in cryptography. Now in 2021, the broader crypto-space has landed a full-time spot in the geopolitical and socioeconomic mainstream, making regular appearances on MSNBC and a number of other prominent news networks, and receiving significant interest from the likes of financial institutions and investment gurus, not to mention government authorities and regulatory agencies looking to crack down on any and all facilitators of anonymous exchange.

In lockstep with their reputations, cryptocurrency protocols themselves have also undergone a radical transformation in recent years, catering to a wide array of unprecedented use cases and financial models. Collectively classified under the DeFi (Decentralized Finance) umbrella, these experimental applications grant users access to a vast expanse of innovative financial services never before seen in human history. The only drawback: crypto's newfound development direction has left its privacy-centric origins on the sidelines; today, users must choose between exploring the cutting-edge tools at the forefront of cryptocurrency innovation **OR** resort to standalone blockchains whose native assets confer privacy as an exclusive feature. Simply put, privacy now comes at the expense of virtually everything else the modern and rapidly evolving crypto-space has to offer. Cryptocurrencies - or, as they have been more recently labeled by those seeking to permanently sever their privacy-centric roots, digital assets - stand in dire need of a technological solution that can eliminate the tradeoff between privacy and everything else - in so many words, a platform that can transform the above **OR** into an **AND**.

At Offshift, our ultimate vision encompasses the formation of a scalable, interoperable, privacy-centric DeFi ecosystem composed of a diverse range of disruptive platforms and applications. We are pioneers playing a decisive visionary role in the development of cryptocurrency's next major growth catalyst: the #PriFi landscape.

INTRODUCTION
THE CRYPTO-SPACE IN 2021: TRENDLINES & PAIN POINTS

Experimental Use Cases and Applications

The recent emergence of the DeFi movement and its breadth of groundbreaking applications is emblematic of the unrivaled innovative potential and development pace that is native to the crypto-space. From various staking models and decentralized lending and borrowing services to synthetic asset generation and non-fungible token (NFT) minting, DeFi applications offer users an endless stream of opportunities to leverage the liquidity vested in their crypto-assets, contribute and access otherwise dormant capital, and of course, farm yields. The budding DeFi space made a precipitous ascent to the forefront of the crypto-asset space in the summer DeFi wave of 2020, and although it has since cooled off, cryptocurrency's largest market segment is now gathering steam for a major surge in 2021.

Emerging Authoritarian Regulatory Presence

As cryptocurrencies have enjoyed newfound popularity in the mainstream, so too have they drawn increased attention from governments and regulatory agencies, whose constituents are preparing to integrate cryptocurrency frameworks into existing financial infrastructure, where users can be identified and transactions surveilled via Know-Your-Client (KYC) implementations - allegedly for the purposes of Anti-Money Laundering and public safety. Most notoriously, in December 2020 the United States Treasury's Financial Crime Enforcement Network (FinCEN) proposed a new rule that stipulates that cryptocurrency exchanges will be required to collect data on all users transferring upwards of $3,000 in USD-equivalents to private wallets.[1] In short, a private wallet - that is, a "non-hosted wallet," in FinCEN's terminology - will be unable to send or receive cryptocurrencies valued in excess of $3,000 to or from exchanges unless the wallet's owner has been officially identified through standard KYC procedures. Despite outrage across the crypto-space, authoritarianism is gaining momentum and such efforts to surveil, limit, and censor cryptocurrency transactions are only just beginning to surface. FinCEN's gesture is merely an early move.

Siloed Privacy Technologies

Fortunately, neither cryptocurrency's newfound development initiatives nor governments' encroaching authoritarianism has been able to sap the space's original ingenuity; many cryptography specialists remain dedicated to the prerogative of personal privacy in property ownership and exchange. However, these groups and the projects they develop and maintain largely comprise standalone blockchains whose native assets confer privacy as an exclusive feature. While they allow users to store and transact their wealth securely and privately, Monero, Zcash, and the rest of the privacy coin community inherently withhold users from engaging the innovative applications of cryptocurrency's emergent DeFi segment, as their siloed, standalone blockchains are integral to their privacy-centric value propositions. What's more, their standalone nature renders them vulnerable to being easily sidelined by on/off-ramps such as exchanges that cave in to pressure from authorities - Bittrex's decision to delist XMR, ZEC, and DASH being the most recent example.[2]

[1] De, N. (2021, January 13). Crypto Industry Unites to Fight 'Arbitrary' FinCEN Rule. Retrieved Jan, 2021 from https://www.coindesk.com/65k-comments-and-counting-crypto-industry-fights-arbitrary-treasury-rule

[2] Reynolds, K. (2021, January 04). Bittrex to Delist 'Privacy Coins' Monero, Dash and Zcash. Retrieved January, 2021, from https://www.coindesk.com/bittrex-to-delist-privacy-coins-monero-dash-and-zcash

The Bottom Line

Throughout 2020 and into 2021, the DeFi umbrella has expanded convincingly over the landscape of cryptocurrency, attracting investors and enthusiasts whose preferences speak for themselves: **DeFi's double-digit APRs and seamless user experience are simply more seductive than the subtle, systemic benefits conferred by privacy-centric exchange.** And who can fault users - for as long as the benefits of DeFi remain at odds with the prerogative of personal privacy, the former will continue to grow at the expense of the latter.

It is no longer a broad lack of awareness that holds back public interest in privacy, but a current of ever-expanding trade-offs that individuals must forfeit in order to retain it. For privacy to become an intrinsic characteristic of our future systems of exchange, it must be released from its burden of mutual exclusivity; only then can it take the form of a universally adaptable feature - a virtually costless accessory of sorts.

VALUE PROPOSITION:
OFFSHIFT

Offshift dissolves the existing tradeoff between privacy and everything-else-crypto using zero-knowledge (zk) proofs to mint synthetic, asset-pegged tokens that are intrinsically private. On Offshift, users can stake a claim on any asset they like, without dealing with slippage, excessive collateral requirements, or liquidation risk, and all while maintaining personal privacy. Essentially, Offshift enables individuals to anonymize their crypto holdings, so they can invest in the technologies they believe in without the drawbacks related to exposure and public profiling. Privacy is a right - not a crime; as all individuals are innocent until proven guilty, they ought to be treated as such.

Here’s what Offshift brings to the table:

zkAssets: Private, On-chain Synthetics for Anonymous Ownership

Offshift’s Private Derivatives Platform enables the minting of zkAssets, a proprietary line of private synthetics. Leveraging zero-knowledge proofs, Ethereum’s turing-complete smart contracts, and Chainlink’s decentralized oracle network in conjunction, Offshift enables users to mint a wide array of zkAssets using its native token, XFT. Users can Shift from XFT into zkAssets, and from zkAssets back into XFT with ease. Simply put, **zkAssets fuse privacy-as-a-service with existing DeFi tools to provision a revolutionary line of derivative instruments that accessorize privacy.**

Asset Diversity: Crypto, Fiat, Commodities, and Anything with a Price Feed - All on One Platform, All Private

Offshift does not make privacy a universal, augmentable feature per se, as the platform never interacts directly with any assets beyond XFT and the zk-varieties it generates; zkAssets are synthetic by default. Consequently, there is virtually no limit to the expanse of assets Offshift’s protocol is capable of tokenizing; Offshift is fully capable of supporting any asset as long as there exists a market and a price feed - that means not only all tradeable cryptocurrencies and fiat currencies, but gold, silver, other commodities, and virtually anything with a price feed. Offshift stands to offer one of the most versatile and diverse trading environments in the global financial industry, and all while providing complete privacy for each and every one of its users.

Stress-Free Exchange: 1:1 Collateral, Zero Slippage, Zero Margin Calls, Zero Liquidations, & Zero Liquidity Risk

Unlike other DeFi platforms that allow users to mint synthetic assets, Offshift's Private Derivatives Platform does not impose excessive collateral requirements of any kind; over-collateralization is an outdated mechanism that is not capital-efficient. With Offshift's proprietary **Burn-and-Mint** mechanism and corresponding elastic supply model, users are afforded a seamless and stress-free trading experience, completely void of slippage and related liquidity risks (see: **IV., A. Shifting with our Burn-and-Mint Mechanism**). Accordingly, when users mint zkAssets, they never have to worry about margin calls, liquidations, or periodic fees to maintain their positions.

Cross-Chain Strategy: Prioritizing Interoperability & Reducing Costs to Users

The vision that is being laid out by the Web3 Foundation, Parity Technologies, and PureStake in the formation of the Substrate Blockchain Framework, Polkadot ecosystem, and Moonbeam Network resonates with our own at Offshift: the future smart economy will most likely consist of a network of diverse blockchains dedicated to specific functions and communities. As such, the technologies that enable interoperability and promote inclusivity across chains will play integral roles in facilitating seamless economic activity. As a powerful, decentralized application dedicated to privacy-centric exchange, Offshift will best serve users and extend access to its community by catering to multiple blockchain ecosystems - an imperative that will only become increasingly important as blockchain-based technologies mature.

Thus, while the Offshift team builds out our Shifting application and releases batches of zkAssets on Ethereum, we will also be advancing development on Moonbeam, Polkadot's leading EVM-compatible Parachain, in parallel. * Furthermore, as per the enhanced scalability provided by Polkadot's parachain architecture, we anticipate that users will benefit from reduced fees on our platform.

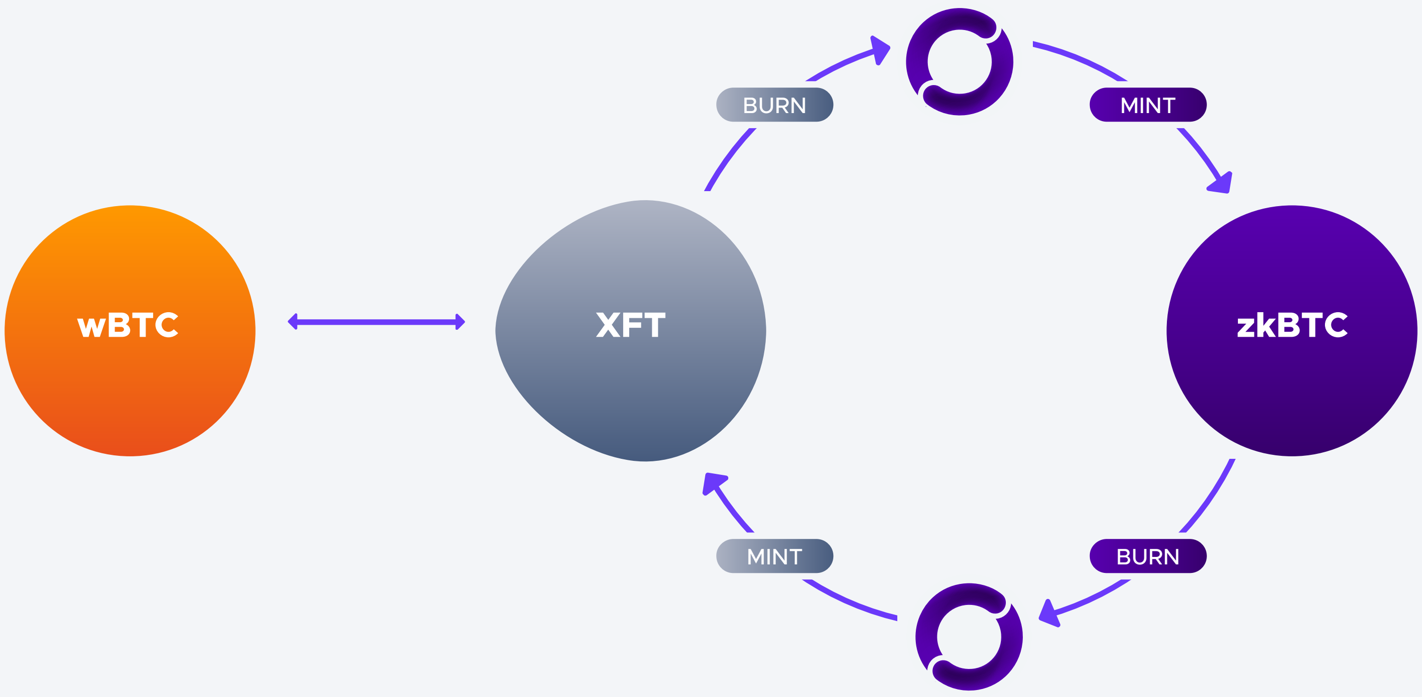
**In light of the fact Kusama, Polkadot's live canary Testnet, will be conducting its Parachain auctions in advance of Polkadot, Offshift is prepared and committed to launch on Moonriver, Moonbeam's Kusama Parachain, in order to advance development and achieve a cross-chain Mainnet launch in the near-term.*

Rug-Pull-Proof DeFi: Hardcoding Integrity into Offshift

As a rising project in a nascent, decentralized industry, Offshift acknowledges and respects the challenges prospective users and community members face in vetting projects for dishonest practice, exploitative tokenomic models, and outright deceit. We further acknowledge that, although the choice of our team members to remain anonymous aligns with the broader ethos of our project, we owe it to our community and everyone exploring our technical solution to take all necessary measures to ensure the ethical, high-integrity operation of our Private Derivatives Protocol. In our commitment to integrity, we have employed a Strategic Vesting Model, Lockboxes for On-chain Reserves, and Liquidity Locks (see: **V., C. High-Integrity Tokenomic Measures**).

PLATFORM TOKENOMICS: UTILITY & INCENTIVES

Offshift has already established the viability of our technical solution, and all developer resources are presently being invested in implementation. Because our technology stands to play a major disruptive role in both the privacy community and DeFi space alike, we have elected to refrain from publishing our open source code on our GitHub Repository until shortly before Mainnet launch. In order to uphold the highest degree of integrity in managing our project development process, we are committed to offering full transparency to our community through our established media channels, providing opportunities to experiment with several iterations of our public Testnet, and providing deep insight into our technical solution in documentation and regular, in-depth blog posts. The Offshift platform's key features and broad functionality are described in detail below



Shifting with our Burn-and-Mint Mechanism

When a user wants to mint a zkAsset, he opens Offshift's proprietary **Shifting application**, and connects his ERC20 wallet. If a user possesses a positive XFT balance and sufficient ETH to cover transaction fees, he is able to **Shift** his XFT into a synthetic zkAsset of his choosing. At the user level, completing a **Shift** is a simple and intuitive operation, but a bit more takes place under the hood. This is where Offshift's Burn-and-Mint mechanism comes into play.

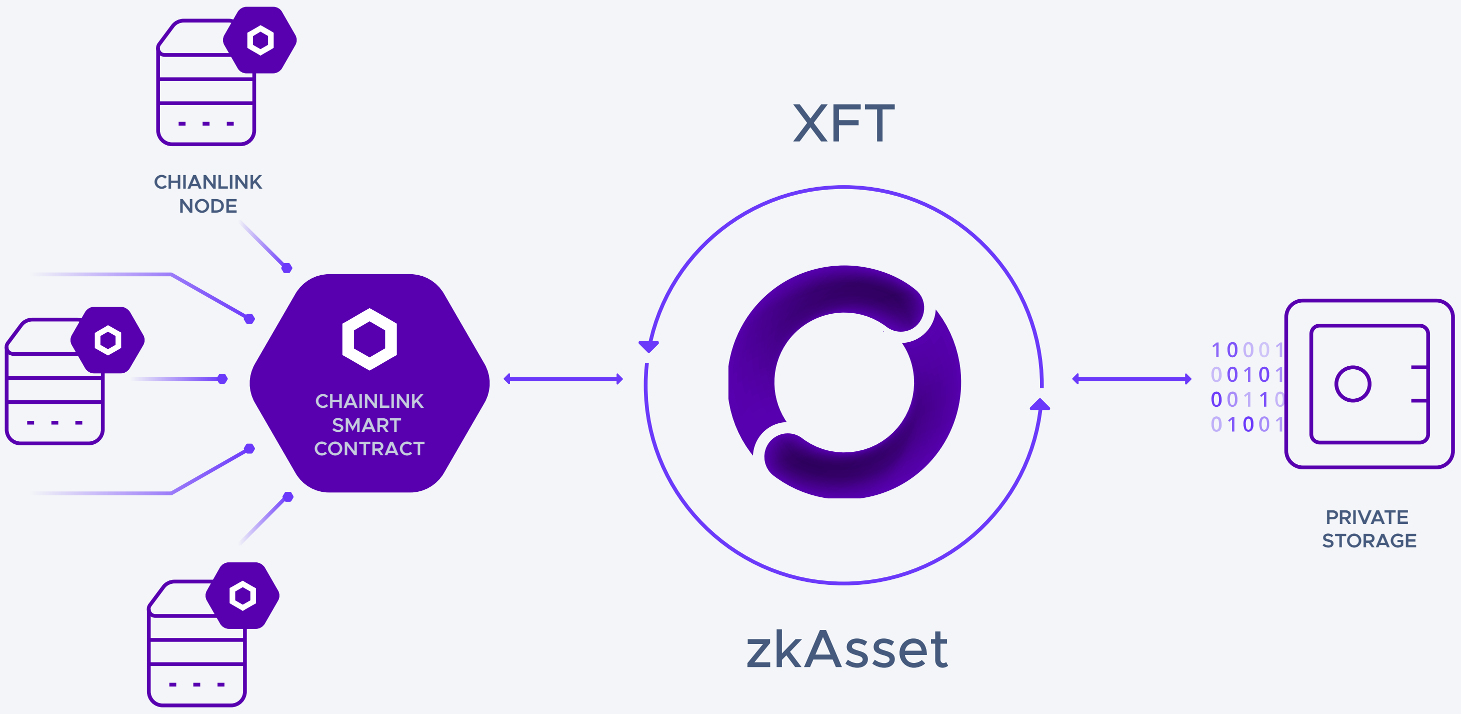
Offshift's **Burn-and-Mint** mechanism burns the user's XFT and mints a new zkAsset of equal value. At any point, the user may **Shift** from his zkAsset into XFT, and the process reverses: the **Burn-and-Mint** mechanism burns the zkAsset, and mints new XFT of equal value to the user's ERC20 wallet address. Such a model enables users to mint, store, and trade private, synthetic zkAssets free from excessive collateralization requirements and the margin calls and liquidations that come with them, making for a cost-efficient and stress-free trading experience. Of course, such a model implies and requires an elastic supply model for XFT; however, it does not imply any risk of monetary instability, nor any propensity toward long-term inflationary or deflationary monetary attributes.

Bridge Fees

Due to the potential for price fluctuation in XFT as users Shift back and forth between zkAssets, there is substantial possibility that various, narrow-interval arbitrage opportunities may arise that will enable traders to exploit other users, and thereby the integrity of the platform at large. In order to address and avert any such exploitation, Offshift charges users a dynamic, depreciating **Bridge Fee** to Shift from zkAssets back into XFT in the first 7 days post-mint. All **Bridge Fees** are sent directly to Offshift's **Staking Rewards** wallet, so that all collected funds are recycled back to community members that are using and contributing to the platform (see: **IV., E. Staking Rewards**).

Chainlink's Oracle Network

In order to provide a seamless and trustless user experience, Offshift sources accurate, real-time price feeds to calculate exchange rates across assets using Chainlink's industry-leading, distributed oracle network. More information on our collaboration with Chainlink is available in our September 30, 2020 Medium Blog post: [Offshift Taps Chainlink to Provide Oracle Feeds for its zkAsset Private Pegs]



Zero-Knowledge (zk) Proofs

Zero-knowledge (zk) proofs are a cryptographic method by which one party (the prover) can prove to another (the verifier) that it has knowledge of a particular piece of information - such as a secret key - without revealing anything other than the fact that it knows that information. Zero-knowledge proofs were originally developed in the 1980s, but were more recently popularized by Zcash, one of the crypto-space's leading privacy coins. Zero-knowledge proofs act as an integral component in Offshift's technical solution, as they allow for the minting of private, synthetic zkAssets. For more information on Zero-knowledge proofs, refer to this link: What Are Zero-Knowledge Proofs?[3]

EIP #1724: zkERC20: Confidential Token Standard

In order to mint private, on-chain assets via zk Proofs, Offshift draws on Ethereum Improvement Proposal #1724, a proposal modeled on Aztec Protocol which delineates a broader set of specifications for an ecosystem-wide confidential token standard. For those seeking deeper insight into Offshift's proprietary technical solution, the following link will serve as a strong starting point for a deep dive into our methodology for provisioning anonymity: EIP #1724: zkERC20: Confidential Token Standard[4]

Staking Rewards

To both incentivize users to hold zkAssets and to incorporate another DeFi function into our platform, Offshift has allocated 15% of our Genesis Total Supply (1,500,000 XFT) to **Staking Rewards.**

[3] Hussey, M. (2020, March 26). What are Zero Knowledge Proofs? A simple 3-minute guide.
Retrieved Jan, 2021 from https://decrypt.co/resources/zero-knowledge-proofs-explained-learn-guide

[4] Zac-willamson. (2019, January 25). ZkERC20: Confidential Token Standard • Issue #1724 • ethereum/EIPs.
Retrieved January 21, 2021, from https://github.com/ethereum/EIPs/issues/1724

On the Offshift platform, users begin staking their zkAssets 7 days post-mint. Staking rewards are sourced from Offshift's Staking Rewards wallet, converted to zkAssets, and distributed to users based on **Total Value Staked** and **Total Time Staked**. Our Staking Rewards feature will go live in Q3 2021, and we will continue to release more detailed and quantitative information as that juncture approaches (see: **VI. Development Roadmap**).

FUNDRAISING & TOKEN METRICS

Capital Raise

Offshift raised capital through one round of seed investment and one round of private investment. In the interests of decentralizing token ownership, individual investment contributions were capped at $5,000 in USD-equivalents in both rounds.

Token Allocations

From the Genesis Total Supply of 10,000,000 XFT:

- → 1,500,000 XFT were sold between the seed and private investment rounds.
- → 250,000 XFT were deployed in the Uniswap liquidity pool.**
- → 1,750,000 XFT comprised Offshift's Circulating Supply as of our August 3, 2020 launch.
- → The remaining XFT allocations are illustrated in the graphics below.

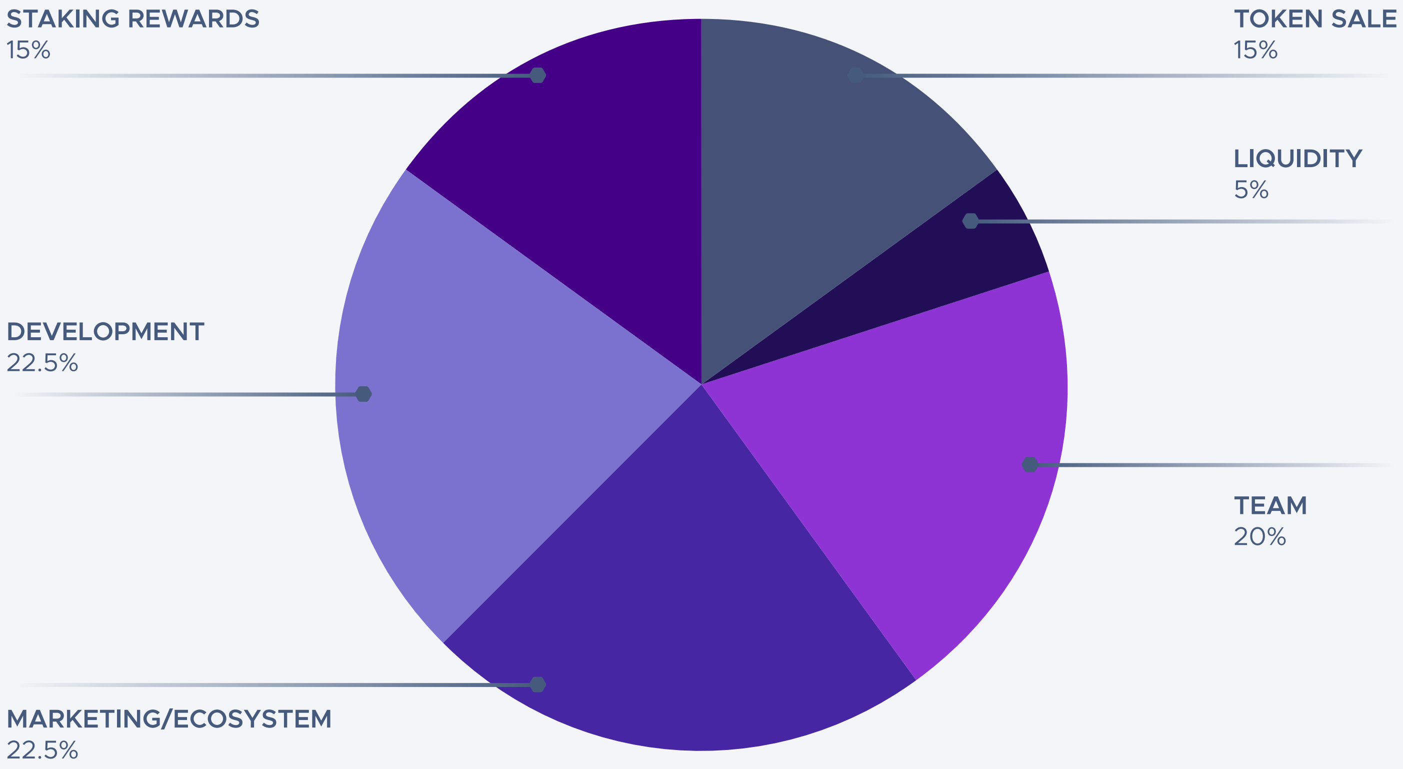
> "Transparency is for those who carry out public duties and exercise public power. Privacy is for everyone else."
>
> _ Glenn Greenwald

**A total of 500,000 XFT were initially reserved for liquidity provision, but only 250,000 XFT were deployed in the Uniswap liquidity pool. The remaining liquidity reserves of 250,000 XFT remain locked on-chain, and will be allocated as follows, pending the discretion of the Offshift community:

- *Distributed to platform users in the future as part of an LP rewards program;*
- *Burned in their entirety;*
- *Some combination of the above options.*

Token Supply	**10,000,000**	Seed Sale Price	$0.10
Seed sale	500,000	Private Sale Price	$0.15
Private sale	1,000,000	Listing Price	$0.20
Liquidity	250,000	Total Raise	$200,000
Initial Circulating Supply	1,750,000	Initial Market Cap (List Price)	$350,000
Initial Circulating Supply %	17.5%	Fully Diluted Cap (List Price)	$2,000,000

Allocation	**Percentage**	**# of Tokens**	**Value at Listing**
Token Sale	15.00%	1,500,000	$300,000
Liquidity	5.00%	500,000	$100,000
Team	20.00%	2,000,000	$400,000
Marketing/Ecosystem	22.50%	2,250,000	$450,000
Development	22.50%	2,250,000	$450,000
Staking Rewards	15.00%	1,500,000	$300,000



High-Integrity Tokenomic Measures

In honor of our commitment to a high-integrity development process, full transparency, and a long-term project vision, we have taken substantial measures to ensure that all token allocations outside of our initial circulating supply will never serve as a source of undue or excessive inflation at any stage in our development lifecycle. Attending to this prerogative, we have taken the following measures:

1. Strategic Vesting Model

We have established gradual, long-term vesting periods for our Marketing/Ecosystem, Development, and Team wallets, as well as for our designated Staking Rewards wallet.

Wallet-specific vesting parameters are available below:

Marketing/Ecosystem (22.5%): 1.25% every 2 months, beginning Oct. 3, 2020

Development (22.5%): 1.25% every 2 months, beginning Oct. 3, 2020

Team (20%): 1% every 2 months, beginning Feb. 3, 2021

Staking Rewards (15%): 0.25% every month, beginning Feb. 3, 2021***

*******All percentage (%) figures above express a nominal amount of XFT tokens relative to the Total Genesis Supply of XFT on a percentage basis.*

2. Lockboxes for On-chain Reserves

To ensure that even our core team cannot modify our token metrics or vesting strategy, we have hardcoded our vesting model using smart contracts called Lockboxes. Full information pertaining to our On-chain Reserves is available at the following links:

- Development/Ecosystem Wallet
- Marketing Wallet
- Team Wallet
- Staking Rewards Wallet

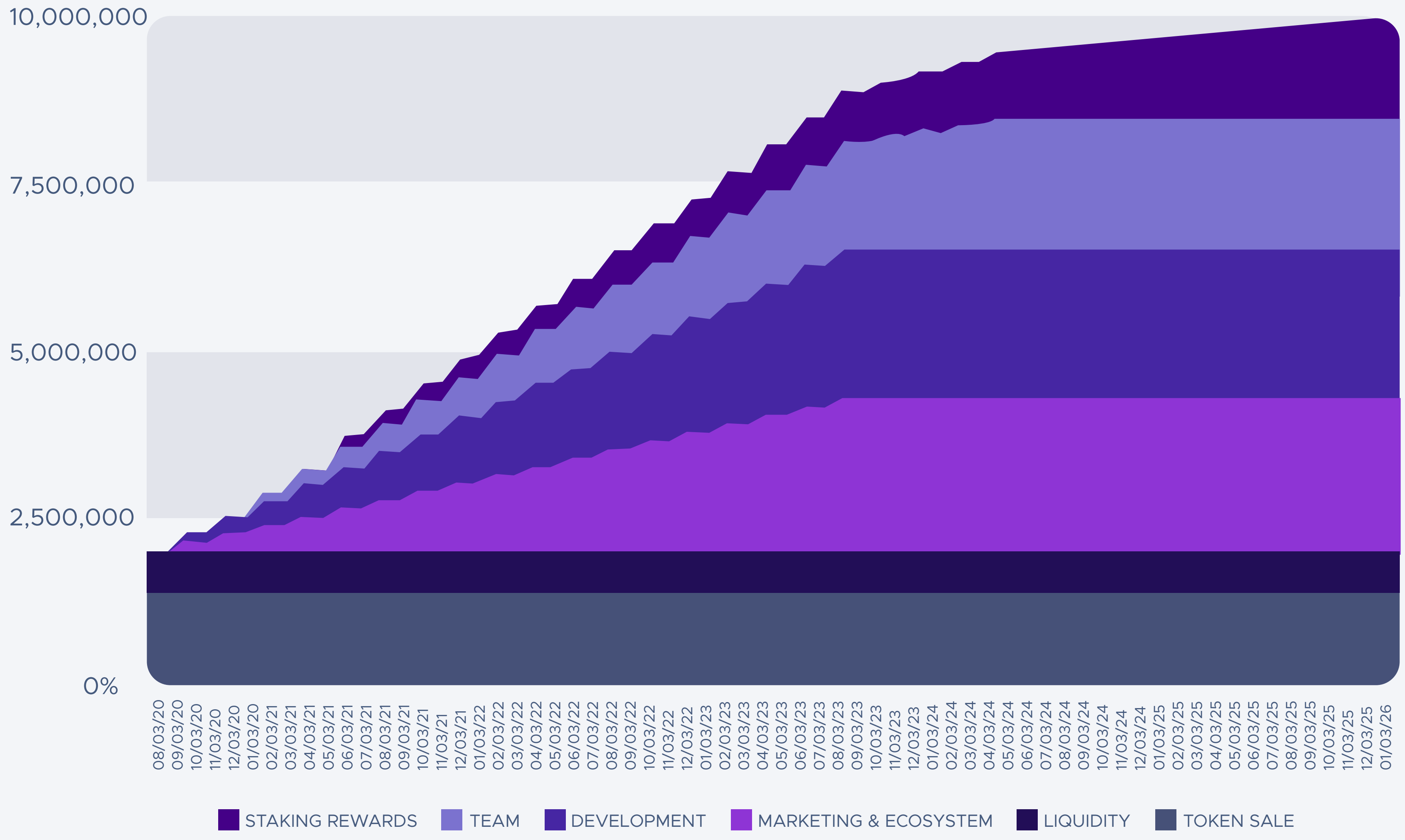
3. Liquidity Locks

In addition to our XFT wallets, we also employ smart contracts to prevent tampering with our Uniswap LP Token. Our Uniswap Liquidity Pool is protected via a Liquidity Lock which can be viewed at the following link:

- Uniswap Liquidity Provider (LP) Token

Token Emission Schedule

In accordance with our Vesting Model, the Genesis Total Supply of 10,000,000 XFT will be gradually released into the Circulating Supply over the course of 5 years and 5 months via the following Token Emission Schedule:



DEVELOPMENT ROADMAP

Q3 2020

- ✓ Project Launch
- ✓ XFT Contract Deployment
- ✓ Oracles Integration

Q4 2020

- ✓ zkAsset Deployment
- ✓ Rinkeby Testnet Shifting Launch

Q1 2021

- ✓ Complete Deployment on Substrate
- ✓ Launch Moonbeam TestNet

LONG-TERM VISION:
A PRIVACY-CENTRIC DEFI ECOSYSTEM

While in the near-term we remain fully committed to the development of our core services, looking ahead we see deeper, protocol-layer potential in the Offshift platform. As users and wealth migrate to Offshift to take advantage of our private derivative instruments, developers too will begin to dedicate attention and resources to the development of unique applications that integrate zkAssets across an array of new use cases.

In the years ahead, we envisage the organic formation of a robust ecosystem whose applications enable users to engage in decentralized lending and borrowing, various forms of yield farming, the formation and exchange of insurance products, NFT generation, and much more - all while remaining fully anonymous, thanks to our proprietary zkAssets. Furthermore, we have the utmost confidence in Moonbeam's long-term development vision, and we are excited at the prospect that such a dynamic, privacy-centric ecosystem can take shape with the support of PureStake and the broader Moonbeam Parachain economy, whose secure, scalable, and interoperable infrastructure stands at the forefront of the crypto-space, and whose open source principles resonate with our own.

RESOURCES

The Offshift team and community are active and can be reached on the following platforms:

Website: offshift.io
Telegram: t.me/OffshiftXFT
Twitter: twitter.com/OffshiftXFT
Instagram: https://www.instagram.com/officialoffshift/
Medium: medium.com/offshift
GitLab: https://open.offshift.io/offshiftXFT/protocol-main
Bitcointalk: bitcointalk.org/index.php?topic=526226
Discord: https://discord.gg/9mZswcKRvz

DISCLOSURE NOTE

As for any crypto-asset, purchasing XFT tokens involves substantial risk and may lead to partial or complete investment losses. Investors should assess all relevant risks before purchasing XFT, taking into account personal financial circumstances and risk appetite.

XFT tokens should only be purchased by investors who fully understand the nature and functionality of the tokens and the protocol on which they operate, and who fully accept all relevant risks. All cryptocurrencies may be subject to expropriation or theft. Hackers or other malicious groups may also attempt to interfere with distributed systems in various ways, including malware attacks, Denial-of-service attacks, consensus-based attacks, and Sybil attacks, and may engage in other malicious tactics that damage protocols. In such an event, there may be no resolution, and holders of cryptocurrencies are not guaranteed any remedies. Lastly, it should be noted that the regulatory and tax status of cryptocurrencies remains unsettled and varies by legal jurisdiction. In the future, there is substantial possibility that laws or regulations applying to cryptocurrencies may be implemented which affect individual rights to own, hold, or sell cryptocurrencies.

THANK YOU