# OFFSHIFT

**Version 1.0**

*July 2020*

**Abstract**

In this paper we introduce a decentralised protocol that enables cryptographically private, asset-pegged stable value "offshore" storage with staking interest on Ethereum.

# Contents

## 1. Crypto isn’t Currency

The term “cryptocurrency,” when used to describe bitcoin and altcoins, is largely a misnomer. While a growing investment class, crypto is rarely used as a transactional currency. Monetary economics tells us that to fulfill the three functions of money, a currency should be 1 *a medium of exchange,* 2 *a store of value and* 3 *a unit of account.*

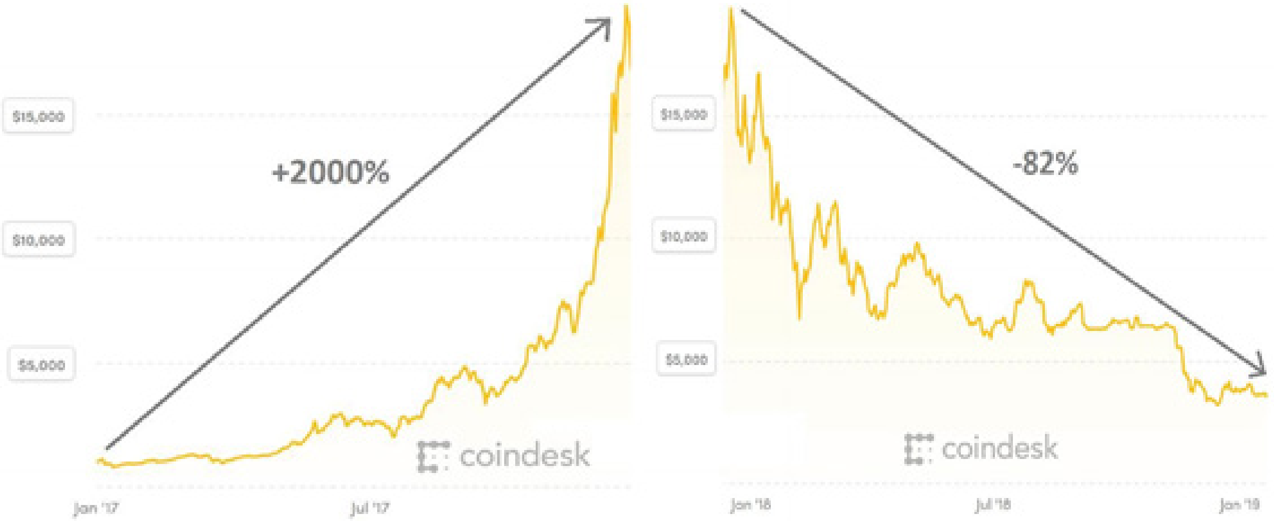
### 1.1 Medium of Exchange

As a medium of exchange, acceptance of crypto by retailers is limited. A 2018 study on bitcoin adoption found, using a large sample of online retailers, that “acceptance of crypto payments is currently modest (2%), but there is substantial interest among retailers to adopt crypto payments in the near future.”[1]

While crypto proponents push for “adoption” and develop scaling solutions like the Bitcoin Lightning Network[2] and Ethereum’s Plasma,[3] it appears the onus for adoption is not so much on retailers, but on consumers. The 2018 study determines “The most serious barrier for crypto acceptance seems to be a lack of consumer demand.”[4]

### 1.2 Store of Value

As a store of value, bitcoin research from the St. Louis Federal Reserve explains, “volatile prices might not seem to be a threat to the store-of-value function of money when prices are rising; but when prices are falling, people are reminded that stable value is an important aspect of store of value.”[5] This point is illustrated below by a graphic from an IMF presentation on cryptocurrencies and monetary policy.[6]



[1] Jonker, N. (2018). *What drives bitcoin adoption by retailers?* [DNB Working Paper]. Retrieved September 24, 2019 from De Nederlandsche Bank: https://www.dnb.nl/binaries/Working%20 1 Paper%20No.%20585_tcm46-373269.pdf

[2] Poon and Dryja (2016). *The Bitcoin Lightning Network: Scalable Off Chain Instant Payments.* Retrieved September 24, 2019 from Lightning Network: https://lightning.network/lightning-network-paper.pdf

[3] Poon and Buterin (2017). *Plasma: Scalable Autonomous Smart Contracts.* Retrieved September 24, 2019 from Plasma.io: https://plasma.io/plasma.pdf

[4] (Jonker)

[5] Wolla, S. (2018). *Bitcoin: Money or Financial Investment?* Retrieved September 25, 2019 from Federal Reserve Bank of St. Louis Economic Research: https://research.stlouisfed.org/publications/page1-econ/2018/03/01/bitcoin-money-or-financial-investment

[6] Franks, J. (2019) *Crypto Currencies and Monetary Policy.* Retrieved September 24, 2019 from International Monetary Fund: https://www.imf.org/~/media/Files/Countries/ResRep/EUO/cryptocurrencies-and-monetary-policy-kingscollege-2019.ashx

Stored value should be stable against future purchasing power both in the short term and in the long term. While the "hodl" culture in crypto assumes that the value of bitcoin and other cryptos will generally increase over time, this is also true of equities traded on stock markets. Stock markets, like crypto markets, over time have been subject to crashes of up to ninety percent in value. It's this potential near-total loss in value that makes crypto no better a store of value than stocks.

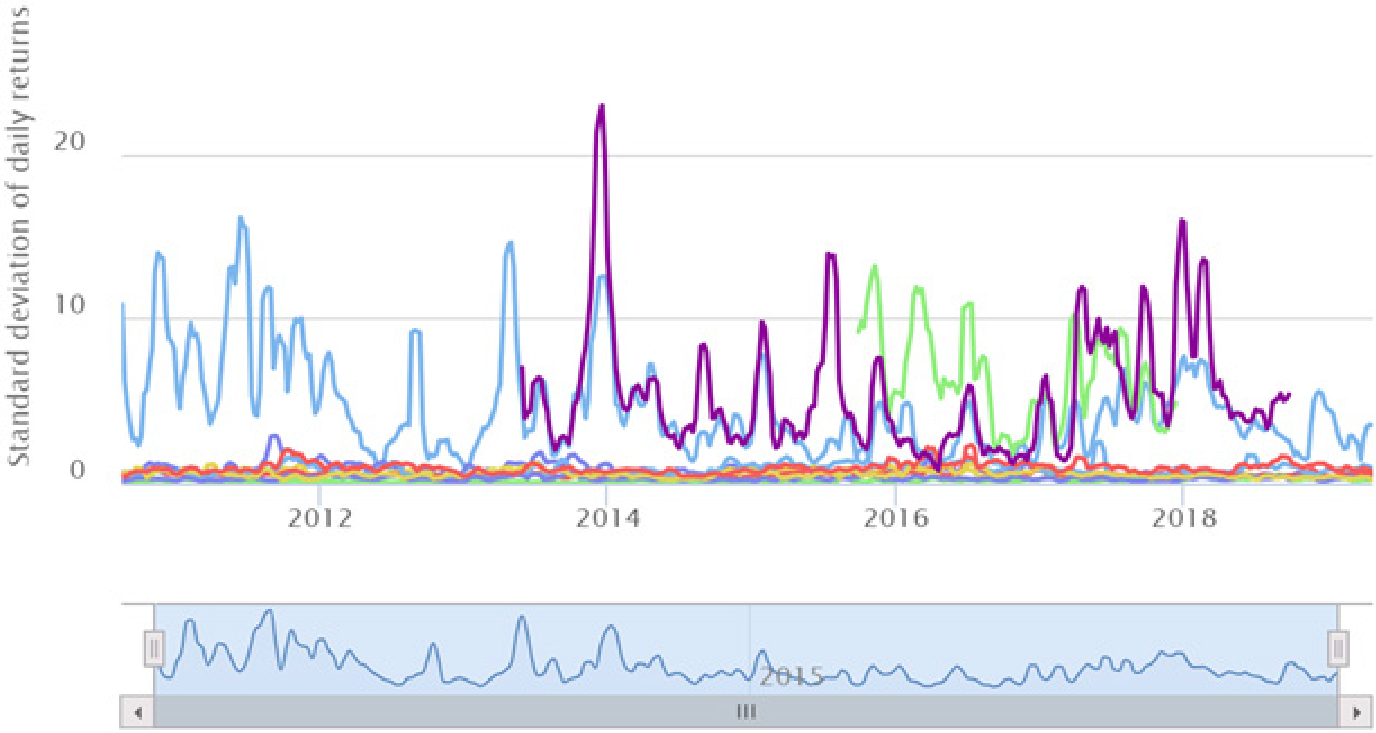
### 1.3 Unit of Account

As a unit of account, the IMF is fairly straightforward regarding cryptocurrencies, saying "No goods or services are priced in cryptocurrencies. Companies continue to report in major currencies, not bitcoin."[7] Economist David Yermack observes, "Bitcoin requires merchants to quote the prices of common retail goods out to four or five decimal places with leading zeros, a practice rarely seen in consumer marketing and likely to confuse both sellers and buyers in the marketplace."[8]

Additionally, the day to day volatility requires retailers to constantly recalculate prices quoted in cryptocurrencies. For accounting purposes, denominating a businesses cost of goods or profitability in bitcoin or ether from month to month would produce meaningless data. The volatility of crypto at present makes it a poor unit of account.

### 1.4 Volatility - The Common Thread

The chart below illustrates just how volatile crypto is compared to the currencies we transact in today.[9] As we can see, the volatility of Bitcoin, Ether and Litecoin is orders of magnitude greater than that of common fiat currencies and gold. Volatility, at present, is the overriding factor undermining cryptos ability to serve as money or reliable currency.



[7] (Franks)

[8] Yermac, D. (2013). *Is Bitcoin a Real Currency? An Economic Appraisal.* Retrieved September 27, 2019 from National Bureau of Economic Research: https://www.nber.org/papers/w19747.pdf

[9] https://www.buybitcoinworldwide.com/volatility-index/

## 2. Stablecoin Shortcomings

While the introduction of centralised, fiat-backed stablecoins like Tether (USDT), USD Coin (USDC), TrueUSD (TUSD), Paxos (PAX) and the Gemini Dollar (GUSD) have sometimes provided a solution to the volatility problem, they miss the mark in all other areas.

### 2.1 Fiat-Backed Stablecoins - A Bank, by Any Other Name

Fiat-backed stablecoins are centralised, for-profit businesses. Centre.io (USDC) raised $40 million in venture funding,[10] TrustToken (TUSD) raised $21.7 million,[11] and Paxos (PAX) raised a staggering $93.3 million.[12] These companies couldn't become profitable or provide a return to investors by taking in fiat, issuing stablecoins and simply holding 1-to-1 fiat reserves.

These businesses are modeled after banks, and they generate revenue the same way banks do. Funds deposited with stablecoin issuers, like funds deposited in banks, are invested. Like a bank, issuers must keep enough cash on hand to fulfill redemptions back to cash, but invest enough customer funds to turn a profit. Despite their use of words like "decentralised" and "redeemable 1-to-1," for all intents and purposes, fiat-backed stablecoin issuers are simply banks.

In April 2019 it was revealed by the New York Attorney General that Tether, purportedly "backed 1-to-1" by U.S. dollars held in cash reserves, was at least $850 million dollars short of 1-to-1 backing.[13] A subsequent filing from Tether Counsel stated "Tether has cash and cash equivalents (short term securities) on hand totaling approximately $2.1 billion, representing approximately 74 percent of the current outstanding tethers."[14] Tether's filing goes on to (favorably) compare them to a fractional-reserve bank, the very thing cryptocurrencies were created to eliminate.

Circle is fairly straightforward about their aspirations to shift USDC reserves from full to fractional at some point. A Circle support article titled "How does a customer know that there are reserves to match their USDC holdings?" states "When you wire fiat funds into our system, we deposit those funds with one of our banking partners. In the future, Circle may also invest these fiat funds in highly-liquid, AAA-rated fixed income securities."[15]

Some will remember the AAA-rated CDOs that were traded leading up to the 2008 financial crisis. According to the US Financial Crisis Inquiry Commission, of all the mortgage-backed securities Moody's rated AAA in 2006, by 2008 73% were downgraded to junk.[16] Whether the AAA-rated securities in which Circle and other fiat-backed stablecoin companies invest customer funds perform better, time will tell.

[10] Crunchbase. Retrieved October 9, 2019 from https://www.crunchbase.com/organization/centre#section-funding-rounds

[11] Crunchbase. Retrieved October 9, 2019 from https://www.crunchbase.com/organization/trusttoken#section-locked-charts

[12] Crunchbase. Retrieved October 9, 2019 from https://www.crunchbase.com/organization/paxos#section-locked-charts

[13] New York Attorney General (2019, April 25). *Attorney General James Announces Court Order Against "Crypto" Currency Company Under Investigation For Fraud.* [Press release]. Retrieved October 9, 2019 from New York Attorney General: https://ag.ny.gov/press-release/attorney-general-james-announces-court-order-against-crypto-currency-company-under

[14] Supreme Court of the State of New York (April 30, 2019). *Affirmation of Stuart Hoegner.* [Affidavit]. Retrieved October 9, 2019 from New York State Courts:https://iapps.courts.state.ny.us/nyscef/ViewDocument?docIndex=SRhgJjZzQXYlFyWilVeUsA==

[15] Circle Support. *How does a customer know that there are reserves to match their USDC holdings?* Retrieved October 9, 2019 from: https://support.usdc.circle.com/hc/en-us/articles/360015278312-How-does-a-customer-know-that-there-are-reserves-to-match-their-USDC-holdings

[16] Financial Crisis Inquiry Commission (January, 2011). *Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States.* [Congressional Report]. Retrieved October 9, 2019 from GovInfo: https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf

### 2.2 More Banks - Not the Solution

Fiat-backed bank coins do usually provide a stable-valued dollar peg to which traders can exit when they anticipate volatility or price declines, but they provide no utility outside of cryptocurrency trading. They are no more spendable than bitcoin or altcoins, are exposed to all the same risks as fiat, and require trust in an (often questionable) central issuer and any banking entities they use to hold reserves. Fiat-backed stablecoins are not the solution to a lack of cryptocurrency adoption.

## 3. Offshift

The primary blame for crypto not being used as a currency lies not so much on retailers, but in fact on consumers. The aforementioned 2018 Jonker study concludes "Information from consumers indicates that those who possess cryptos, don't use it for online payments. It seems therefore unlikely that the adoption of cryptos by retailers will increase substantially, making it highly unlikely that cryptos like bitcoin will drastically change the existing retail payment system.

Crypto's observed volatility is both:

a) the reason it's been successful as a speculative investment, and

b) the reasons it's not yet been adopted as a consumer currency.

Volatility is important in that it provides the incentive - potential profit from trading or holding - for people to buy the asset in the first place, but those people, especially traders, aren't properly incentivised to keep value in crypto, as for the most part they can't safely store it or spend it.

With this in mind, Offshift is designed to adequately incentivise both speculation and use as a currency. XFT, an ERC-20 token, incentivises investing and trading, while private stablecoins zkUSD, zkETH and zkBTC incentivise use as currency for storage and spending.

### 3.1 XFT Token - Listable, Tradeable, Speculative & Convertible into zkUSD

The XFT token is the utility token that enables use of the Offshift protocol, and the potentially volatile side of the ecosystem. XFT value is determined by the market. Like any ERC-20 token, price will likely be driven by perceived utility and speculation. As liquidity is paramount in the model, an ERC-20 token is ideal due to the number and popularity of Ethereum DEX protocols. XFT is easily listed on DEXs, centralised exchanges, and easily integrated into any wallet app with support for Ethereum tokens.

XFT is convertible into zkUSD using a mint-and-burn mechanism made possible by Ethereum smart contracts. Other stable value private storage projects like Haven (XHV) and Triton (XTRI) are forks of the Monero protocol and lack smart-contract capability. While mint-and-burn is still very much theoretical on those protocols, it's widely used today in Ethereum smart contracts.

### 3.2 zkAssets - Private, Stable-Value, Storable, Stakeable & Spendable

Offshift's zkAssets, the private, stable-valued side of the Offshift ecosystem, are the first cryptographically private stablecoins on any protocol. The value of assets like zkUSD, zkETH, and zkBTC are pegged to the US Dollar, Ether and bitcoin, respectively. Privacy, value stability and interest from staking incentivise the conversion of XFT to zkAssets.

zkAssets are an implementation of EIP #1724, "zkERC20: Confidential Token Standard."[17] Offshift uses zero-knowledge proofs to keep ownership values and the values of transfers encrypted and confidential.

Through a mint-and-burn mechanism, zkAssets are (and can only be) created when XFT are burned. For every 1 USD in XFT sent to the burn address, 1 zkUSD is minted and sent to an output address provided by the sender. XFT per zkUSD, zkETH and zkBTC conversion rate is determined via decentralised price oracle.

The zkAsset pegs are supported by their ability, at any time, to be redeemed for their equivalent value in XFT through mint-and-burn. Additionally, the pegs are supported by the existence of a liquid XFT market in each pair, so that converting from (for instance) zkETH to XFT, then selling XFT to ETH is practical.

[17] Williamson, Z. (2019). *zkERC20: Confidential Token Standard #1724.* Retrieved October 27, 2019 from Github: https://github.com/ethereum/EIPs/issues/1724

## 4. Maintaining Stablecoin Price Using a Semi-Decentralised Oracles Network

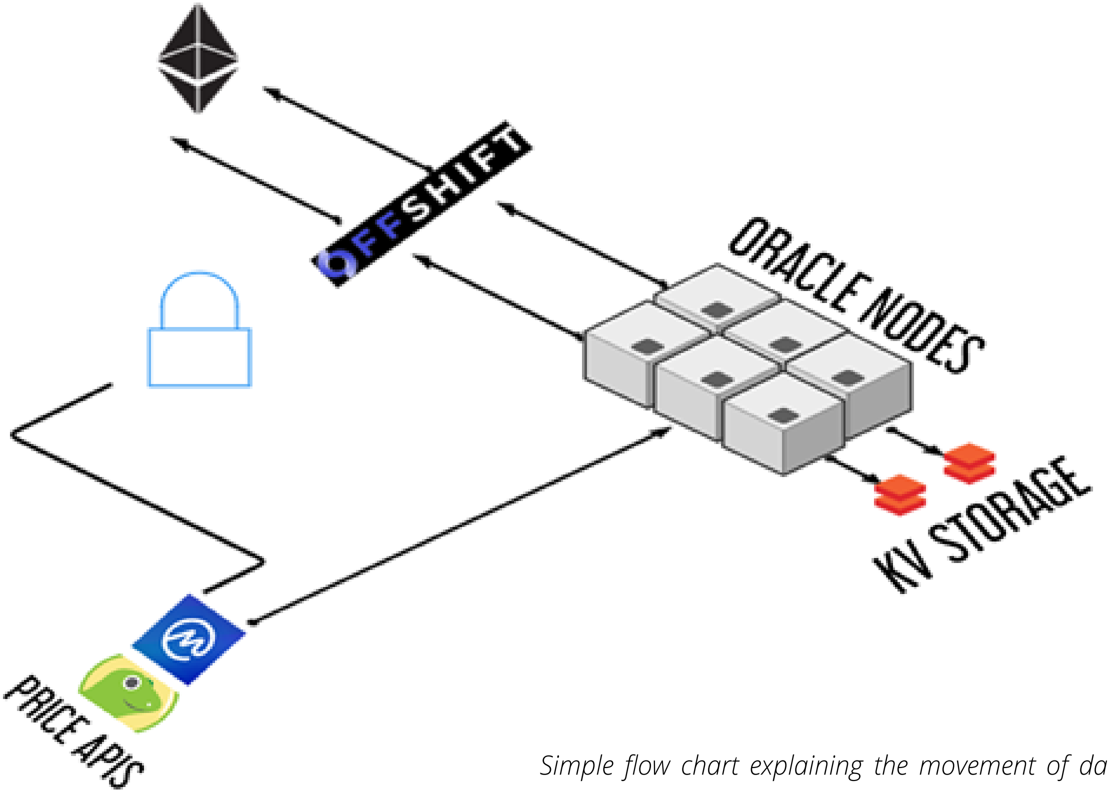
Offshift uses a semi-decentralised network of oracles to maintain stablecoin price.

### 4.1 What is a semi-decentralised network of oracles?

A distributed network of oracles is constructed to provide a continuous stream of price data, aggregate the data, and determine the current price of assets to be pegged. The software is constructed with arbitrary rules to protect it from unwanted and malicious external manipulation efforts.

### 4.2 How are the oracles semi-decentralised? And why?

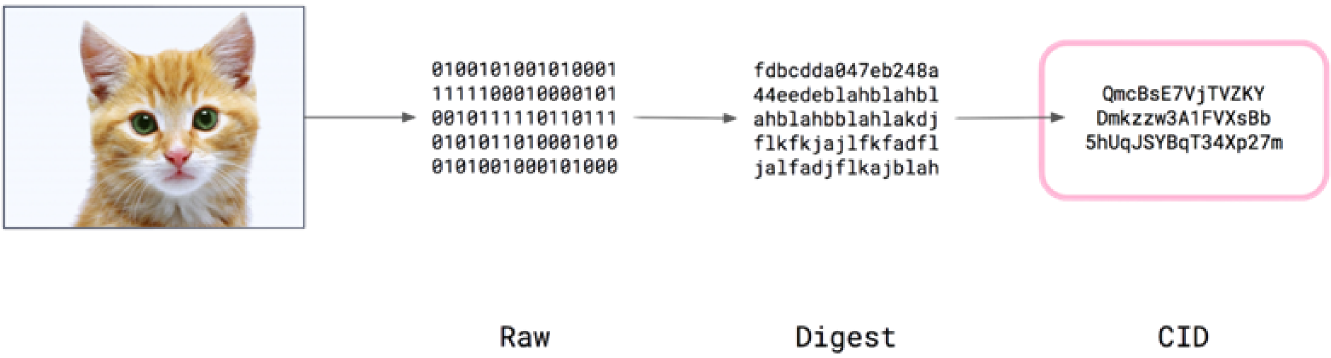
The oracles are run on geographically distributed nodes which collect data from various sources like CoinMarketCap and exchanges, and submit the data they collect into a fast key-value database. Offshift mint-and-burn contracts only accept an asset value if, at the time of the mint-and-burn execution, all nodes agree on the data that's been collected. In the event the nodes can't agree, the contract uses a moving average of the most recent agreed upon data.



*Simple flow chart explaining the movement of data to and from the oracle*

By using a distributed network of nodes and various sources rather than pulling price data directly from APIs, we mitigate the risk of a malicious actor manipulating data from any single source.

The price data used in the Offshift oracle nodes is also subject to public scrutiny. Each node is assigned an InterPlanetary File System (IPFS)-based address. Once every twenty four hours price data collected by each node is automatically updated and made available for download, allowing for independent verification. This cannot be subject to manipulation as files containing the same contents will always have the same IPFS hash.



*Simple diagram of how IPFS CIDs work.*[18]

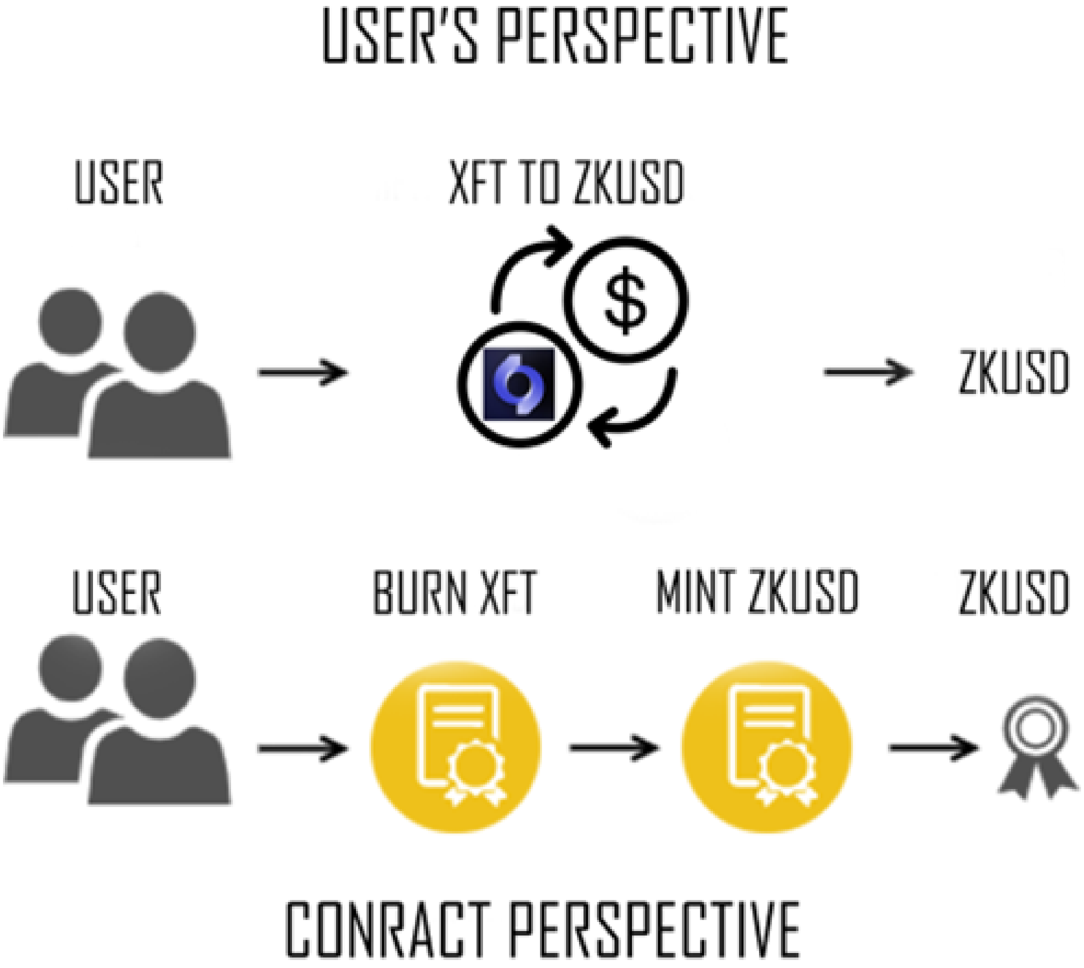
[18] Farmer, C. (2018). *What's really happening when you add a file to IPFS?* Retrieved March 2020 from Medium: https://medium.com/textileio/whats-really-happening-when-you-add-a-file-to-ipfs-ae3b8b5e4b0f

### 5. Mint-and-Burn

Through a process we call shifting, Offshift users are able to shift back and forth between XFT tokens and zkAssets with the use of two Ethereum contracts, a mint contract and a burn contract. The contracts communicate and interact in a way that results in an equivalent value in one token being minted when another token is burned.

To discourage use of mint-and-burn as a tool for flipping coins with the intent of acquiring more of either coin (and thus increasing supply), a dynamic bridge fee is imposed on zkAsset-to-XFT conversion. The bridge fee diminishes to zero over a period of about seven days, after which zkUSD can be staked.

*The figure below illustrates a typical mint-and-burn transaction.*



### 6. Bridge Fee

A one-way dynamic bridge fee is imposed on newly minted zkAssets crossing back to the public side (re-minting XFT from a zkAsset) to eliminate the potential for the bridge to be gamed for profit. The bridge fee diminishes to zero over a period of 40,320 blocks, or about seven days, after which zkAssets can be staked.

Bridge fees are distributed in their entirety to stakers.

### 7. Staking

zkAssets automatically begin staking 40,320 blocks, or about 7 days after they're minted. Staking rewards are distributed in the zkAsset staked. For example, a user staking zkUSD will receive zkUSD staking returns, and a user staking zkETH will receive staking returns in zkETH. The return percentage, or interest rate for all intents and purposes, is the same for all stakers regardless of stake size, and varies depending on percentage of supply staked.

Of the initial total supply of 10,000,000 XFT, 15% (1,500,000 XFT) is designated to bootstrap staking returns while the protocol gradually transitions to a model where bridge fees alone are sufficient to fund staking rewards.

The Offshift staking model will be further described in a staking paper prior to zkAssets launch.

### 8. Potential Use Cases

As the first private, stable-valued cryptocurrency, zkUSD provides some unique use cases, a few of which are outlined below.

### 8.1 Private peer-to-peer transactions

zkAssets serve as a private peer-to-peer currency in the same way as any other private cryptocurrency, but arguably with far more useability and potential for adoption due to their compatibility with any ERC-20 wallet, by far the most commonly used and most actively developed cryptocurrency wallet.

### 8.2 Point-of-Sale

Point-of-sale transactions with zkUSD allow both parties to transact in familiar units, privately, and protected from the volatility typically associated with cryptocurrency. Any merchant that currently accepts ether or ethereum tokens is able to accept zkUSD, zkETH and zkBTC. Merchants not currently accepting crypto can integrate XFT and zkAssets with the Offshift app when launched, or any number of ethereum point-of-sale solutions.

### 8.3 eCommerce

eCommerce has seen the most adoption of cryptocurrency payments of any sector, as well over 100 online merchants accept Monero[19] and dozens accept ERC-20 tokens.[20] Like point-of-sale merchants, online merchants presumably would prefer to transact in familiar units and be protected from volatility. zkAssets provide this denominational familiarity and stability, and additionally integrate seamlessly with existing Ethereum eCommerce solutions.

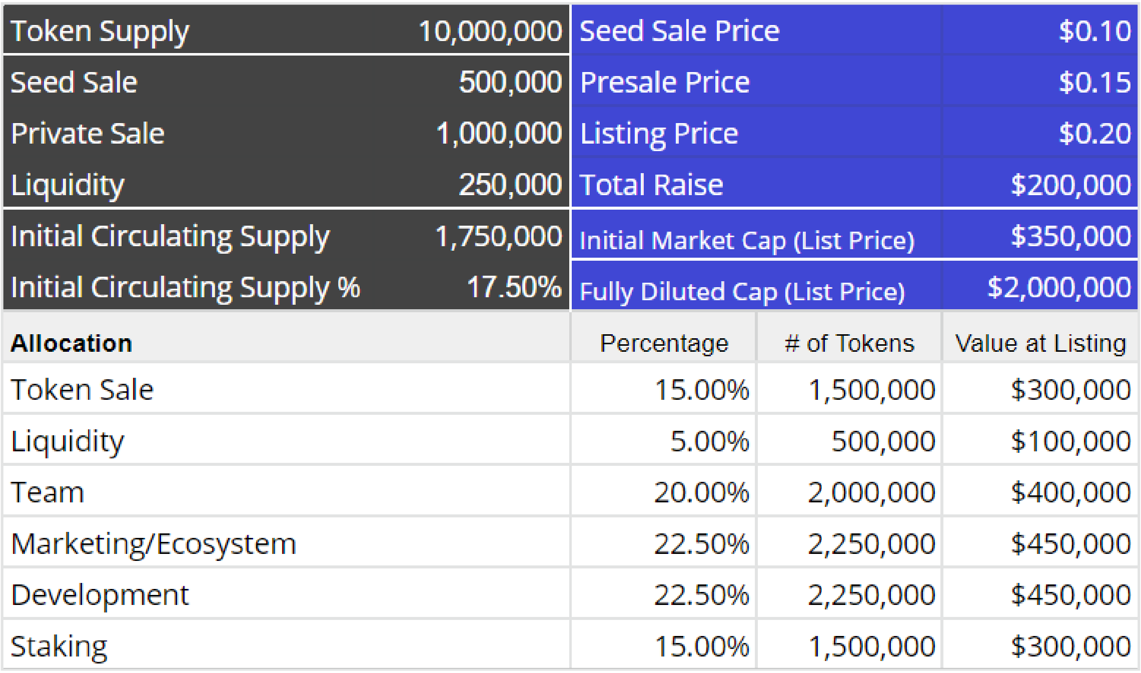
### 8.4 "Offshore" Savings

Perhaps zkAssets most appealing use case is as a method of private wealth storage, away from the prying eyes of government and untraceable with blockchain analytics. Stable value, cryptographic privacy and trustlessness make zkAssets similar, but superior to, offshore storage in a bank account.

[18] GetMonero. Retrieved January 24, 2020 from: https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf

[19] CryptWerk. Retrieved January 24, 2020 from: https://cryptwerk.com/pay-with/erc20/

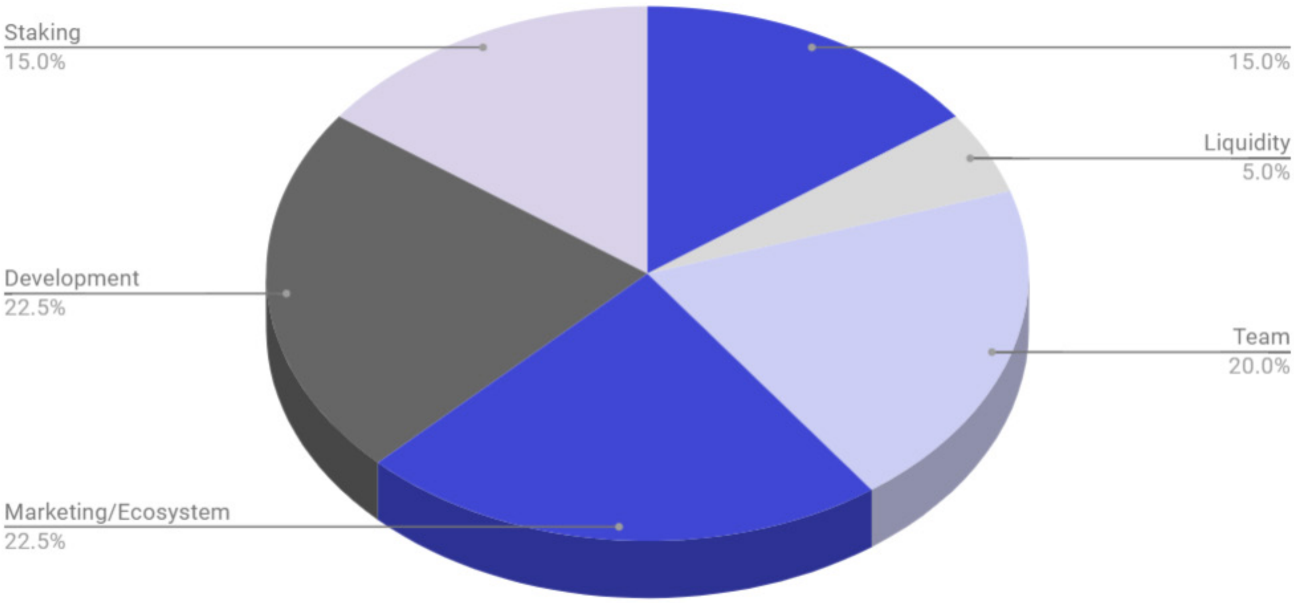
## 9. Tokenomics



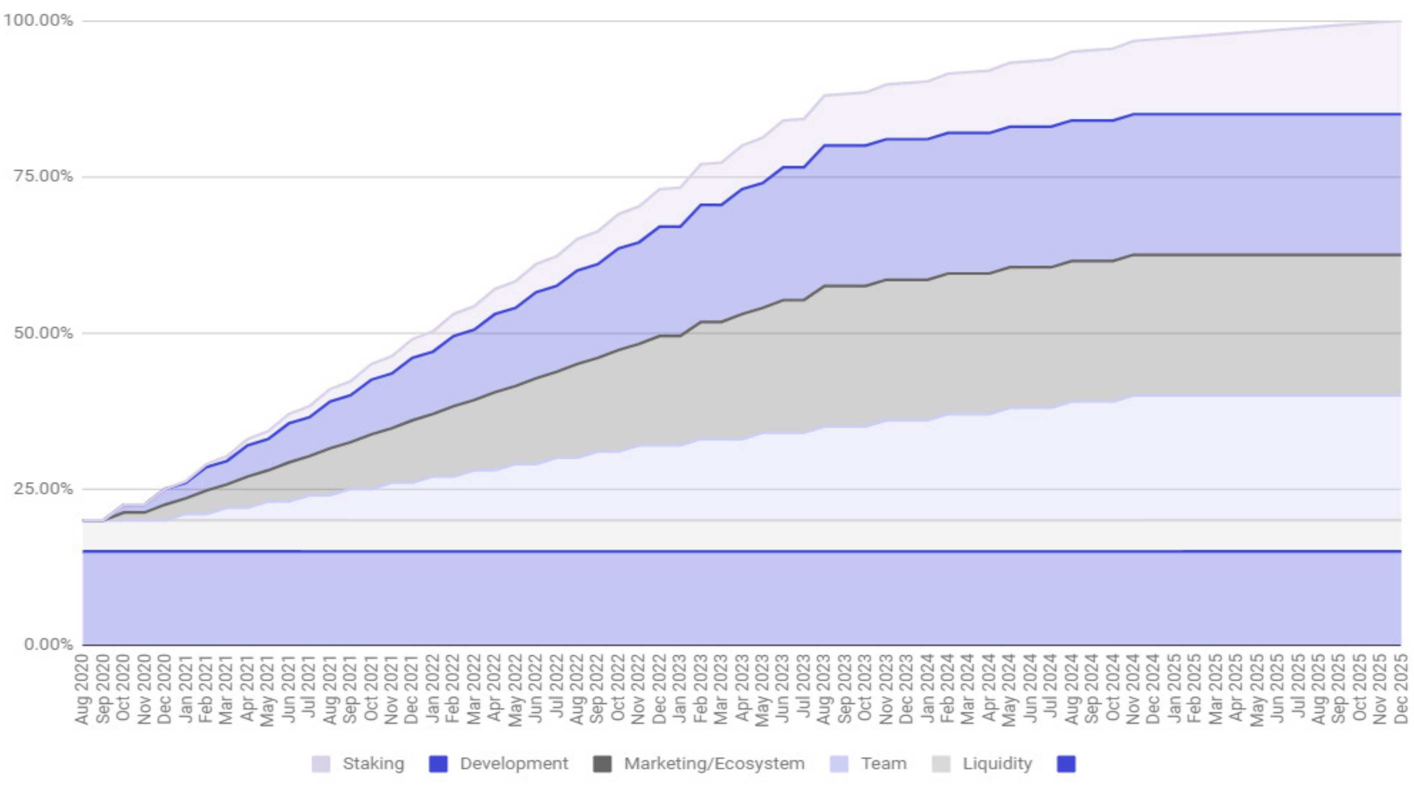
| | | | |
|---|---|---|---|
| Token Supply | 10,000,000 | Seed Sale Price | $0.10 |
| Seed Sale | 500,000 | Presale Price | $0.15 |
| Private Sale | 1,000,000 | Listing Price | $0.20 |
| Liquidity | 250,000 | Total Raise | $200,000 |
| Initial Circulating Supply | 1,750,000 | Initial Market Cap (List Price) | $350,000 |
| Initial Circulating Supply % | 17.50% | 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 | 15.00% | 1,500,000 | $300,000 |

## 9.1 Token Allocation



## 9.2 Token Release Schedule



## 10. Official Social Media & Other Accounts

Website

https://offshift.io

Telegram

https://t.me/OffshiftXFTt

Medium

https://medium.com/@offshift

Twitter

https://twitter.com/OffshiftXFT

GitHub

https://github.com/offshift-protocol

Bitcointalk

https://bitcointalk.org/index.php?topic=5262262

## 11. Risks

Purchasing XFT tokens, like any cryptographic token, involves substantial risk and may lead to a loss of partial or full amount of money invested. You should carefully assess the risks before purchasing, taking into account your own appetite for risk.

You should only purchase XFT tokens if you fully understand the nature of the tokens and the protocol, and if you accept the inherent risks.

Cryptographic tokens may be subject to expropriation or theft. Hackers or other malicious groups may attempt to interfere with distributed systems in various ways, including malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, or in other ways that damage the protocol. In such an event, there may be no remedy, and holders of cryptographic tokens are not guaranteed any remedy.

The regulatory and tax status of digital assets remains unsettled and varies by legal jurisdiction. It’s possible that in the future laws or regulations applying to digital assets may be implemented which affect your rights to own, hold or sell digital assets.