The Relay Stablecoin System

Whitepaper

v1.0

https://relaystablecoin.com

Contents

The Relay stablecoin system

The Relay stablecoin system establishes a two-token system to back the first private stablecoin pegged to the US Dollar (the Relay Dollar, ticker XRD) with a public volatile collateral token (the Relay Token, ticker XRL). The assurance of privacy and fungibility through integration of CryptoNote protocol features positions the Relay Dollar as a leading stablecoin contender for cash-like usage such as simple purchases from merchants who should not be able to see the buyer's total cash balance.

The XRD supply is controlled through an XRL collateralization mechanism secured by the Relay Decentralized Autonomous Organization ("Relay DAO"). XRD is issued as a network token in return for committing XRL, the primary network currency, to the Relay DAO. XRD is additionally issued to accounts with XRL contributed to the DAO to maintain the dollar peg or collateralization ratio when the price of XRD or XRL respectively rises, creating a direct revenue stream for tokenholders tied to XRL speculation and XRD adoption. When the value of XRD drops below the dollar peg due to undercollateralization or market perception of a risk thereof, XRD holders are incentivized to decrease the XRL supply by redeeming their XRD for XRL, with the redeemed XRD burned and removed from circulation. Price stability mechanisms are discussed at length in the "Price stability mechanisms" section.

Unlike Ethereum, the Relay stablecoin system has a fixed total XRL supply and does not have mining block rewards. Nodes are incentivized to operate and confirm transactions by the existence of transaction fees collected in XRD, which also serves as the 'gas' of the network. Should an address without XRD attempt an XRL transaction, XRL shall be deducted instead. XRD is the only network token with which this alternative transaction fee payment mechanism is possible. Transaction fees can be set by the sender and will vary with network demand, but are baselined at $0.005 (one-half of one cent) per transaction.

The Relay stablecoin system operates on an blockchain based on the Ethereum codebase with added CryptoNote features to provide privacy for the Relay Dollar, while the Relay Token will operate as a public token on the same blockchain. Ethereum was selected as the base technology for the Relay stablecoin system due to its long history of successful functioning with smart contracts, which are required for the DAO-based collateralization system. A public collateral token provides visibility into information such as the level of DAO collateralization and distribution of token ownership, while a private stablecoin brings with it the transactional advantages of a fungible currency.

There is technical precedent for incorporating CryptoNote privacy features into the Ethereum codebase. Fully functional implementations of a CryptoNote tumbler on the existing Ethereum network have existed since Q1 2018, and the Relay stablecoin system built on that work with the implementation advantage of operating on a separate network free of the compatibility requirements that inhibit projects that seek to function on the live Ethereum network. Integration specifics of privacy features are discussed at length in the "Privacy" section.

The ability to write new smart contracts and issue additional tokens on the Relay stablecoin system remains possible as on the Ethereum network, and this opens the potential for substantial additional value creation through dApps and other use cases. However, these are entirely ancillary benefits beyond the committed scope of the Relay team, and so will not be discussed further in this document.

Addressable market and actors

There are two primary markets when contemplating use cases for a stablecoin. First, stablecoins are critical to the successful functioning of cryptocurrency exchanges, as they provide a fixed fiat value for traders to safely maintain their trading assets. In the exchange scenario, the addition of privacy functionality into a stablecoin has value in maintaining the transactional privacy of users who deposit the stablecoin into the exchange. This incentivizes traders looking for a stablecoin trading pair to prefer the Relay Dollar as their store of value, and exchanges will respond to user demand. Concerns around money laundering or other privacy-based coin risks are assuaged by KYC/AML requirements of exchanges. In the exchange scenario, the actors are exchanges and traders.

The second and more significant market is common use as a digital currency. Existing stablecoins are hampered by centralized collateralization requirements which make them unable to scale, and/or by the lack of privacy features necessary for practical usage in a cash-like context. The DAO-based collateralization mechanism allows the Relay stablecoin system to scale to any value necessary to meet adoption demand, as demand for XRD will raise the value of XRL as additional XRD is printed to XRL depositors, increasing the value of the collateral held by the Relay DAO. Any current user of fiat currencies is a potential actor in this market.

As adoption of the Relay stablecoin grows, price stability will increase alongside due to the smoothing effect of having a larger number of use cases to absorb demand volatility in any specific application.

Price stability mechanisms

The Relay DAO collateralization mechanism is the heart of the Relay stablecoin system. Addresses sending XRL to the Relay DAO are granted XRD to the amount of 50% of the value of the deposited XRL. This initial collateralization ratio of 200% is set to minimize the risk of an undercollateralization event in case of a market crash. The collateral ratio may be adjusted in the future, but will remain as such for a minimum of one (1) year.

XRL and XRD prices averaged across all listed exchanges are reported to the DAO every network block. To prevent scenarios of reporting error, outlier prices with a >20% difference of all reported prices inclusive of the outlier are discarded, and price float is capped at 1% per block. The latter constraint results in the Relay DAO being slow to respond should the price spike up or down, which makes the system more stable over time as extreme price swings should significantly stabilize by the time the pricing mechanism ‘catches up’. In addition to smoothing natural market volatility, this also minimizes the impact of a rogue actor seeking to manipulate prices to ‘trick’ other network participants.

When available, Chainlink oracles (or the first fully functional decentralized Ethereum oracles) will be utilized to report accurate XRL and XRD prices. Until that time, a native Relay DAO oracle acquiring prices from exchange APIs as described above is the sole source of XRD and XRL price information into the Relay stablecoin system. The utilization of a centralized oracle to convey prices to the DAO is likely to be the most contentious part of the Relay stablecoin system. Other price reporting mechanisms do exist, such as staked bids submitted by collateral holders, but they have a substantial barrier to entry due to their complexity and are unsuitable at this time for a currency focused on simplicity of use and mass adoption.

When the value of XRD exceeds $1.01, new XRD will be issued in the amount of 1% of the current circulating supply of XRD. To prevent excessive issuance of XRD due to price changes lagging behind the injection of new supply, printings can only occur approximately once per day. XRD in circulation can be returned to the Relay DAO at any time to be redeemed for XRL. An identical portion of XRL held in the DAO will be redeemed as the amount of XRD returned relative to the total circulating supply of XRL. The returned XRD is burned. The high level workflow can be summarized as follows:

1. Users send XRL collateral to the Relay DAO
2. Relay DAO receives the collateral
3. Users receive XRD in return for collateral
4. Users return XRD to the Relay DAO
5. Relay DAO burns the received XRD
6. Users receive XRL from the Relay DAO

This approach brings a number of critical advantages, outlined below, that contribute to the stable functioning of the collateralization mechanism.

With regards to scenarios where the value of XRD drops below the dollar peg, proportional redemption of XRL instead of a fixed amount claim based on the initial deposit creates a group insurance feature of the Relay DAO. Traditional deposit accounting systems such as those used in traditional banks result in a ‘run on the bank’ scenario when trust or solvency in the system is low, as depositors rush to withdraw their funds before the bank is emptied. In this scenario, the DAO (which substitutes for the bank) spreads the gains or losses from an under or over-collateralization event evenly across all market participants. Therefore, user incentives to redeem XRD for XRL are independent of insolvency risk, as it simply does not exist in the Relay stablecoin system. For a given proportion of circulating XRD, the first withdrawal receives the same proportion of XRL as the last, unlike in a traditional bank run where the earlier withdrawals receive their full deposits and the stragglers receive nothing. Apart from ‘exits’ from the Relay stablecoin system in the form of selling into fiat via XRL, speculative expectations of the future XRL price are the sole driver of XRD redemption activity.

XRL can be issued or destroyed with every block.

Economic considerations in cryptocurrency construction

Cryptocurrencies and blockchain technology are expected to greatly influence payment and financial systems as they continue to mature and develop. Already the People's Bank of China, perhaps the most powerful central bank in the world, has indicated its intent to create a national digital currency on the blockchain, and other financial authorities around the globe are pursuing or researching similar objectives. As interest in cryptocurrencies as digital analogues for traditional fiat currencies is growing rapidly, thoughts on the applications of economic theory to cryptocurrencies are maturing as well.

Due to the novelty of the space and poor economic frameworks of most existing cryptocurrencies, cryptoeconomics is in its formative stages and early movers incorporating robust economic and monetary strategies stand to excel as cryptocurrencies transition from speculative assets to widely adopted mediums of exchange. Bitcoin and similar cryptocurrencies intended as a medium of exchange, including so-termed DAGs such as Iota or Nano, are more accurately categorized as investment assets rather than proper currencies. Key characteristics of currencies that most cryptos fail to uphold are low transaction costs (both in time and money), fungibility, variable supply in response to economic conditions, and wide acceptance, and stability of value. That said, cryptocurrencies are not strictly disadvantaged versus traditional fiat currencies.

In addition to production and replacement costs, physical fiat currency carries the substantial burden of never being able to truly solve for counterfeiting, and the ongoing U.S. Superdollar problem is a recent example of how serious the issue can be, to the extent of being used to fund rogue nations. While acceptance and price stability are presumed here to come over time as cryptocurrencies gain wide usage, transaction costs, fungibility, and intelligent supply variability are not so automatically solved. These issues must be explicitly addressed in a cryptocurrency, or long-term viability as a currency cannot be expected. Cryptocurrencies are uniquely equipped to solve for fungibility via the inclusion of privacy features, which is an advantage over traditional fiat currencies. The remaining issues require the incorporation of monetary features in order to first maintain viability as a currency, and second support the economic health of the systems utilizing the cryptocurrency as a medium of exchange.

A significant limitation of cryptoeconomic systems derives from their decentralized nature. An economic system is typically maintained via the dual application of fiscal and monetary policies, with the former being the actions of the central bank and the latter being the actions of a central government, typically in the form of taxation and spending. However, with no central authority to conduct wealth redistribution mechanisms, a cryptocurrency must assume that only monetary policies can be employed to maintain the health of economic characteristics of the network currency.

In the long run, it is highly likely that collectives of users holding significant influence over other network participants, probably in the form of ownership of major services provided to that network, will be able to form a centralized governing body with power sufficient to enact a limited form of fiscal policy, but that cannot be assumed in the construction of a cryptocurrency and thus the Relay stablecoin system is designed to stand on its monetary features alone via market incentives in its collateralization system.

Notable to cryptocurrency economics is that network confirmation activities are a public good, while the primary risk of double spending the cryptocurrency is mitigated by transaction reversals dependent on individual incentives. As a result, a cryptocurrency is most efficient when the volume of transactions is large relative to the individual transaction size, as in a retail payment system. Fortunately, this relationship is beneficial to a cryptocurrency over time, as increasing adoption should both increase transaction volume and decrease average transaction size, increasing the economic efficiency of the system.

Common cryptocurrency systems with consistent inflation rates through mining rewards and price volatility due to lack of a clear driver of value are clearly unsuitable at their current level of maturity for common usage as a medium exchange, and perhaps will never be able to break through these constraints. On the other hand, a stablecoin system with variable supply capable of closely tracking a baseline, fiat currency through an appropriately designed collateralization mechanism affords all of the transactional and security advantages of digital currencies while piggybacking on the monetary and economic expertise of the traditional financial systems influencing the fiat peg’s price. From the perspective of cryptoeconomics, stablecoins are the clear ‘best of both worlds’ frontrunner in the digital currency world.

Privacy

A resource is considered fungible when different units of the resource can be used indistinguishably from one another. In traditional fiat currencies, bills or coins are nearly entirely fungible, as they are largely indistinguishable apart from serial numbers or other added markings. Despite these markers, it is typically difficult to trace the full history of transactions a given unit of cash has been used for, apart from in specific situations involving currency specially prepared for the purpose, so fungibility can be generally assumed.

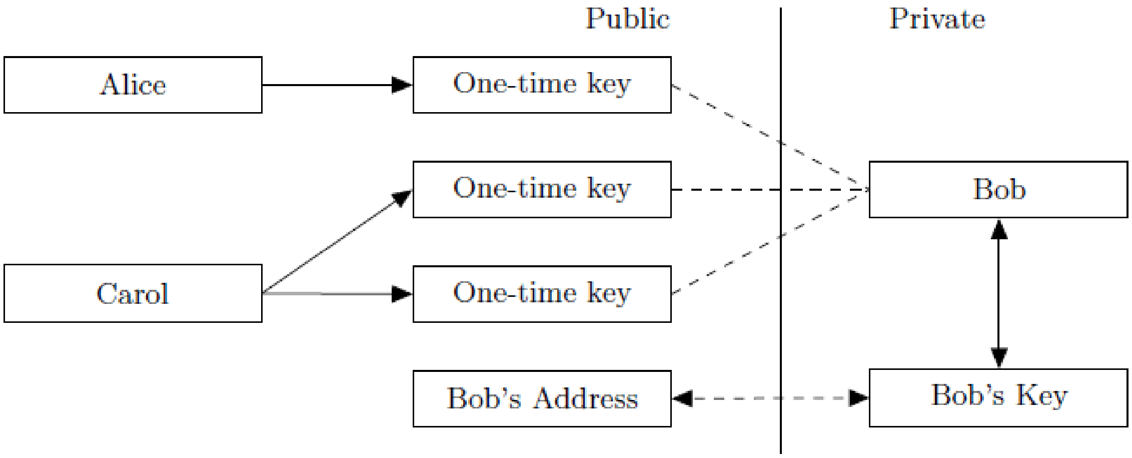
Cryptocurrencies are an entirely different matter. By nature of blockchain technology, a fundamental appeal of many cryptocurrencies is that transactions are recorded and publicly visible for all time in an easily accessible ledger. A critical benefit of the concept of a trustless, immutable ledger as applied to currencies is that there is absolutely no risk of counterfeit currency entering circulation. Counterfeit fiat currency is a major concern for central banks today, and the cryptocurrency advantage of eliminating this risk entirely cannot be overstated.

However, this traceability comes at the cost of privacy in many cryptocurrencies, and fungibility is lost when a given unit of currency can be traced through every transaction it has ever been used in, going back to the genesis block. This poses a number of basic concerns, from the mundane desire to conceal common spending habits to an unlikely, but still possible, event of specific tokens involved in illegal activity being frozen or otherwise excluded from circulation regardless of their current owner. Even the basic case of exposing daily spend on common goods poses a privacy risk, as in a blockchain-based economy it is not difficult to imagine data mining services that examine ledger histories to construct consumer profiles far beyond what financial firms are capable of today.

As illustrated above, the typical consideration of privacy features in a cryptocurrency as being a fringe application useful mostly for illegitimate activities is a short-sighted perspective that fails to consider the ramifications of public blockchains should cryptocurrencies ever become a primary medium of exchange. Therefore, for any cryptocurrency to be able to claim long-term value as a medium of exchange or transactional store of value, total fungibility through transaction privacy is an absolute prerequisite.

The Relay privacy protocol is adapted from the body of work created by the CryptoNote technology and the numerous cryptocurrencies based on the protocol, foremost among them Monero. Incorporation of ring confidential transactions, stealth addresses, and ring signatures provide autonomous privacy for each address to conceal its token balance and expose only transaction amounts and approximate times to transaction recipients, while exposing to outside observers only that a transaction was at an approximate time.

Stealth addresses protect receivers by disassociating transaction outputs with blockchain addresses through use of the Elliptic-Curve Diffie–Hellman protocol.



Stealth addresses in a private transaction

A typical transaction sequence is described below.

Given parameters and terminology:

E: an elliptic curve equation; $-x^2 + y^2 = 1 + dx^2y^2$

G: a base point; $G = (x, -4/5)$

l: a prime order of the base point; $l = 2^{252} +$

$27742317777372353535851937790883648493$;

$\mathcal{H}_s$: cryptographic hash function $\{0, 1\}^* \rightarrow \mathbb{F}_q$;

$\mathcal{H}_p$: deterministic hash function $E(\mathbb{F}_q) \to E(\mathbb{F}_q)$;

private ec-key: elliptic curve private key: a number $a \in [1. l - 1]$;

public ec-key: elliptic curve public key:

a point $A = aG$;

one-time keypair refers to a pair of the above;

private user key: a pair (a, b) of two different private ec-keys;

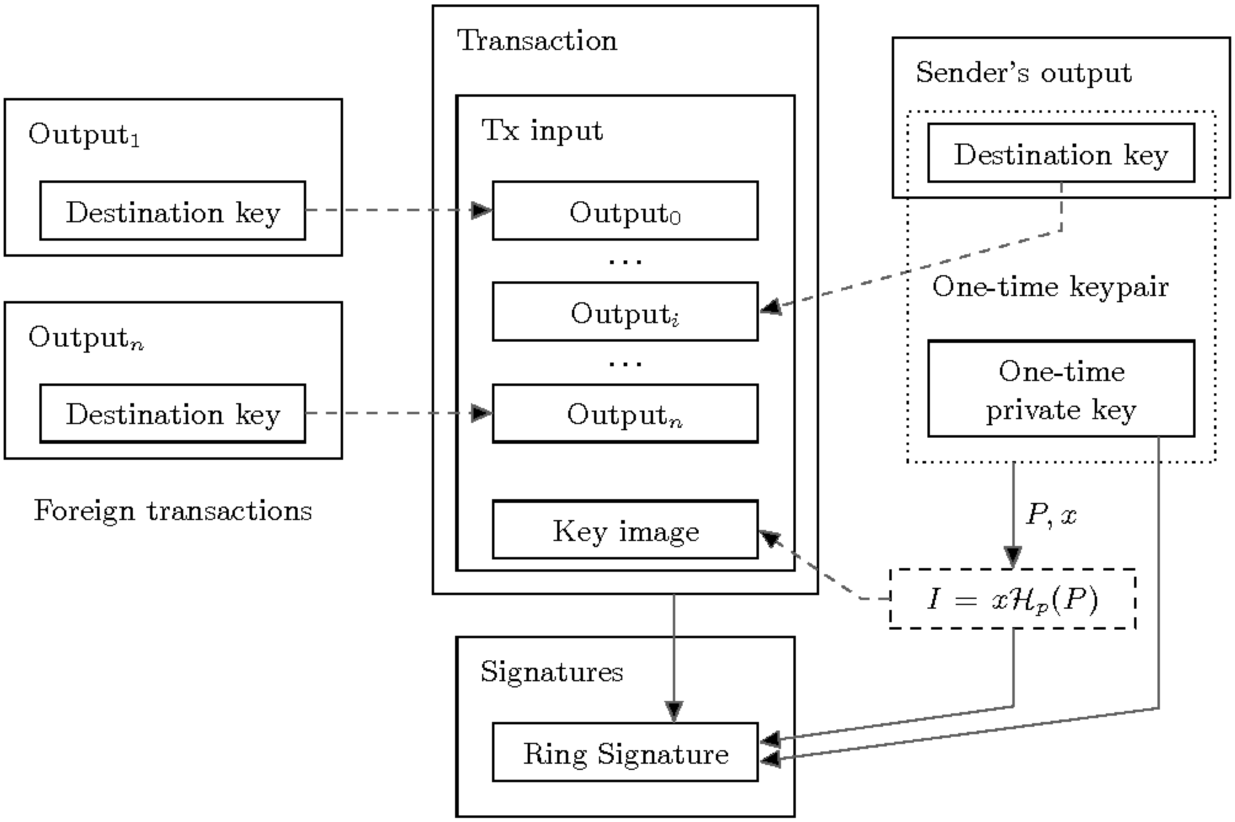
public user key: a pair (A, B) of two public ec-keys derived from (a, b)

Transaction occurs as:

- Sender obtains recipient's public key (A, B).
- Sender generates a random $r \in [1, l - 1]$ and computes one-time public key $P = \mathscr{H}(rA)G + B$.
- Sender uses P as destination key for output and packs value $R = rG$ into transaction and sends transaction.
- Recipient checks passing transactions with their private key (a, b) and computes $P' = \mathscr{H}(aR)G + B$. For the matching transaction, $aR = arG = rA$ and $P' = P$.

Recipient can recover the related one-time private key, as shown by $x = \mathcal{H}(aR)G + b$, so as $P = xG$. Recipient is able to sign a transaction with x to spend outputs.

Ring signatures, invented by Ron Rivest in 2001 as a particular form of group signature, protect transaction senders via obfuscation of the outputs (public keys) applied as inputs when creating a new transaction. The legitimate signer of a transaction produces a signature checkable with a given set of public keys, the others of which are pulled from the blockchain history. There exist several types of ring signatures utilizing non-interactive zero-knowledge proofs, of which the one-time variant is used here, which itself is a modification of E. Fujisaki and K. Suzuki's traceable ring signatures.



Ring signatures in a private transaction

Key images are incorporated into transaction data and utilized as the consensus mechanism to prevent double spend issues.

Ring sizes are not pre-specified by the CryptoNote protocol, which allows for permissiveness in user selection of level of security versus costs. The Relay stablecoin system mandates a ring size of 10 for all transactions. A standard ring size provides additional privacy security by eliminating the risk of outlier (potentially unique) ring sizes leading to partial transaction traceability, and provides technical benefits by limiting the file size of a given transaction, which otherwise grows linearly with the number of peers.

Ring confidential transactions (RingCT) improve upon ring signatures and complete CryptoNote's privacy features by obfuscating the value of funds involved in a transaction. This is done by applying Multilayered Linkable Spontaneous Anonymous Group Signatures (MLSAG) to prove the authenticity of a transaction without exposing the sums involved.

The RingCT protocol is defined below:

- Let $\{(P^1_\pi, C^1_\pi), \dots, (P^m_\pi, C^m_\pi)\}$ be a collection of addresses / commitments with secret keys x_j, $j = 1, \dots, m$.

- Find $q + 1$ collections $\{(P^1_i, C^1_i), \dots, (P^m_i, C^m_i)\}$, $i = 1, \dots, q + 1$ which are not already tag linked.

- Decide on a set of output addresses $(Q_i, C_{i,ut})$ such that $\sum_{j=1}^{m} C^j_\pi - \sum_i C_{i,out}$ is a commitment to zero.

$$\{(P1, C1), \dots, (Pm, Cm), (\textstyle\sum j\ Pj + \sum m\ \ Cj\ - \sum i\ C \qquad)\},$$

- $\mathfrak{R} := \{ \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad j{=}1 \quad 1 \quad i{,}ut \quad \}$

$$\dots, \{(P1\ , C1\ \ ), \dots, (Pm\ , Cm\ ), (\textstyle\sum j\ Pj\ + \sum m\ \ Cj\ \ - \sum i\ C \quad)\}$$

$$q{+}1 \quad q{+}1 \quad q{+}1 \quad q{+}1 \quad q{+}1 \quad j{=}1 \quad q{+}1 \quad i{,}ut$$

- The above is the generalized ring on which to compute the MLSAG signature $\sum$

The usage of the MLSAG ring signature is as follows, given that each signer of a generalized

ring with n members holds m keys $\quad i{=}1,\dots,$

$$\{Pj\} \qquad :$$

$$i \quad j{=}1,\dots,$$

- Demonstrate that one of the n signers holds the secret keys to their entire key vector.

- Ensure that should the signer use any of the m keys in another MLSAG signature, the rings are linked and the second MSLAG signature is discarded.

The addition of privacy features does result in lower transactional performance versus an equivalent non-private system due to privacy layer requirements. However, as a general rule there is not a impactful delay to the end user. Additionally, second layer solutions being developed by the CryptoNote community such as bulletproofs hold promise that performance gaps may be further reduced.

Risks

Risks are discussed here along with their defenses.

Risk: Transaction tracing through unusual ring sizes. In CryptoNote currencies such as Monero that do not have a prescribed ring size, unusual (typically very large) ring sizes have negative security implications.

Defense: Mandated ring size of 10 prevents this entirely.

Risk: Sybil attack via creation of a massive number of nodes. Distributed networks are most vulnerable to Sybil attacks in their infancy, when relatively few 'good' nodes exist and a malicious actor can acquire a significant portion of total networking computing power at relatively low cost

Defense: A portion of public round funds will be dedicated to bootstrapping network growth by establishing a number of 'good' nodes to secure the network until such time that organic growth has sufficiently mitigated the risk of a successful Sybil attack, as the costs of staging such an attack will grow with the volume and value of the network.

Risk: Fiat on-ramp exchanges are particularly selective regarding the properties of the coins that they select. Namely, privacy coins are a concern to the regulators that oversee these exchanges. While there is precedent for successful privacy listings with Zcash having been added to exchanges with fiat trading pairs, only non-private transactions are permitted due to the desire of regulators to be able to trace the transaction history of funds.

Defense: The Relay Dollar's privacy functionality is entirely mandatory, and thus there is no way to meet a potential requirement that only unshielded transactions be sent to an exchange. Therefore, it is possible that XRD may face challenges in being listed on fiat on-ramp exchanges. However, it is important to note that the Relay Token is not private and could be listed without this issue.

Risk: Massively adverse market conditions could result in a 'run on the bank' scenario in which XRD holders rush to redeem their funds for XRL due to a severely undercapitalized DAO being unable to meet withdrawal demand.

Defense: As described under the price stability mechanisms section, the group insurance feature of proportional redemptions eliminates the risk of a self-reinforcing withdrawal panic scenario that could rapidly erode the value of the collateralized XRL.

Token Generation Event

The total supply of XRL is 1,000,000,000 (one billion). XRD has a variable supply dependent on the amount of XRL held in the Relay DAO as well as the value of XRL. Both XRL and XRD are divisible up to 18 decimal places.

The Relay stablecoin system's public round will begin on September 1, 2018, and continue through October 1, 2018. Up to 2000 ETH will be raised in the public round for 75% of the total supply, which is 750,000,000 (seven hundred and fifty million) XRL. Of the remaining 25% supply, 12.5% is allocated to the team, 2.5% to the bounty program, and 10% to the Relay Foundation Ecosystem Development Fund. Team tokens are subject to a 1 year lock.

There is no private round. Institutions and other large investors will participate in the public round with no preferential distribution ratios or other advantages to other participants.

To minimize project risk from ETH price volatility, up to 1500 ETH or 75% of raised total, whichever is greater, will be liquidated into USD upon conclusion of the fundraising round to secure funding, with the remainder to be kept in ETH and liquidated as needed.

The purpose of the public round and intended usage of funds is as follows:

- Generate publicity and acquire an initial adoption base in the form of token owners who participate in the public round.
- Establish initial funding for the Relay Foundation Ecosystem Development Fund, which will provide guidance, support, and financial resources to enable the growth and development of the Relay stablecoin system.
- Provide funding for a third party code audit and public bug bounty program to ensure a successful blockchain network launch.
- Pay for additional exchange listings. This will be done very selectively and only if the listing has the potential to significantly grow Relay usage.

The public round of the token generation event will be conducted exclusively on the Ethereum network. Because the Relay stablecoin system will begin life as its own network, no placeholder tokens will be issued. Public round participants will be able to claim their XRL via the private keys of the wallets used to participate in the public round. This is made possible by forking the public round participant wallet address into the Relay stablecoin system. If users have security concerns around reusing a private key on another network, they are advised to ensure that their participation comes from a single-purpose wallet created specifically for the Relay public round.

The Relay team has signed agreements under NDA with two (2) exchanges to premiere listings for both XRL and XRD on the date of network launch. The Relay stablecoin system testnet and code will be opened to a public bug bounty program following the third party code review, which is currently in progress and expected to conclude in September or October. The public bug bounty program will begin immediately following the conclusion of the third party audit and run for a duration of three (3) weeks or until all no critical / major issues are open, whichever is later. The mainnet launch, XRL token distribution, and exchange listings will be held one (1) week after the successful close of the public bug bounty program.

References

Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols, 1994
https://www.win.tue.nl/~berry/papers/crypto94.pdf

CryptoNote v 2.0, 2013
https://cryptonote.org/whitepaper.pdf

The Welfare Cost of Inflation in General Equilibrium, 1994
https://fraser.stlouisfed.org/files/docs/historical/frbrich/wp/frbrich_wp94-4.pdf

Ring Confidential Transactions, 2016
https://pdfs.semanticscholar.org/4335/b2887dfb649e98a7c937c362e7404d9c1048.pdf

Mobius: Trustless Tumbling for Transaction Privacy
https://eprint.iacr.org/2017/881.pdf

A Next-Generation Smart Contract and Decentralized Application Platform
https://github.com/ethereum/wiki/wiki/White-Paper