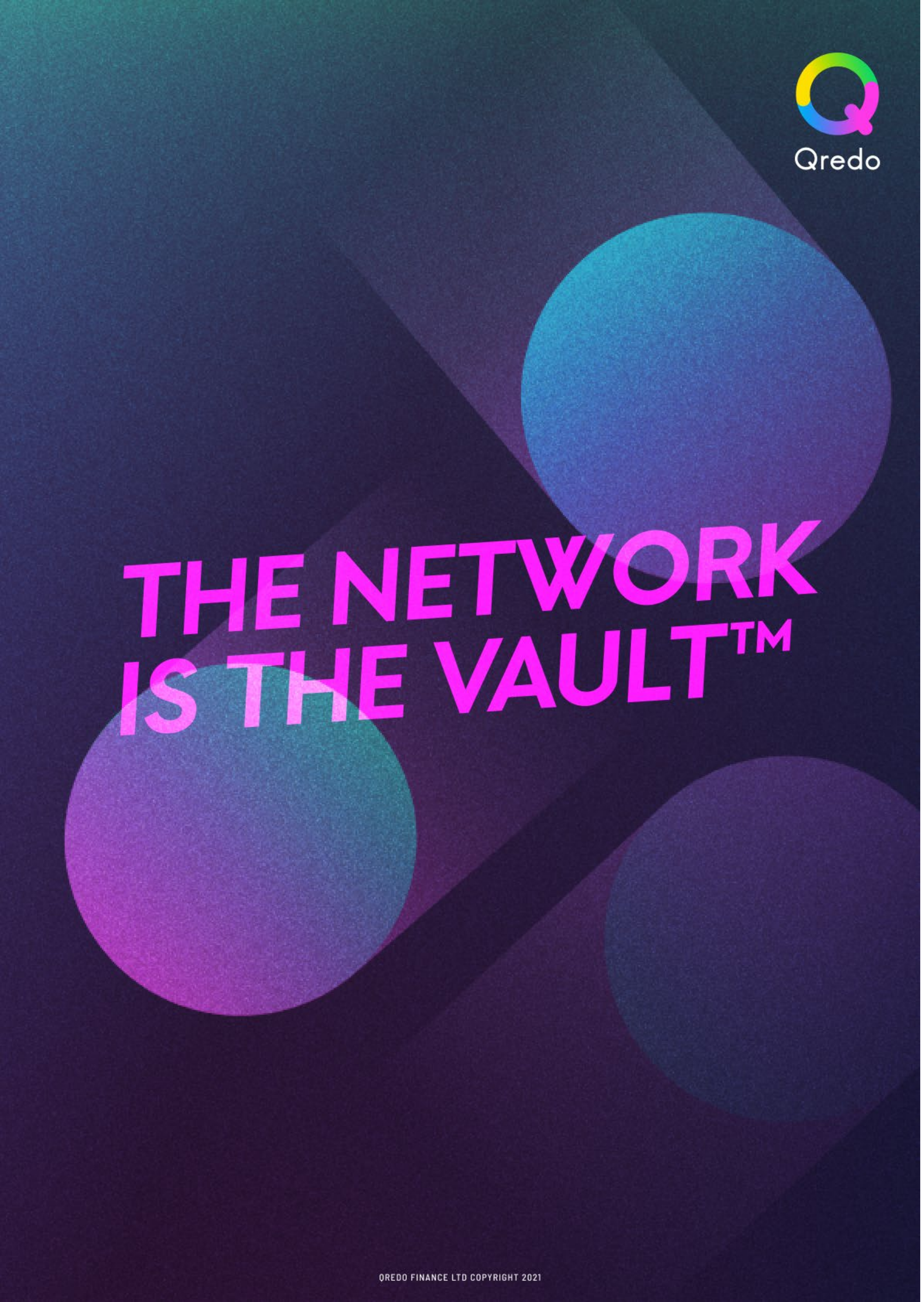
Qredo

QREDO WHITEPAPER

Radical new infrastructure for digital asset ownership and blockchain interoperability

QREDO WHITEPAPER JUNE 2021



Qredo

THE NETWORK IS THE VAULT™

CONTENTS

DIGITAL ASSETS & TRADING RISKS

CENTRALIZED CUSTODY

It's an odd irony; in spite of the explosive growth of DeFi, traditional finance traders migrating to DeFi are forced to use centralized custodians that naturally create counterparty and regulatory risks. As an example, if a custodian has any control at all over my wallet it can fall within a law enforcement or regulatory edict to shut down all operations as a service provider, depriving all customers of access to their digital assets.

We can define a centralized custodian as one that holds, has any access to, or can stop access to the private keys to a user's digital assets. In contrast, a non-custodial decentralized custodian does not hold users' keys and therefore cannot stop user-generated transactions. Qredo belongs to the latter category.

Recently, custodians have been migrating from a cold storage/hot wallet architecture to one that is built around multi-party computation (MPC). MPC is a massive leap forward in cryptography: for the first time, public keys and digital signatures can be produced in a manner that does not need a private key. Digital signatures, verified by public keys, are the cornerstone of blockchain cryptography.

Up until recently, a digital asset holder would have to manage and securely store the private key used to generate a digital signature (to move funds) and a public key (to verify the signature). Unauthorized access to a private key, or the outright theft of the private key, became the main attack vector for 99% of the large-scale cryptocurrency thefts reported in the media. The only other alternative to 'self-custody', where a trader manages their own private keys, is to enlist the services of a digital asset custodian.

The thinking behind this trend was that the digital asset custodian would manage their private keys more securely than the trader. The main issue being that in order to use a centralized custodian, the trader has to generate a transaction which transfers all of their assets to a wallet under the control of the custodian. This deprives the trader of control of their digital assets, as they have no access to the private key of the wallet, which is under the control of the custodian. As the publicly reported thefts of digital assets from within centralized exchanges and centralized custodians over the last five years proves, this is an imperfect solution: managing the security of private keys is difficult.

The development of MPC from 'theoretical' to 'practical to deploy' promised some security innovation for centralized custodians; eliminating the requirement to have a private key in order to produce a public key and a digital signature.

Multi-Party Computation is the ability of multiple parties to jointly perform mathematical computations without any party revealing its secret to the others. Multiple parties work together to solve signature equations without ever creating a key to begin with – nor ever exposing any critical information to one another. Centralized custodians could, by employing MPC, become decentralized. Unfortunately, that hasn't happened. Instead, these MPC enabled custodians are themselves continuing to be centralized and have become a concentration of counterparty risk.

While most centralized custodians have deployed MPC to lower the risk of private key theft, they run most if not all of their MPC nodes themselves, and they store all digital asset ownership information in a SQL database. It defeats the purpose of running an MPC network. Why?

Because a hacker attacking an MPC enabled centralized custodian can completely bypass the security of the centralized MPC network and focus on a much easier target: The database that stores[1] the ledger of which customer is entitled to what asset upon redemption from the centralized custodian.

Simply changing the values inside the database by creating a fake record of ownership enables the hacker to pull whatever she wants out of the centralized custodian. Only an immutable record (not changeable), like an entry on a blockchain, would provide the adequate security to record asset ownership and not be easily modified.

To make matters worse, many centralized custodians are operating without the proper authorization of the financial regulatory authorities where they are doing business, jeopardizing the regulatory and compliance standing of their customers. Customer's deposits are commingled, not segregated, running against the long-required capabilities that would be expected of licensed traditional custodian.

The combination of single points of failure, non-compliance with regulatory and compliance mandates, or flat out operating illegally without a custodian license, has created a large risk that there will be a hack of an MPC-enabled centralized custodian who controls all operations in the protocol. Such a theft from a large custodian could set off a panic within the market.

DEFI TRANSACTION INSECURITY

Blockchains were promised to bring unprecedented transparency to market operations, making all transactions—from simple orders to complex sequential smart contract trades—visible to all.

Yet paradoxically, blockchain transparency has enabled practices that compromise the security of transactions; malicious behavior that would be illegal on any regulated stock exchange and, according to academic research, this behavior poses a "systemic risk to consensus-layer security." [2]

FRONT-RUNNING BOTS

As public blockchains make transactions and their corresponding fees visible to the world, anyone can simply submit their own transaction with a higher fee—jumping the queue and getting their own transaction mined first.

This has resulted in the widespread deployment of bots that target ordinary users on decentralized exchanges by copying their trades. These bots will lie in wait, watching the mempool for profitable trade ideas, and then execute them before the original trader. Prices of the asset being traded then move, creating slippage for the original trader as the difference between the expected price and the price of execution widens.

Adding insult to injury, the presence of bots on decentralized exchanges inflates transaction fees: Bots compete for these opportunities by engaging in a bidding war to get their transaction processed first, inflating the cost of trading for all users on the exchange. This phenomenon has been referred to as Priority Gas Auctions or PGA[3] for short.

MINER EXTRACTABLE VALUE (MEV)

For miners, extracting profits at the expense of decentralized exchange users is even easier. Whereas bots have to pay to jump the transaction queue, miners can take advantage of what has become known as Miner extractable value (MEV), and arbitrarily reorganize transactions within a block for their own benefit: allowing them to frontrun profitable trading opportunities by simply sniping them from the mempool and discarding the original.

SEQUENTIAL SMART CONTRACT TRADES

The problems created by frontrunning bots and MEV are most evident for traders using smart contracts to package complex trades that are executed sequentially within a single block. These strategies take advantage of the atomic processing of Ethereum smart contracts, which are processed in discrete batches and will throw an exception if any trade in the batch fails. All trades must complete within the block, or none will.

For example, a trade relying on this strategy might take advantage of price discrepancies between exchanges, executing a complex sequential arbitrage trade if the prices are sufficiently different to generate profit. Yet if the price discrepancy is not sufficient to guarantee profit, no trades will be executed.

Once the smart contract containing this trading strategy is broadcast to the network however, all of the potential profit of the transaction is public to anyone with sufficient skill in creating a software program to analyze the trade, making it

[1] Fireblocks Being Sued for Allegedly Losing Over $70M of Ether: Report

[2] Research paper Flash Boys 2.0

[3] https://arxiv.org/pdf/1904.05234.pdf

irresistible for bots to attempt to be the first to execute the atomic transactions and steal the trade by submitting it with a higher fee prompting the Miners to process it first.

This damages the profits of retail traders obviously, but for hedge funds that typically operate under a shroud of secrecy because they need to recoup considerable investment in research and development, it could mean the difference between the firms success or failure.

FAULTY TRANSACTION RELAYING

Research has shown manipulation of Ethereum's mempool is resulting in stuck transactions, dropped transactions, and even huge losses through mass liquidations. In one instance during the market crash of Black Thursday 2020, over 50,000 transactions an hour were being dropped from the pending pool.[4]

THE NONCE GAP ISSUE

A broader problem with dropped transactions relates to an Ethereum quirk known as the nonce gap issue.[5]

Each Ethereum account must associate a nonce with its transaction, and the nonce must increment by 1 for every mined transaction. For example, if you send 6 transactions in a row and transaction 4 is dropped, the child transactions (5 and 6) will never be confirmed.

In the event, most traders would simply assume gas fees are too low and submit with higher fees, but the out of sequence transaction will not be processed by any miner, regardless of gas fees. This problem can be traced back to faulty transaction relaying.

THE ROLE OF THE RELAYER

In the Ethereum ecosystem, the role of the relayer is to help transactions compete in the block space fee market by deploying different strategies to get the transaction into the next block.

[4] Evidence of Mempool Manipulation on Black Thursday: Hammerbots, Mempool Compression, and Spontaneous Stuck Transactions

[5] A nonce is an arbitrary number that can be used just once in a cryptographic communication.

If a transaction has relatively low computational requirements, such as voting in a DAO, a relayer might opt for a low transaction fee. Whereas for quickly swapping tokens on a decentralized exchange, the relayer might use high fees to optimize for speed. This functionality is critically important as it ensures that Ethereum transactions have enough gas to motivate the miner to include the transaction in the next block, without overpaying.

For example, a package of smart contracts containing sequential transactions might require 100 units of gas worth of computational power to be executed. Any gas amount lower than this will be rejected as insufficient, and the ETH sent for gas is returned to the account minus the gas paid to the miners for the calculation. It's effectively the miner saying to the trader, "not only did your transaction not go through, we deducted gas fees from you for misunderestimating the fees we charge." Ouch. To avoid this, traders often create transactions with high gas fees to process the transaction quicker and overpay, but this is prevented by the gas limit which limits the amount a trader can pay to a miner to process their transaction. Double whammy.

Accurately computing gas fees for different types of transactions in an often volatile market can be challenging, and the relayer must also account for the nonce gap issue. But creating a relayer is complex and requires dedicated infrastructure. However, there is a huge opportunity for Layer 2 networks to solve these challenges by providing strong incentives for their decentralized Validators and MPC Nodes to collaboratively ensure orders placed on a Layer 1 like Ethereum are immune from MEV, front running, and are properly structured so there is no faulty transaction relaying.

LACK OF COMPLIANCE SUPPORT

In a world of low bond yields and negative interest rates, opportunities like yield farming have driven strong demand for DeFi from institutional trading firms looking to maximize returns.

Yet interacting with DeFi and meeting fiduciary duties don't go hand in hand: despite endeavours to protect smart contracts with improvements and third party audits, security concerns abound as it remains challenging to ensure digital assets are protected from internal and external attack vectors. Regulatory compliance is equally challenging, with authorities still struggling to devise governance and fragmented infrastructure making reporting difficult.
The root of the problem lies in DeFi wallet infrastructure that is designed for

individuals, not institutions. This infrastructure lacks the institutional controls that could allow businesses to legally operate in DeFi, and makes it impractical to manage large numbers of transactions across multiple protocols.

DeFi traders are now challenged to balance this need for security and compliance with the need to overcome scalability problems that lead to slow settlement, missed opportunities, and needless liquidations when markets become volatile.

TRADEFI INCOMPATIBLE WITH DEFI

Fund managers in traditional finance will use financial models to make portfolio allocations that quantify risk with metrics in the form of greek letters—alpha, delta, theta, etc—representing the sensitivities of price to various parameters.

Modelling traditional finance models on the blockchain however, is impossible as it requires floating point [decimal] numbers, which are not supported by Ethereum's programming language for smart contracts, Solidity, and by extension, Ethereum's smart contracts.

Decimals are required for everything from buying a cup of coffee for $4.20 to complex financial modelling, hence all modern programming languages support floating point numbers. But in Solidity, the lack of floating point numbers means you can't do real-time financial modeling on-chain, making manual calculations of implied volatility with something like the Black Scholes Model impossible.

For financial professionals to adopt smart contracts as a viable transparent money management solution, the floating point number problem must be solved. Until then, all modeling, trade strategy development and automation has to happen off chain. There is a big opportunity for Layer 2 networks to provide a bridge between these applications, commonly known as TradFi apps, and Layer 1 networks.

SUMMARY

Qredo's network is designed to address the challenges described that all traditional financial firms face when entering the DeFi space and provides an open protocol that continually updates its capability with the support of its DAO and community. For digital assets traders looking for best in class digital asset custody, Qredo provides a Layer 2/Layer 3 decentralized architecture with a programmable governance layer to encourage digital asset custodian adoption, or enable easy self-custody.

This is an important point: Qredo is not a threat to a digital asset centralized custodian's business model; it provides an opportunity for centralized custodians to grow their businesses and maintain relevancy as the world moves to decentralized infrastructure. These centralized custodians can use their existing infrastructure to run Qredo Clients which generate custodian approval transactions, and in turn offer customized programmable compliance and governance flows to their customers.

Qredo developers build with a 'network is the vault' design ethos in mind. Qredo's protocol declares asset ownership rights on a decentralized ledger rather than storing ownership information in a centralized database. A decentralized ledger obviously provides data durability and immutability.

Why is this important?

By way of a series of high-profile incidents reported in the media, the digital asset trading industry is now recognizing an uncomfortable fact: A centralized MPC enabled service provider storing asset ownership information in a database doesn't offer any better protection against theft, malfeasance or incompetence than a cold storage custodian. In fact, because of the complexity of MPC operations, the security model could indeed be worse, making your digital assets ***less safe***. Simply put, in order to attack a centralized MPC enabled custodian with ownership information in a database, it's not necessary to attack its MPC network. One merely needs to change ownership information in the database, or worse, delete it.

Enterprise compliance and governance officers can obtain the highest operational confidence that enterprise assets are safe and any compliance and regulatory trade flows can be supported whether they self custody or use one of Qredo's digital asset custody partners. This is because the **compliance rules and authorizations that govern trade flows are also written into Qredo's blockchain, just like the ownership information**, thereby gaining the data integrity and security that comes by using an immutable and durable data store (a blockchain).

He said, she said[6] arguments about who was operationally responsible for digital asset theft, loss or misuse are not possible with Qredo. Every asset's ownership information, transaction records, and governance approvals are recorded on a blockchain, and approved by a super majority of Validators that verify transactions do not infringe compliance policies, which are also recorded on the same blockchain. Even actions undertaken by the MPC network to produce wallet addresses or Layer 1 transaction signatures are interrogated, validated and recorded into Qredo's blockchain.

Whether accessing DeFi protocols from MetaMask or using in-house trading strategies and automating those strategies using the Qredo Client's Integration Libraries (Python, Java, .Net), all trade operations utilize the BLS signature scheme[7] to enable multi-custodian-approvals (either manual, automated, or both) which ensures the highest operational integrity. Why?

Because the Custodian actor's approval signatures are also part of the auditable data that is recorded in Qredo's blockchain.

The protocol's inbuilt Consensus-Driven Multi-Party Computation (CD-MPC) network ensures that the signature process that controls digital assets is never at risk of compromise, because private keys, the Achilles' heel of wallet security, are made redundant. CD-MPC enables public keys and signatures to be generated without private keys, immunizing assets from private key theft and compromise.

Lastly, the software that performs CD-MPC operations, validating transactions and voting on block proposals, is packaged for and run in secure enclaves. Applications are distributed using a secure pipeline mechanism direct from an open source code repository to trusted hardware or cloud environments offering secure enclaves.

Secure enclaves are an advancement in secure computing delivering an isolated, hardened, and highly constrained environment to host security-critical applications. The leap forward is a cryptographic process called attestation. This means application users can now authenticate the hardware integrity the software is run on, and the integrity of the software used to run these applications.

An attestation process programmatically audits the source code, and enables the user to receive cryptographic proof the data is being processed according to specification, and all software and hardware integrity checks have passed. Proof of these attestation checks are written into the Qredo blockchain. This helps to eliminate attack surfaces and shut off any unauthorized operations attempting to write to the blockchain, or invoke any interaction with other nodes.
The Qredo protocol was designed with traders in mind, with ease of enterprise integration, transaction security and privacy all available out-of-the-box on top of the decentralized custodian platform. Like any well-built enterprise software, Qredo Client offers an easy enterprise integration path and well-documented APIs. Qredo's Client Integration Libraries (Python, Node.js, Java) enable rapid integration and standalone application development so support for TradeFi modeling and trading systems execution is seamless.

The trading strategies developed are interpreted by Validators, and they invoke Qredo's open source Broker software, a module of the Validator server bundle. The Broker software module connects to the full nodes of any supported Layer 1. Doing so enables the Broker to not only write and submit transactions to the supported Layer 1 networks, it enables the Broker to act as an Oracle for smart contracts deployed on networks like Ethereum, interacting with smart contracts based on trading strategy conditions, and using smart contracts deployed by the community to obtain transaction security. The Broker software module acts as a traditional relayer would, to help transactions compete in the block space fee market by deploying different strategies to get the transaction into the next block.

The combination of the Broker software and Qredo's MPC network enables best-in-class transaction security against front running, Miner Extracted Value (MEV) operations and other dangers lurking in the Dark Forest[8] to achieve the highest levels of trade execution secrecy and security, guaranteeing the biggest ROI against the costs of strategy development and R&D. Defensive strategies are adaptable and upgradable. Qredo believes that defensive strategies are a dimension that can greatly benefit from advancements in AI and the ease of deploying applications to accomplish this objective.

[6] Fireblocks CEO Denies Negligence In $75 Million Ether Loss

[7] BLS Multi-Signatures With Public-Key Aggregation

[8] Ethereum is a Dark Forest

QREDO: THE WAY FORWARD

THE NETWORK IS THE VAULT

Qredo's Version 2.0 protocol reinforces and enables a rollout of its decentralized approach to crypto asset custody, delivery and settlement. The consequence of decentralization is that secured transfer, lending or atomically swapping crypto assets between parties is realizable via Qredo's decentralized settlement network, which accrues numerous benefits for its users over other systems in use today. The network is indeed becoming the vault.

The idea is straightforward: A distributed ledger is used to record the ownership of a Layer 1 crypto asset, which is represented by a synthetic token/wallet combination on the Qredo blockchain that maps exactly one to one in value to the asset's wallet on the Layer 1 blockchain. In other words, if a Qredo synthetic BTC wallet has 10 BTC deposited to it, 10 qBTC (the synthetic counterpart to the real asset) are minted on the next block and will show as the deposit in the Trader's qBTC wallet.

Using Qredo's blockchain explorer one can see exactly where the qBTC links its value on the Layer 1 blockchain, i.e., its mapping. This is repeated for every Layer 1 and ERC-20 token supported. Critically, the Qredo network never engages in rehypothecation. Meaning, the Qredo network stays provably solvent at all times. 1 qBTC on the Qredo blockchain will always map to 1 BTC on the bitcoin blockchain. The mapping of these synthetic values to values on the Layer 1 blockchain is called 'crystallization' and will be covered in detail in the following sections.

Qredo combines a fast-finality blockchain (Layer 2) for digital asset tracking and settlement with a Consensus-Driven Multi-Party Computation (CD-MPC) network, and a secure, end-to-end encrypted decentralized conversation replication network (Layer 3) to handle everything from machine to machine communications to storing and providing an audit trail for regulated pre-trade communications. Layer 3 has been introduced as part of the Version 2.0 protocol.

By acting as a Layer 2 network for any blockchain, Qredo eases scalability bottlenecks without impacting the security and consensus models of the underlying chains. This eliminates many of the risks that financial firms face when investing, holding or trading digital assets, and opens up a new global capital market with unique revenue opportunities for digital asset market makers, crypto hedge funds, digital asset custodians, centralized exchanges and more.

Qredo's Version 2.0 protocol leverages its Layer 3, a decentralized conversation replication store built on the Matrix protocol, in unique ways that are covered later in the document. The combination of Layer 2 + Layer 3 and enterprise grade Integration Libraries enables enterprises to rapidly integrate Qredo into their front, middle and back office applications.

CAPITAL EFFICIENCY

Qredo is a new approach to digital asset custody. It's arrival signals the end of 'passive' custody platforms that extract rent from customers. Qredo's design provides the best digital asset security through decentralization, multi-party computation and advanced crypto protocols, economic security and incentives, and thoughtful use of best-in-class infosec technologies like secure enclaves. But more importantly, it is the first digital asset custody platform designed from the ground up to ***make custody a profit center for its customers.***
The return on investment from using Qredo comes from accrued indirect benefits arising from capabilities such as eliminating wallet pre-funding,

enabling users to act as a prime broker to their counterparty, increasing transaction velocity and therefore capital efficiency. Qredo is the first decentralized custody platform and the first to introduce custody and transaction mining (described below), directly compensating its users. The sections below illustrate how Qredo delivers capital efficiency to its users.

RISK FREE SETTLEMENT

Qredo can confirm transactions between users in seconds with no counterparty, settlement or payment risk, including Layer 1 atomic swaps (BTC for ETH), or crypto-to-fiat transactions (ETH for GBP). No atomic swaps or transfers can be invoked or acted on with another counterparty using Qredo unless the ownership of assets on both sides of the transaction is cryptographically verified in an automated, frictionless, behind-the-scenes process ("Proof of Coin"). Transactions can't be assembled unless the digital assets are there. Users benefit from increased settlement throughput, the elimination of counterparty risk from exposure to unverified funds, and saved costs from the elimination of Proof of Coin fees. Put simply, there is no more "who goes first" when executing an exchange of Layer 1 assets for other Layer 1 assets or fiat. Settlement is instant.

NO PRE-FUNDING

Qredo eliminates the need to pre-fund wallets, eliminating settlement and delivery risk on centralized crypto exchanges.

Qredo enables centralized exchanges to sync the state of their central limit order book post any trade, triggering the atomic swap of assets on market and limit order fills, yet still preserving the privacy of makers and takers. The centralized exchange performs the role of ***settlement orchestrator***, invoking the atomic swap transactions between makers and takers on the Qredo network.

The key takeaway is that the makers and takers keep **their** digital assets in their Qredo Network created wallets, under their control, up until the requirement for settlement and delivery materializes because their orders are filled on the exchange. The exchange never touches or has to receive their customer's digital assets. Alice's limit order is filled by Bob and Charlie. The exchange creates atomic swaps between Alice / Bob and Alice / Charlie and submits them to the Qredo Network where settlement happens in a second or less. A setup flow between customers and the exchange eliminates any risk to the exchange of payment or settlement default.

This capability enables a new type of centralized crypto exchange that is custody-less. Why is this an advantage for centralized exchanges?

- **Reduce regulatory burden.** All centralized exchanges in mature jurisdictions face increasing regulatory scrutiny and pressure. All exchanges will eventually accept being regulated, and obtain and comply with their in-country custody licensing, or, be forced to use a licensed crypto-custodian. Qredo presents a third option, which is to operate without taking custody of customer assets at all. This has the potential to significantly reduce, or even eliminate, the associated regulatory licensing burden.
- **Serve more profitable customers.** Larger institutional traders often rank centralized exchanges as too high a risk to pre-fund their deposit wallets. This prevents centralized exchanges from acquiring these customers who would bring much higher transaction velocity and trading volume resulting in more profits. By removing the requirement to remit capital to an exchange's deposit wallet, it becomes possible for the exchange to capture customers in this market segment.
- **Reduce operational and financial risk.** The list of centralized exchanges who have been wiped out from hot wallet or cold storage theft is long. Exchanges who accept customer deposits have a duty of care that creates a reserve of unproductive capital on the balance sheet in order to make customers whole in the event of loss. Exchanges will only face more operational scrutiny as the industry matures, further increasing the operational burden of securing their customers' digital assets.
- **Reduce expenses and tighter operational focus.** Exchanges who jettison the operational burden of securing customer deposits and benefit from the subsequent financial savings can deploy capital to their core business operations (i.e., user experience, matching engine technology, etc.) resulting in a more streamlined and competitive business with a much lower risk profile.

TRADE CREDIT

Qredo Version 2.0 protocol enables the creation of Loan Pools to easily access highly leveraged trade credit, as appropriate for flash loans or yield farming. For liquidity providers, they will resemble a short term money market fund whose function is to primarily loan digital assets to borrowers on the Qredo Network at short durations, at highly leveraged ratios (8x - 10x). Loan Pools are created with the intention of returning high yields from the fees charged to the borrowers who take out loans for short term trading or yield farming. Because of the anticipated high yields and ease of obtaining trade credit, liquidity providers and loan borrowers do not participate in QRDO rewards schemes.

Loan Pools are single-sided pools with their own Layer 1 outward facing wallet that interacts with dApps programmatically via functionality in the Validator's Broker module. All buy/sell orders for the traders interacting with external blockchains are executed using the Loan Pool wallet directed by the Validator's Broker module, so the counterparty risk remaining is the order acceptance and digital asset delivery efficacy of the Layer1 blockchains (ETH, BTC, etc.), making collateral management scalable enough to offer leverage loans. Qredo's developers will constantly tune and update the Broker module to handle complex transactions and conditions.

LOAN POOL INTEREST RATES

The mechanisms used to set interest rates for decentralized applications providing credit are an intense area of research and development within the blockchain industry. Interest models play a critical role, balancing supply and demand between the users who want to borrow digital assets and users looking to earn yield on digital assets by lending them out. In practice, the interest rate models used in credit protocols have to balance the goals of liquidity and capital efficiency; this is an evolving field because, in reality, no one has got it all figured out.

Delphi Digital, a research-driven firm dedicated to advancing the understanding and development of the growing digital asset market, has recently released a research paper on the subject, which Qredo engineers believe advances the state of the art. The paper, "Dynamic Interest Rate Models Based on Control Theory", presents a novel approach to setting interest rates based using a PID controller (proportional-integral-derivative controller). Those readers who understand the mechanisms behind refrigeration units, or other systems that require regulation of industrial control applications may wonder what a PID controller has to do with interest rate setting in credit protocols. So did we.
As it turns out, Delphi Digital's paper robustly confirms that using a PID controller with a standard Ziegler-Nichols method to tune parameters creates a mechanism for setting interest rates that is much more accurate and fair than additional approaches. Qredo will be implementing this mechanism for interest rate setting. For further information, we recommend reading Delphi Digital's paper.[9]

COLLATERAL

Some important takeaways; **The trader looking to borrow does not need to move any collateral out of their Qredo created wallet into a margin account controlled by a counterparty, ever. Instead, there are two ways they can provide collateral. Everything stays within the Qredo networ**k.

1. The borrower adds the correct amount of collateral to borrow to the Loan Pool itself, receiving redemption tokens that enable them to withdraw their collateral. Lastly, the borrower creates a special wallet type called a Dedicated Wallet, which is still under their control, and they deposit the redemption tokens to this wallet, or;
2. They can select to use their staked QRDO tokens deposited with a Validator as margin. In the event a trader is using their staked QRDO tokens as collateral this necessitates a different fee schedule to incorporate compensation for the Validator, who is, in effect, agreeing to loan the customer's staked assets back to the customer to use as collateral to access a Qredo Loan Pool.

Some important points to note:

1. While the QRDO tokens are being used as collateral, they STILL COUNT as deposits within the Validators pool of customer's staked QRDO tokens, and are earning yield.
2. In the same way as above, the trader is able to offset borrowing costs by earning yield if they deposit the required collateral that matches the asset type it is borrowing into the Loan Pool as a Liquidity Provider. Example: To borrow from the BTC Loan Pool, deposit the required BTC collateral to the Loan Pool, in effect, becoming a Liquidity Provider at the same time as being a borrower. Use your redemption tokens as collateral.

Key Takeaway: **The trader is able to continue to earn APY on assets that are being used as collateral to obtain an undercollateralized loan.**

[9] Dynamic Interest Rate Model Based On Control Theory

TRADE & CUSTODY MINING

Qredo also employs a novel reward system to incentivize Market Makers, Validators, Trader Users and Custody Users to adopt the network via two QRDO token emission schemes that are distinct but work together to create high yield for all participants encouraging rapid adoption.

One token distribution mechanism is a rebate model, derived from a set, predictable inflationary schedule. These newly minted, inflationary tokens are distributed to active users who incur the protocol's Transaction Fees by trading, or Custodian Fees for storing their assets. These fees are calculated every epoch and distributed pro-rata based upon an emissions schedule, which divides up the available allotment of tokens for that epoch between Trader Users, Custodian Users, Validators and Market Makers. The intention is that the majority of Transaction Fees and Custodian Fees incurred are instantly rebated back to Users. This feature and others necessitate that the protocol is price aware.

To become price aware, the protocol uses a combination of:

- **Its own Time Weighted Average Price oracle - where each Loan Pool's activity is used to establish a TWAP;**
- **Chainlink oracles - https://data.chain.link; and**
- **Open Price Feed oracles - Compound | Docs - Open Price Feed**

Oracle deployment and utilization is covered in more detail in Qredo's technical yellow paper available for download from the website.

The second token distribution mechanism is funded by the Layer1 assets the protocol obtains via the Transaction Fees it collects at the moment the transaction is finalized in the blockchain. The protocol charges traders 0.5 basis points of both maker's and taker's trading principal. If for example two traders were exchanging BTC for ETH, the protocol would obtain ETH and BTC. The protocol exchanges Layer 1 assets for QRDO tokens using the protocol's Request For Quote mechanism which queries both Market Makers and DEXs on multiple networks. The protocol distributes the majority of these acquired tokens to Validators on the network. As above, this mechanism also leverages the protocol's oracle's for price awareness.

TOKEN DISTRIBUTION

The total number of tokens is hard capped at two billion tokens.

- **One billion tokens are set aside for investors in Qredo Ltd; including contributors, team, an initial fund for Treasury Management, a fund to help initial bootstrap initial Validators, and a fund to bootstrap the ecosystem as shown in the figure above. Also included in this one billion is a portion (10%) that will be sold between a mix of private investors and the general public.**
- **Another billion tokens are set aside for when Version 2 of the protocol goes live, and are to be distributed to actors on the network as a combination of rebates on fees and inflationary rewards, taking the float from 1 billion to 2 billion over an estimated 50 years.**

Qredo has published a tokenomics white paper, "Qredo Tokenomics Rewards and Emissions" to coincide with this publication. Emission schedules, governance and economic incentives are covered in detail, and the publication is available to download from Qredo's website.

STAKING QRDO TOKENS

The Qredo Network's blockchain, and the application it runs, use the open source Tendermint state machine software. Tendermint is best described as a general purpose blockchain consensus engine that can host arbitrary states of deterministic applications. Tendermint is software for securely and consistently replicating an application on many machines. Non-faulty machines see the same transaction log and compute the same state.

Tendermint consists of two chief technical components: a blockchain consensus engine and a generic application interface:

- **The consensus engine, called Tendermint Core, ensures that the same transactions are recorded on every machine in the same order.**
- **The application interface, called the Application BlockChain Interface (ABCI), enables the transactions to be processed in any programming language according to rules coded up by the application developer.**

The result is a binary that contains both Tendermint and the custom application hooked into the Application BlockChain Interface that determines if and how the transactions are processed.

Another way to think about it is that Tendermint is a protocol for ordering events in a distributed network under adversarial conditions, which is called Byzantine Fault Tolerance (BFT). This has been a highly studied academic field[10], and the latest research on the protocol is that the network is operational as long as more than 66% of the Validator nodes are not malicious. In the event that the number is less than 66%, operation of the network becomes unstable. In the event more than 66% of the Validators become malicious, transactions can be re-ordered.

However, in many systems, not all Validators will have the same "weight" in the consensus protocol. In a delegated proof of stake protocol (DPoS) like Qredo's protocol, it becomes not a matter of whether one-third or two-thirds of the Validators is corrupt or honest, but in proportions of the voting power, which will not be uniformly distributed across individual Validators.

Since Tendermint can replicate arbitrary applications, it is possible to define a currency (QRDO), and denominate the voting power in that currency. This is what Qredo protocol achieves with the QRDO currency. When voting power is denominated in a native currency, the system is often referred to as Proof-of-Stake. Validators can be forced, by logic in the application, to "bond" their currency holdings in a security deposit that can be destroyed if they're found to misbehave in the consensus protocol. This adds an economic element to the security of the protocol, allowing one to quantify the cost of violating the assumption that less than one-third of voting power is Byzantine (malicious). This is covered in more detail in the "Validator, MPC and Economic Security" white paper.

As a Delegated Proof-of-Stake based blockchain system, Qredo incorporates a system where holders of the QRDO token can add their balance to a Validator's balance in exchange for some of the rewards the Validator receives for performing its role. The Validator is paid for achieving consensus during the generation, voting for and validation of new blocks. The Validator's voting power is proportional to the number of QRDO tokens each Validator holds, including those QRDO tokens that have been 'staked', or deposited, with the Validator in the expectation of receiving some share of the rewards that the Validator earns for performing its role. There is no mandate governing Validator's staking offerings. The only condition is that every Validator must offer staking as a service in a non-discriminatory manner.

In most Layer 1 blockchains, Validators are paid out according to an emissions schedule that is inflationary. Meaning, more new coins are added to the overall supply of the fully diluted supply via the awards the Validator receives. Qredo has this type of emissions schedule, but also pays out form transaction and custodial fees collected by the protocol—a valuable proposition. This is described in detail in the "Qredo Tokenomics Rewards and Emissions" white paper.

It's worth noting that if a Validator misbehaves or does not work efficiently, its stake of QRDO tokens and the tokens of its depositors can be 'slashed', and the Validator may even be replaced by another one. This could have serious consequences for the QRDO token depositors expecting a positive return, not a negative one. Therefore, the reputation of the Validator relative to its operationally efficacy is important to attract QRDO token depositors in its staking service.

[10] [1807.04938] The latest gossip on BFT consensus

KEY FEATURES

COMPLIANCE AUTOMATION

Each synthetic wallet has at least one Trader (role) that can invoke a transfer or an atomic swap (trade) of synthetic assets with a counterparty (ex: qBTC for qETH). Each asset has at least one Custodian (role) that must approve the transfer or trade of the synthetic asset to/with a counterparty. Both of these roles are appointed by a Fund Manager, who sets up a Fund on the Qredo blockchain, populates it with deposit wallets for different asset types, assigns the Traders and Custodians to each Layer 1 wallet type. The amount of Custodians and the threshold of signatures needed to approve a transaction is extremely flexible, designed to meet the most complex trade approval flows.

When a synthetic wallet is created by the Fund Manager, it requires, as a part of initialization, a Custodian policy as described above. Qredo uses the BLS signature scheme[11] specified signature algorithm that each Qredo Blockchain Client emits when signing transactions as Traders or approving transactions as Custodians. The Custodian policy writes an aggregated BLS public key that can be thought of as a sum of different public keys which serves as the check that the Custodian policy has been met, meaning the right amount of Custodians plus Trader have signed the transaction to approve it. In other words, each Custodian policy has its own BLS public key, made from the combination of other public keys. This process is called public key aggregation, and the same capability holds true for BLS digital signatures in that they can be aggregated as well. This process is covered more in depth in Qredo's technical yellow paper, available for download.

When a transaction receives the right amount of digital signatures from the Trader and the threshold of Custodians alike, these signatures are aggregated by the Trader's blockchain client and pushed into the Qredo Network. The Validators in the Qredo Network will use the aggregated public key that represents the Custodian policy to verify that transaction's aggregated signature. If the transaction signature verifies, the synthetic asset will be transferred or atomically swapped for other synthetic assets in the next block as the transaction (and its signature) will be written into the next block.
Using the Integration Libraries, customized rule sets can be written in Turing complete languages (Python, Java, .NET) that expose all functionality described so that compliance and approval trade flows that require transaction interrogation can be automated or invoke other services by accessing their APIs.

Messages requesting signatures, responses, and other communications necessary to obtain and aggregate signatures happen over Qredo's Layer 3 network, securing message flows with end-to-end encryption.

CONSENSUS-DRIVEN MULTI-PARTY COMPUTATION (CD-MPC)

The security benefits of MPC in blockchains have been well studied and are now being rolled out en masse across the decentralized application landscape.

MPC technology does not require a private key to be created, so it cannot be compromised. As a result, single points of failure are eliminated. MPC works by multiple parties jointly performing mathematical computations without one party ever revealing its secret to the others. In order to compromise an MPC network, the minimum number of MPC nodes stipulated in a threshold to complete a public key or signature creation operation would need to be breached. The number

[11] BLS Multi-Signatures With Public-Key Aggregation

of computers necessary to breach in order to gain their secrets vs a single computer holding a private key makes it exponentially harder to compromise a wallet and steal funds. The major innovation of an MPC network is simply that, for the first time, public keys (to create wallets) and signatures (to create Layer 1 transactions) can be created by some other process and cryptographic primitive other than a solitary private key. In this case, it's a network of decentralized computers under the control of different organisations.

In the Qredo network, the CD-MPC Nodes running the MPC protocol together can either a) create a public key used to create an address for Layer 1 crypto assets to be deposited into the Qredo network, or b) create a signature on a Layer 1 transaction recognized by the underlying Layer 1 blockchain (example: Bitcoin) to spend or move the crypto assets out of the Qredo network. A software module called the Broker which is run by each Validator acts as a middleware controller and interface to each Layer 1 Qredo support. As an example, with Eterheum, it is able to interact with a variety of dApps via the Ethereum client it interfaces to.

The Broker uses the Qredo blockchain as an oracle to boot itself into action. When a transaction to exit the Qredo network is verified and included into the next block, each Broker software instance (which is run by each Validator) deterministically creates the Layer 1 transaction and submits it to its local MPC node to sign. This is an important takeaway: The MPC protocol only works if each MPC node inputs the exact same thing (i.e., a bitcoin transaction) to sign at the beginning of the protocol. One MPC node signing a different or modified transaction will abort the MPC protocol.

A (Consensus-Driven) CD-MPC network is created when the MPC nodes operating the MPC protocol refer to an on-chain dataset for instructions and affirmation of the operations, just like the Broker. Meaning, they use a blockchain to verify state and organize themselves into action if required. They inherit the current state of the blockchain and thereby the verification of transactions that the Validators have performed (trust) but they also engage in their own verification (but, verify) of the transactions in the blockchain that are compelling them to create a digital signature. Trust, but verify.

Qredo's CD-MPC network has other defense mechanisms built into its operations such as network obfuscation, node segregation and cryptographic organization, and MPC secrets security using threshold decryption, confidential computing and distributed key generation. These techniques are covered thoroughly in the "Validator, MPC and Economic Security" white paper.

EASY APP DEVELOPMENT

Qredo is not one but two protocols working in sync and cryptographically bound together to provide privacy (encryption), authentication, message integrity and non-repudiation (digital signature and verification).

Layer 2 is a Tendermint based protocol that acts as a side chain to Layer 1 protocols. Qredo enables decentralized custody and atomic swaps of Layer 1 assets between traders through its Layer 2 synthetic asset issuing and the rules that track synthetic asset ownership across its blockchain. Tendermint is a robust, fast finality state machine application that has been well studied academically and deployed in running blockchains today. Qredo Validator software includes a module called the Broker, a middleware bridge, smart contract oracle and viewer into activity on the Layer 1 blockchains that Qredo supports.

Layer 3 is an end-to-end encrypted, decentralized conversation replication system that uses the cryptographic identity of users from the Layer 2 blockchain as one of the building blocks to provide end to end encryption (privacy), authentication into message stores, message integrity and non-repudiation. The Layer 3 protocol is based on Matrix[12], which describes itself as a "decentralized conversation store rather than a messaging protocol". When sending a message through Matrix, it is replicated over all the Matrix nodes whose users (man or machine) are participating in a given conversation - similarly to how commits are replicated between Git repositories. There is no single point of control or failure in a Matrix conversation which spans multiple nodes. It is truly decentralized.

While Tendermint does come with its own P2P network capability, a Tendermint P2P network is really designed for the different kinds of nodes with different requirements for connectivity to one another as designed by the Tendermint developers. Using Tendermint's on-board P2P network for applications and functions not anticipated by the Tendermint developers would cause bottlenecks in communication ultimately degrading the performance of Qredo's Layer 2 blockchain overall. As an example, in the absence of a Layer 3, if a Trader signs an atomic swap transaction with a counterparty, the partially completed transaction would have to traverse Tendermint's P2P network to find the Custodian's Qredo

[12] Matrix.org

Clients, alert them to a pending transaction, obtain the Custodian's digital signature, and send the obtained signature securely back to the Trader's Qredo Client over the same network. Once there the Trader's Qredo Client must aggregate the signatures into a complete transaction, then submit it to the Qredo blockchain. With Layer 3 compiled into Qredo's blockchain client, all the steps outlined above are not only removed from Tendermint's P2P network, but the entire signature flow can be automated, so there is no manual interaction whatsoever. Further, all messages above are digitally signed for providing non-repudiation, message integrity and privacy via the end-to-end encryption using the same type of security found in the Signal app (double ratchet)[13]. This attention to security has led Matrix to be adopted widely within both the UK and French governments, and a number of defense consortiums. Matrix has been widely reviewed and received high marks in security audits.[14] It is open source with a number of implementations and a wide developer community.

Leveraging a Layer 3 based on Matrix enables the development of secure applications that bridge the gap in capability that exists between TradeFi and DeFi. As an example, Qredo's decentralized RFQ (Requests for Quotes) system securely interacts with Market Makers and enables private pre-trade negotiations between a Trader User and another known counterparty to finalize a P2P transaction, enabling a 'Bloomberg Chat' like experience for all users.

Using Qredo's Client software and open source Integration Libraries (Python, Java, .NET) financial institutions can craft messages containing Travel Rule information about a particular transaction between regulated Virtual Asset Service Providers (VASPS), or messages sent to or from VASPs.

Qredo's choice of Layer 2 / Layer 3 and enterprise ready Integration Libraries create a foundation that enables developers to rapidly create stand alone applications that extend the Qredo capabilities resulting in rapid time to value.

TRANSACTION SECRECY & SECURITY

Trading secrecy and security encompasses a number of different dimensions. Institutional traders moving into crypto trading are often surprised at the absence of regulations, infrastructure and technology to secure order execution and trading strategy IP that are common in FX or equity trading. The inability to execute trading strategies on Layer 1 networks such that the strategy is hidden from other network participants is the most stark difference. Hedge funds, algorithmic trading specialists, and other large scale operations spend significant sums of money in R&D to develop strategies and robust automated trading systems that protect the firm's intellectual property and maximise returns. This isn't possible on smart contract enabled Layer 1 networks such as Ethereum.

As covered earlier in the document, an array of adversarial actors are engaged in rogue tactics to steal potential profit and glean observable information that reveals strategies in plain view. A smart contract executing a series of transactions in sequential order that is necessary to profit immediately reveals all intended actions and their desired sequence the moment the transaction is submitted to the Ethereum blockchain. Every node examining the mempool knows all. The situation is no different on Layer 2 blockchains. Transactions are placed into the mempool, and in almost all Layer 2 networks operating today, these transactions have no privacy: They are exposed to all network actors.

Prominent trading security challenges can be summed up in two topics:

1. **Layer 2 Transaction Secrecy.** How can a trader keep secret transaction details before it is submitted into a Layer 2 mempool so it leaks the least amount of information to other traders on the network? Qredo's Layer 2 blockchain must enable transactions to be evident for data immutability and durability, without risk of loss for any reason at all. The requirement is not to keep secret transactions after the fact, but to encrypt them and keep them secret from other traders, who have access to the same mempool, while they are waiting to be processed by the Validators.

2. **Layer 1 Transaction Security.** How can one execute a complex automated trading strategy on a Layer 2 network that executes orders on one or more Layer 1 networks (e.g. BTC and ETH arbitrage) requiring exact order sequencing without revealing the strategy itself to other traders on those networks? When trading on a smart contract enabled Layer 1 network, how can a Layer 2 network executing orders on behalf of a trader protect the trader from adversarial network participants and miners who will steal the profit by submitting their own orders which will displace the trader's orders (MEV, PGA bots, etc.), i.e., the Dark Forest.

[13] matrix.org End-to-End Encryption implementation guide

[14] Matrix's 'Olm' End-to-end Encryption security assessment released - and implemented cross-platform on Riot at last!

Qredo is a platform with the capabilities to overcome these challenges. To fully understand how, it is necessary to describe at a high level how Validators are organized. Further, it's also necessary to use a cryptographic scheme called threshold decryption. A more in-depth description of this structure, the reasons behind it and the cryptographic algorithms deployed is in the "Validator, MPC and Economic Security" white paper which is available on the Qredo web site.

To solve challenge #1, the Qredo Client who finalizes a transaction, readying it to be pushed into the network where it will be visible within the mempool, performs one last act. It generates an AES encryption key, and encrypts the entire transaction payload, save for a unique transaction ID that it generates, and any optional ordering information if this order is part of a multiple transaction strategy.

Qredo's Validators do not operate in silos. They are organized into groups of three called Pods. Pods give Qredo's economic security design a level of strength and sophistication that is unrivaled across functioning Layer 2 networks. Again, this design is broken down in detail in the "Validator, MPC and Economic Security" white paper which is available on the Qredo web site.

The key detail here is that the Pods, as part of the initialization process, run a setup protocol that enables the Pod to perform threshold decryption operations. During the setup process, the three Pod members communicate to each other and the result of this operation is a public key that is published to the Qredo blockchain, identified as a Pod threshold decryption public key. Every operating Pod creates a threshold decryption public key and writes it into the blockchain. This public key can be used by any Qredo Client or network actor to encrypt messages so that only the Pod members can see them.

For every operating Pod, the Qredo Client encrypts the AES key used to encrypt the transaction with the Pod's threshold decryption key. Channels are set up for each Pod on Qredo's Layer 3 to receive encrypted symmetric keys that once decrypted, enable the Pod to decrypt the specific transaction and verify its legitimacy, and then vote on its insertion into the blockchain. To decrypt the AES symmetric key, all Pod members run the threshold decryption protocol. The key detail is that all three members must partake in the protocol, because no one Pod actually has the ability to decrypt the AES symmetric key on its own.
Further, Pods containing Validators have their own communication protocol used to vote on block creation. This communication protocol is not accessible by any other Qredo Clients on the network and is independent of the mempool.

The result is that transactions are encrypted and impossible to analyze by other traders on the Qredo network when encrypted transactions reside in the mempool. Only Validators in an operating Pod can decrypt the transaction, and only when the decrypted transaction is written into a block is it possible to analyze by other network participants.

The side benefit of this design is that transactions can be batched to reduce Gas fees.

To solve challenge #2, we take the workflow described above and add additional steps. A new order type will be present in Qredo's Version 2.0 protocol. The new order type is called a **Trading Strategy Order**. It exists because the Tendermint protocol does not have the capability to force Validators to correctly sequence transactions, among other drivers. If Validator A receives transaction #3, it will process the transaction without regard to the fact Validator B receives transaction #1 in the sequence. If the transactions are split up across different Validators, there's no way to ensure they are processed in the expected order.

When the Qredo Client creates multiple transactions that must be sequenced on its blockchain, a condition may stipulate that the 2nd transaction is not submitted to Layer 2 until the 1st transaction is confirmed in a block. Qredo Validator's Broker modules handle this condition, and will continually expand their condition processing capabilities as the platform matures.

Once the Pod decrypts the 1st transaction in the sequence, it will reveal the Qredo Client's on-chain ID Document. This contains an array of public keys necessary for Qredo Clients to operate on the Qredo network and also contains the Qredo Client's Layer 3 dedicated address. The Pod creates and sends a message to the Qredo Client acknowledging they have received the transaction, and provides a one-time Layer 3 address to directly send to the Validator Pod a) the encrypted AES keys that have encrypted the transactions and, b) the encrypted transactions.

The Validators in the Pod are compensated for making sure their Broker modules handle the 2nd - *n* transactions directly going forward and correctly following the 1st transaction's Layer 2 order instructions and sequence. Validators present cryptographic proof of a completed transaction sequence to the Qredo protocol, and receive a reward for their work in QRDO tokens. All Pods charge an uplift to the protocol's charges via an additional fee that is written into the Relayer order field. The uplift is uniform and is set by the DAO through proposal and proposal acceptance in a vote on chain. More information on fees will be provided towards the Version 2.0 protocol mainnet launch date.

Orders that include orders on Layer 1 blockchains use the Trading Strategy Order (TSO) even though they are not a Loan Pool borrower. This order was previously described in the Loan Pool section preceding this section of the document. The key takeaway is that the trader assigns a Pod the responsibility of executing her TSO in the best manner to avoid detection and achieve trading profit. The Validators in the Pod will execute the orders through their Broker modules.

To do this, the Qredo protocol and Validator Pods can deploy an array of transaction security tools to get the best outcome possible for the trader. Each Qredo Client creating a TSO order that involves order execution on a Layer 1 blockchain automatically prepends the order sequence with an order on Qredo's Layer 2 to move the trader's principal into the Loan Pool that matches the digital asset being traded. This enables the Validator Pod to use the Loan Pool's wallet to place the transaction, via their own Broker modules and the CD-MPC network. The benefit is that the high number of transactions created by independent active traders are aggregated into one wallet (per digital asset) creating a signal to noise ratio which obfuscates an individual strategy. Obviously the higher the transaction volume that utilizes Loan Pool wallets, the greater the obfuscation efficacy.

Transaction security solutions that address Ethereum specific challenges will also be developed as part of the Version 2.0 protocol rollout. These challenges on the Ethereum blockchain were described in the previous Digital Asset Trading Risk section. The Validators, working together in Pods, not only have the ability to perform threshold decryption, they can perform distributed key generation. This enables a Pod to interpret a smart contract order sequence described in the TSO (in Solidity), and modify it to encrypt one or more transactions in the smart contract sequence to anchor it in the next available Ethereum block. The new smart contract order sequence uses the ciphertext within the encrypted transaction(s) already written into the blockchain. The Brokers modules act as an oracle for the smart contract being called to decrypt the data which guarantees order sequencing. The Pod acting as an oracle will only decrypt the ciphertext passing back to the smart contract being executed after the encrypted transaction is included in a block. This provides protection against frontrunners, because key portions of the order sequence have already been written into the block, as encrypted data. They have no visibility as to the true nature of the order sequence. Even more powerful solutions can be created on the fly using counterfactual contracts[15] and metatransactions.[16] As an ever evolving field requiring vigilance and development of new methods of protection, Qredo will be publishing new research papers that delve further into this topic on its website.

SECURE ENCLAVE READY

A quiet revolution has been taking place in container security called secure enclaves. This technology is here now, deployed in production by nearly every server and cloud platform, including Intel, AMD, Amazon AWS (with their new Nitro Enclaves), Microsoft Azure, VMware, Google, Docker, and Red Hat. HSM vendors like Entrust support running applications within their HSMs in a secure enclave to achieve FIPS 140-2 Level 3 security. This already enables the widest range of deployment options, in the cloud or in your own datacenter on your own servers, of any new security technology in many years.

Simply put, secure enclaves isolate the software and data from the underlying infrastructure (hardware or OS) by means of hardware-level encryption. Within these secure enclaves, Qredo applications, like Validator software, MPC network nodes, Qredo Blockchain Clients, and the application data (including encryption keys, MPC secrets, and private keys for transaction signing) is protected from theft or attack—even in the event that an insider or attacker gains full physical or "root" access to the machine these applications are running. These hardware-grade security features fully protect computer memory, storage and network communications as well.

Even better, a process called attestation, which is available as standard from any provider listed, allows enclaves to authenticate the hardware inside which they run as genuine, and to attest to the integrity of enclave memory to a remote party, such as a blockchain. In other words, a Validator booting up their software could have the enclave perform an attestation check that the software package is indeed to official release and has not been tampered with in order to exploit a vulnerability. The absence of an attestation certificate tied to the cryptographic identity of a Validator, MPC node or a Qredo Blockchain Client enables an early warning system, further protecting the other secure enclaves operating Qredo network services from a potential rogue actor. Secure enclaves protect applications, data, and storage—locally, across the network, and in the cloud—simply and effectively.

[15] https://medium.com/coinmonks/understanding-counterfactual-and-the-evolution-of-payment-channels-and-state-channels-9e939d7c6f34

[16] https://medium.com/coinmonks/ethereum-meta-transactions-101-de7f91884a06

It's surprising that other Layer 1 and Layer 2 networks have not fully leveraged the leap forward that secure enclaves bring to blockchain-based platforms. The wide availability in both cloud vendors and on-premise hardware, the fact that it is free or in the case of two cloud vendors a slight uplift, and that attested applications are a natural fit for decentralized networks makes the policy to mandate all applications on the Qredo network must be invoked and run within a secure enclave. This is easily enforced by requiring that every application runs an attestation check, producing a certificate for the Qredo blockchain which is tied to the identity document of the user.

Qredo will have more in-depth deployment guidelines and administration documentation as it moves closer to the date of its Version 2 protocol testnet launch. Until then, expect more updates on how Qredo will leverage this exciting technology in development. One area where secure enclaves have an immediate impact is in the design of the economic security models for blockchain-based systems. Protocol designers can now incorporate, as an example, network obfuscation protocols so a set of MPC nodes would be kept 'dark' as to the other MPC nodes they are running the protocol with. Qredo's economic security takes advantage of secure enclaves to remove the friction when scaling the network, removing the need to continually scale Validator's deposits relative to the growth of the network. More details on Qredo's use of Secure Enclaves are covered in the "Validator, MPC and Economic Security" white paper.

ALWAYS AUDITABLE

A longstanding conundrum in the blockchain space that's never been solved is the lack of any truly certifiably accurate method of determining the asset base of any centralized entity, centralized exchange, centralized custodian, bank, etc. Exchanges or projects that suddenly go dark with 'exit scams', custodians that lose private keys—there is a long list of events that cost individuals huge sums of money. The overhang of this continues to affect the industry, as many large financial institutions continue to have a problem trusting entities with their digital assets because of the very real threat that these entities are not solvent.

Qredo Network is programmed to always be solvent. The mapping feature that enables a Qredo Client to display every qBTC, qETH, etc. wallet balance 'link' down to the underlying layer 1 blockchain wallet is a core capability of Qredo. These links are made visible for every Qredo Wallet. The sums in the Qredo Wallets always equal the aggregate sums of the links for every Layer 1 supported. Qredo creates these links and connections dynamically using several algorithms to

derive the lowest cost Layer 1 fees on exit transactions. This process is called crystallization.
Below is a simple overview of the relationships between Layer 1 Assets & Layer 2 qAssets and how crystallization maps the two together within the Qredo network

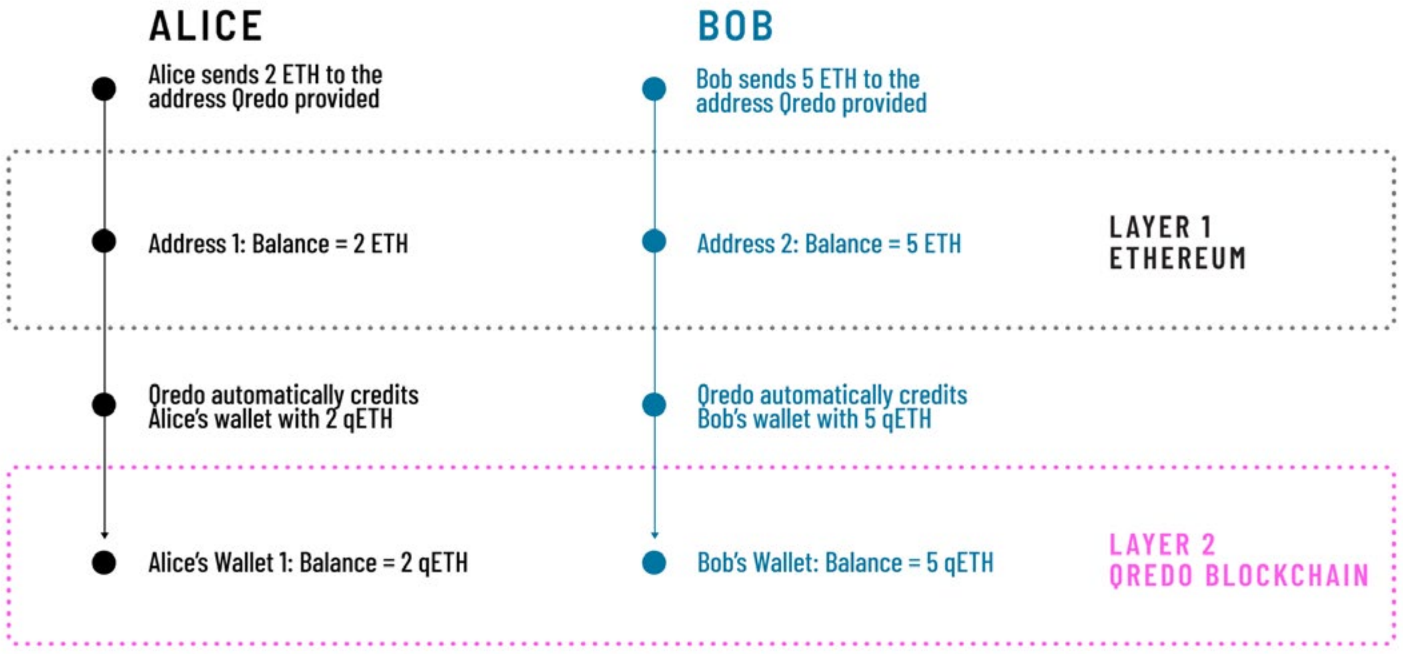
SETUP PHASE

- Both Alice & Bob have Qredo Accounts, they both set up an ETH Wallet and Qredo gives them ETH addresses to deposit their funds.
- Alice has Wallet 1 which is assigned Address 1.
- Bob has Wallet 2 which is assigned Address 2.

DEPOSIT PHASE

- Alice using Metamask transfers 2 ETH into the Qredo supplied Address 1 for Wallet 1.
- Bob using Metamask transfers 5 ETH into the Qredo Supplied Address 2 for Wallet 2.

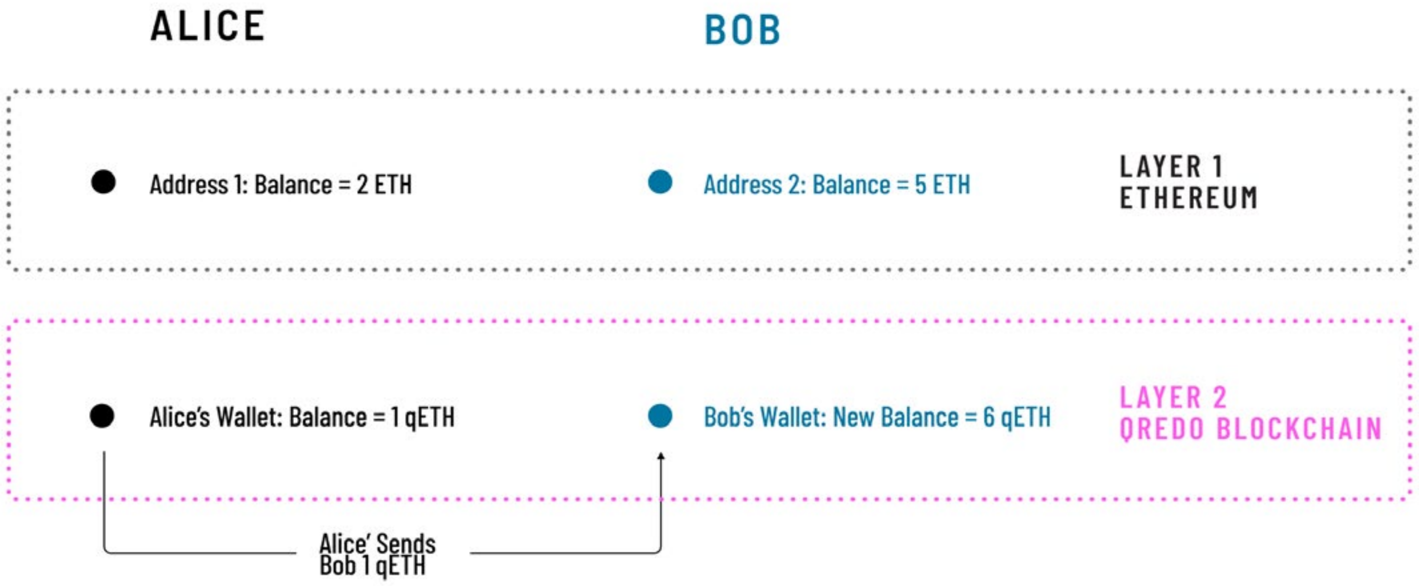
The diagram below shows the state of the system after Setup & Deposit. As you can see Layer 1 mirrors Layer 2. (Alice's Qredo Wallet contains 2 ETH, and the address assigned to that wallet Address 1 has 2 ETH... same for Bob).


ALICE
Alice sends 2 ETH to the address Qredo provided
Address 1: Balance = 2 ETH
Qredo automatically credits Alice's wallet with 2 qETH
Alice's Wallet 1: Balance = 2 qETH
BOB
Bob sends 5 ETH to the address Qredo provided
Address 2: Balance = 5 ETH
Qredo automatically credits Bob's wallet with 5 qETH
Bob's Wallet: Balance = 5 qETH
LAYER 1 ETHEREUM
LAYER 2 QREDO BLOCKCHAIN

TRANSFER

- Using Qredo, Alice transfers 1 ETH to Bob. This updates Qredo's Layer 2 blockchain so Alice now has 1 ETH left, and Bob has 6 ETH.
- Notice Layer 1 remains unchanged.

  After Transfer Qredo's qAsset register on its blockchain looks like this:


ALICE
BOB
Address 1: Balance = 2 ETH
Address 2: Balance = 5 ETH
LAYER 1
ETHEREUM
Alice's Wallet: Balance = 1 qETH
Bob's Wallet: New Balance = 6 qETH
LAYER 2
QREDO BLOCKCHAIN
Alice' Sends
Bob 1 qETH

CRYSTALLIZATION

Qredo's Crystallization process works out which Layer 1 funds map to the Layer 2 wallets.

In this case Crystallization would produce:

Alice's Wallet which has 1 ETH maps to part of Address 1, i.e., 1 ETH of the 2 ETH total.

Bob's Wallet which has 6 ETH maps to the other part Address 1; the other 1 ETH of the 2 ETH total and all of Address 2 (5 ETH).

Address 1(1 ETH) + Address 2(5 ETH) = 6 ETH in Total

As Qredo's platform grows beyond two users, the relationships between Layer 1 & Layer 2 becomes a more complex 'many to many' relationship.

However, the relationship is recalculated every block, so at any point in time,

The sum of Layer 1 ETH (2+5=7 ETH in total) is equal to the Sum of Layer 2 qETH (1+6 = 7 ETH in total) - thus proving Qredo is solvent.

Alice & Bob can always see the underlying Layer 1 transactions which are 'backing' their Qredo Wallets.

These relationships are constantly changing but should always be correct and available through Qredo's blockchain explorer.

CONCLUSION

Once funds enter the Qredo network the relationship between those deposited funds and the user they were originally allocated to gets modified. This is the same as any normal crypto currency exchange, as they allocate to you a deposit address, but what happens to the funds after they are deposited, is of no direct concern to you.

The difference between a normal exchange and the Qredo network is that at any point in time Qredo can demonstrate which underlying Layer 1 funds map to their Qredo Wallets containing qAssets (Layer 2), and even though this relationship is in constant flux, every Qredo Blockchain client will calculate the same relationship at each block. So it is defined by consensus of the nodes and Validators and is always solvent as funds are never rehypothecated.

This mapping gives Qredo the ability to make a "proof of funds claim" at all times.

Any member of the public who runs a Qredo Client (whether validating or not) and the accompanying Qredo Broker module can prove that all the Layer 2 funds (wallets) in our system map to real Layer 1 funds and they can see exactly the details of these mappings. This is something that conventional exchanges can't do without some degree of trust, because they could simply omit some records from their database tables to make the numbers tally. Qredo's register lives on a decentralized ledger, inheriting all the security properties of data immutability and durability.

USE CASES

DECENTRALIZED CUSTODY & DEFI

The Qredo Network is the perfect complement to DeFi protocols and applications enabling rapid adoption in financial firms that have to comply with compliance and governance workflows as part of their trading and order execution strategy. Qredo's approach to DeFi protocol integration is based on some key first principles.

First, let the user continue to use the native interface built by the dApp's developers. Trying to create an alternative user experience because of technical limitations is not an approach that leads to adoption. This is done using a browser with a wallet browser extension.

Second, be as unobtrusive as possible and in no way disrupt or impede the actions of the trader.

As an example, let's assume the trader is using the most popular Ethereum wallet, MetaMask. MetaMask allows users to access their Ethereum wallet through a browser extension which can then be used to interact with decentralized applications. MetaMask allows users to store and manage account keys, broadcast transactions, send and receive Ethereum-based cryptocurrencies and tokens, and securely connect to decentralized applications.

Qredo developers have created a DeFi proxy software program installable on Windows, Mac and Linux that enables a trader to stay in the dApp's native interface, but be connected to the Qredo network. Wallets interacting with the dApp are intercepted by the proxy and routed into the Qredo network. From there, custodian approval workflows, signature aggregation, transaction encryption, Validator verification and block inclusion happen behind the scenes. To the dApp trader, there is minimal to no difference in user experience.

DeFi adoption in firms that must comply with compliance and governance requirements, particular trade approvals and audit struggle with DeFi applications. The issues can be distilled down to a few challenges.

1. **The main application that is used to access DeFi applications and create transactions using the wallet's private key is a browser extension. This application is always connected to the internet. This is one of the worst locations to store a private key because a browser is designed to have APIs that are as open as possible. Cryptocurrency wallet thefts that occur because hackers were able to access a MetaMask wallet via a nefarious script installed without the user's knowledge when they visited a website controlled by a hacker are commonplace. While MetaMask is easily the best Ethereum wallet for user experience, it won't pass security reviews of financial institutions looking to access DeFi applications.**
2. **There is no centralized crypto custodian service that interoperates with MetaMask in a way that satisfies financial services firms need for dependability, reliability, security and ease of deployment. Qredo's DeFi proxy is meant to address these challenges and provide a rapid time to value solution.**

As an example, a trader placing capital into Aave (a popular DeFi lending service) using MetaMask browser extension in a desktop browser with the Qredo DeFi proxy also installed will be able to access the user interface as normal and access to all capabilities on Aave's web interface. Qredo's DeFi proxy is silent, requiring no interaction from the trader or systems administrators. It's programmed to intercept communication from MetaMask to Aave and back again in a way that exceeds security safeguards and enables Qredo's compliance and custodian workflows to interact seamlessly with the traders workflow. A generalized view of the requirements shared across a section of financial service firms that need to secure capital deployed into DeFi protocols and invoke compliance and governance flows related to trading activities are:

- **Wallet private keys that create signatures on transactions cannot be stored in a browser. Qredo's MPC network eliminates the need to store private keys at all so risk of MetaMask wallet compromise is eliminated.**
- **Custodial controls and approvals on the transactions prior to signature generation and enterprise-grade audit logging of custodian's transaction approvals. The firm's compliance flows for transaction approval are invoked by the trader's activity, buying and selling, lending or borrowing using DeFi protocols. The workflow that collects approval signatures from Qredo Clients, aggregates the signatures, secures the transaction and submits**

it to Qredo's blockchain is no different than if it had been invoked by a Qredo Client rather than MetaMask wallet. All transactions data, custodian approvals and relevant metadata is written into Qredo's blockchain for data durability and immutability.

DECENTRALIZED TRADING

DECENTRALIZED RFQ

Qredo's Layer 2 / Layer 3 design includes an automated, decentralized RFQ bot that is built into the Version 2.0 protocol. The RFQ bot enables a simple Uniswap-like Web3 interface to facilitate the exchange of Layer-1 assets (BTC / ETH) using Market Makers that have staked and bonded QRDO tokens with a Validator. Market Makers take part in the token rewards scheme and are incentivized to offer the best prices and market depth as covered in the previous section, and explicitly covered in the white paper entitled, "Qredo Tokenomics Rewards and Emissions" available on Qredo's website.

Qredo's RFQ system uses the Layer 3 network for Users to issue RFQs to and receive from Liquidity Providers actionable quotes that they can digitally sign and submit to the Layer-2 blockchain. To become a Liquidity Provider on the Qredo network, the Liquidity Provider must acquire and stake a minimum number of QRDO tokens in a Liquidity Provider staking wallet, and deposit a minimum USD value of digital assets into Liquidity Provider inventory wallets. Inventory wallets are used to trade with Users. The number of QRDO tokens needed to stake are determined by protocol using the economic activity indicators measured from the genesis block up to the current block as input.
The Request For Quote ("RFQ") trading method is an asymmetric trade execution model. In this method, a Trader User invokes, through the Web3 interface or Qredo Client API, the RFQ bot which queries a finite set of participant Liquidity Providers who quote a bid/offer ("a market") to the protocol using the Layer-3 network. The protocol will show the Trader User the best quote from all collected. The protocol enforces a rule where the User may only "hit the bid" (sell to the highest bidder Liquidity Provider) or "lift the offer" (buy from the cheapest seller Liquidity Provider). The User is prohibited from stepping inside the bid/ask spread and thereby reducing the execution fees. In a typical RFQ system Trader Users would not be able to trade with each other, and importantly, they can not make markets themselves to the entire network. Qredo protocol provides an exception to this in that Trader Users can trade privately with known, trusted counterparties bypassing the RFQ system, but is like a typical RFQ system in that Trader Users cannot make markets themselves to the entire network.

OTC DARK POOLS

Qredo's Version 1.0 protocol already enables trustless atomic swaps between counterparties on the Qredo network. In order to create this kind of P2P order, the transaction initiator must have registered the identity of this counterparty into a 'Trusted Network' list, which is a whitelist its Qredo Client maintains of single counterparties it is approved to either act as a maker or taker. In doing so, each counterparty in a Qredo Client's Trusted Network whitelist is made aware of that Qredo Client's wallet's shortcodes. Shortcodes are simple three word mnemonics that are created on the Qredo blockchain whenever a wallet is created. By adding a counterparty to a whitelist, that Qredo Client discloses its wallet's shortcode.

In Version 2.0 of the protocol, a group of Qredo Clients can come together to implement their own dark pool that utilizes an expansion of the shortcode system in use today. One Qredo Client can create a Dark Pool, which also receives its own shortcode mnemonic which is registered to the Qredo blockchain. This client can then, with Custodian approval, invite other Qredo Clients into the Dark Pool, effectively becoming a member of the Dark Pool's Trusted Network. The Dark Pool's members have their own Layer 3 communications channel, which enables direct order entry into the Dark Pool's Liquidity Hub. The hub is a repository of quotes submitted into the Dark Pool by its members. It's important to note what the Liquidity Hub is not.

A Dark Pool's Liquidity Hub is simply a dedicated topic in the decentralized communications channel; it is not a CLOB (Central Limit Order Book). It does not support limit orders, stop limits, etc.

- **Quotes can be updated and removed**
- **Quotes can have set time limits for expiration**
- **All taken quotes are guaranteed to be executed**
- **All maker quotes will contain an expiration and are equivalent to Fill or Kill orders: https://www.investopedia.com/terms/f/fok.asp**

MARGIN TRADING

Margin trading requires a Trading Strategy Order (TSO) that needs to be signed by the transaction initiator and their appointed Custodians. It is then sent to the Counterparty for completion, like an atomic swap order. The difference is the Trading Strategy Order's counterparty is a Validator Pod.
A Validator Pod is selected randomly using a verifiable random function derived from block height, and once called up for this particular order, the Validator Pod becomes responsible for shepherding the trading strategy's orders to completion or aborting it if it is infeasible to execute. The Pod members will receive additional income for the work they undertake with this order
.
NOTE: **the exact mechanism (profit, percentage of trade size, etc.) of how they are compensated is to be determined.**

The Validator Pod's chief responsibility is to monitor the position of the margin collateral during the window where the collateral is in play and the trade is outstanding. If the borrower's value of their security drops in relation to the loan amount, the borrower may exceed the maximum Loan to Value Ratio. This will trigger a 'margin call' and Pod will be required to close the position out via another order type, imaginatively called Margin Call which is pre-signed by the borrower and requires ⅔ of the Pod to approve. Any remaining funds not needed to pay off any liabilities of the borrower can be returned to the trader, minus any liquidation penalties incurred.

From the trader/borrower's perspective, though they may have had to deposit collateral into the Loan Pool, they have not remitted any of their assets out of Qredo's decentralized network to any exchange, saving on fees. Even better, they can access QRDO tokens staked at a Validator as collateral as well, even if it is locked. In effect, the accruing rebates traders received on transaction fees and custody fees can now be used as collateral.

The mechanics of this system enable a trader to pledge collateral to create a loan that is highly leveraged, typically 8x to 10x, because the counterparty risks are highly quantifiable. In the case of a Leveraged, Cross-Chain Secret Flash Loans (described below), the counterparty risks are very well known. The first one is the efficacy of the Qredo network itself. And the second is the efficacy of the Ethereum network or other reputable Layer 1.

The evaluation questions are:

1. **Can the Qredo network place the orders correctly?**
2. **Can the Ethereum network (or other Layer 1) confirm their transactions and deliver the acquired digital assets in an expected time frame?**

Qredo's Loan Pools enable Liquidity Providers to deposit assets to obtain a share of the fees the Loan Pool collects by issuing these loans to trader/borrower's on the network. This **enables a liquidity provider to obtain a passive income from an asset already in custody in the Qredo Network.** Custody Users are able to utilize their staked QRDO tokens, collateralize them in a longer term loan, and take the resulting ETH (as an example) and move that into an ETH Loan Pool for greater capital efficiency and yield on top of yield.

Uniquely, **the trader acquiring the loan doesn't receive the loan principal themselves**, they create and execute leveraged trading strategies using the Qredo Loan Pool's wallets which connect directly to the DeFi protocol's smart contracts, providing out-of-the-box obfuscation of the trader's trading strategy on the Layer-1. As multiple traders execute these strategies through the Loan Pools wallets, the signal to noise ratio becomes untenable for a MEV bot acting nefariously as more traders utilize the same Loan Pool wallets. It becomes impossible to assess a strategy from a cascade of what appears to be random orders.

Trader/Borrowers pay fees back to the Loan Pool once the trade is concluded, and these fees are distributed to the depositors in the Loan Pool in the form of additional deposits of Layer-1 assets to the Liquidity Provider's balance in the Loan Pool. Each depositor in the Loan Pool receives a redemption token enabling them to withdraw their deposit from the Loan Pool at any time. Redemption tokens can also be used as collateral to secure other loans.

Leveraged Cross-Chain Secret Flash Loans - Note that the 'Flash Loan' pertains to the atomic transactions being executed on the Qredo blockchain, not the underlying Layer-1 chains. These loans are secured with a margin balance for each asset they are going to take a leveraged loan on, typically at 8x-10x leverage depending on volatility. As an example, if the borrower executes an arbitrage trade on two different DEXs using YFI and USDT, the User would need both YFI and USDT margin balances in both a YFI Loan Pool and a USDT Loan Pool, or an amount of QRDO tokens equaling to the aggregate value of the entire trade. Qredo Flash Loans make sense for arbitrage trades across exchanges and even across blockchains where the commands issued to the Qredo blockchain to execute buy/sell orders will fall within the same block on Qredo blockchain to maximize execution parallelism.

These buy/sell orders, if they are on the same Layer-1 blockchain may not necessarily get confirmed in the same block, but the commands to issue the buy/sell orders will fall within the same block on the Qredo blockchain. Importantly, the main characteristic of a Qredo Leveraged Cross-Chain Secret Flash Loan is that the commands to invoke buy/sell orders that **both open the loan balance and close it must be in the same block in the Qredo blockchain**. This enables a higher level of leverage to be obtained by the borrower placing the trade, as the counterparty risk is immediately placed on to the Qredo protocol's order execution and the Layer-1 blockchain's resilience until the digital assets are delivered back to the Qredo network.

IMPORTANT: The trade to buy/sell assets is funded directly by the Loan Pool's wallet in the Loan Pool from the Trader's deposit of collateral. In leveraged loan scenarios which include trading and flash loans, the Trader never receives the asset being loaned. The Qredo network makes the trade on their behalf. This has the added effect of disguising the Trader's identity from surveillance as all leveraged loans use the wallets within the Loan Pool that interact with the Layer 1 blockchain client.

The big idea here is that for the first time any trader on the Qredo network can create atomic swap transactions with any DEX that Qredo can access and a) arbitrage trade across multiple DEXs and b) completely offload the counterparty delivery and settlement risk to Qredo Loan Pools, for a fee.

In other words, a trader can create atomic swaps between DEX's on the same Layer-1 chains (ETH) or even between different Layer-1s (ETH to BSC, ETH to BTC, etc.) without being detected by the Dark Forest and have immediate settlement. Multi-leg strategies are also easily executed with this capability.

Leveraged Trading Loans - These loans are used for longer term, speculative bets on the rise or fall of a particular asset. As above, the Trader must deposit the collateral in the same asset being borrowed/traded into the Loan Pool or use their stake QRDO tokens. As above, the trade to buy/sell assets is executed by the Loan Pool's wallet in the Loan Pool. In leveraged loan scenarios which include trading and flash loans, the Trader never receives the asset being loaned. Instead, the Qredo network makes the trade on their behalf. This has the added effect of disguising the Trader's identity from surveillance as all leveraged loans use the wallets within the Loan Pool as the funding source of all trades on any Layer 1 CEX or Layer 2 DEX the Qredo Wallet Pools have access to. As more traders execute orders out of the same wallets, the signal to noise ratio decreases, making interpreting one trader's strategy out of potentially hundreds of transactions within the same block unrealistic.

Over-Collateralized Loans - These loans are standard across DeFi and are made popular by services like AAVE and Compound. There is a significant difference to how these loans originate via the Qredo Loan Pools. The main difference between this loan type and the two above is that the loan balance is remitted directly to the trader/borrower's Qredo Layer 2 wallet, so the Trader is responsible for deploying their loan capital, returning the capital and closing the loan. This is where the similarities with AAVE and Compound end. To borrow a digital asset, the Trader must add liquidity to the other side of the Loan Pool. As an example, if there is a collateral rate of 80% and a Trader wants to borrow ETH and has BTC for collateral, the Trader would deposit $1000 of ETH into the ETH/BTC Loan Pool ETH wallet and would receive $800 of BTC into their Qredo BTC wallet. The Trader can use this BTC as they see fit, and there is no restriction on this BTC exiting the platform (to send to a centralized exchange, for example).

MINTING QTOKENS

Qredo's Version 2.0 protocol will include an additional feature to 'mint' qTokens which are redeemable by any 3rd party who presents the token to the network. This capability works for any Layer 1 asset supported by the Qredo network. Wrapped tokens have become a critical part of the Bitcoin and Ethereum landscape, enabling Bitcoin speculation on Ethereum based DEXs. Currently, the market cap for WBTC has been proliferating since its launch to the point of just above $2 billion[17] in value, with an average daily trading volume of $90 million.

We will use Bitcoin to describe the capability. A user who has a balance of BTC in their Qredo wallet in reality has the synthetic asset qBTC, containing 'links' down the underlying Layer 1 that cryptographically demonstrates solvency of the Qredo network and proof of coin.
Qredo will enable any wallet holder to designate an asset in their wallet (i.e. BTC), create qBTC for sending to an external address, and send qBTC to that external wallet address, for a small transaction fee of 0.5 basis points. This external wallet

[17] https://coinmarketcap.com/currencies/wrapped-bitcoin/

address can exist on any Layer 1 blockchain that the Qredo network supports. This process moves the BTC that was under the user's control to a special custody wallet under control of the protocol itself. This is no different to the processes observed to mint WBTC or other entities that act as centralized custodian's in charge of warehousing BTC, except for three very important points.

- **Decentralized -** Qredo is a decentralized protocol, and built into the protocol are safeguards that eliminate the prospect of rehypothecating assets. The amount of minted qTokens (of any supported Layer 1) is always auditable by using the Qredo Client blockchain explorer.
- **Auditable -** The amount of Qredo qBTC tokens that have been minted and are floating in circulation across all Layer 1 blockchains in aggregate value will always equal the amount of minted qBTC tokens recorded on Qredo's blockchain, so the system is probably solvent.
- **Universal -** Qredo's capability will not just support one blockchain. This capability will exist for every Layer 1 that Qredo supports, opening up a broad world of economic opportunities across chains. As an example, a user could mint qBTC for Algorand, Polkadot, Binance Smart Chain as well as Ethereum.

Anyone is able to redeem a qToken into a real asset if they have a wallet on the Qredo network for that particular asset type they wish to redeem.

TRADER CHAT

The combination of Qredo's Layer 2 / Layer 3 design creates a unique opportunity for Version 2.0 protocol to be invoked by interfaces other than a static web page. Qredo's product roadmap includes the release of a Layer 3 module called Trader Chat, which is able to invoke all actions within a user's Qredo wallet from within a chat interface.

The key benefit of this module is its ability to rapidly speed up the transaction flow between counterparties negotiating prices on a Dark Pool or P2P trade. The Trader Chat module also addresses the key need for financial service firms to aggregate their pre-trade negotiations under one mechanism that can satisfy the need for privacy, non-preduation, message integration and strong authentication. Qredo's choice of the Matrix protocol for Layer 3 end-to-end encrypted communications makes this a relatively straightforward capability to produce. If you are interested in becoming an early adopter or learning more about Trader Chat, please email sales@qredo.com

COMPLIANCE & GOVERNANCE

TRAVEL RULE

The FATF Recommendation #16 (Travel Rule) creates many technical challenges for VASPs. First, how to comply with the requirement to exchange information while still protecting user privacy. When a VASP wishes to send transaction originator and beneficiary information to another VASP in support of Travel Rule requirements, they must establish secure communication with the other VASP. So in both cases end to end encryption is required. Secondly, for full compliance, if the inbound transaction is from a regulated VASP, the receiving VASP should not make funds available to the beneficiary until the Travel Rule transaction identity information is received and recorded.

Many VASPs—primarily exchanges who have large daily transaction volumes—are looking to retrofit Travel Rule compliance onto existing cryptocurrency transaction flows. The idea is to support batch transaction processing at the end of a day of trading and transactions. The challenge is how batch processing can be done without impacting the Straight Through Processing (STP) of existing VASP data processing and transaction processing pipelines.

For example, some VASPs have optimized blockchain transactions to group 50-200 payments in a single blockchain transaction, which dramatically reduces transaction costs. According to FinCEN, batch processing is acceptable, but funds received cannot be delivered to the recipient until the corresponding originator information has been provided and scanned for sanctions and risk compliance. The onus for checking transaction identity data for sanctioned or suspicious persons or entities falls on both sending and receiving VASPs. This requirement can delay the availability of outbound/inbound cryptocurrency payments to many customers for many hours if manual processes are applied to Travel Rule compliance.
Additionally, originating VASPs should always ensure they receive a signed receipt of transaction identity information from a Beneficiary VASP before transactions are placed onto a layer-1 blockchain. This requirement can complicate the processing systems at sending VASPs because multiple transfers of value are typically batched up into a single transaction in order to reduce blockchain processing fees. That workflow would have to be reworked to queue only transfers to happen once the Travel Rule processing between sending and receiving VASPs has been confirmed, which could increase transaction costs for VASPs dramatically.

This challenge can only be solved by employing a decentralized platform that incorporates both real-time decentralized communications, a Layer 3, with asset transfers over a Layer 2 network. The platform must bind the asset transfer with the Travel Rule data exchanged between VASPs cryptographically and must be capable of near-real time transaction finality as well as having end-to-end encryption built in. Anything less will force a delay in customers accessing their funds and risk customer data leaks.

For regulated institutions who must adhere to in-country regulations, register as a VASP and begin sending and receiving Travel Rule information on transactions, Qredo is an optimum choice. Qredo will create and release scripts within the Version 2.0 protocol's Qredo Integration Libraries that quickly enable any VASP to get into compliance with in-country regulations without disrupting their transaction flow, as well as integrating the outgoing and incoming messages, transactions records and custodian approvals to take advantage of external services and speak to internal compliance and accounting systems.

ARCHIVING

Qredo's Version 2.0 protocol takes full advantage of its ability to archive data in both the Layer 2 and Layer 3 infrastructure. Qredo's 1.0 protocol is now close to a year old, and it has proven the viability of recording ownership information, transaction flows between participants, and self-appointed custodian approvals over wallets. As described earlier in this document, Version 2.0 protocol will enable 'secret transactions', i.e., the ability to encrypt, as standard, transactions before they leave the Qredo Client and travel through the mempool.

Qredo will be the first Layer 2 that can comply with what, up to now, has been looked at as mutually exclusive requirements.

- **Transaction Security -** The ability to keep secret user's transactions from other traders until after they are written into the Layer 2 blockchain. Once they are written into the blockchain, the identities of the Traders, Custodians and they're counterparties remain pseudo anonymous.

- **Data Immutability and Durability -** That this transaction data be forever available, and that one can make reasonable assurances that if the network is not vulnerable to a minority of malicious nodes, then the data can be trusted.

Ironically, both requirements above are required by different regulators, law enforcement, compliance agencies and internal compliance teams. An important point is that the Qredo network is pseudo anonymous. Qredo does not proclaim that transactions remain secret (i.e. Monero), only that they are not vulnerable to front running or MEV like activities from malicious validators.

Qredo's choice of the Matrix protocol for its interlinked Layer 3 over Layer 2 resulted from the same requirements as above. How to enable end-to-end encrypted messaging that was accessible by human and machine, but yet provide a mechanism for export on conversations in cleartext should it be a user requirement.

The functionality that Matrix as a Layer-3 provides includes (but not limited to):

- **Creation and management of fully distributed chat rooms with no single points of control or failure**

- **Eventually-consistent cryptographically secure synchronisation of room state across a global open network of federated servers and services**

- **Sending and receiving extensible messages in a room with (optional) end-to-end encryption from client to client**

All data exchanged over Matrix is expressed as an "event". Typically each client action (e.g. sending a message) correlates with exactly one event. Each event has a type which is used to differentiate different kinds of data. type values MUST be uniquely globally namespaced following Java's package naming conventions, e.g. com.example.myapp.event. The special top-level namespace m. is reserved for events defined in the Matrix specification - for instance m.room.message is the event type for instant messages. Events are usually sent in the context of a "Room".
Therefore, data is replicated via 'rooms'. A room is a conceptual place where users can send and receive events. Events are sent to a room, and all participants in that room with sufficient access will receive the event. Federation maintains shared data structures per-room between multiple Qredo Clients, assuming that Qredo Client has been 'invited' to that room or been granted access by another mechanism.
End-to-end encryption is applied to any data created by a Qredo Client and sent to another Qredo Client. The encryption protocol uses the Olm and Megolm cryptographic ratchets, the same cryptographic system deployed in Signal. Messages can be encrypted for multiple clients all subscribed to the same room,

or even just a subset. Most importantly, this encrypted data cannot be decrypted by the Qredo Client admin. The cryptographic keys generated by each Qredo Client are encrypted before being backed up to the homeserver, and only the operator of the application created by the Qredo Integration Library knows the phrase to generate the decryption keys, decrypting the keys enabling end to end encryption. These operations take place on the Qredo Client only.

What this enables, simply stated, is that the Qredo Client itself can become an encrypted data store of the messages received until they can be decrypted by an authorized application and moved into a long term archiving. Qredo Integration Libraries contain sample scripts which a developer can use to create an archiving solution on premise that contains information such as pre-trade negotiation chats, trade initiations, custodial approvals of transactions and other pertinent information.