**Decentralizing the Finance Industry:**
**A Layer 2, Corporate-Grade, Settlement Network**

www.qredo.com

**Abstract.** By ignoring its own principles and centralizing custodian operations, the cryptocurrency industry undermines its own growth. Institutional investors cannot tolerate the risks inherent in non-compliant centralized custody. Moreover, the foundations of crypto-decentralization, such as anonymity and trustlessness, violate the governance requirements of global fiduciary concerns. Qredo's Layer 2 settlement network offers governance and compliance guarantees while providing a decentralized architecture that retains the robustness of trustless, consensus architectures, and a secure and transparent data ledger. The design eliminates common issues with blockchain technology such as unacceptable transaction verification delays, currency limitations, complex multi-party signatory functionality, amongst others. We are now onboarding customers and institutional clients ready to invest in the Qredo network and code against our technology stack. Our backend blockchain ledger, secured by an open-source, MPC, industrial-scale signing application, supports numerous crypto-trading web applications and around 35 ERC20 tokens to date including BTC, ETH, and Algorand. Qredo is taking the next step and evolving into a decentralized financial settlement system, owned and operated by users. Investors and validators will benefit from a unique fees rebate model, fueled by the QRDO ECR20 token.

## Summary

The future of global finance lies in the power of decentralized markets. The Qredo doctrine is decentralization and everything we do is guided by this principle. We are now onboarding corporate clients[i] keen to participate in the evolution of crypto capital markets. As the international financial community renounces centralized control over crypto-trading, Qredo's inbuilt compliance and governance will pacify once-jittery investors and widen crypto financial use cases to a hitherto unknown scope.

Qredo's core tenets include open sourcing the codebase for full transparency and unlimited network participation. Currently, our six-node, decentralized-design, blockchain application is running in hardware-secured Equinix data centers alongside an MPC cluster that secures user transactions and resides in tamper-proof, hardware security modules (HSM).

Validating nodes and investors will benefit from a unique Delegated Proof of Stake protocol with rebates on transaction fees. The community will eventually govern itself through a Decentralized Autonomous Organization (DAO).

## Qredo vision

Suggest using a top-level section like this for the "positive and awe-inspiring" material, if you think this doc needs that, and leave the factual sections (Qredochain, MPC, etc) as they are.

## ERC20 token sale

To realize our long-term vision, we are minting 1 billion QRDO tokens for distribution and 1 billion on a 10-year inflationary schedule for the participant rebate scheme.

Participants are buying into a customer-centric, token protocol that allows early adopter validators, along with institutional and user stakeholders, to benefit from a unique fees-rebate scheme.

Of the initial distribution of QRDO tokens, we are releasing 6% for private sales taking place over the run up to the public sale. We are then releasing 4% of the total supply for public sale through our partner platform Coinlist.[ii]

Tokens will be available to the public on decentralized exchanges such as UniSwap[iii] and any centralized exchange listing the QRDO token once the private sales are complete.

Token holders will receive retrospective rebates on QRDO fees paid on the Qredo

Layer 2 network once the staking and rebate protocols are live.

Qredo is a long-term player in the crypto financial markets. We believe it is only a matter of time before crypto-finance breaks though into universal global acceptance. Which of the countless concerns, vying for operational space by offering unique approaches to common crypto problems, will drive the evolution forward, and reap the rewards, remains to be seen.

**Open source decentralization**

Crypto-finance suffers from a number of problems unique to the industry that cause a lack of liquidity and impede common financial market operations. Transaction confirmation times are extremely slow[iv] causing pre-funding, lending, and borrowing to require 100% lock-up capital; transaction fees are prohibitively high[v]; and the industry is well-known to be vulnerable to hacking and blatant theft.[vi] Larger capital market players, likely keen to participate, shy away due to the lack of corporate-grade crypto-infrastructure with built in audit trails, governance, and compliance to support cross-platform liquidity. Qredo solves all these problems.

Qredochain

Currently, Qredo Limited manages six hardware-secured, validator nodes that are the foundation of the Qredochain network. We are in the process of transitioning the network into a fully decentralized state. The Qredochain Layer 2, decentralized network will open up the crypto markets to regulated and nervous financial players. Running on Byzantium fault-tolerant Tendermint nodes that can handle around a hundred transactions per second[vii], the Qredochain supports multi-coin custody and rapid transactions at reduced fees. Flexible account ownership hierarchies are coded into Layer 2 wallet definitions, and all activity is written onto an immutable blockchain ledger. BLS signatures[viii] secure Layer 2 activity and all transactions on any underlying Layer 1 blockchain is managed by an MPC cluster.

The Qredochain Golang API will eventually be open sourced. The code provides developer access to the transaction types and transfer functions that the chain implements. The decentralized design takes care of custody, corporate authorization, and hierarchy controls over multi-asset funds. Current functional use cases include cross-chain native swaps, Layer 2 atomic swaps, sweeps, and instant settlements, and the design ensures flexibility for implementing new financial use cases. The code enforces authorization rules over all transactions with built-in programmable governance. Users pool their underlying crypto-holdings to enjoy common financial use cases that require cheap and immediate verification. Our crystallization technology ensures the system enforces a one-to-one value mapping over both layers. This safeguards the Qredo network against insolvency. In development for more prudent users is a one-to-one account wallet implementation which tracks Layer 1 holding addresses.

The Watcher

A Watcher module listens for system-relevant activity on Layer 1 blockchains and reports back to the Qredochain nodes. The Watcher is currently non-decentralized but we are in the first stage of designing a decentralized Watcher network. The first stage implements three security controls over all Watcher activity. Firstly, by forcing the MPC signing authority to oversee and authorize all Watcher activity; secondly, for the Qredochain to confirm the activity against the underlying Layer 1 blockchain ledgers; and lastly by reverifying Watcher-notified transactions against public keys. The second stage of decentralizing the Watcher is still in design. One Watcher module currently runs on a managed server and serves all six hardware-secured Qredochain nodes. We are also currently running our own Bitcoin and Ethereum nodes that supply the Watcher with info.

Qredo applications

Qredo manages a full set of frontend applications that run on top of our managed nodes. Qredo customers may operate their multi-crypto fund management dashboards using the live web applicationix and authorize sign-in activity with the mobile signing app. External parties may build their own applications on our decentralized Layer 2 with the Partner & Core Client APIsx. We are

researching developer libraries in Java, Python, Node JS, and .NET that support event driven workflows and integrate directly with our APIs. We remain committed to research into protection against quantum computing attacks for when the time comes.

Partner integrations

Qredo partners are now designing and building unique crypto-financial applications for their clients on the Qredo network with the Partner & Core Client APIs. The APIs give access to account management and custodial functionality to address a range of use cases.

- Hardware wallet specialists Ledger[xi] are developing a hot wallet for use by financial institutions.
- Algorithmic market maker Wintermute[xii] is building a crypto liquidity hub for its clients on the Qredo network.
- Prime services specialist Deribit[xiii] is developing trading software using the Qredo network that offers its client base crypto-trading strategies with no pre-funding requirements or counterparty risk.
- Portfolio management company, with hands in traditional and crypto markets, HedgeGuard[xiv] is building a Layer 2, end-to-end fund management solution that includes instant reconciliation, treasury management, and reporting strategies which address crypto-trading security and governance.
- Crypto prime brokerage Genesis[xv] is working with us to produce a compliant decentralized network, based on the Matrix protocol, that covers the travel rule and offers auditable KYC. The software will plug into existing compliance systems.

Future developments

Solid market desire for decentralized custody with corporate controls has inspired us to design the code to support a number of state-of-the-art crypto-trading applications:

- A peer-to-peer encrypted OTC trader chat application for pre-trade negotiation, RFQ, and clearing built with Matrix[xvi] which enables transaction private and message non-repudiation.
- Treasury services such as platform plug-ins for native accounting software.
- Cross-chain DeFi smart contract protocols.
- Full range of prime brokerage services.
- Multi-dealer P2P dark pool trading, de-risked with audit history.
- Relayer functionality to pay third-parties for broker-type use cases such as quoting.

The Qredochain code will be available open source so that the community may improve on the design and build support in for limitless new features.

**Securing the network**

BLS signatures enforce Qredo Layer 2 transaction security, as mentioned, and an MPC cluster environment provides wallet functionality to the whole of the Qredo network by securing all transactions on underlying blockchains. The Qredo technology stack uses the Qredo-managed, open source Apache Milagro core security infrastructure libraries for decentralized networks and distributed systems[xvii]. These robust encryption libraries offer an alternative to centralized trust providers and solve common implementation issues, such as scaling for example.

Qredo's multi-party computation (MPC) signing application, based on the Threshold Signature Scheme (TSS)[xviii,xix,xx], provides keys and ECDSA signatures to an authorizing Qredochain node for Layer 1 transactions[xxi]. MPC enables multi-party signature functionality for Layer 2 account wallets. Removing single-point-of-failure concerns around users having to protect their own wallets, MPC safeguards the generation and storage of private key shares across the Qredo ecosystem. It provides trustless secrecy, transaction correctness, and customer privacy.

Like Bitcoin or Ethereum wallets, Qredo's MPC signing functionality is external to the underlying blockchain technology. The MPC can be seen as an industrial-scale, trustless cryptocurrency user wallet. An MPC cluster, currently managed by Qredo, supports our live applications.

The MPC cluster generates private key shares, signs transactions, and guarantees that an attack will only succeed if a bad actor gets access to more than the signing threshold of secret shares. The signing threshold is around two

thirds of the total shares that make up a private key. Private key share generation and storage is managed by nodes. Proactive security controls rotate keys around nodes at regular intervals.

The MPC code is written in C for speed, efficiency, and security. A Python wrapper enables application development against the C code; for example, by supporting communication over a point-to-point protocol. MPC cluster nodes communicate point-to-point over HTTPS, or listen to a broadcast channel (currently in development). MPC code will be open-sourced this year.

Qredo has secured its MPC clusters in tamper-proof hardware modules residing in six Equinix hardware boxes across the globe. A Zymbit HSM[xxii] stores a key that encrypts the hardware boxes. If pressure triggers the sensors, the system destroys the key, the device powers down, and it cannot restart.

The MPC was written with decentralization in mind and we continue to research ways to fully decentralize the MPC clusters while maintaining the security of private key shares. Decentralizing the MPC may provide the ultimate security and controls required by institutional investors.

The next step of the MPC evolution, due for release this year, is a fully distributed MPC. Qredo will provide the MPC system microservices in Docker containers and each validator will run one MPC node. An MPC node is responsible for producing private key shares across the network on request. Like today, each node will generate keys, sign transactions, and rotate the keys. The main difference is that the MPC protocol will involve many nodes, rather than between two fixed nodes as it is today.

Today, nodes communicate over PPP and use Redis as a broadcast channel which is available to all other nodes. The private broadcast communication system, in development, will use Matrix secure and decentralized encryption to share information required to run the GG20 protocol.

In Q3 of 2021, we will also release MPC code that implements identifiable aborts by notifying the system of any malicious activity across the MPC nodes. Bad behavior will result in node shutdown; given the stringent requirements for validators, we do not expect much of this.

We continue to improve the current MPC development and code is due for release as open source in June 2021.

**User-centric tokenomic model**

The motivations for validators on a decentralized network are distinct to those of other network users. Therefore, lucrative Layer 2 models must encourage a wider range of user activity and behavior. Qredo's Delegated Proof of Stake offers QRDO token reward schemes that benefit four distinct user types: liquidity providers, traders, custody users, and validators.

Liquidity providers issuing quotes to users must stake a minimum USD value of QRDO to join the network. They must also maintain an inventory wallet with a sufficient QRDO balance for fulfilling network RFQs that swap Layer 1 assets to QRDO for reward distribution schemes. Traders swap assets with liquidity providers and other Qredo network users. Before trading is allowed, a trader has to first be a custody user who holds QRDO tokens on the network. Validators propose, vote on, and validate transactions on the Qredochain. To join the network, a validator must deposit a specific USD value of QRDO into a special staking wallet.

The system matches Layer 1 assets to a notional synthetic asset on Layer 2, i.e. 1BTC maps to 1qBTC in the user wallet.

To issue a request for quote (RFQ), traders query network liquidity providers over Qredo's encrypted messaging system. The network enforces selling to the highest bidder, and buying from the lowest. This stops users from being able to reduce transaction fees.

There are two main incentive schemes: a fee-based compensation scheme, and a per-epoch token distribution scheme with a semi-variable inflation rate.

Fee-based rewards

The Qredo network charges a percentage of Layer 1 assets as a fee for custody and transactions. These fees are distributed to validator and treasury management wallets by the protocol. Fees, and thus rewards, are calculated against three scenarios: known

counterparty transactions charged at half a basis point, user and liquidity provider transactions where only the user pays a fee, and custody.

**Known counterparty transaction fees**

A user swaps 50 qETH for 1 qBTC:

- 1 qBTC x 0.000025 = 0.000025 qBTC paid by the qBTC seller
- 50 qETH x 0.000025 = 0.000025 qETH paid by the qETH seller

**User and liquidity provider transaction fees**

No fee for the liquidity provider. User pays 0.5 basis points.

**Custody fees**

Custody users pay 0.75 basis points per month on an AUM model.

When validator and treasury management wallets contain sufficient Layer 1 assets, the protocol sends an RFQ to the liquidity providers to swap those assets for QRDO tokens to distribute back to the validators and treasury management as rewards. There is no lock up period on these.

The following table sets out the distribution of rewards coming from fees:

| | Validator | Liquidity provider | Treasury management |
|---|---|---|---|
| **Known counterparty transaction** | 80% QRDO | 0% | 20% QRDO |
| **User & liquidity provider transaction** | 60% QRDO | 20% Layer 1 assets | 20% QRDO |
| **Custodian fee** | 80% QRDO | 0% | 20% QRDO |

Custody users can participate in the fee rewards scheme by staking QRDO tokens in a validator staking wallet with a minimum lockup period.

Validators offering staking services may advertise via API or block explorer. Liquidity providers can add uplift fees, commission, or charge for additional services, such as prime brokerage, via the relayer field in the RFQ response. Connections to DEXs, such as Uniswap, will enhance the system's liquidity pools.

In time, the DAO will govern fee-based compensation distribution schedules. Until then, Qredo may optimize token distribution towards demand.

Per-epoch token inflation rewards

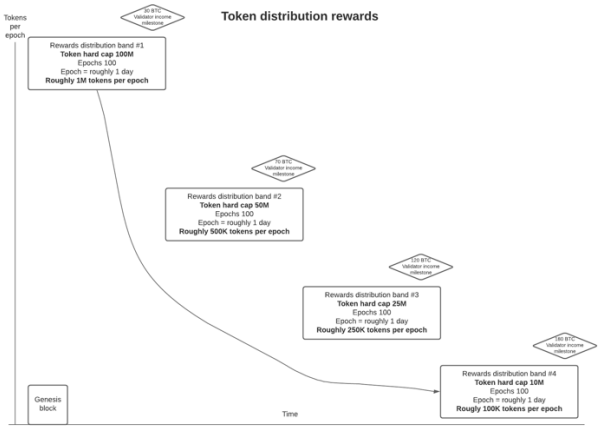
The Qredo protocol seeks to distribute a fixed number of QRDO, per epoch, over a limited number of reward distribution bands, to eligible users, based on the following formulae:

$$Ep_n = Ep_{n-1} - (Ep_{n-1} * Df)$$

$$T_n = EP_n * Df$$

where $Ep_n$ is the emission pool in block $n$, $Df$ is the distribution factor, and $T_n$ is the number of tokens distributed in block $n$.

The model defines reward distribution band periods against two milestones: validator income and token hard-cap levels per band. Validator income metrics will map to BTC/QRDO.




Each reward distribution band covers 100 epochs. Each epoch lasts, roughly, one day. In the first distribution band, 1000 QRDO tokens are rewarded per epoch. The token hard-cap for this band is therefore 1M tokens. The scheme proceeds to the next distribution band on hitting either of the two milestones.

If the protocol hits the validator income milestone first, the remaining tokens in the distribution band will be immediately distributed to validator and treasury management wallets. The validator share is based on staking level during the rewards distribution band period. If the network hits the token hard-cap milestone first, there are no remaining QRDO for that period.

Token reward share percentages per distribution band are dependent on transaction and user type. As an example, traders: 20%,

custody users: 10%, liquidity providers: 20%, validators: 50%. The split is adjustable and open to optimization; i.e. if there is insufficient liquidity, more rewards can go to market makers; if there are insufficient users, more rewards can go to traders. The DAO may adjust the split ratio between user types on a biweekly/bimonthly voting basis.

In the following examples, traders receive 20% of the total rewards for that epoch. The first example covers what happens when trader activity doesn't reach the full rebate amount.

- Trader rewards per epoch: 1000 QRDO
- Trader A spent 400 QRDO in fees.
- Trader B spent 300 QRDO in fees.
- Both receive a full refund.
- 300 QRDO in change goes to custody users.

In the case that traders spend more fees than the rebate figure for that epoch, the refunds are proportional to the fees spent over the epoch. The following example demonstrates this:

- Trader rewards per epoch: 1000 QRDO
- Trader A spent 800 QRDO in fees.
- Trader B spent 600 QRDO in fees.
- Trader A receives 57.1% of the rewards = 571 QRDO.
- Trader B receives 42.9% of the rewards = 429 QRDO.

**Custody user example**

Custody users receive rewards based on the value of the assets they hold on the Qredo network. In the following example, custody users receive 10% of the total rewards per epoch. User A has $10K in their Qredo wallet and user B has $30K.

- Custody user rewards per epoch: 500 QRDO.
- User A receives 25%, 125 QRDO.
- User B receives 75%, 225 QRDO.

In the token surplus situation mentioned in a previous section where 300 non-rebated QRDO tokens filtered through to custody users.

- User A receives 25%, 75 QRDO.
- User B receives 75%, 125 QRDO.

**Liquidity provider example**

Liquidity providers don't pay fees, so their rebate is based on the % of total transactions volume generated by all liquidity providers. For the sake of the example, 1 QRDO token = 1 USD, and there are 1000 QRDO for distribution.

Liquidity provider A has facilitated the following trading volume:

- 1000 USD in ETH for 1000 USD in BTC.
- 2000 USD in QRD for 2000 USD in BTC.
- Total volume 6000 USD.

Liquidity provider B did:

- 1000 USD in ETH for 1000 USD in BTC.
- Total volume 2000 USD.

Rewards:

- Liquidity provider A: 750 QRDO (75%).
- Liquidity provider B: 250 QRDO (25%).

**Validator example**

Validators' rewards percentages are calculated against the proportion of staked QRDO (owned and delegated). For example:

- Validator A stakes 200,000 QRDO with 50,000 QRDO delegated.
- Validator B stakes 500,000 QRDO with 10,000 QRDO delegated.

Rewards:

Validators receive 50% of total rewards per block (2500 QRDO).

- Validator A receives 825 QRDO (33%)
- Validator B receives 1675 QRDO (67%)

We believe the incentivization schemes just presented will not only benefit a range of network user types but will also encourage activity on the network and thus generate considerable liquidity.

## Security, compliance, and governance

We expect Qredo's unique decentralized approach to Layer 2 operations, and its commitment to fulfilling compliance and governance requirements, to settle market nerves around crypto trading. Customer account security requirements are built into Layer 2 transactions at the code level. Robust MPC security protocols ease account hierarchy management and compliance functions for regulatory concerns. Qredo application dashboards provide transparency for account administration, audit trails, and reporting. Qredo is also developing a number of governance features that further address regulatory challenges faced by market participants.

Travel rule reporting

Qredo will provide ecosystem features that allow customers to comply with Travel Rule (TR)[xxiii] requirements. The Matrix industrial and encrypted messaging protocol[xxiv, xxv] will act as a governance layer over the Qredo network to comply with TR data transfer directives. Matrix is a real-time, fully encrypted, stress tested and audited communication standard for processing immutable transaction and audit log data. The Matrix protocol is currently in use by European governments for secure communication.[xxvi] It is a decentralized conversation store, rather than a messaging protocol, and supports secure storage of transaction metadata, including originator and beneficiary information. These features enable compliance with FATF standards for VASPs,[xxvii] and also fulfill Travel Rule obligations for businesses.[xxviii] Qredo is currently piloting the scheme with one of the largest VASPs in the industry.

Self-defined insurance coverage

Bolstered by the recent developments in security services for emerging technology and smart contracts,[xxix,xxx] Qredo will offer bespoke insurance coverage to clients, tailored to match individual risk tolerances. Premiums will be available through the web application or via partner integration. It will be possible to insure all assets in custody with the proviso that assets in transfer cannot be insured.

We are also investigating extended cover options, including cover for crime and specie risks, with the aim of offering our clients hybrid cyber-crime cover in the future.

KYC/KYT

Software products such as Universal Digital Identity[xxxi] are simplifying regulation across crypto finance. Qredo will be launching tools that ease corporate onboarding into the crypto space and provide a low friction journey to partnering with leading exchanges and services. The Know-your-customer/know-your-transaction technology will feature safe storage for corporate digital documentation collections. Such regulatory information will then be available to share with partners.

Qredo is also investigating next generation coin screening tools to help exclude illicit assets from pools or network interaction.[xxxii]

Audits

Qredo has committed to undertaking annual or half-annual security audits with several leading crypto security auditors.

- MarshMcLennan[xxxiii] risk management company is scheduled to perform a broad company audit, with an operational focus, around June 2021.
- TrailOfBits[30xxxiv] will also perform a deep security audit on the Qredochain code sometime in the Autumn of 2021.

**Conclusion**

Tbc.

**Roadmap**

H1 2021:

- Qredo operated, v1.0, main net live.
- MPC code open source.
- Internal security controls preparation for Marsh audit.
- Releasing insurance for clients.
- Corporate account hierarchy & authorization.
- Core client and partner integration API's operational.
- Client onboarding.
- Cross-chain native swaps: BTC<>ETH.
- 15 ERC-20 tokens.
- Stable coins: USDT & USDC.

H2 2021:

- QRDO token public and private sale.
- Qredochain code open sourced.
- Qredo network v2.0 test net live.
- Strategic validators selected.
- QRDO staking protocol operational.
- Customer-centric QRDO fees rebate protocol launches.
- Quantstamp security audit.
- TrailofBits security audit.
- Layer-1 token support: BSC, Polkadot, Cardano & more.
- Fiat on/off ramp integration.
- DeFi Dashboard

H1 2022:

- v2.0 main net.
- Complete transition to DAO governance.

H1/H2 2022:

- DeFi aggregators integration.
- Top 100 tokens & assets.
- Native AMM.
- Compliance app.
- Relayers.
- Python/Node/JS integration library.
- Synthetic derivative – qASSET.
- Self & corporate insurance app.

**Qredo Team**

- Anthony Foy, CEO/Co-founder
- Brian Spector, CPTO/Co-founder
- Josh Goodbody, COO
- Duncan Payne-Shelly, CFO
- Stanislav Mihaylov, VP Engineering
- Clarence Sittampalam, Design Executive Officer
- Ben Whitby, Head of Compliance and Regulatory Affairs
- Chris Morris, Lead Blockchain Architect
- Alexander McKay, Blockchain Architect
- Kealan McCusker, Lead Cryptographer

**Advisors**

- Miles Perry

**Investors**

Strategic investors:

TBC

Financial investors:

TBC

[i] Current developer partners include hardware wallet specialists, Ledger; algorithmic market maker, Wintermute; crypto futures and options trading company, Deribit; crypto-fiat portfolio management and middle-office outsourcing company for hedge funds, HedgeGuard; and crypto currency prime brokerage service, Genesis.

[ii] https://coinlist.co

[iii] https://uniswap.org

[iv] https://www.blockchain.com/charts/median-confirmation-time

[v] https://ycharts.com/indicators/bitcoin_average_transaction_fee

[vi] https://www.securitymagazine.com/articles/94627-19b-in-crypto-currency-stolen-by-hackers-last-year

[vii] https://atrium.lib.uoguelph.ca/xmlui/bitstream/handle/10214/9769/Buchman_Ethan_201606_MAsc.pdf

[viii] https://en.wikipedia.org/wiki/BLS_digital_signature

[ix] https://qredo.network

[x] https://support.qredo.com/docs/api-ref/#qredo-partner-amp-core-client-api

[xi] https://www.ledger.com/

[xii] https://www.wintermute.com/

[xiii] https://www.deribit.com/

[xiv] https://www.hedgeguard.com/

[xv] https://genesistrading.com/

[xvi] https://matrix.org

[xvii] http://milagro.apache.org/docs/milagro-intro/

[xviii] https://eprint.iacr.org/2019/114.pdf

[xix] https://en.wikipedia.org/wiki/Threshold_cryptosystem

[xx] https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

[xxi] https://www.qredo.com/blog/mpc-over-ecdsa-signatures

[xxii] https://www.zymbit.com/

[xxiii] https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf

[xxiv] https://en.wikipedia.org/wiki/Matrix_(protocol)

[xxvi] https://portswigger.net/daily-swig/enter-the-matrix-secure-communications-network-hits-30-million-user-milestone

[xxvii] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

[xxviii] https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf

[xxix] https://www.lloyds.com/news-and-insights/product-innovation-facility/

[xxx] https://app.nayms.io/

[xxxi] https://synaps.io/

[xxxii] https://www.coinfirm.com/solutions/defi-liquidity-pools/

[xxxiii] https://www.marsh.com/us/home.html

[xxxiv] https://www.trailofbits.com/