Qredo

Brian Spector[1]

[1]Affiliation not available

June 30, 2018

Abstract

The design of the Qredo distributed ledger cryptocurrency and payment protocols reflect the known requirements of mobile operators, consumers, merchants and governments for a safe, secure, interoperable mobile payments network that works across borders and carriers.

Design choices encompass many elements that you will read in the following sections of this paper, from the selection of the quantum-resistant cryptographic protocols to the modular design of Qredo's software stack to the economic models used to drive incentives on the Qredo network.

Many of the design choices are intended to deal with the realities of moving money internationally, of complying with the multitude of financial services regulations that are specific to various domiciles and governments. Compliance with privacy legislation such as GDPR and a forward look to guaranteeing consumer privacy and security, along with the need for telecoms to interact with governments and comply with investigatory or legal intercept mandates are critical requirements. Reducing fraud while increasing consumer protection in itself is a significant design factor.

The resulting work created a cryptocurrency architecture wholly unique among others in the field, as evidenced by Qredo's Proof of Speed transaction validation protocol and incentive paradigm, its use of modular components addressing cloud and mobile deployment realities, and an API first design that envisions an ecosystem of participants that can create real value around extending core services.

Qredo, out of the box, can be used by anyone as a secure, completely anonymous cryptocurrency and is by no means limited to use among mobile operators and network service providers. The full Qredo client is capable of running in the cloud, on the desktop or smartphone. However, Qredo differentiates itself through a modular design that recognises the fact that most consumers in the world want to transact as directly and conveniently as possible, without the need to procure cryptocurrency online through an exchange, just to buy a coffee at Starbucks.

The needs of the telecoms industry dictate Qredo's development direction. Our emphasis now is to facilitate cross-border, cross telecom payments, but as the protocol matures, ample room remains to extend Qredo to solve industry challenges such as fraud prevention and IoT device and data security and IOT initiated payments.

Introduction

Qredo is building a distributed ledger system harnessing two types of Directed Acyclic Graph (DAG) technologies into a dual chain architecture. The rationale behind having two graphs, or chains, addresses critical commercial realities. First, the current performance issue that plagues current cryptocurrency 1.0 solutions like Bitcoin and Ethereum regarding transaction velocity. The second is a recognition that telecoms entering financial services must adhere to a broad set of regulatory regimes that include legal intercept to GDPR, and all other domicile specific regimes regulating financial services, KYC, and AML.

The graph, or chain, that is utilised by all Qredo clients is called Graph A. Graph B is a semi-permission chain operated and maintained by telecoms or other entities also operating a Qredo transaction validation node, called a Qredo Minter.

Graph A utilises a code-based post-quantum secure ring signature algorithm[1] to achieve extremely high levels of anonymity about the transaction participants, and a non-interactive zero-knowledge proof protocol[2] for transaction confidentiality[3], so the details are secured. Transactions in graph A are formalised by Qredo Minters using a coopetition model called Proof of Speed.

Proof of Speed is an incentive paradigm with foundations derived from the conditions of pre-selection of public parameters using a post-quantum secure threshold ring signature scheme[4] together with a distributed public randomness beacon[5]. A threshold ring signature scheme effectively proves that a minimum number of users of a certain group must have actually collaborated to produce a signature on a message, while hiding the precise membership of the subgroup.[6] Stated another way, a (t, N) threshold ring signature scheme allows at least t signers in the ring of N signers to cooperate with each other to sign a message without leaking any identity information of the t signers.

Every transaction creates a unique identifier in Graph A, which can be utilised as a pointer back to a more expansive set of data housed within Graph B. A Qredo management service operated by telecoms or other entities is used to create this link. An unmanaged Qredo client produces an orphan identifier in Graph A, i.e., no resulting link to Graph B. These transactions remain entirely anonymous and opaque outside of the transaction participants. Materially, these are the only transactions that will require a transaction fee to be paid to a Minter, explained in the following section detailing the Proof of Speed paradigm.

Graph B runs a permission-less tamper-proof graph structure[7] for storing transaction records of subscribers between telecoms, creating an immutable chain of temporally ordered interactions that happen between each subscriber in each telecom. These records in Graph B use the unique transaction record established in Graph A.

Graph B stores an order of magnitude more data than Graph A. Graph B includes all the transaction information necessary to be compliant in a regulated financial services environment and adhere to strict AML and KYC safeguards. Think of Graph B as a shared compliance database spanning a consortium of telecoms and network service providers running on top of a completely anonymous cryptocurrency (Graph A).

The information stored in Graph B becomes secured, and non-repudiated, by encrypting the uniformly written data written using a shared key[8] between the two transacting telecoms with AES-256 symmetric encryption, itself believed to be quantum-resistant at this time. Encrypted information in Graph B is only accessible by each telecom or service provider involved in the transaction, but not to other Graph B operators/telecoms who receive updates to the entire Graph B chain; they do not have access to the agreed symmetric key.

Graph B encrypted transactions are replicated widely across all operators. This replication makes the system resilient but also enables non-repudiation of transactions between telecoms themselves, i.e., a hash of the encrypted data structure comprising the transaction issued by Telecom A should be the same as the corresponding one published by Telecom B.

A transaction needs two signatures on Graph B, one from each issuing telecom, to have the final signature process completed by other telecoms selected to validate that particular transaction, a design called 'stacked signatures'. The entries in Graph B are signed by Qredo Minters once each telecom mutually signs the other's Graph B entry of the same transaction. If transactions happen between subscribers of the same telecom, the transaction will be issued and signed twice by the same telecom.

Each Graph B operator decides on their bulk storage of transactions, resulting in partial storage of the global directed graph, as other transactions on the chain are encrypted, irrelevant to their operations and inaccessible in any case.

As each telecom creates their unique copy of their chain, so it becomes an accurate historical transaction record of activity between its mobile subscribers (whether they be consumers, merchants or enterprises) and the mobile subscribers on other telecoms.

Graph B's key agreement algorithm can be invoked at any time to generate the AES key to decrypt information as required in legal intercept or dispute resolution scenarios. An advantage of Qredo's quantum resistant key agreement implementation is that long-term storage of symmetric keys used to decrypt Graph B transactions is not necessary. Only the parameters and secrets generated by the telecom before the key agreement protocol are required.

Qredo Minter's receive Qredo by validating both sets of transaction data in Graph A and Graph B. First in Graph A, which then creates the responsibility for the Minter to confirm the signatures behind the encrypted entries in Graph B. These responsibilities form one of the underlying basis of the Qredo protocol itself. That is, the advantages that come with a consortium network of permissioned transaction validators running on top of a permission-less chain.

As discussed in the Qredo white paper, Qredo Minters secure their license to operate a Minter Server, called a Minter Medallion, by buying into the network in one of two ways. First, either initially through Qredo's auction of Minter Medallions, or, after the establishment of the Qredo network is operational, buy buying into the Qredo network as a new Minter Medallion owner.

Establishing this consortium model up front, before the establishment of the network, removes the centralisation risks that hamper other implementors of Directed Acyclic Graphs, such as IOTA.[1].

Qredo, by design, skips this weakness in DAG implementations with a pre-established consortium before its launch. Qredo rewards Minters for validating transactions with Qredo, inflating the supply of the cryptocurrency. As stated in the Qredo white paper, the inflation rate is set before launching in a range of 2% per annum. The Qredo produced from inflation is the reward distributed to Qredo Minters.

These design choices reflect a belief that Qredo should be an actual currency or means of transacting value and not a digital store of value. Bitcoin, by any analysts' account, has failed as a currency because of the distortions created by its inbuilt scarcity of supply.

A natural question to be asked: What are the incentives for Minters for honest behaviour? Qredo takes the approach that a Minter Medallion is an optionally renewed token to create a mechanism of enforcement on Minters for ethical conduct in addition to meeting commitments to uptime and availability.

Qredo's design seeks to enforce standards on Minters through the use of a time-bound Minter Medallion Token. As an example, a Minter's Medallion Token usage term is for six months, after which the Minter must exchange it's expiring Medallion Token for another 'fresh' medallion to keep running it's Minter service.

Qredo uses pairing-cryptography[9] to create a time-bound mechanism[10] that burns up a Minter Medallion if standards of performance and ethics are violated. The selection of these protocols and workflows are described in the following sections devoted to this mechanism. Qredo is actively researching alternative protocols that are quantum-resistant to achieve the same ends, and we expect further iterations to happen shortly.

One aspect that will remain is the intent that new Medallions are acquirable at any time after the Qredo network is established and operational for an, as of yet undetermined term. It is during this term that a 'buy-in' algorithm will determine the price of a Medallion Fee by taking as input several factors.

One such element may be what the potential revenue is for a new Medallion holder based on the growth rate and transaction velocity over the current term. Another may be what the potential costs are to existing

[1]IOTA has a central point of failure. Analysis of its current design revealed a 34% attack by dishonest participants on IOTA is equivalent to a 51% attack of dishonest miners on Bitcoin. The IOTA network created a temporary centralised element – the Coordinator node ("Coo") – to prevent malicious activity in awareness of this issue. For now, every transaction goes through Coo to be validated and, therefore, at this point, a centralised entity is directing the path of the IOTA's DAG tree.

This arrangement also results in the network's poor performance. According to the founders, COO is obsolete once the IOTA generates enough organic activity to be able to evolve unassisted. However, until the platform (without Coo) undergoes a maturation process in production, it is unknown if this scenario will result in success.

Medallion holders currently on the network are for the release of an additional Medallion, hence reducing the potential revenue to existing holders.[2].

As the platform matures, it may be possible for a Minter to sell their Minter Medallion on an open market. Medallion Tokens can be bought/sold in secondary markets if the 'Medallion Fee' as set by the automated algorithms is too high. Rationally, the Medallion Token prices would probably fall just under the current "Medallion Fee" price set by the buy-in algorithm.

Qredo takes a component approach to separating the full Qredo client from a tethered Mobile Client/SDK. This decision stems from a desire to create payment token flows that can work with existing NFC technologies and yet are more secure and leaner than current payment mechanisms which utilise NFC channels.

A Qredo mobile payment token is secured using a quantum-resistant undeniable blind signature scheme[11] that enable the extension of a managed full Qredo client onto a smartphone. We recognise the deployment characteristics of smartphones and IoT devices need to be handled differently than a desktop running a full Qredo client.

To this end a Qredo mobile client is cryptographically[12] tethered to the full Qredo client so that the full Qredo client and tethered devices can be managed by a Management Service running in the cloud, as an example. The Mobile Token Flow and Mobile Client are designed to use the advancements and availability in the GSMA's RCS protocol in addition to NFC availability.

This extension model enables rapid deployment at telecom scale and addresses a multitude of payment scenarios including online, in-store and peer to peer, and eliminates the need for specialised payment terminals (i.e. card readers), a legacy tax on merchants worldwide. This architecture also makes possible open the embedding of Qredo Mobile Code code into multitudes of different applications running on smartphones and IoT devices via an SDK, so that payment between apps on a device, or between distinct IoT devices becomes a reality.

Proof of Speed

Introduction

[2]If you are from New York City, then this cost basis for Medallions should be familiar to you. It's how New York City taxicab medallions used to be bought and sold.

References

1.S. Chen, K. Choo, X. Dong, P. Zeng: Efficient Ring Signature and Group Signature Schemes Based on q-ary Identification Protocols. Presented at the (2017).

2.B. Bünz, B. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell: Bulletproofs: Short Proofs for Confidential Transactions and More, (2017).

3.Bootle, J., Groth, J.: Efficient Batch Zero-Knowledge Arguments for Low Degree Polynomials, (2018).

4.Chen, S., Choo, K.K.R., Zeng, P., Zhou, G., Yuan, X.: An Efficient Code-Based Threshold Ring Signature Scheme with a Leader-Participant Model. In: Security and Communication Networks. Hindawi (2017).

5.Syta, E., Jovanovic, P., Kogias, E.K., Gailly, N., Gasser, L., Khoffi, I., Fischer, M.J., Ford, B.: Scalable Bias-Resistant Distributed Randomness, (2016).

6.Aguilar, C., Cayrel, P.-L., Gaborit, P., Laguillaumie, F.: A New Efficient Threshold Ring Signature Scheme based on Coding Theory, (2008).

7.Otte, P., Vos, M.D., Pouwelse, J.: TrustChain: A Sybil-resistant scalable blockchain. Presented at the (2017).

8.C. Costello, L. De Feo, D. Jao, P. Longa, M. Naehrig, J. Renes: Supersingular Isogeny Key Encapsulation, (2017).

9.Scott, M., Guillevic, A.: A New Family of Pairing-Friendly elliptic curves, (2018).

10.Scott, M., Spector, B.: The Carnac protocol – or how to read the contents of a sealed envelope, (2015).

11.S., S.M., Chandrasekaran, V.: Isogeny-based Quantum-resistant Undeniable Blind Signature Scheme, (2016).

12.Güneysu, T., Oder, T.: Towards lightweight Identity-Based Encryption for the post-quantum-secure Internet of Things. Presented at the (2017).