Whitepaper

Table of Contents

1 Abstract

Q is a novel blockchain that combines the benefits of a public, open and decentralized ledger with the transparency and reliability of enforceable private contracts. Its governance framework provides predictability on how the system works and evolves and enables sophisticated decentralized decision making beyond the limitations of a "code-is-law" logic. Q further introduces the concept of integrated applications, which improve the security of both the base layer and the applications built on top of it, enabling rapid scaling of new use cases. Q seamlessly integrates into the thriving crypto ecosystem, making it easy for participants to use Q, build on Q and transfer value between Q and other decentralized ledgers.

Q System Elements

The **Q Constitution** lays down the rules of the system. It is agreed upon by all participants in Q and forms the foundation on which all other elements of the system are built and is effectively enforceable through the Q governance framework.

Validators Nodes maintain the Q ledger. Positions for Validator Nodes are limited in number and are automatically granted to the candidates who have staked the highest number of Q Tokens. The distribution of positions is automated, continuous and anonymous, allowing anyone with a sufficient amount of Q Tokens to become a Validator Node without requiring permission.

Q Token Holders can delegate their Q Tokens to Validator Nodes, thereby earning rewards for improving the governance and decentralization of Q. They can make governance proposals and vote on such proposals.

Root Nodes are the guardians of the integrity of Q. They monitor Validator Nodes and enforce compliance with the Q Constitution. This second layer of nodes vastly improves the security of Q while ensuring that the system can scale while being permissionless and decentralized.

The Q **Dispute Resolution** mechanism applies established private international arbitration rules and procedures. It is fully integrated into Q's consensus and governance framework and ensures that Root Nodes act in compliance with the Q constitution, safeguarding participants' rights without creating a centralized point of control.

Integrated Applications are systems of smart contracts built on Q which are integrated into the governance framework of Q and – in return for receiving governance services – share some or all of the fees generated by the respective application with Q Token Holders. Through integrated applications, a market for governance emerges. Linking base layer and application layer economics significantly improves the security of both layers, creating a positive feedback loop whereby usage of one layer benefits the security of the other layer.

By integrating a universal governance framework and sustainable economics into a state-of-the-art blockchain, Q creates ***future-proof technology****. Participants in Q benefit from high scalability, low transaction fees and a level of robustness which is unparalleled in other smart contract platforms. Q aims to attract many financial and non-financial use cases into the crypto ecosystem which desire decentralization, scalability and dependability.*

2 Motivation

Since early 2009, when the genesis block of Bitcoin [1] was mined, blockchain-based systems have come a long way: Today, technically sophisticated smart contract platforms [2] offer functionality far beyond Bitcoin's original idea of creating a "peer-to-peer electronic cash system". Valuations of the largest networks are in the billions of USD, testifying to the large investor interest in these networks. The recent surge of Decentralized Finance applications within the Ethereum ecosystem, and lately also on other smart contract platforms, is the final proof that the future of finance will largely be based on decentralized systems.

At the same time, we are still in the early days of this paradigm shift. Only a small fraction of global financial transactions happens within the crypto ecosystems. "Real-world" usage of cryptocurrencies remains limited and many applications built on smart contract platforms still cater mostly to niche audiences.

Q has been developed to address some of the major challenges which – if solved – will promote mass adoption of blockchain-based systems:

Transparent and enforceable governance

Traditionally, public permissionless blockchain-based systems have not had any formalized governance mechanism. In Bitcoin and Ethereum, for example, the rules of the system are defined by the code that is run by the majority of miners. There is no defined set of rules on how decisions about the future of the network are made, and the systems have evolved organically based on unstructured, informal and often chaotic processes.

While such unstructured governance processes can be considered a strength in a limited set of circumstances, we consider this a major weakness of existing blockchain systems. With people and organizations committing significant value to blockchains, they demand and deserve clarity about the rules that apply. This is not primarily a question about ethics or philosophy, but about value creation: As research shows, the quality of governance has a massive impact on the value that an organization or system creates [3].

Historically, the crypto community's answer to questions around governance has been that "code is law", meaning that crypto systems should work just as they are programmed. This principle works just fine for simple transactions – e.g. sending a coin from participant A to participant B – where the only decision to be made by the network is whether a specific transaction is valid or not. As soon as more complex – and therefore more valuable – financial transactions or products are involved, decisions become less binary. The vast majority of modern financial products (e.g. savings accounts, insurance contracts, investment funds) require nuanced decisions that cannot easily be automated via a chain of binary input parameters. Often (e.g. in the case of insurance contracts), decisions require some form of judgement or discretion.

A common argument brought forward by the crypto community is that participants in open blockchain systems can "vote with their feet" – either through hard forks or by simply moving assets to other chains. While this again might work for simple use cases, it is not economically practical once systems and applications become more advanced. For example, as soon as off-chain assets are attached to tokens (e.g. security tokens), it must be clear which token references the asset, therefore forking of the respective network must be ruled out. Furthermore, research indicates that governance through hard forks tends to lead to extreme and economically suboptimal decisions [4]. And while some observers argue that a "social contract" that is implicitly shared by a network's participants provides a degree of reliability, the very nature of a social contract implies that it can change without the consent or explicit approval of its main stakeholders. This is certainly true for cryptocurrencies such as Bitcoin, where the community's understanding of what Bitcoin represents has changed several times in its short history [5].

With the security and future development of major blockchain systems being uncertain, many potential participants are reluctant to transition to blockchain-based systems for business-critical applications. Uncertainty around governance has therefore become a major factor that limits adoption. Conversely, fixing governance will unlock blockchain's potential for further growth.

While some public blockchains try to address this by making governance principles explicit [6], they do not offer a mechanism for reliable enforcement and are therefore dependent on participants' goodwill. Private blockchains, on the other hand, do provide certainty and enforceability of rules for its participants, but do so at the expense of being open, permissionless and immutable – which are the main reasons why people and organizations want to transact on blockchains in the first place.

In contrast, Q aims to foster the adoption of decentralized systems by creating a universal governance framework that combines the benefits of a public, open and decentralized ledger with governance concepts that have proven themselves in other established legal and social systems.

Sustainable economics

While cryptocurrencies have opened up a whole new space of economic exploration, the long-term viability of many blockchain-based systems is still uncertain today. The most salient challenges which blockchain systems face are the volatility of crypto assets, the reliance on subsidies for miners or validators to secure the network, high energy use of proof-of-work consensus algorithms and inherent security limitations of proof-of-stake consensus algorithms.

Furthermore, the value of many blockchain systems is largely driven by speculation, with at best only an indirect link between on-chain activity and protocol valuations. This is true for both base layer blockchains and for many applications built on top of them. On both levels, this raises questions whether those systems are sustainable in the medium- to long-term: For base layer blockchains, the security is dependent on the price of its native asset. A stronger foundation of the native asset's price therefore translates directly into more robust security of the respective blockchain. At the application layer, the security is typically dependent on a separate governance token, which serves as the medium via which decisions regarding the protocol are made. The robustness of the respective application's security model is therefore dependent on the price its governance token. Limited or unclear value accrual potential of a governance token adversely impacts security.

Q addresses these issues through its concept of integrated applications, which create a strong link between usage and value both on the base layer blockchain as well as on the application layer.

Future-proof technology

Traditionally, blockchains have faced a "trilemma" [7], needing to make trade-offs between scalability, decentralization and security. So far, different blockchains have typically optimized for one specific property, sacrificing performance on the other properties. For example, Bitcoin is decentralized but not scalable; XRP is on the other end of the spectrum, providing scalability but being highly centralized, raising questions about the system's transparency and immutability of its ledger.

As long as the trilemma is unsolved, the application of blockchain systems will likely remain limited to specific niches. "Digital gold", for example, may not need to be scalable in terms of transaction speed or transaction throughput, just as physical gold is slow and expensive to trade, move and store, but nevertheless provides utility for a specific use case (inflation-protected store of value).

We believe that decentralization - which translates into immutability of a ledger and the ability of participants to enter and leave the system at their own free will - is essential for blockchain systems. Without being decentralized, blockchains just become clumsy databases which are of limited value in most situations. The challenge then becomes to achieve a high level of security and scalability in a decentralized system at the same time.

Unlike other blockchain systems that look for purely technical solutions for the blockchain trilemma, Q employs a different approach. The key insight is that blockchain is essentially a social technology. Q therefore heavily draws on ideas and principles from the social and legal sciences. Through a combination of state-of-the-art technology, cryptoeconomic incentives and enforceable legal principles, Q achieves a best-in-class level of scalability, decentralization and security, all at the same time.

Furthermore, new blockchains have traditionally attempted to create their own ecosystems. In doing so, they faced the problem of how to bootstrap network effects: To be useful, base layer blockchains need an ecosystem of applications built on top of them; however, to motivate developers to build applications on a specific blockchain, an ecosystem with an existing user base already needed to be in place. This chicken-and-egg problem is very hard to solve.

An alternative approach is to build on the basis of an existing technology stack. This way, a new blockchain can be integrated into existing ecosystems in several ways: Developers can use their existing tooling to create new applications; users can use the wallets and user interfaces they are already comfortable with; and finally, assets can easily be transferred from other blockchains, allowing liquidity from other ecosystems to be deployed on a new blockchain.

We believe that in the future, crypto ecosystems will be interconnected, with little use for ecosystems that are isolated from the rest of the world. Consequently, Q is being built on the basis of Ethereum's technology, which has the largest, liveliest and most robust community of developers and users.

3 The Q Blockchain

Technical basis

The Q Blockchain is an independent blockchain based on Ethereum technology. It runs on a permissionless peer-to-peer network. The code base of Q is fully open source.

Consensus mechanism

Network consensus on the Q Blockchain is achieved via a Delegated Proof of Stake (DPoS) mechanism, whereby a defined subset of network nodes - so-called Validator Nodes - form a consensus on the state of the network. Valid transactions are recorded in blocks, which are published by the Validator Nodes in a rotation system. With a limited set of Validator Nodes, Q's consensus mechanism allows for high transaction throughput with a high fault tolerance. Through its use of a second layer of nodes that are independently selected and enforce Validator Nodes' compliance, Q offers a substantially higher level of robustness against collusion between nodes compared to other DPoS systems.

Native asset

Q Tokens are the native assets of the Q Blockchain. Q Tokens are bearer assets that are fully fungible and do not carry any technical transfer restrictions.

The supply schedule of Q Tokens is known, with a pre-determined number of Q Tokens minted with the genesis block of the Q Blockchain and a fixed amount of Q Tokens per block (block subsidy) being newly created indefinitely thereafter. This leads to a disinflationary supply schedule, where the rate of inflation decreases continuously and asymptotically approaches zero.

The price of a Q Token is not fixed or pegged but determined solely by supply and demand for the asset. Q Tokens fulfill a number of functions within Q to align incentives of the stakeholders of Q and secure the network. All fees and similar transactions within Q are paid with Q Tokens.

Validator Nodes

The Q Blockchain is maintained by a set of Validator Nodes, which validate transactions, record valid transactions in Q's public ledger and append blocks to the Q Blockchain. This implies that they need to run an up-to-date software implementation of the Q protocol and operate a Q full node at all times.

The maximum number of Validator Nodes is capped. Entry to the current set of Validator Nodes is permissionless and determined solely based on the number of Q Tokens which are staked to the respective Node, whereby both owned and delegated Q Tokens are counted.

Root Nodes

Root Nodes monitor Validator Nodes to ensure they comply with the Q Constitution. While Root Nodes cannot influence the state of Q's ledger directly since they do not validate transactions, they are in charge of confiscating Q Tokens from Validator Nodes in case of non-compliance, thereby indirectly enforcing the rules as laid down in the Q Constitution.

The maximum number of Root Nodes is capped. Root Nodes have to stake Q Tokens to demonstrate their commitment to the network. They are elected by Q Token Holders based on specified criteria, which promote the diversity and independence of the panel of Root Nodes.

Stake delegation

Holders of Q Tokens can further delegate all or part of their Q Tokens to Validator Nodes or candidates for Validator Node positions, thereby increasing the number of Q Tokens staked to the respective Validator Node or candidate for a Validator Node position. While Q Tokens are staked, they cannot be spent or otherwise moved. Staked Q Tokens are time-locked and can be unlocked with a waiting period. However, staking Q Tokens to a Validator Node does not limit the Q Token holder's ability to participate in governance votes in Q. For the service which they provide for the Q network, Validator Nodes and Q Token Holders who delegate Q Tokens receive a reward in the form of additional Q Tokens.

4 Governance

4.1 The Q Constitution

Function of the Q Constitution

The basis for the governance of Q is the Q Constitution.

The Q Constitution lays down the rights and obligations of all stakeholders of the Q system. It is the highest-ranking authoritative document for Q and provides certainty and predictability for everyone using Q or building on it.

This explicit form of agreement between stakeholders differentiates Q from other projects, which mostly rely on an implicit set of rules and participants' goodwill to interact with each other responsibly. While some projects have made attempts to introduce an explicit set of rules, they generally still rely on network participants' goodwill to comply with those rules, since there are no effective enforcement mechanisms built into the respective protocols.

Q, on the other hand, has introduced architectural on-chain and off-chain elements into its protocol that allow for an effective enforcement of its Constitution, which turns the Q Constitution into a contract that has the same weight and meaning as a contract concluded between parties in the "real world".

Legal classification and status

The Q Constitution is a private contract among all stakeholders. All stakeholders interacting with Q have to comply with the rules as laid down in the Q Constitution.

Stakeholders in Q enter into this contract either explicitly, e.g. in case of Root Nodes which are required to provide proof that they have signed the Constitution, or implicitly, e.g. in case of Q Token Holders by simply acquiring Q Tokens.

Enforcement of the Constitution

There are two ways in which the Q Constitution is enforced:

- With regards to Validator Nodes and Root Nodes, the Q Constitution can be enforced indirectly through "slashing" (i.e. confiscation and redistribution) of the Q Tokens which they have staked. Validator Nodes and Root Nodes thus have a very strong economic incentive to comply with the Q Constitution because severe or repeated non-compliance would come at a prohibitively high cost to them. This enforcement mechanism works for Validator Nodes even though they do not have an obligation to reveal their identity.
- If the identity of a stakeholder (which can be a natural person or an organization) is known, the Q Constitution can be enforced directly via the Q Dispute Resolution mechanism. This is the case for Root Nodes, but it can also be the case for other Q Stakeholders who voluntarily decide to reveal their identity. The Q Dispute Resolution mechanism relies on international private arbitration to enforce the rules of Q, thus linking the Q Blockchain to the off-chain reality of its participants.

Changes to the Constitution

As any complex system, Q will have to evolve over time to remain relevant and useful for its stakeholders. While the Q Constitution is designed to have a "long shelf-life", it will and should be amended from time to time. Depending on the gravity of such amendments, they will require different majorities:

- Fundamental principles of Q are expected to be changed very rarely and require the highest quorum and majority of Q Token votes.
- Basic rules of Q are expected to be changed from time to time and require a somewhat lower quorum and majority of Q Token votes.
- Detailed rules and parameters of Q are expected to change regularly and require a relatively low quorum and majority of Q Token votes.

In the future, it is envisioned that all decisions by Q Token holders regarding Constitutional matters can be vetoed by Q ID Holders with a pre-specified quorum and a simple majority vote. With Q ID Holders being natural persons, this introduces a balancing element that prevents situations sometimes observed in other proof-of-stake or proof-of-work blockchains, where a small but wealthy group of "oligarchs" or "plutocrats" effectively controls changes to the protocol [8]. The Q Constitution enjoys a high degree of protection against such abuse scenarios, ensuring that the protocol cannot be changed in a way that benefits a small group of stakeholders to the detriment of others.

4.2 Validator Nodes

Validator Nodes maintain the Q Blockchain in compliance with the Q Constitution. This implies that they have to reject invalid transactions and may not refuse to record valid transactions at will.

In case of a Validator Node's non-compliance with the Constitution, Root Nodes execute penalties in the form of "slashing" the respective Validator Node's staked Q Tokens (both own and delegated tokens). The share of a Validator Node's tokens that shall be slashed corresponds to the severity of the Validator Node's violation. For example, in case of a light technical violation such as temporary downtime, only a fraction of a percentage may be slashed, while for a severe violation that significantly harms other stakeholders, up to 100% of staked Q Tokens may be slashed. Percentage ranges for various categories of non-compliance are defined in the Q Constitution, which is binding for all slashing decisions by Root Nodes.

While it is expected that the slashing of a Validator Node is a rare event, it is nevertheless crucial to incentivize Validator Nodes to comply with the Q Constitution and make deliberate non-compliance prohibitively expensive.

4.3 Root Nodes

Background

Using a DPoS model allows for high scalability in terms of transaction throughput and predictable transaction costs. Typically, though, DPoS-based blockchains have trade-offs in terms of decentralization and network security: One third of faulty or malicious nodes can corrupt the network, and due to the large amount of communication between validating nodes that is necessary in some consensus protocols, an increase in the number of validating nodes leads to a strong decrease in network performance. A limited number of validating nodes, on the other hand, lowers the threshold for collusion between nodes, thereby reducing decentralization and robustness against malicious attacks.

The Q Blockchain solves this dilemma by deploying a second set of nodes, so-called Root Nodes, that monitor Validator Nodes and penalize them in case of faulty or malicious behavior. Penalties are executed through confiscation of Q Tokens staked by Validator Nodes (so-called "slashing"). This drastically reduces the likelihood of network corruption since Validator Nodes have a very strong economic incentive to act according to the rules. At the same time, admission to the validator set can remain entirely permissionless, providing no angle for censorship attacks from actors outside the system.

As a result of this unique two-tier node architecture, the Q Blockchain has a higher level of security and reliability compared to other blockchain networks without compromising decentralization or network performance metrics.

Responsibilities of Root Nodes

The Root Node layer enables the effective enforcement of the Q Constitution both on a technical and on a governance level.

The prime mechanism how Root Nodes ensure Validator Nodes' compliance with the Q Constitution is through their obligation to slash a Validator Node’s Q Tokens in case of non-compliance. However, Root Nodes do not actively select or permission Validator Nodes. And while Root Nodes have to run a Q full node to fulfill their obligations, they do not validate transactions, do not amend the Q Blockchain and do not have the ability to reverse transactions or reorganize the Q Blockchain.

In addition to their role in monitoring (and in case of misbehavior penalizing) Validator Nodes, Root Nodes protect the Q Constitution by providing a list of malicious Validator Nodes (Validator Nodes Exclusion). Such malicious behavior can occur if Validator Nodes collude to prevent the execution of legitimate slashing transactions, thereby avoiding the exclusion of the current Validator Node set. The Validator Nodes Exclusion is timestamped and propagated on the Q Blockchain’s peer-to-peer network, making use of the existing network infrastructure. This can be considered as a second set of blockchain-like data underlying Rood Node consensus. As it is not part of the Q Blockchain, it is not subject to potential attacks by Validator Nodes. The Validator Nodes Exclusion can be queried by all network participants to ensure that transactions which have been validated by excluded nodes are ignored.

In the first block of every validation cycle, a Validator Node Whitelist is added to the block. The Whitelist contains the valid set of Validator Nodes for the respective validation cycle, which is derived from the most current Validator Node stake ranking and the Validator Exclusion. The Whitelist is co-signed by the Root Nodes to provide additional certainty that the Validator Node set is correct and the Root Node panel is active and has not been compromised.

Of course, Root Node’s themselves are bound by the Q Constitution. In case of non-compliance, Root Nodes can be penalized via “slashing” of their staked Q Tokens. Such slashing decisions can be challenged via the Q Dispute Resolution procedure.

Determination of Root Nodes set

There maximum number of Root Nodes is capped.

Candidates for Root Node positions have to fulfill the following eligibility criteria:

- They need to disclose their identity;
- They need to be resident in a jurisdiction where decisions according to the Q Dispute Resolution mechanism can be enforced;
- They need to confirm their acceptance of the Q Constitution.

New Root Nodes can be elected at any time by a simple majority vote of the Q Token Holders with a pre-specified quorum. The election of Root Nodes shall be based on the following criteria:

- Commitment to Q - this is demonstrated by the size of the stake which is committed,;
- Diversity – this is measured by the distribution of Root Nodes amongst different geographies and institution (e.g. corporate, academic, not-for-profit).

For the vote to become effective, the respective Root Node has to stake the amount of Q Tokens as indicated in its application to become a Root Node. The term of elected Root Nodes is indefinite.

Root Nodes provide a list of the current Root Node set (Root Node Whitelist). This eliminates the risk that the Validator Nodes collude to provide false information about the Root Nodes. The Root Node Whitelist includes the public key of each Root Node in the current Root Node set. The Root Node Whitelist is timestamped and propagated on the Q Blockchain's peer-to-peer network, making use of the existing network infrastructure. However, it is not part of the Q Blockchain and therefore not subject to potential attacks by Validator Nodes. The Root Node Whitelist can be queried by all network participants and thereby represents a source of truth for the makeup of the current Root Node set.

4.4 Q Token Holders

Q Token Holders have a strong governance function within Q. Since they represent all major stakeholder groups within Q, their vote is required for all major decisions related to Q. Their role is thus of critical importance to the running and functioning of Q. Without their continued involvement, neither the Q Blockchain nor Q Integrated Applications that are built on it would work.

In particular, Q Token Holders have the right to:

- propose changes to and amendments of the Q Constitution;
- vote on proposed changes to and amendments of the Q Constitution;
- propose changes and amendments of the Q protocol;
- vote on proposed changes to and amendments of the Q protocol;
- propose new Root Nodes;
- vote on proposed new Root Nodes;
- propose slashing of Root Nodes' staked Q Tokens;
- propose additions and removals of experts in Expert Panels;
- vote on proposed additions and removals of experts to be included in Expert Panels.

Q Token Holders can exercise their governance rights without revealing their identity. They can also choose to delegate all or part of their votes to other Q Token Holders.

Lastly, Q Token Holders can challenge decisions related to Q through the Q Dispute Resolution procedure. When doing so, they will need to reveal their identity.

4.5 Q ID Holders

Q ID is Q's native identity system which can store pseudonymous identification details for Q stakeholders. Q ID is expected to allow users to voluntarily provide a personal ID, thereby confirming that they are a unique natural person. Such confirmed unique natural persons are called Q ID Holders.

Q ID Holders are expected to receive governance rights in the form of veto rights to important decisions such as the election of Root Nodes or the amendment of the Q Constitution. This is an important aspect of the Q governance as soon as Q has reached a level of maturity, since it prevents the development of an "oligarchy" that is often seen in other blockchains (both proof-of-work and proof-of-stake). The active involvement of Q ID Holders in Q's governance therefore represents an element of direct democracy that is woven into the fabric of Q.

The rationale for not granting Q ID Holders veto rights from the very first day of the network launch is that a critical mass of diverse Q ID Holders is required before the veto function can be implemented. If this governance feature were implemented too early, a small group of Q ID Holders could veto important changes and prevent the development of Q during the early phases of the project. The introduction of veto rights for Q ID Holders will require a corresponding amendment of the Q Constitution.

4.6 Expert Panels

Within Q, there are certain parameters that require regular adjustments. Examples include the setting of transaction fees for the Q Blockchain or the list of eligible assets in the Q Decentralized Finance System.

While it is beneficial to automate the adjustment of parameters as much as possible, it is not always possible or sensible to do so. Reasons that preclude automatic adjustment can be that there is no simple algorithmic formula that can be deployed (as in the list of eligible assets, which requires some qualitative judgement) or that possible algorithms might lead to unreliable, unfair or "gameable" results.

This is a common problem for all blockchain systems that exceed the absolute minimum level of transaction complexity.

There are two conventional ways to address this:

The first way is to let token holders vote. While this seems a good solution at first glance, since it engages the community that should care about the project, in practice this does not work. Frequent votes lead to "voter fatigue" and very low voter turnouts, making votes susceptible to manipulation. Furthermore, many decisions require in-depth domain-specific knowledge that cannot be expected from regular token holders.

The second way is to have special administrator keys, which enable a specific person or organization - e.g. a Foundation that acts as project sponsor - to manipulate parameters. Clearly, this is not in line with the idea of openness and decentralization.

Q employs a third way: The election of Expert Panels by the Q Token Holders. This combines the best elements of both worlds: On the one hand, Q Token Holders as the ultimate risk bearers of Q get to decide on matters that impact the functioning of Q and its Integrated Applications. On the other hand, technical decisions that require a deep expert knowledge in a specific field are taken by people with the know-how necessary to make those decisions in an optimal way.

4.7 Dispute Resolution

Decisions within Q can be challenged via Q's Dispute Resolution mechanism, which relies on international private arbitration as a way to resolve disputes.

Participants in Q agree that all disputes arising in connection with the Q Constitution are resolved by way of arbitration before an arbitration tribunal under the Rules of Arbitration of the International Chamber of Commerce (so-calls ICC Rules [9]). The ICC rules provide a tried-and-tested set of rules that can be applied to arbitration proceedings independently of the subject matter and the place and jurisdiction where the proceedings take place. This provides procedural certainty to all participants in Q and ensures that high quality standards will be met in the arbitration proceedings.

In order to limit abuse and unnecessary arbitration proceedings, a party making a claim under the Q Dispute Resolution mechanism will have to pay the advance costs (if any) related to such claim. In order to improve the transparency and certainty related to legal and governance issues around Q, all binding rulings awarded by an arbitration tribunal in accordance with the Q Dispute Resolution mechanism will be made public.

Q's Dispute Resolution mechanism provides additional security for all participants in Q and is a cornerstone of Q's governance system. The inclusion of “real-world” dispute resolution mechanisms ensures that even in the unlikely case that previous protective measures fail, participants in Q can rest assured that the Q Constitution will be upheld and enforced. The Dispute Resolution mechanism is particularly (but not only) relevant for slashing decisions, insofar as Validator Nodes and Root Nodes can contest slashing decisions if they feel it is unfair and not in line with the rules as laid down in the Q Constitution.

4.8 Q Foundation

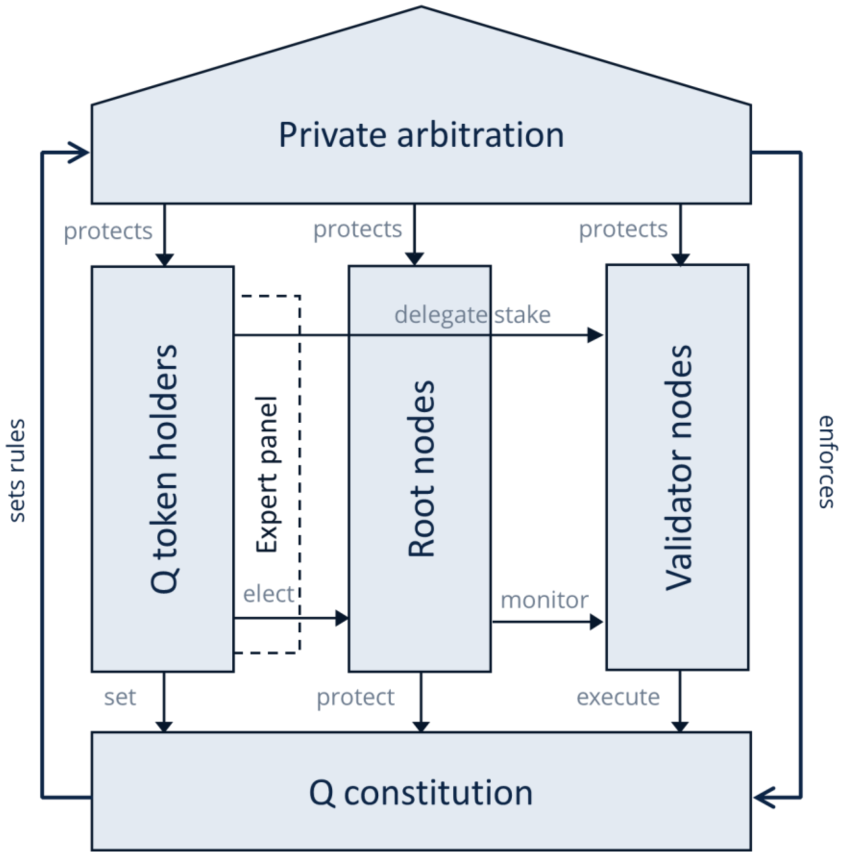
Q is initiated with the support of the Q Foundation, which is tasked with kick-starting, promoting and supporting the project. The Q Foundation is an independent not-for-profit organization. It has no owner, no controlling entity and is bound solely by its bylaws and the legal framework of its host country. It is such fully independent and cannot be used or abused by a specific stakeholder or stakeholder group.

Within Q, the Q Foundation has no special governance privileges. If it holds Q Tokens, it can exercise its voice as a Q Token Holder, but is equal among all other Q Token Holders.

The Q Foundation is expected to adhere to the highest standards of openness and transparency in the industry. The ultimate goal of the Q Foundation is to lead Q towards full decentralization and eventually not be necessary and disappear.

4.9 Overview

The following graph provides a simplified summary of the governance framework of Q:



5 Integrated Applications

Integrated Applications are systems of smart contracts which are bound by and benefit from aspects of Q's governance and are thereby deeply integrated into Q's governance framework. In return for the governance services they provide, Q Token Holders can receive all or part of the fees generated by such integrated applications. Thus, Q breaks with the conventional wisdom of the blockchain space, where the blockchain layer is separate from the application layer. This radically changes the economics of Q compared to other blockchains, since fees that are generated by Integrated Applications are available for distribution to Q stakeholders. As outlined in the section Economics, this greatly improves the robustness and sustainability of Q.

Changes to Integrated Applications may require a change of the Q Constitution, and such changes are monitored and protected by the Validator Nodes, Root Nodes and can be challenged via the Q Dispute Resolution mechanism. The existence of Integrated Applications does, however, not preclude anyone from building other non-integrated applications on Q. To the contrary, the added security provided by Integrated Applications into Q increases the attractiveness of building non-integrated applications on Q.

The depth of integration can vary between applications – from no integration at all to a full integration, where the application is fully governed by Q Token Holders and 100% of the fees generated by such Integrated Application accrue to Q Token Holders. We expect that the degree of integration will greatly depend on the type of application and will be the subject of negotiation between application developers and the Q Token Holder community. Applications which benefit more from a deeper level of integration will be willing to share more of their fees and vice versa. In this way, effectively a market for governance services will emerge.

In the early phases of the project, Q is expected to offer two Integrated Applications - the Q Decentralized Finance System and Q ID - which are briefly described in the following:

Q Decentralized Finance System

As a proof of concept, Q starts out with an integrated Decentralized Finance System is comprised of a decentralized borrowing platform and a system of stablecoins. On the Q Borrowing Platform, people and organizations can borrow a stable digital currency against tokenized assets. Through the collateralization of these tokenized assets, stablecoins that are stable against a specific benchmark, such as the USD, are created. These can be used in everyday transactions at minimal costs. In the future, the Q Decentralized Finance System is expected to offer more services and functionalities.

Q ID

Q ID is an identity system that allows users of Q to associate Q addresses with their verified identity. Initially, the verification of identities will be performed by third parties that provide such services. At a later point, identities may be certified through other more decentralized approaches as well.

Q ID follows the Decentralized Digital Identifier (DDI) standard of the World Wide Web Consortium (W3C) [10] . This means that no personal data needs to be stored on the Q Blockchain, preserving users' privacy while allowing them to benefit from identity services.

Users of Q who identify themselves through appropriate documentation (e.g. a passport or a national identity card) as unique natural persons are “Q ID Holders”. Q ID Holders can participate in the governance of Q in various ways. For example, it is envisioned that in the future, Q ID Holders will have a veto right on the election of new Root Nodes and thereby control an important part of the security and governance infrastructure of Q. Furthermore, Q ID Holders receive a part of the fees generated within Q. Lastly, Q ID can form the basis for more applications and governance features – e.g. on Q Integrated Applications – which require a “vote-per-person” logic. It opens up entirely new possibilities for the governance of blockchains and decentralized applications.

6 Economics

6.1 Background and goals

The economics of Q are designed to achieve three goals:

1. The economic model shall be sustainable in the long-term.
2. The underlying economic incentives shall support Q’s security and robustness.
3. Everyone who participates in Q and contributes to the project shall benefit from its success.

As detailed below, these goals are achieved through Q’s tokeneconomic design.

6.2 Flow of funds within Q

In the following, we describe the flow of funds within Q. The description is simplified but illustrates the basic principles that are relevant to the overall economics of Q.

Sources of funds

Within Q, there are four sources of funds which are generated within the system:

- Inflation subsidy: As most blockchain-based protocols, Q incorporates an inflation subsidy: With every new block that is mined, new Q Tokens are created that are available to reward network participants. The number of Q Tokens created per block is fixed, resulting in a disinflationary supply schedule where the rate of inflation decreases continuously and asymptotically approaches zero in the long-term. Q’s supply schedule is therefore predictable, providing participants with certainty about the amount of Q in circulation, while at the same time continuously reducing the dilution suffered by the network owners as the project matures.

- Transaction fees: Usage of the Q Blockchain, including the execution of smart contracts, is paid for through transaction fees denominated in Q Tokens. The level of transaction fees is determined on a “cost-plus” basis, reflecting the costs that Validator Nodes have to incur for the provision of their services. The details of the transaction cost calculation are determined by an Expert Panel which is responsible for setting the level of fees in line with the guidance given in the Q Constitution. In contrast to most other public blockchains, this results in a high level of predictability of transaction fees, enabling stakeholders to build applications that require predictable economics. At the same time, the cost-plus basis ensures that spamming attacks are not profitable.
- Slashed Q Tokens: If and when Validator Nodes or Root Nodes violate the Q Constitution, they are subject to “slashings” of their staked Q Tokens. Slashed Q Tokens are available for distribution to network participants.
- Integrated Application fees: Q introduces the novel concept of Integrated Applications, which are decentralized applications built on the Q Blockchain that are integrated into the Q governance framework. Fees that are generated by Integrated Applications are available as rewards to participants of Q. As described below, the availability of fees generated by Integrated Applications for distribution to Q stakeholders greatly improves the economics of Q.

Importantly, all sources of funds within Q are denominated in Q Tokens.

Recipients of funds

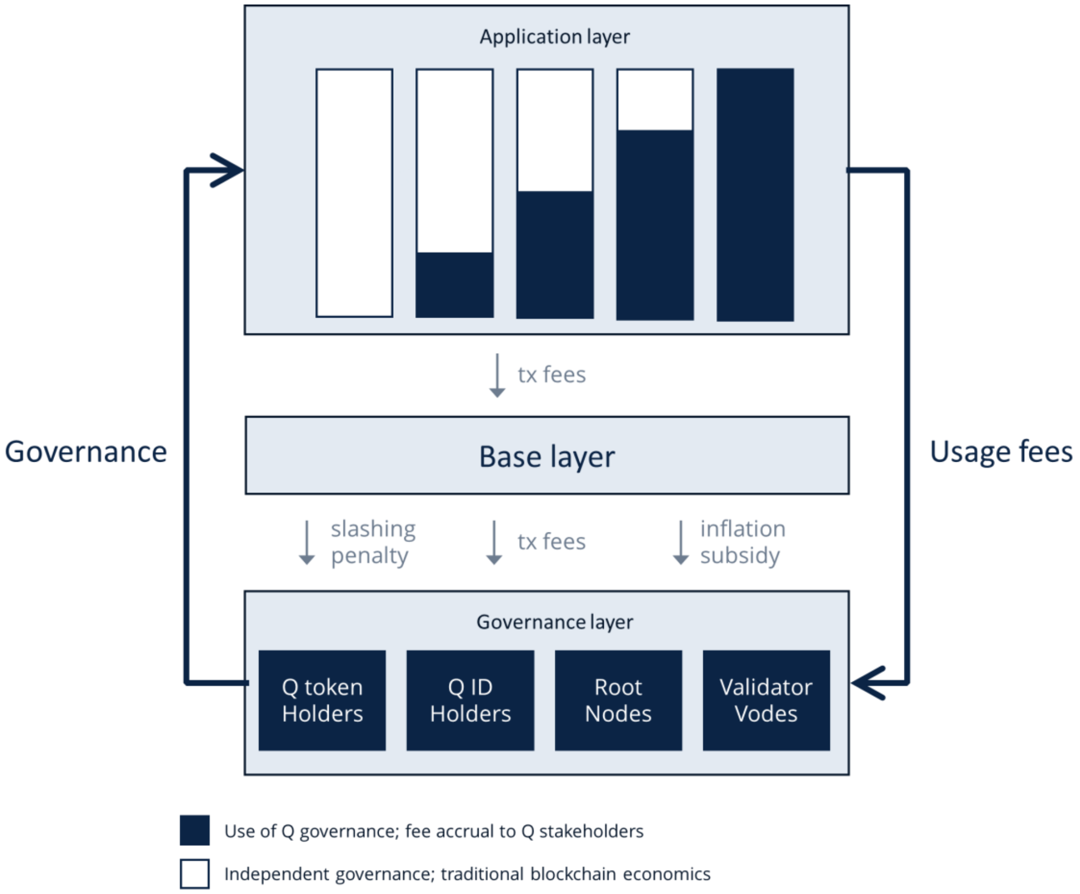
Within Q, there are four major participants groups which are eligible for receiving a share of the funds which are generated within the system:

- Validator Nodes, which maintain Q’s public ledger, are eligible to receive funds proportionate to the amount of tokens (own and delegated) which they have staked.
- Root Nodes, which monitor Validator Nodes and ensure compliance with the Q Constitution, are eligible to receive funds which are equally split among all Root Nodes.
- Q Token Holders, which play a significant role in Q’s governance, are eligible to receive funds proportionate to the number of Q Tokens which they hold.
- Q ID Holders, who contribute to Q’s governance, are eligible to receive funds on a per-person basis.

The percentage of funds which each participant group receives is defined in the Q Constitution.

Overview

The following graph provides a simplified summary of the flow of funds within Q:



In order to avoid a large transaction volume from the distribution of funds, Q Token Holders and Q ID Holders will have to claim their tokens periodically. It is expected that a claiming features will be implemented in Q wallets, making the process easy and convenient for users.

6.3 Economic properties of Q

Sustainability

Historically, blockchains have relied on two sources of funding: Inflation and transaction fees. Of the two, inflation is by far the more important source of funds in most blockchains. However, it is clear that inflation is not a sustainable source of funding since it dilutes the value of token owners' assets, reducing the attractiveness of owning the protocol's native asset. Therefore, inflation is typically reduced according to some schedule, with the idea being that transaction fees should increase as the network matures. The transition from inflation funding to transaction fee funding is, however, anything but safe: Firstly, it is entirely unclear today in how far network participants will be willing to pay transaction fees and whether an equilibrium in which transaction fees provide an adequate level of funding will emerge. Secondly, high transaction fees necessary to achieve a reasonable security budget prevent certain use cases from being deployed on-chain. And thirdly, a transaction-fee-based regime introduces new risks and elements of instability to a blockchain [11]. Some researchers have proposed solutions how existing blockchains could transition to sustainable economics [12], but given the strong vested interests of stakeholders in the status quo and the lack of a structured governance process that could drive such fundamental change, it is questionable whether such transitions can ever be implemented on an up-and-running blockchain.

Q introduces a novel approach by integrating Integrated Applications into the core of its protocol. As outlined above, fees which are generated via such Integrated Applications are available for distribution to Q's stakeholders that support the network. This reduces, and ultimately eliminates, the need for non-sustainable funding via inflation or transaction fees and - at the same time - incentivizes all stakeholders to promote "real" usage of applications that are built on Q.

Overall, Q's integration of fees derived from Integrated Applications results in economics which are supported by fundamental factors and do not rely on speculation or non-sustainable sources of funding.

Security

The integration of Integrated Applications into Q greatly improves the security and robustness of both the Q Blockchain and the Integrated Applications that are built on it.

In proof-of-stake blockchains, the network is secured through the staking of its native asset. Arguably, this creates a self-referential relationship: The security of the network is dependent on the value of its native asset, whose value in turn is dependent on the security of the network. Of course, it could be argued that the value of layer 1 blockchains reflects the expectation that there will be demand for its native asset to pay for transaction fees. However, rising transaction fees would reduce the utility of the network for many use cases, which would in turn limit its fundamental value in the medium- to long-term.

Q breaks this circular logic. The value of Q Tokens is supported by usage of its Integrated Applications, since fees generated by such applications partially accrue to Q Token Holders. Hence, there is an external reality to which the value of Q Tokens are anchored [13] . The valuation of Q does not depend on speculation, but is supported by the utility of the applications that are built on it.

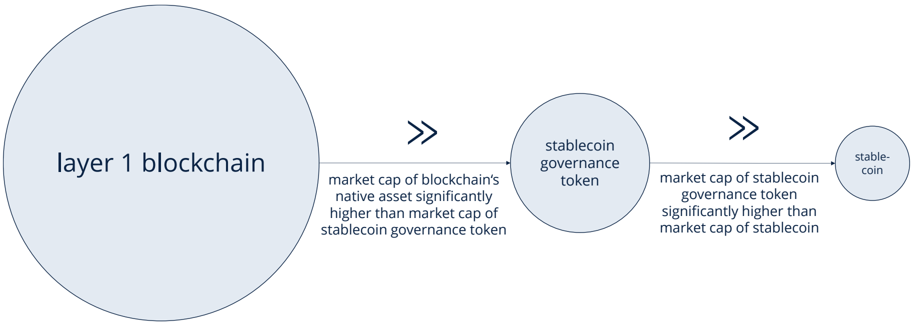
The integration of Integrated Applications into Q's economics creates a positive feedback loop. With increased usage of its Integrated Applications, the security of the Q Blockchain increases, which in turn makes it more attractive for people to build and use applications that contribute to the fees that are generated in Q. With such strong fundamental support, Q is much less susceptible to speculative attacks that could compromise the network's security.

Also, Integrated Applications built on Q enjoy a significantly higher level of security compared to traditional decentralized applications which are built on top of layer 1 blockchains: They use the governance and security framework underlying the Q Blockchain, which is much stronger than typical application-only governance and security frameworks.

This can be illustrated using the example of a collateralized stablecoin:

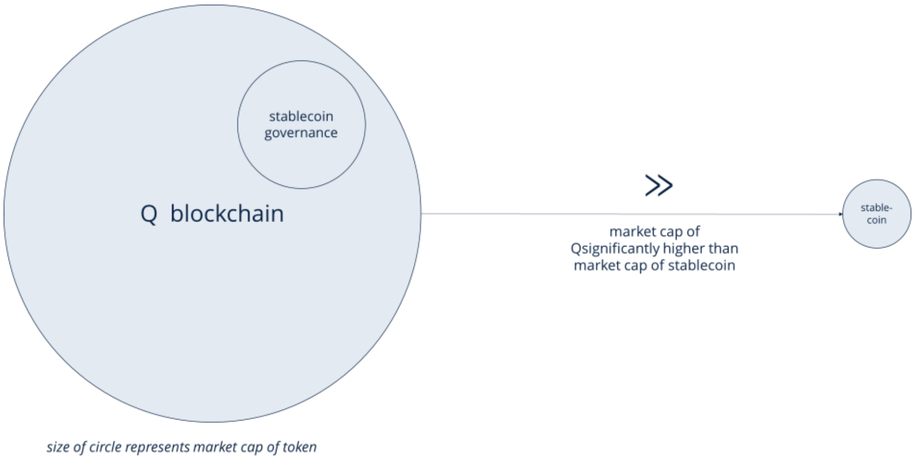
In a traditional setup where the application layer is independent of the blockchain layer, there are three tokens: The native asset of the underlying blockchain, a governance token of the stablecoin application and the stablecoin itself. For the system to be secure, the total market value of each token has to be significantly lower than the market value of the token of the layer on which it is built. If that were not the case, an economic attack would be possible. For example, if the value of the governance token were lower than the value of the stablecoin, an attacker could acquire a majority of governance tokens and effectively control the governance parameters underlying the smart contracts of the collateral system. In this way, the attacker would gain access to the collateral. The cost of this attack would be lower than the "bounty" of the collateral that could be stolen (this is strongly simplified and serves to illustrate the basic economic logic - an actual attack would more complex). A potentially profitable attack vector exists, jeopardizing the application's security.

A similar argument can be made for the relation between the native asset of the layer 1 blockchain and the governance token of the application. The required relationship between the required market values of the different tokens is illustrated in the following graph:


layer 1 blockchain
>>
market cap of blockchain's native asset significantly higher than market cap of stablecoin governance token
stablecoin governance token
>>
market cap of stablecoin governance token significantly higher than market cap of stablecoin
stable-coin

size of circle represents market cap of token

In Q, on the other hand, an attacker who wants to compromise the integrity of a collateralized stablecoin system that is implemented as an Integrated Application would need to attack the layer 1 blockchain - i.e. Q - itself. Since the value of Q exceeds the value of its individual applications that are built on top of it, this is orders of magnitude more expensive, rendering any attempt of an attack economically unattractive. As a result, Integrated Applications exhibit a higher level of resilience against economic attacks compared to traditional decentralized applications. This relationship is illustrated in the following graph:


stablecoin governance
Q blockchain
market cap of Qsignificantly higher than market cap of stablecoin
stable-coin
size of circle represents market cap of token

The improved security characteristics allow Integrated Applications to scale much faster than their counterparts which are based on a traditional blockchain architecture.

Economic incentives

Q provides economic incentives for all major stakeholder groups which contribute to the system. This differentiates Q from other blockchains, which typically have economic incentives favoring specific network participants (e.g. in proof-of-work blockchains, rewards accrue exclusively to miners). The following summarizes the economic positions of Q's stakeholders:

Validator Nodes provide a valuable service to Q by maintaining its public ledger and executing the rules as defined in the Q Constitution. They receive funds in proportion to the amount of Q Tokens (own and delegated) which they have staked. Each Validator Nodes can decide which portion of those funds are passed on to Q Token Holders who have delegated Q Tokens to the respective Validator Node. This creates a competitive staking market, where potential Validator Nodes compete for the delegation of Q Tokens. Since the risk and return profiles can vary between different staking providers, Q Token Holders are expected to diversify their delegated Q Tokens, thereby promoting decentralization of staking power.

Root Nodes provide a valuable service since they enforce the Q Constitution. They also receive funds as a reward for their service, whereby the Q Token reward is shared equally among all Root Nodes. In contrast to Validator Nodes, the staking of Q Tokens by Root Nodes is not competitive in the short-term, since the committed amount of stake for each Root Node is fixed. However, the amount of committed stake is one of the main criteria for Root Node elections, so successful Root Node candidates are expected demonstrate their commitment to Q by locking a significant amount of Q Tokens. This ensures that Root Nodes as "guardians of the Q Constitution" have skin in the game. Since their stake is also at risk for slashing if they do not honor their obligations, they are incentivized to deliver high-quality governance services.

Q Token Holders are eligible to receive funds in proportion of their amount of Q Tokens owned. This incentivizes ownership of Q Tokens, which is necessary for any form of participation in Q, and ensures that Q Tokens Holders whose vote is important in all aspects of governance have skin in the game. A part of the funds which are earmarked for Q Token Holders is accumulated in the Q System Reserve, which can be used for funding in the unlikely case of shortfalls in Q Integrated Applications or unexpected system failures.

Q ID Holders receive funds on a per-person basis. In other words, each Q ID Holder receives the same amount of funds. This incentivizes natural persons to engage with Q. As described previously, involving Q ID Holders in Q governance decision can be regarded as a form of direct democracy that balances the asset-weighted votes of Q Token Holders. Furthermore, the distribution mechanism for funds to Q ID Holders is open to third parties and can thus form the basis for a Universal Basic Income distribution mechanism.

7 Outlook

On the basis of its unique governance structure, Q will keep evolving. While the direction of further development and the setting of priorities is determined by the Q community, there are a number of themes along which we envision strong development following the launch of Q:

7.1 Usage of Q

Q is designed to be used in real-life. Its effective and transparent governance, combined with its high performance characteristics and great usability, makes it particularly attractive for use in large-scale applications where many people have so far been reluctant to deploy decentralized and permissionless crypto systems. To further the goal of promoting mass adoption of cryptocurrencies, the Q community is expected to work actively in bringing new users on board. This will include individuals - e.g. those who have no or limited access to digital financial products, or those who simply enjoy fast, cheap and transparent peer-to-peer payments - but also organizations such as online merchants and large global businesses. We are confident that when someone has used Q once, the advantages over the legacy financial system will be so obvious that it will be hard to go back. The first step is therefore the most important. With strong support of the Q Foundation, the Q community will work tirelessly to promote adoption of cryptocurrency usage by onboarding users to Q.

7.2 Features and functionality

While Q is useful from Day 1, development never ends. Improving the protocol is therefore an ongoing process and the Q Constitution provides a transparent and structured framework for how this is done. While - again - concrete development priorities are determined by the Q community, from today's point of view we can already see some areas that will likely be in the focus in the early days of the project. Three examples: Firstly, the further development of Q ID is expected to be in focus, offering more people around the globe the opportunity to actively participate in Q as natural persons. Secondly, adding more stablecoins to the Q Decentralized Finance system would be valuable to many users around the world, providing them with a cryptocurrency that fits for their individual needs. Thirdly, more features and functionalities can be added to Q, fully leveraging potential of “programmable money”. For example, adding a referral and loyalty function to Q USD would be immensely useful particularly to small merchants who lack such systems today.

7.3 Community development

As any decentralized project, Q can only be as good as the community which supports it. Developing a strong and lively community is therefore key to its success. We expect community development to be a bottom-up process, initiated by the early sponsors, developers and users of Q, and supported by the Q Foundation. Early stakeholders are expected to grow relationships with other sets of stakeholders, in particular users and node operators but also policy makers and the public at large. As an inclusive and borderless project, Q encourages diverse sets of stakeholders to engage in the project.

7.4 Security

For any system where real value is transacted, staying on top of security developments should be a prime concern. While this should go without saying, it is worth stressing this point since it is unfortunately sometimes overlooked in decentralized projects. Achieving the highest level of security is a question of mindset as much as it is a result of concrete actions and measures taken. Acknowledging that security is never absolute and staying alert is key. We envision that a significant amount of development work will be devoted to security issues, but also that the community will be actively involved, e.g. through bounty programs. Importantly, security is not limited to Q’s code but needs to be addressed holistically, incorporating aspects of economic incentives and game theory, governance and participants' interests and potential threats resulting from developments outside of Q.

7.5 Decentralization

Q is a decentralized project. The term “decentralized” - however - has often been misunderstood or even misused, so we make it explicit what we mean by it, where Q stands at the launch of the project and what the vision for the future is.

From Day 1, Q is decentralized in the technical sense: The power over the network is in the hands of its participants, and there are no specially privileged tokens or “administrator keys” in the hands of single entities. However, upon network launch, the majority of Q Tokens is in the hands of the Q Foundation. And while the Q Foundation is a not-for-profit entity that is bound by its statutes, which clearly spell out that its sole purpose is to promote systems such as Q, it is nevertheless a dominant Q Token Holder initially. Some projects have chosen for Foundations with large token holdings to pledge that they will not exercise voting rights, while at the same time granting far-reaching owner-privileges to the Foundation or other central parties. We believe this approach is not optimal, since the degree of central control is hard to assess for outsiders.

Q has therefore chosen a different path: The Q Foundation is a regular Q Token Holder without any ownership, governance or other privileges. While it provides transparency over its token holdings, there are no restrictions attached to those token holdings. We believe that stating this openly and transparently is the right thing to do. Further, we believe that decentralization is a process, not a specific state [14]. No matter where a project starts, the direction in which it moves is important. Q will strive towards greater decentralization of Q token ownership in the future. Concretely, this means that the Q Foundation is tasked to distribute its Q Token holdings in a transparent way with the goals of (i) funding development of Q and (ii) dispersing ownership of Q Tokens. As Q evolves, it will therefore become progressively more decentralized.

8 Endnotes

[1] S. Nakamoto (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

[2] cf. White Papers of smart contract platforms, e.g. Ethereum, https://ethereum.org/whitepaper/

[3] e.g. Paul A. Gompers, Joy L. Ishii, Andrew Metrick (2003): Corporate Governance and Equity Prices in *Quarterly Journal of Economics, Vol. 118, No. 1, pp. 107-155*; the authors find that stocks of companies with best-in-class corporate governance exhibit an outperformance of 8% p.a.

[4] cf. Barton E. Lee, Daniel J. Moroz, David C. Parkes (2020): The Political Economy of Blockchain Governance, *SSRN Working Paper*, (http://dx.doi.org/10.2139/ssrn.3537314)

[5] cf. Hasufly and Nic Carter (2019), Visoins of Bitcoin - How major Bitcoin narratives have changed over time, https://medium.com/@nic__carter/visions-of-bitcoin-4b7b7cbcd24c

[6] examples include EOS and decred

[7] the the term “blockchain trilemma” is often attributed to Vitalik Buterin, co-founder of Ethereum; it was predated by a concept called “Zooko’s triangle”, developed by computer scientist and cypherpunk Zooko Wilcox-O’Hearn, which describes a trilemma between desirable properties of names in a network protocol: decentralized, secure and human-meaningful

[8] cf. Vitalik Buterin (2018): Governance, Part 2: Plutocracy is still bad, https://vitalik.ca/general/2018/03/28/plutocracy.html

[9] https://iccwbo.org/dispute-resolution-services/arbitration/rules-of-arbitration/

[10] https://www.w3.org/TR/2020/WD-did-core-20200421/

[11] cf. M. Carlsten, H. Kalodner, S. M. Weinberg, A. Narayanan (2016): On the Instability of Bitcoin Without the Block Reward, *in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security pp. 154–167,* (https://doi.org/10.1145/2)

[12] Hasu, James Prestwich and Brandon Curtis (2019): A model for Bitcoin's security and the declining block subsidy, https://medium.com/@hasufly/research-paper-a-model-for-bitcoins-security-and-the-declining-block-subsidy-11a21f600e33

[13] The "external anchoring" is an argument that is often made by proponents of proof-of-work algorithms, who rightly point out that proof of work requires input that is external to the blockchain system, e.g. computer hardware and electricity. This can loosely be related to the Incompleteness Theorems by Austrian logician and mathematician Kurt Gödel, who showed that no system can prove its own consistency purely from within the system. Applying this logic to blockchains, the anchoring to an external reality improves a blockchain's robustness.

[14] many observers have pointed out that decentralization should follow a path, see for example https://a16z.com/2020/01/09/progressive-decentralization-crypto-product-management/