Quickbit

Decentralized Ledger and Mass Distributed Private Key Management

Ryan Condron

June 21, 2017

Draft Version 0.1

Table of Contents

The Quickbit Protocol

Abstract: Quickbit is a peer-to-peer protocol that passively extends the functionality of a blockchain network through the use of a decentralized side chain without the need for two-way pegging or predefined payment channels. Tokens can be seamlessly translated between blockchains and side chains while maintaining decentralization and anonymity.

Background

Back in 2014 Bitcoin entered a three year valley in the currency exchanges [1]. The community had just tasted its first hockey stick spike in price the previous winter and began to experience its first large dead cat bounce through the rest of the year. During this time massive amounts of scrutiny began to flood online forums and live conventions alike. People began to question the long term validity of the Bitcoin chain and several key shortcomings of the protocol were put in the spotlight.

The most prominent of these shortcomings remain unresolved at the time of this white paper and mainly revolve around the aspects of transaction speed and volume. Since each block on the Bitcoin blockchain currently has a maximum size of one megabyte the theoretical maximum rate of transactions is about ten every second [2]. Furthermore, due to the current block time of ten minutes, a user must wait on average around forty minutes for their transaction to fully confirm [3].

The final nail in the coffin is the rate of increase in popularity and in turn transaction demand. Since 2013 daily transaction volumes have roughly doubled each year [4]. This combination of low transaction volume, high confirmation times, and increasing popularity has driven transaction fees up to new all-time highs and has quickly proven that Bitcoin is just not cut out to be an everyday currency.

In late 2014, Blockstream introduced the new concept of “side chains” [5] that would create a way to offload transaction volume to another ledger and in effect bypass the Bitcoin network’s shortcomings. Unfortunately, to implement this ingenuitive concept the Bitcoin network would need to implement an extension to its transaction scripting via a soft-fork.

Around this time we began to brainstorm a better way that could passively extend any blockchain and thus Quickbit was born.

A New Approach

Our brainstorming went something like this:

Thought 1 (The concept):

> "To send a transaction you sign the funds with your private key and transfer it to someone else's public key at which point their private key now controls the funds…"

Thought 2 (The thesis):

> "I could just bypass this entire transaction workflow if I just give someone my private key… that way it would be instant and I wouldn't need to pay any fees."

Thoughts 3 - 4,961* (The delemma):

> "But how do I give someone a private key without retaining a copy of it myself?"

Thought 4,962* (The solution):

> "If the network controls the private keys then the network can facilitate exchanges in ownership in a side ledger."

** Actual number of thoughts was not properly recorded and therefore may have been exaggerated for effect*

The core innovative concept that we propose through Quickbit is that of mass distributed private key management.

Private Key Generation

For the proposed solution to work each node on the Quickbit network must be assigned and track ownership of parent chain public addresses without ever having full control of the private keys behind them.

The current proposed workflow is as follows, but may be altered over time to overcome unforeseen fallbacks and to increase security.

Proposed Private Key Generation Workflow:

Bitcoin (BTC) parent chain & Quickbit (Qb) side chain

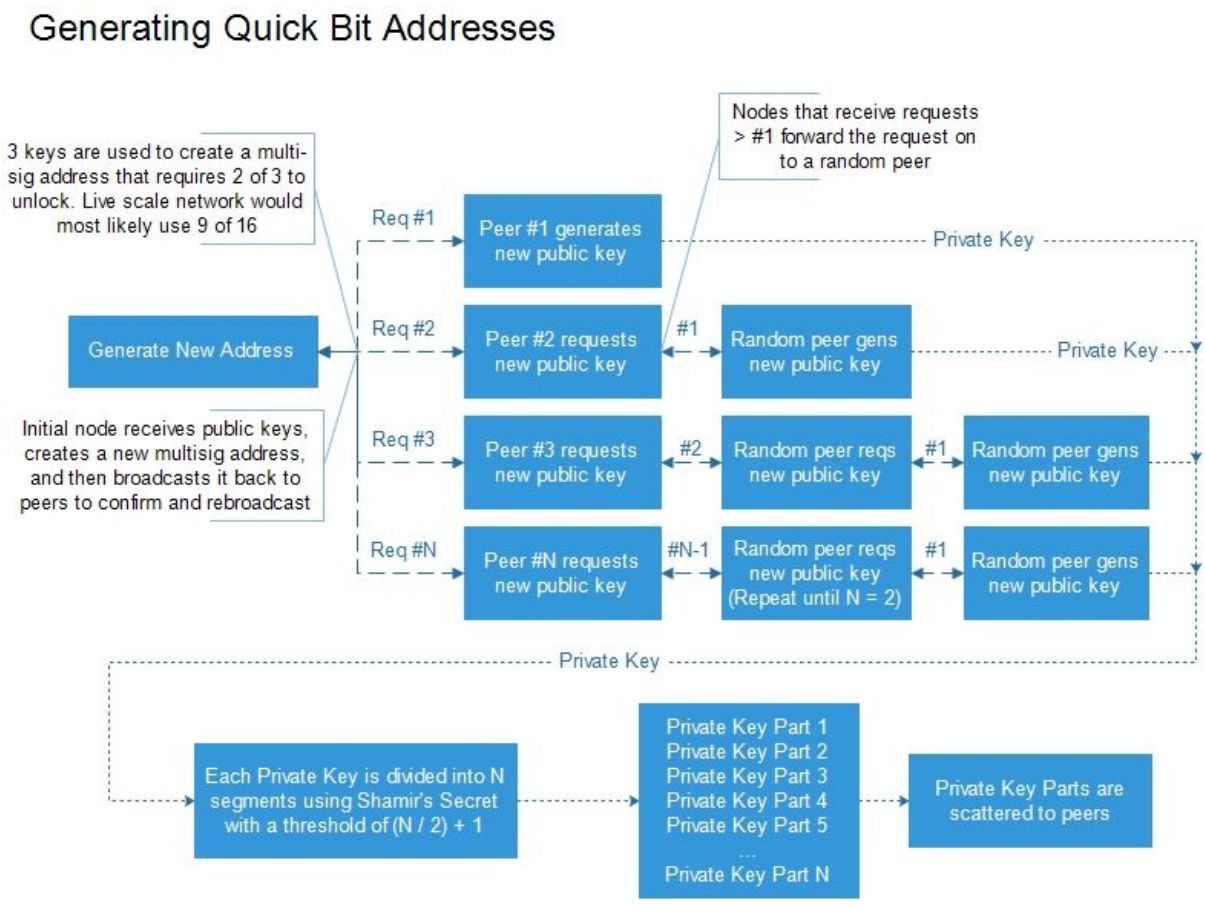
“Generation Address” - a parent chain address used to deposit/withdrawal tokens to/from a side chain.

N - a number that will increase with the size of the Quickbit network.

Shamir’s Secret - is an algorithm in cryptography where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret [5].

Qb Node Command: Create Generation Address

Qb node creates a new Qb private key and broadcasts its Qb public key address along with the BTC address request to *N* Qb peers.



As seen in the diagram above each peer will receive a request along with directions on how many times to pass the request. This way as the Qb network grows private key generation and distribution will become more and more secure.

Each BTC private key shard is stored with a unique identifier that consists of a reference to the BTC private key the shard is a part of and the Qb public key that it belongs to.

Transaction Signing & Consensus

Bitcoin (BTC) parent chain & Quickbit (Qb) side chain

Qb nodes will only store private key shards that are given to them and will not broadcast these shards. This provision will create a clustered network effect around the private key shards and in turn make validating and broadcasting transactions a “node cluster” process.

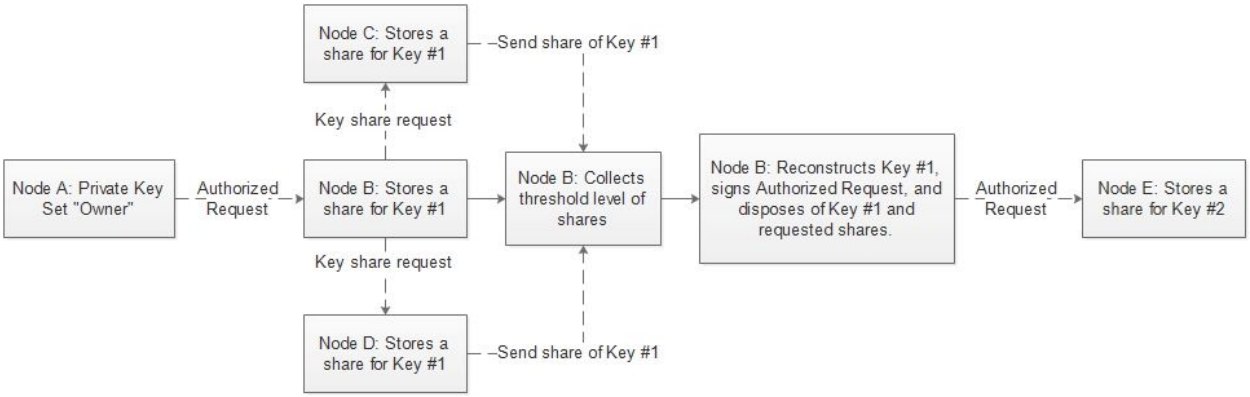
For a transaction to be valid on the BTC network it must be signed by the majority of the private keys in the BTC multisig address. To reconstruct a private key a single node must first confirm that the unsigned or partially signed transaction is valid on the Qb network* and then must acquire the needed amount of private key shares from peers in the node cluster. Once the private key is reconstructed the node will sign the transaction and rebroadcast it. The signing node will then dispose of the private key and any unowned shards. Next the signing node will record the transaction in its own shard ledger and broadcast the transaction to each node that supplied a shard to do the same.
The signing node will be eligible to collect a portion of the transaction fee for its services in acting as a “notary” when the transaction is added to the blockchain.

** To be valid on the Qb network a transaction must be signed by the Qb private key of the Qb public address that owns the funds, the transaction amount must not exceed the funds available, and the node must not have already signed a transaction for the same funds.*

In order to receive private key shards from its peers a node must prove that it holds a Qb signed transaction from the fund owner and a shard of the needed private key.

This process will repeat sequentially for each private keys until a valid signed BTC transaction is achieved. The final signing node broadcasts the completed transaction to the Qb network and to the BTC network. This workflow only takes place if an “output” address in the transaction is not registered on the Qb network (Qb managed private

keys). This process is called a withdrawal transaction and essentially destroys the Quickbit tokens sent to that output.



Since each node in a cluster acts as an transaction authenticator the initial confirmation of a transaction happens at the cluster level before it is even recorded on the blockchain. Because of this, transactions can be considered securely confirmed within seconds. Once a transaction is included in the blockchain each node will purge any shard ledger entries for that transaction and thereby freeing up the funds to be sent by the new owner.

Double Spend Scenario:
In the event of a double spend, the transaction that receives the majority of the signatures first will prevail. If a node receives a transaction for already sworn funds the transaction will be deleted. Since the protocol will process key signings sequentially the event of a signature race is highly unlikely.

Auditing and Risk Avoidance

One of the main risks of decentralized key management is losing key shards due to unreliable network nodes. To counteract this risk we propose an auditing algorithm that runs periodically to check the percentage of available shards for each key.

If the percentage of available shards reaches a lower threshold each node with an endangered shard will automatically divide up its shard using Shamir's Secret [6] into sub-shards and then scatter them among peers not already in the cluster.

This technique of creating and scattering sub-shards will create a deceleration effect making it exponentially less likely that a private key will ever be lost and even less that a multisig address would ever become unredeemable.

The Quickbit Network

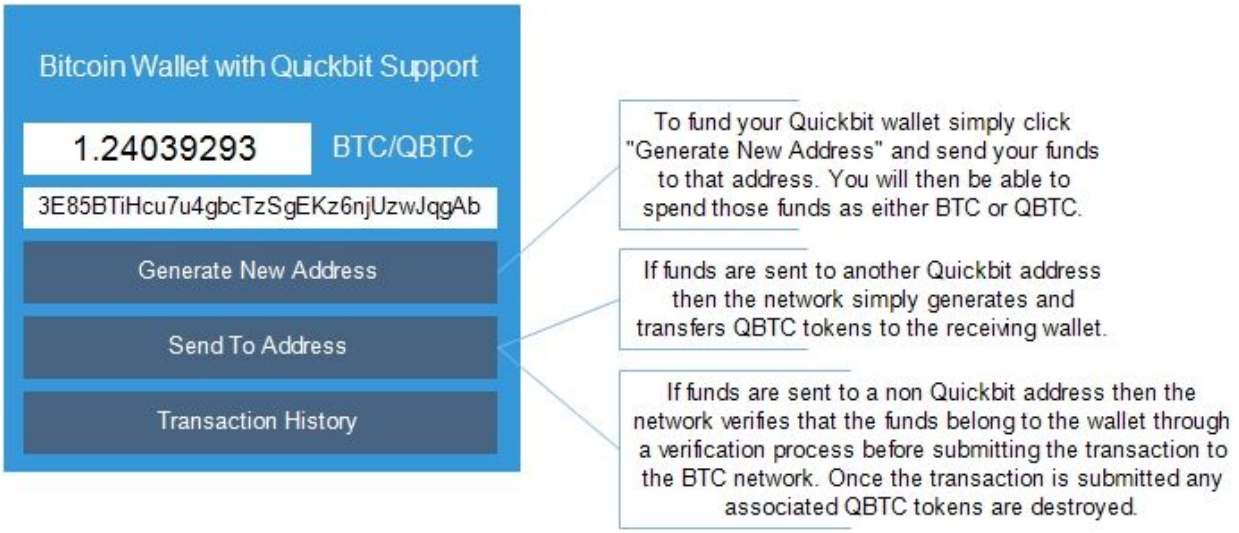
Now that we have laid out the basics of the Quickbit protocol let's dive into more details about the actual Quickbit network.

The Quickbit Token (QBTC)

In many countries gold was used as a currency for everyday commerce, but as gold grew in value it was necessary to create a commodity-backed currency to fulfill the need for smaller transactions [7]. Quickbit (QBTC) is a digital currency that is backed by Bitcoin. One QBTC is equal to one Satoshi (.00000001 BTC). QBTC does not fluctuate in value in relation to BTC like other cryptocurrencies and can be freely converted to and from BTC seamlessly through the Quickbit protocol.

If the value of 1 BTC was equal to $100,000 USD then 1 Satoshi or 1 QBTC would be worth $0.01 USD. This ratio will give BTC a lot of room to grow before QBTC ever comes close to not being viable for micro-transactions.

The core of the Quickbit network is essentially a ledger of shared Bitcoin addresses that keeps track of what amount of QBTC each Quickbit wallet owns.



Quickbit Transaction

In a Quickbit network there are three types of transactions: deposits, transfers, and withdrawals.

- Deposit: Moving tokens in a parent chain into a Quickbit controlled parent chain address and generating new Quickbit tokens on a side chain in a predefined ratio.

- Transfer: Moving Quickbit tokens from one Quickbit controlled parent chain address to another Quickbit controlled parent chain address.

- Withdrawal: Moving parent chain tokens from a Quickbit controlled parent chain address to an uncontrolled parent chain address and destroying the associated Quickbit tokens on the side chain in a predefined ratio.

Deposit Workflow

Bitcoin (BTC) parent chain & Quickbit (Qb) side chain

Once a Qb node requests a BTC multisig address from the Qb network the Qb node then monitors the BTC chain for transactions on the new BTC address. When a new confirmed BTC transaction is received the Qb node creates a new signed Qb generation transaction indicating the BTC transaction Id, BTC address, Qb address, and the amount of the transaction. This new generation transaction is then broadcasted to the Qb network, confirmed by receiving nodes, and hashed into a block. Once the transaction is recorded in the Qb blockchain the node that generated the funds will reflect the new QBTC balance per the established ratio.

When a node “confirms” a generation transaction broadcasted to it the node checks for accuracy if the transaction against the BTC chain and confirms that the signer of the transaction is in fact the owner of the Qb address that the BTC address was created for.

Transfer Workflow

Bitcoin (BTC) parent chain & Quickbit (Qb) side chain

Transfer transactions are internal transactions that happen between two Quickbit controlled BTC addresses. Since the tokens are being transferred “in-network” there is no transaction broadcasted to the parent chain. Transfer transactions are created and executed on the Quickbit network in a very similar manner to that of other chains, and therefore there is no need to explain the workflow in detail.

Withdrawal Workflow

Bitcoin (BTC) parent chain & Quickbit (Qb) side chain

A Quickbit withdrawal transactions removes tokens from the Quickbit network and sends them on the parent chain in a predefined ratio. Withdrawal transactions are subject to parent blockchain confirmation times and transaction fees. The withdrawal workflow is described extensively in the section entitled “Transaction Signing & Consensus”.

Blockchain: Weighted Proof of Stake

Proof-of-stake (PoS) is a consensus algorithm that uses each node’s quantity (and in some implementations, age) of tokens to determine its block creation difficulty. [8]

> “Peercoin's proof-of-stake system combines randomization with the concept of ‘coin age’, a number derived from the product of the number of coins times the number of days the coins have been held. Coins that have been unspent for at least 30 days begin competing for the next block. Older and larger sets of coins have a greater probability of signing the next block. However, once a stake of coins has been used to sign a block, they must start over with zero ‘coin age’ and thus wait at least 30 more days before signing another block. Also, the probability of finding the next block reaches a maximum after 90 days in order to prevent very old or very large collections of stakes from dominating the blockchain.” [9]

Quickbit will utilize a PoS algorithm for its blockchain that is weighted not only by the age of the QBTC tokens but also the amount of Quickbit share tokens (XQBS) a node controls. Further details of the specific PoS algorithm are still being determined and will likely transform as development progresses.

For more information about XQBS and how it will relate to the Quickbit network read the section entitled “Quickbit Network Token: Quickbit Shares (XQBS)”.

Acknowledgement of Risks

Both the Quickbit protocol and Quickbit network have inherent risks associated with the proposed technological methods. The bulk of these risks revolve around the development of key shard distribution, management, and storage protocols. Other risks include scaling issues, withdrawal transaction complexity, and malicious nodes.

Key Shard Risks

To the best of our knowledge at the time of this white paper there are no decentralized systems that manage distributed private key storage. The very premise of sharing private keys across a p2p network seems rather ludicrous at first, but we believe in combination with multisig addresses that this type of system will prove to be both safe and reliable at scale.

For shared key storage to work properly and securely we must be able to ensure that each node stores unique shards, shards are not shared with unauthorized requesters, and no single node can store more than one shard of any given private key.

Withdrawal Transaction Complexity

Another possible risk is that of overly complex withdrawal transactions. The longer QBTC funds stay “in-network” the more scrambled a given node’s collection of funds will become. A node could potentially end up controlling a few Satoshi from thousands of different Bitcoin multisig addresses. If the user attempts to withdrawal the full balance of their funds the resulting withdrawal transaction would be incredibly large and its correlated fees may be greatly inflated. While we don’t have a specific solution for this given scenario yet, we do have several ideas for solutions that will need to be tested.

The Quickbit Foundation

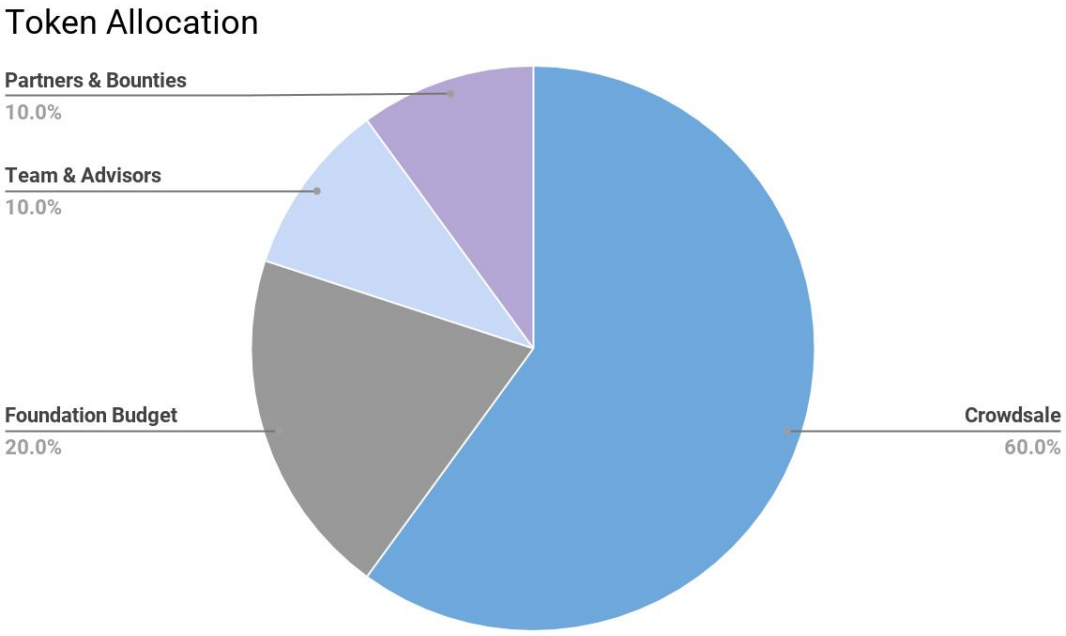
The Quickbit Foundation will be a non-profit entity formed with the objectives of overseeing and managing protocol development, community relations, and industry adoption. By contributing to the Quickbit Foundation through donation or participation in an initial coin offering (ICO), contributors are supporting these objectives.

All contributors represent and warrant that they are not exchanging bitcoin (BTC) or any other crypto-currency or capital for Quickbit tokens for the purpose of speculative investment. Furthermore all contributors represent and warrant that they are acquiring Quickbit tokens to help facilitate development of the Quickbit protocol, build the Quickbit community, or aid in the industry adoption of a Quickbit network.

Quickbit Network Token: Quickbit Shares (XQBS)

The Quickbit network token will be called “Quickbit Shares” (XQBS). The token will be generated and released through the Counterparty protocol [10].

A total of 21 million XQBS tokens will be generated and the cost of each token will be defined by the total amount raised. Once the crowdsale is over tokens will be divided among contributors in ratio to their contribution.



XQBS tokens will play a very important part in securing the Quickbit network. Nodes that control XQBS tokens will be considered more reliable and therefore benefit in the following two key areas: PoS stake calculations and private key shard storage capacity.

XQBS PoS Multiplier

XQBS Tokens will act as a 0.1 multiplier to a nodes QBTC balance.

Example:

Node 'A' controls **10** QBTC and **1** XQBS. ***10 x (1 + (1 x 0.1)) = 11 stake***
Node 'B' controls **10** QBTC and **5** XQBS. ***10 x (1 + (5 x 0.1)) = 15 stake***

And just for kicks:

Node 'C' controls **10** QBTC and **5,000** XQBS. ***10 x (1 + (5000 x 0.1)) = 5,010 stake***

Nodes with XQBS tokens will have the highest likelihood of solving blocks and in turn a greater probability of regularly collecting transaction fees. This benefit will cause nodes staking with XQBS to mimic the behavior of an interest bearing savings account.

Private Key Shard Storage Capacity

All nodes with a QBTC balance by default will be able to store key shards to help secure the network; however, there will be a limitation to how many shards a single node can store. XQBS tokens will increase this limit allowing nodes to store significantly more shards.

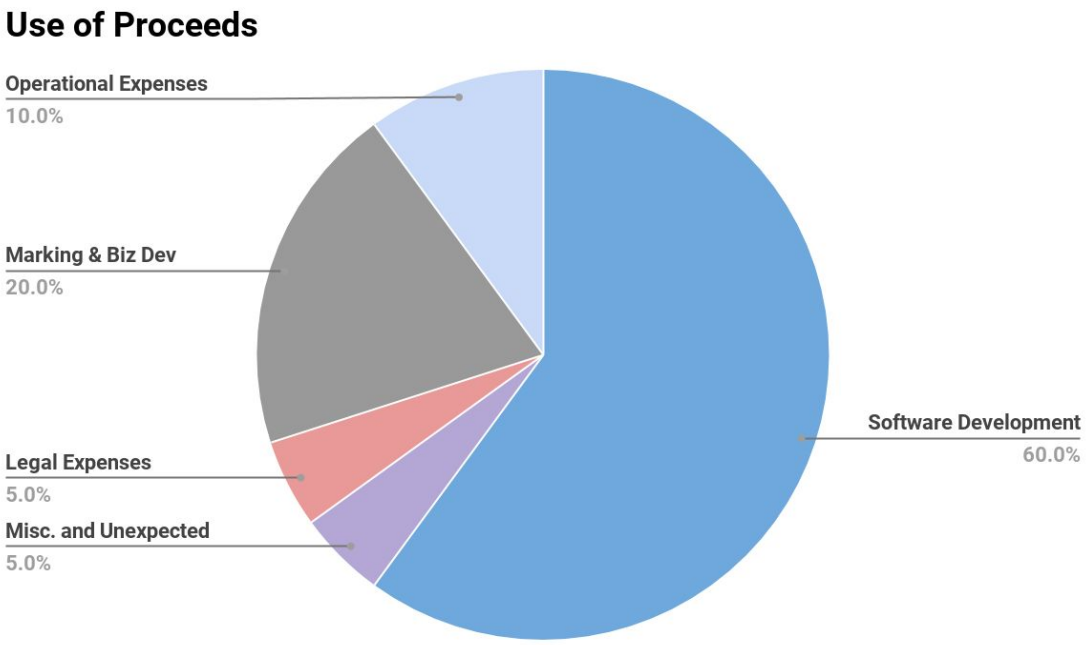
Every node that signs a transaction with a reconstructed key will collect a small amount of the transaction fee as payment for its notary services. Since a node must store a key's shard to be eligible to act as the notary, the capacity of a node's shard storage will directly affect its profit potential. While details of the exact storage limitations and XQBS capacity benefits are still being worked out, we believe this aspect of the token will greatly increase network security and node reliability.

XQBS Crowdsale Objectives

- A portion of the funds raised will be used to fund protocol development and implementation, development of support related technologies and applications such as user-friendly wallets (desktop and mobile), ATM kiosks, or point of sale terminals, and technology and partnership acquisitions.

- A portion of the funds raised will be used to cover Quickbit foundation objectives and legal costs in areas which will include marketing, government applications, and organizational management.

- A portion of the funds raised will be used to support community development and open-source application initiatives built around the Quickbit protocol. These may include activities such as hosting hack-a-thons, participating in conventions, or sponsoring other initiatives in the cryptocurrency community.



Summary

The Quickbit protocol can extend any blockchain seamlessly creating a fully anonymous, distributed, and secure side chain layer. The Quickbit protocol provides this functionality through the use of parent chain multisig addresses, mass distributed private key management, and custom proof of stake algorithms. The focus of the Quickbit foundation will be to build the Quickbit protocol and implement it as an easy to use peer to peer currency network backed by Bitcoin. The foundation will issue a token to help secure the network by using it to identify reliable and trustworthy nodes. This protocol proposes the first passive solution to any blockchain's transaction volume limitations, block time constraints, micro transaction limitations, and node identity exposures.

[1] https://blockchain.info/charts/market-price?timespan=all
[2] https://en.bitcoin.it/wiki/Maximum_transaction_rate
[3] https://www.theverge.com/2016/3/2/11146584/bitcoin-core-classic-debate-transaction-limit-crisis
[4] https://blockchain.info/charts/n-transactions?timespan=all
[5] https://blockstream.com/sidechains.pdf
[6] https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing
[7] https://en.wikipedia.org/wiki/Monetary_system
[8] https://peercoin.net/assets/paper/peercoin-paper.pdf
[9] https://en.wikipedia.org/wiki/Proof-of-stake
[10] https://counterparty.io