CIRCLERESEARCH

Analyst: Mrinalini Bhutoria (Ria) (@riabhutoria)

Updated: 9 August 2018

Qtum (QTUM)

Price

$5.25

Avg. Daily Traded Volume (30D)

$158b

Market Cap

$466m

Project Announced

March 2017

Consensus mechanism

Proof of Stake

Nodes	Transactions per second (tps)
~6,300	70 tps

Block height	Developer Team
>205,000	~30 developers

Telegram followers

~13,100

Source:
onchainfx.com,
qtum.info

Date:
As of 08/08/18 at 05:05PM ET

The Qtum (pronounced Quantum) blockchain is a public smart contract platform that combines aspects of Bitcoin with aspects of Ethereum.

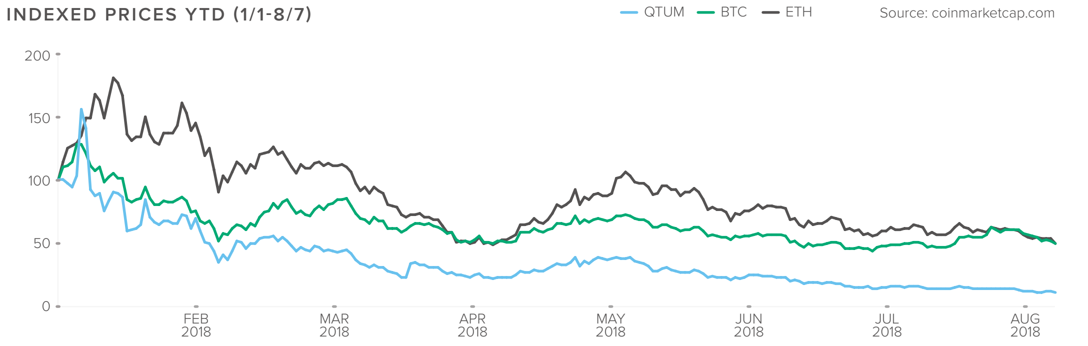
Qtum was founded by Patrick Dai, Neil Mahi, and Jordan Earls. Prior to founding Qtum, Patrick Dai was employed by Alibaba and has been involved in the space since 2012. Neil Mahi has 20 years of software development experience. He has been involved in the space for four years.

Qtum chose Bitcoin core as the base because the team believes that Bitcoin is the most mature, secure, and stable blockchain. However, Bitcoin cannot run Turing complete code needed to build smart contracts. Thus, Qtum integrated EVM and will integrate additional VMs capable of supporting dApp development.

Bitcoin uses a UTXO model and EVM - and most other VMs - use an account-based model for simplicity. In order to make virtual machines with the account-based model compatible with Bitcoin's UTXO model, Qtum had to place a conversion layer in between. This layer is called the account abstraction layer (AAL).

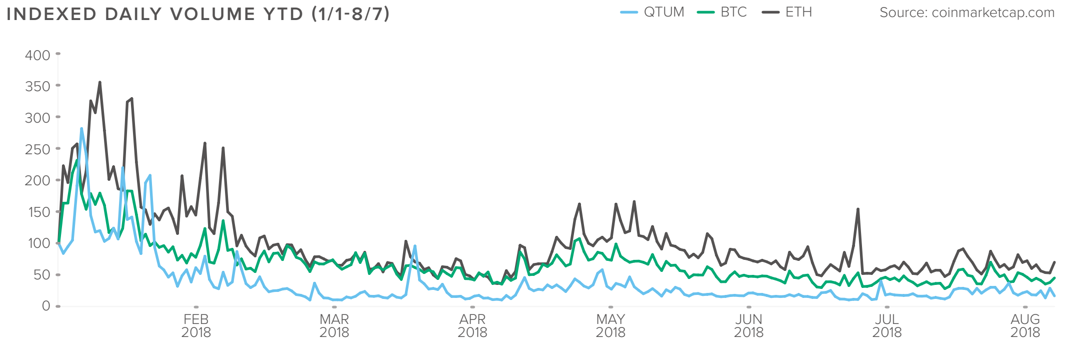
Using Bitcoin core code allows Qtum to integrate developments in Bitcoin. The EVM integration allows Ethereum developers to port dApps built on Ethereum to Qtum since both platforms use the same virtual machine (though it is unclear if any have done so). Qtum also recently announced plans to integrate X86VM, which would allow developers to build dApps in non-blockchain programming languages.

INDEXED PRICES YTD (1/1-8/7)



Source: coinmarketcap.com

INDEXED DAILY VOLUME YTD (1/1-8/7)



Source: coinmarketcap.com

Additional Resources

→ Website
→ Whitepaper
→ Twitter
→ Github

Consensus

Qtum uses an adaptation of Blackcoin's version of proof of stake (PoS 3.0) to reach consensus. Bitcoin and Ethereum currently use PoW, but Ethereum is working on transitioning to PoS.

Governance

Qtum uses a Decentralized Governance Protocol (DGP) that is meant to decentralize decision making and allow the community to modify a number of parameters if it requires these parameters to be changed. These include block size and base gas fee, among others. The Qtum Foundation is responsible for development and promotion of the Qtum blockchain.

Other features

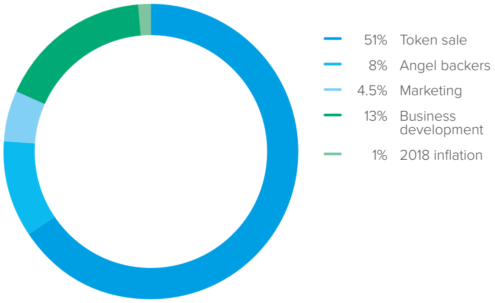
Qtum allows for "master contracts", Qtum's name for smart contracts that can be triggered by off-chain data. Qtum also provides smart contract execution on light clients (mobile and IoT devices), among other things.

Token sale

Qtum sold 51% of the total supply of tokens for $15 million in the token sale, which took place in March 2017. Prior to the token sale, Qtum received an initial round of funding from Anthony Di Iorio. Qtum has an annual inflation of 1% and the maximum supply as determined by the team is 107 million. The current circulating supply as outlined by the team is ~88.5 million tokens.

TOTAL SUPPLY OF TOKEN

Source: blog.qtum.org



UTXO VS ACCOUNT MODEL

UTXO model

Bitcoin uses the unspent transaction output (UTXO) model. This model can be compared to using coins and bills to pay (versus using a credit or debit card). For example, Alice wants to buy a $30 shirt but she has two $20 bills. She can't just give the merchant one and a half bills. Rather, she gives the merchant both bills and receives a $10 bill back as change.

The UTXO model functions in a similar way: Alice has two transaction outputs of 1 BTC and 0.5 BTC from prior transactions. Alice needs to pay a merchant 1.3 BTC. She sends out 1.5 BTC and her wallet creates two new transaction outputs. The merchant receives 1.3 BTC and Alice receives 0.2 BTC back as change (less transaction fees). Bitcoin users can check the block explorer and will notice that their bitcoin address often sends a higher amount of bitcoin than specified.

Account model

Ethereum's account based model is similar to a bank account model. The total funds of an account are pooled together to form a single balance. Every transaction uses the exact amount needed - there is no need for change. For example, Alice has $40 in her account and wants to buy a shirt for $30. She sends the merchant exactly $30. Now she has $10 in her account.

One reason Qtum chose bitcoin core as its base is to use the UTXO accounting model. The Qtum team

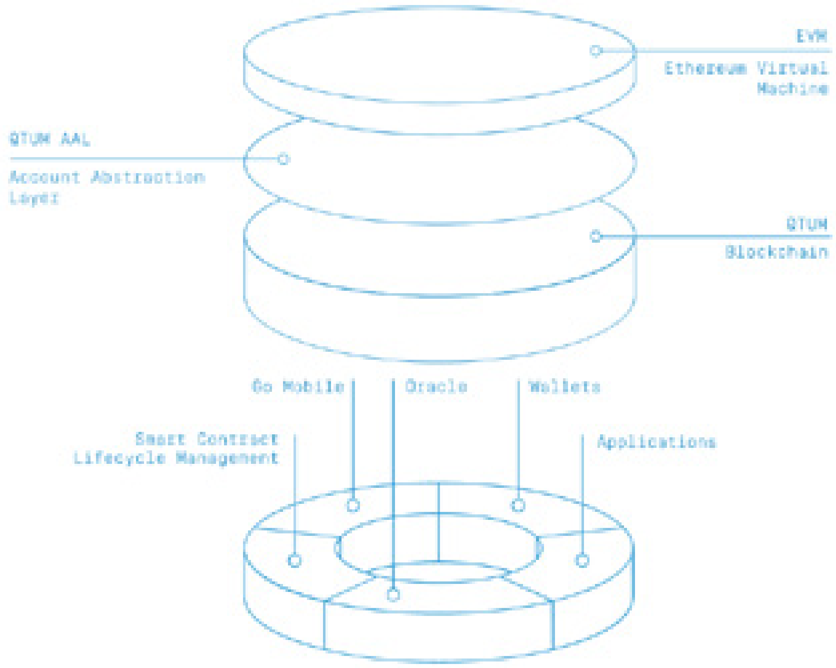
[1] Ethereum uses transaction nonces to protect the network against replay and double spend attacks.

believes that the UTXO model offers greater protection against replay and double spend attacks by requiring each output to only be spent once[1] and offers greater scalability from transactions being processed in parallel because each transaction uses independent outputs. While UTXO works for currency use cases, it is not seamless or practical for smart contract use cases. The account-based model is more simple and flexible, and easier for developers to code when building smart contracts and dApps.

Account abstraction layer (AAL)

From a developer's point of view, it is not trivial to convert UTXOs to accounts. Qtum uses AAL to integrate the UTXO and account models. AAL is an interpretation layer developed by Qtum that translates UTXOs to accounts. With AAL, Qtum can use a consensus model based on UTXOs while presenting an account-based system to virtual machines running smart contracts. This allows developers building on Qtum to treat Qtum as they would Ethereum.

QTUM



Source: en.bitcoinwiki.org

CONSENSUS

Qtum uses an adaptation of Blackcoin's version of proof-of-stake protocol (PoS 3.0) to secure the network and achieve consensus. In short, validators stake tokens (i.e. lock up tokens in escrow) in order to validate transactions and produce blocks. The likelihood of being chosen to produce a block is proportional to staked tokens as a percent of total tokens in circulation. If participants are dishonest and try to game the system, PoS aims to punish them by confiscating some or all of the coins staked.

In Qtum's version of PoS, there is no minimum staking requirement to increase decentralization by encouraging participation in consensus. The challenge is that participants with less at stake also have less of an incentive to be honest if the payoff from being dishonest is greater than the punishment. Qtum incorporates coin maturity to make it challenging for bad actors to launch an attack. Coins must be "mature" (at least 500 blocks deep) to participate in staking and block production.

In PoW, miners uses electricity to calculate a hash that meets the network's difficulty conditions, allowing the miner to produce a block and win a block reward. In PoS, participants stake their coins to create a kernel hash. The pieces of data needed for the kernel hash are not readily modifiable.The greater the participant's stake, the greater the chance that the kernel will match a random seed created by the blockchain based on data from prior blocks (aka the “staking difficulty”). A participant’s seed is the base difficulty reduced by the ratio of coins staked. The base difficulty applies to one coin. Simply put, if two coins are staked, the difficulty is half of the base. If four coins are staked, the difficulty is a quarter of the base, and so on. However, there is a limit to how much the base difficulty can be reduced. The kernel that most closely matches the seed wins the right to create a block.

Qtum’s reasoning for choosing PoS (and the reasoning of many crypto projects using or planning to use PoS) is that PoW is energy intensive, wasteful and unsustainable. While the energy usage of the network has significantly increased since 2009 when it went live, the throughput of the network has stayed the same (by design). Further, while both PoS and PoW have centralization risks, centralization is arguably more difficult to dislodge in PoW because the probability of winning accrues to the largest mining pools with superior hardware.

In Qtum, a 2 MB block is produced every 120 seconds (or two minutes). The inflation is currently set to 1% per year and is designed to halve every four years for thirty-two years. The circulating supply is ~88.5 million, at the time of writing, and the maximum supply is expected to be ~107 million.

The current block reward is 4 QTUM tokens. 0.4 QTUM is rewarded at the time the block is created. This amount is locked up until it is mature (500 blocks). The remaining 3.6 QTUM are added over 9 blocks after the initial 0.4 reward has matured. Qtum uses the lock-up and delayed reward as a safety feature to make it difficult for a bad actor to attack the network. The chart below shows how the block reward is distributed over time.

Block	Block reward staked	Block reward mature	Total block reward received
5	0.4		0.4
6	0.4		0.4
7	0.4		0.4
...	0.4		0.4
506		0.4	0.4
507	0.4	0.4	0.8
508	0.8	0.4	1.2
509	1.2	0.4	1.6
510	1.6	0.4	2
511	2	0.4	2.4
512	2.4	0.4	2.8
513	2.8	0.4	3.2
514	3.2	0.4	3.6
515	3.6	0.4	4
...			
1008	3.2	0.8	4
1009	2.8	1.2	4
1010	2.4	1.6	4
1011	2	2	4
1012	1.6	2.4	4
1013	1.2	2.8	4
1014	0.8	3.2	4
1015	0.4	3.6	4
1016	0	4	4

Source: https://medium.com/@jb395official

Security - Gas

Like Ethereum, Qtum uses gas to deter bad actors from spamming the network by making it expensive. Flooding the network with fake transactions would fill up blocks and prevent the inclusion and verification of legitimate transactions. Gas is denominated in Qtum satoshis, the lowest unit of Qtum (0.00000001 Qtum). If the price of Qtum falls to a point where it is cheap to flood the network, the base cost (40 Qtum satoshis) can be adjusted to increase the fee and make it sufficiently expensive to attack. If the Qtum token price rises and gas becomes prohibitively high, the base cost can be adjusted down to lower the fee. Qtum plans to use DGP as the mechanism to implement such changes to the minimum cost of gas, though the Qtum team monitors it for now. The challenge Qtum will face as it grows is ensuring that gas limits and rising prices don’t make it impractical to deploy complex smart contracts.

VIRTUAL MACHINES

Qtum offers support for EVM and recently announced that it will launch a second virtual machine known as X86VM. By running EVM, Qtum offers developers the ability to create QRC-20 tokens (identical to ERC-20 tokens, but on the Qtum blockchain). A few of these projects are highlighted below. However, Qtum claims that AAL allows Qtum to integrate any number of virtual machines. Qtum recognizes that EVM and the programming language it uses (Solidity) were developed with some major design flaws and a lack of sufficient verification tools.

Thus, Qtum is developing Qtum X86VM to allow developers versed in more mainstream, and tested non-blockchain specific programming languages like C, C++, Rust, Python, etc. to build dApps on Qtum. The process for implementing X86 is that Qtum will first launch a public testnet and deploy a bug bounty program and collect feedback for a number of months before rolling out a mainnet version. According to the team, Qtum can integrate any number of virtual machines on top of the AAL. The challenge X86 introduces if and when it is implemented is how difficult will it be to provide formal verification support for multiple programming languages.

GOVERNANCE

Qtum has developed an on-chain Decentralized Governance Protocol (DGP) for carrying out changes to a limited set of parameters. However, Qtum will also use hard and soft forks (off-chain effort) when needed, but only for adding new features (such as X86VM) or implementing more significant changes that cannot be implemented without forking.

Items under the purview of DGP include block size and the base cost of gas, among other parameters that are not publicly defined. Qtum plans to use DGP to prevent disrupting the network via forking so long as it is safe and makes sense[2]. The four steps of the DGP are as follows:

1. A stakeholder group creates a proposal for changing parameters.
2. All stakeholder groups then vote for or against the proposal.
3. The proposal is accepted (and implemented) or rejected.
4. The proposal data is archived.

Stakeholders can be divided in multiple ways - by industry or vertical (financial services, healthcare, supply chain, etc.), by user group (users, developers, block producers, etc.), by region (Americas, Europe, Asia, Africa, etc.) and more. Regardless of the way they are segmented, different groups will likely have different needs and interests and should have equal representation, according to Qtum.

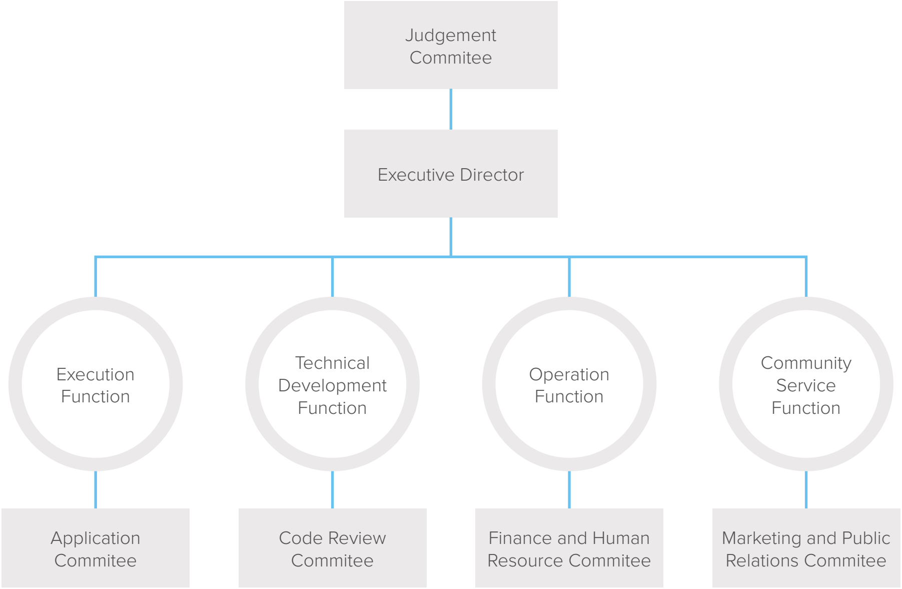
Therefore, Qtum might implement a system whereby each group of stakeholders can vote for a governing party to represent them in making decisions about the future of the platform. If a such a democratic structure is implemented, Qtum will have to create an accompanying voting mechanism. At this time, there is limited information on the exact mechanism and structure Qtum will use.

Qtum Foundation

The Qtum Blockchain Foundation is a not-for-profit organization based in Singapore. The core mission of the Qtum Foundation will be to develop and enhance the codebase and promote the use of the Qtum blockchain. The Foundation has a Judgement Committee and four subcommittees (Application, Code Review, Finance & Human Resource, and Marketing & PR).

When Qtum launched, it released a whitepaper with the help of PWC that outlined the functions and responsibilities of the Foundation and its respective committees. That whitepaper has since been hidden, since much of the information about the Foundation's functions and members is stale and inaccurate. The team has said that it plans on sharing a new whitepaper with updated information at some point. Qtum plans to use open elections to allow tokenholders to elect members into each committee.

[2] A fork requires stakeholders to download new software or upgrade their version of the protocol, which interrupts normal operations, though it is sometimes necessary.


Judgement Commitee
Executive Director
Execution Function
Technical Development Function
Operation Function
Community Service Function
Application Commitee
Code Review Commitee
Finance and Human Resource Commitee
Marketing and Public Relations Commitee

Subcommittees

- The Application Committee was created to identify industries best suited for implementing the Qtum blockchain.
- The Code Review Committee comprises core developers and was created for API, product, and technology development.
- The Finance and Human Resource Committee was created to monitor project finances and operating expenses, set developer compensation, recruit, etc.
- The Marketing and Public Relations Committee was created to promote Qtum, make announcements, and respond to public affairs.

FEATURES

Compatibility - Account Abstraction Layer & Opcodes

In order to merge bitcoin's UTXO model with EVM, Qtum had to develop the account abstraction layer (AAL). The AAL converts UTXOs into accounts for developers building dApps on EVM so they don't have to program smart contracts to pick their own outputs. Thus, Qtum has added a consensus-critical coin picking algorithm for all contracts to use. The technical details of how Qtum converts UTXOs to an account based model are beyond the scope of this report. Although the initial purpose of AAL was to integrate Qtum's underlying UTXO-based blockchain with the EVM, it enables integration of additional virtual machines as well. X86VM is next in the pipeline. AAL is also designed to make it easy for developers to port smart contracts built on Ethereum to the Qtum blockchain and vice versa. In addition, Qtum enables the refund of unspent gas fees despite using a UTXO model. Getting a refund of unspent gas fees works on Ethereum because it doesn't use a UTXO model.

Another tool needed to integrate EVM is opcodes. An opcode is the part of a line of code that defines what operation needs to be performed. Qtum uses Bitcoin's scripting language and added three new opcodes that (along with AAL) enables smart contracts.

Light Clients - Simple Payment Verification

As mentioned above, one reason Qtum chose bitcoin core and the UTXO model as its base was to use SPV (Simple Payment Verification). SPV allows a light client to execute smart contracts without downloading the entire blockchain - block headers are sufficient for verification. Light clients refer to mobile phones, tablets, IoT devices, etc. In the context of Qtum, SPV allows light clients to interact with smart contracts and dApps without downloading the entire blockchain. One challenge is that light client transactions in Qtum are limited to transfers of the native Qtum token.

When Qtum launched, the team believed light client execution of smart contracts was a differentiating factor. Since then, new projects have launched that offer similar functionality. Further, the Ethereum community has published research that shows that the UTXO model isn't needed for enabling smart contracts to execute on light clients. Ethereum is also working on solutions such that light clients are not limited to executing transactions in the native ETH token (i.e. they can execute smart contracts associated with ERC20 tokens).

Real world - Data Feeds, Oracles, Master Contracts

Blockchains don't have direct access to off chain information, but they need a way to validate the conditions that smart contracts are based on. Qtum is using data feeds and oracles to allow blockchains to use real world data to trigger smart contracts, which Qtum calls master contracts.

Data feeds refer to data collected from off-chain sources. Examples include FX rates, temperature, pricing data, etc. In the whitepaper, Qtum gives the example of the temperature as measured by a thermometer dropping below 55 degrees F, which could in turn automatically trigger the heating. In this example, the temperature is the off-chain (or real world) data feed.

Oracles refer to a trusted organization, entity, node in charge of selecting the most accurate data to be the input for a smart contract when there are multiple data sources reporting on the same topic.

Master contracts are Qtum's name for smart contracts that use both on and off chain data. Smart contracts are triggered by the occurrence of some predefined event. Through its use of data feeds and oracles, Qtum provides a way for developers to build smart contracts that use real world data.

Compatibility - Bitcoin Improvement Proposals

Running bitcoin core code allows Qtum to incorporate network updates such as Segwit, Lightning Network, and future Bitcoin Improvement Proposals. Segwit is activated on Qtum, though participants haven't had a need to use it yet. Qtum has built a prototype for Lightning Network, though it has not yet been implemented.

Enterprise - Qtum X

Qtum announced Qtum X in May 2018. Qtum X is a private blockchain designed for enterprises. All that is known at the moment is that the system will use proof of authority as its consensus mechanism to enable higher transactions per second. Qtum X is separate from Qtum and we do not know if the two will be interoperable (i.e. if the Qtum token will be used on both platforms).

PROJECTS BUILDING ON QTUM

At the time of writing, there are about thirty dApps building on Qtum. Specific industries the team has highlighted include financial services, supply chain, digital media, and especially IoT. The team has mentioned that Qtum is involved in the Trusted IoT Alliance, but it is unclear if the Qtum blockchain is actually being used for IoT applications right now. A few other dApps across multiple use cases are outlined below.

Name	Description	Stage
HalalChain	Supply chain	Demo
Ink	Art	Prototype
Bodhi	Prediction markets	Prototype
Luna	Dating app	Prototype
Vevue	P2P video network	Live
Qbao	Social Network	Live
HyperPay	Payments	Live
Energo	Energy trading platform	Live
Dedge	Mobile platform	Live
Bitclave	Search engine	Live
Medibloc	Healthcare records	NA
SpaceChain	Space exploration	NA
PlayCoin	Gaming	NA
Beechat	Encrypted messaging	NA
Datawallet	Data ownership	NA

RISKS & CHALLENGES

Qtum is complicated.

One criticism of Qtum is that it is overly complicated. It is a patchwork of Bitcoin's UTXO, Ethereum's EVM, Blackcoin's PoS, and its account abstraction layer. Piecing multiple pieces together like this could create additional points of attack, failure, or inefficiency, and dissuade developers from building on the platform.

Further, the team claims that developers would choose to build on Qtum because it provides the security of the UTXO model for the currency layer and the flexibility of smart contracts via the EVM. However, there is debate around whether UTXO actually provides significant security and privacy advantages over the account model. Further, EVM and the code that runs on EVM (Solidity) are known to have major design flaws and don't offer good verification tools.

Competition.

This brings us to competition. At this time, it is unclear if the incentive to build on Qtum over Ethereum is compelling enough. This could change if Qtum's X86VM provides enhanced security and flexibility over EVM, but we cannot make that call until we get more information about X86VM. All that is known about X86 right now is that it will enable development in multiple mainstream programming languages. However, Ethereum is simultaneously working on integrating the WASM (WebAssembly) virtual machine, which will provide support for mainstream programming languages like C, C++, Rust, etc. Competing platforms are also working on building out support for multiple programming languages via alternate virtual machines.

Further, about 83% of dApps are built on Ethereum right now, making it the dominant platform with a large community of developers. As far as we know, less than 1% of total dApps are built on Qtum. Although Ethereum may have scalability issues and uses PoW right now, the community is actively working on developing layer 1 and 2 scaling solutions (Sharding, Plasma, Raiden, state channels) and a Proof of Stake consensus protocol (Casper). DApp developers may choose to stay on Ethereum knowing that solutions are on the way.

Scalability.

Qtum is capable of processing 70tps (though actual tps is a lot lower at the moment). Although this is higher than Ethereum's 15-20tps and bitcoin's 3-5tps, it is lower than the throughput that competitors are promising (as high as thousands of transactions per second). Scalability tools that Qtum could deploy include Segwit (which is activated but there hasn't been a need to use it), Lightning Network (which is currently in prototype phase), and other scaling methods (but there is still uncertainty around if, when, and how these will be implemented). Qtum X plans to use Proof of Authority for higher throughput, but it will be a private blockchain.

Note on Lightning: By using bitcoin core code, Qtum benefits from implementations on the Bitcoin blockchain. One of these updates is the Lightning Network. One challenge with Lightning is that, at the moment, it only works with the native Qtum token. Nothing has been said about the team expanding the capability to non-native QRC-20 tokens.

On-chain governance uncertainty.

Qtum is still working on creating a fair voting mechanism for voting on issues governed by the DGP and voting for governing parties to represent different stakeholder groups. Eventually, Qtum claims that governing parties will participate in governance by submitting proposals around changes to network parameters. As a reminder, these governing parties will supposedly represent different stakeholder groups.

At this time, there is no information available about who the people in the governing parties will be, how they will be chosen, how they will be incentivized to implement their stakeholder group's wishes, or how they will be punished if they don't.

In addition, the team has not outlined how it plans to incentivize users participate and to vote for governing parties. The challenge of preventing participant complacency and making all stakeholders feel like their vote matters has been discussed at length in the community and there is no clear cut answer yet. The governing party structure also raises questions about collusion and centralization and its dangers to the continuity of the platform in the short and long run.

CONCLUSION

The Qtum blockchain project is still young and many facets need to be proven out. The X86VM won’t be implemented until late 2018, there is no concrete timeline for voting mechanism implementation, and there is little information about which on and off chain scaling solutions will be incorporated and how they will apply to non-native tokens. Further, governance, an important aspect of the evolution of dApp platforms, has yet to be ironed out and how it shapes up remains to be seen.

Disclosures

This report has been prepared solely for informative purposes and should not be the basis for making investment decisions or be construed as a recommendation to engage in investment transactions or be taken to suggest an investment strategy in respect of any financial instruments or the issuers thereof. This report has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research under the Market Abuse Regulation (EU) No 596/2014. Reports issued by Circle Internet Financial Limited ("Circle") or its affiliates are not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services and are not recommendations to buy, sell, or hold any asset. The information contained in this report is based on sources considered to be reliable, but not guaranteed, to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of this date, and are subject to change without notice. Circle will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents. Circle and its affiliates hold positions in digital assets and may now or in the future hold a position in the subject of this research.

Sources

news.8btc.com/qtum-introduce-master-contract-and-id-identification-option-into-blockchain

smithandcrown.com/sale/qtum-ico-building-first-utxo-proof-stake-smart-contract-platform/

Economy white paper - qtum.org/wp-content/uploads/2017/02/Qtum_blockchain_economy_whitepaper_20170217_EN.pdf

reddit.com/r/Qtum/comments/7d7mtj/response_to_vitaliks_thoughts_on_utxo_article/

smithandcrown.com/definition/unspent-transaction-outputs-utxo/

github.com/ethereum/wiki/wiki/Design-Rationale#accounts-and-not-utxos

forum.qtum.org/topic/86/what-is-utxo/3

blog.icoalert.com/the-ethereum-challengers-ep-6-qtum-qtum-d3278493c61d

blog.qtum.org/whats-the-difference-between-a-blockchain-currency-and-platform-dbd6a3d5a1c6

reddit.com/r/Qtum/comments/7ch7ze/qtumscalability_how_scalable_is_it_exactly_in/

seebitcoin.com/tag/proof-of-stake/

earlz.net/

medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-qtum-5f2e6daf798a