Business Review, 2020 Q1

A Q1 report on Dusk Network

Executive summary

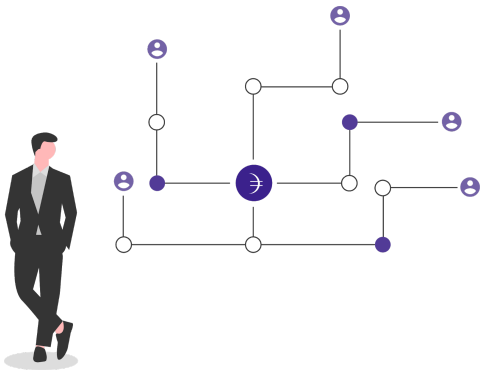
At Dusk Network we develop the privacy blockchain for financial applications. This relies heavily on our zero-knowledge proof system (PLONK), which has been the subject of fine-tuning and optimization in this quarter. Commercial initiatives on Dusk Network include the Firm24 Cap Table Management use case, preparation of the 2Tokens fundraiser, and ongoing development of our upcoming Stock Exchange. In order to meet industry demand, we are putting into place a Node Partner Programme, allowing companies to set-up a full Node with our support. As per Q1 2020, available company assets total USD 6.2M. Even in our most conservative scenarios, this means that we will be developing at full steam well into 2023. Cost-breakdown indicates a 57% spend on tech development, and 24% on marketing and business development. In the wider market, we see the demand grow for privacy-respecting technology, such as applications to track COVID-19 cases, and the creation of privacy implementations for the Ethereum blockchain. In France the regulator shows further support for blockchain and calls for a Europe wide security token sandbox.

Highlights

1. **Our** zero-knowledge proof system PLONK has been updated and other pieces are set in motion to ease platform integration down the line.

2. **We** have started to reveal our commercial strategy when we shared our partnership with Firm24 to tokenize the Dutch shareholder registry.

3. **Despite** COVID-19 our work continues unabated. Even in stress scenarios we are able to develop at full steam well into 2023, thanks to our minimization of foreign currency exposure, and hedging.



COVID-19 measures

Everyone experiences the effects of a worldwide pandemic. Fortunately the Dusk Network team has been unaffected, and our work continues remotely.

01 Goals and Objectives

Everything that we do at Dusk Network is in service of delivering our technology to the masses. On the one hand we provide guidance and integration support for our partners and early adopters. On the other hand, we are continuously improving and optimizing our cryptographic libraries and network components. To fulfill the overarching goal of making Dusk Network: the privacy blockchain for financial applications, available to any size enterprise.

Technical Development

Integration, optimization and streamlining. The R&D teams made stellar progress on fine tuning our zero-knowledge proof system, while the development team focussed on the stability of the network's nodes, consensus chain and integration with the VM. The UI and UX team finished the integration of the UI-Kit with Figma, a design management system. The Dusk UI-Kit is ready for open-source release and is a modular front-end framework that can be used to deploy, maintain and update various Dusk-related web interfaces.

Zero-Knowledge Privacy
PLONK, our zero-knowledge proof system, has undergone various tests and optimizations. The team drastically improved the prover and verification speeds.

Security Token 2.0
We finalized the second iteration of the Confidential Security Contract (XSC) standard, expanding the functionality that issuers of security tokens can choose from.

Third-party services
We have unified our protocol, allowing for a more intuitive integration with third-party services.

Upcoming Development Milestones

All development milestones in the next wave of releases center on three key focal points: (1) fine tuning our zero-knowledge proof system and implementation of PLONK Gadgets for programmability, (2) conversion towards our native DUSK, and (3) Enable plug and play interfacing capabilities to ease platform integration.

PLONK Gadgets
Gadgets enable developers to easily build zero-knowledge circuits. These circuits are used to program zero-knowledge smart contracts. The library supports Elliptic Curve Cryptography & Hashing gadgets.

Phoenix Code Release (*Pending: PLONK Gadgets*)
Phoenix is an UTXO-based transaction model that provides absolute on-chain privacy. Even for non-obfuscated outputs such as block rewards and gas fee refunds.

RUSK VM Code Release (*Pending: PLONK Gadgets*)
Rusk VM is a custom developed Virtual Machine designed specifically for zero-knowledge smart contract deployment and operations.

Zedger Code Release (*Pending: PLONK Gadgets*)
Zedger integrates with Phoenix and RUSK VM, providing UTXOs with account-based capabilities that power features required by Confidential Security Contracts ('XSC').

- **Plug and Play: Smart Contract Interface**
  The interface enables issuers to easily customize the featureset of their smart contract.

- **Native DUSK**
  Support conversion of ERC-20 and BEP-2 DUSK tokens to native DUSK.

Business development

We intend to "eat (y)our own dog food" every step of the way. There are commercial initiatives surrounding every deployment of Dusk Network. We will test, pilot and deploy our technology in order of increasing complexity.

- ❏ Fundraiser, Cap Table Management (Firm24, 2Tokens)
- ❏ Security Token Offering (STO)
- ❏ Security Token Exchange (MTF)
- ❏ Consolidate Asset Custody Chain (CSD)

Sandbox Mainnet | Partner Program

Q4 2019 we announced the launch of the Sandbox-version of our Mainnet. With it, partners get early access to our technology, while the development team continuously works on new features and further optimization of the stack.

Customer Integration | Firm24

In February we revealed our partnership with Firm24 - the company incorporation platform serving more than 35,000 SMEs in the benelux region. Expanding their offering beyond company incorporation and notarial services, they have revealed their digital shareholder registry that is freely available for anyone to use. Firm24 is the first example of how Dusk Network is used to tokenize equity for thousands of Dutch companies, in collaboration with LTO Network technology.

> "Thanks to Dusk we are now ready to deploy our Tokenized Share Register, automating corporate actions, and lay the foundation to connect our customers directly with the world of alternative finance." - Martijn Migchelsen, CEO of Firm24

Accelerating Agendas | 2Tokens

Dusk Network joined the 2Tokens Advisory Board and R&D team in Nov, 2019. The initiative has been very successful with hundreds of business executives in the Netherlands and wider Europe seeing their tokenization agendas accelerated. As the project is moving into its next phase we have been fortunate enough to be identified as the technology provider for the initiative's financing needs; over the course of next months you will learn more about the 2Tokens tokenized fundraiser, and can expect to see Dusk return in many of the initiative's marketing and media appearances.

Security Token Exchange

A fully tokenized stock exchange that also works for the traditional sector is a significant undertaking, and we can safely say it's been quite a ride behind the scenes to get the various approvals, liquidity providers, assets, users, tech partners, and many more of the moving pieces required for such an operation onboard. There is a lot more work to be done yet, but you can expect a registration environment to be released ahead of the full launch for users to complete their accounts and KYC checks, allowing them to hit the ground running on launch day. The exchange will be primarily focused on users from the EU region.

Node Partner Programme

Next to deploying the first commercial collaborations ourselves, we are also experiencing demand for companies to run their own pilots using the Dusk Network technology. We have freed up some resources to work on the Node Partner Programme, which will allow companies to set-up a full Node with our support.

Organization

Due to our recent growth we have made our organizational structure scalable. Teams work in small and dedicated teams and present finalized products during weekly demos.

- ❏ The marketing team expanded with PR-executive, Sabine and Marketing Strategist Robin.
- ❏ The development team expanded with distributed-computing expert Thomas Modeneis.
- ❏ The business team expanded with business controller Stijn Lucieer.

We have 1 open vacancy at the moment for an experienced Rust/WASM developer and welcome open applications, even if we don't advertise for it.

02 Financials

In Q4 2018 we announced the end of our sale raising a total of USD 8.1M. At the time, we made plans for a multi-year runway. As per Q1 2020, available company assets total USD 6.2M. Even in our most conservative scenarios[1], this means that we will be developing at full steam well into 2023. More than 82% of company assets are held in fiat (*see fig. 1.1*). Hedging our foreign currency exposure provides the benefit of little exposure to market fluctuations.

We are emerging from a period of heavy technical development, and have started the allocation of more resources towards business development and marketing. In Q1 2020 we report a 57% spend on Tech Development, 24% on marketing and business development, and 19% on Other[2].

[1] Conservative scenarios do not include any cash flow from the sale of budgeted tokens, revenue streams, or subsidies and grants.
[2] includes: HR, Finance, Office, Legal, accountant and other services.

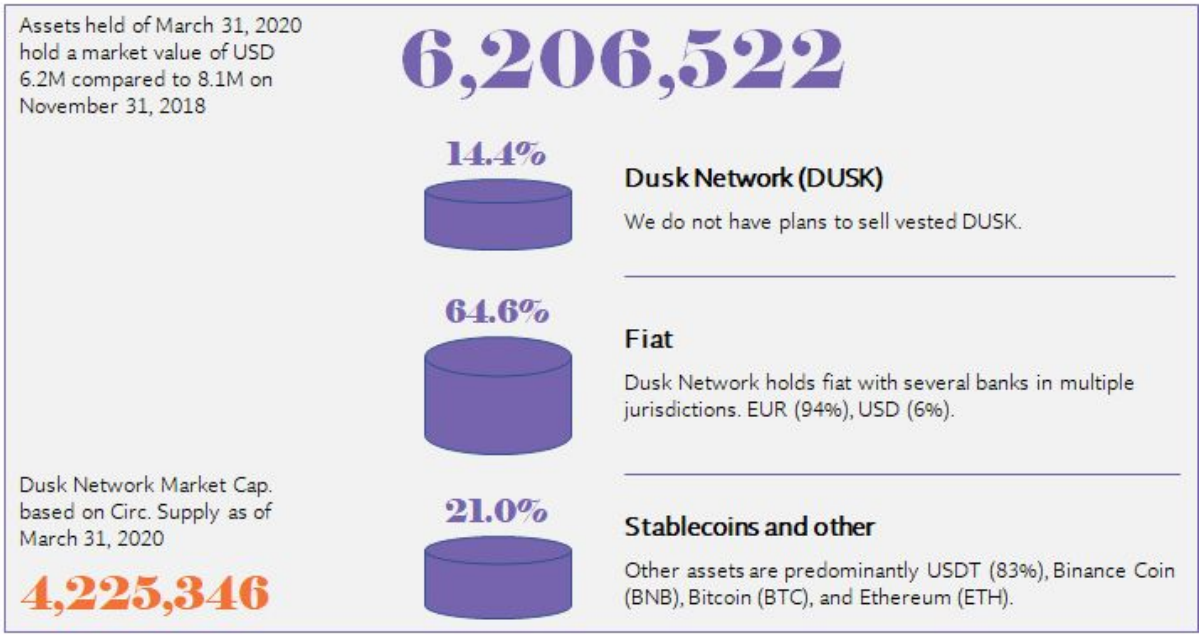


Fig. 1.1. Company assets held of March 31, 2020

We are proud to confirm that Dusk's token spend in Q1 has been as little as 1.97M tokens (*fig. 1.2.).* All tokens are allocated to developers who opt for partial token remuneration. We continue to keep this diligent mindset and use our token reserves for direct value-add to Dusk Network.

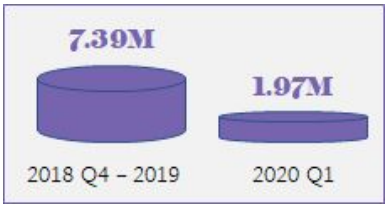


Fig 1.2. Company native token spenditure

03 Industry developments

Privacy-preserving applications

The demand for privacy-respecting technology and applications is growing. On the 10th of April, Apple and Google shared in a joint-collaboration their designs for a bluetooth based application to track Covid-19 cases. They call the app: "Privacy-Preserving Contact Tracing". Jennifer Granick (ACLU) said. "People will only trust these systems if they protect privacy, remain voluntary, and store data on an individual's device, not a centralized repository."

Privacy in blockchain

Ernst and Young (EY) released their third- generation zero-knowledge proof privacy systems for the Ethereum public blockchain. "The release of the third-generation ZKP technology comes on the heels of a study conducted by Forrester on behalf of EY (pdf) in November 2019 in which half of respondents cite security (49%) and data privacy (46%) as top blockchain concerns. Additionally, 45% of respondents cite interoperability as a stumbling block of private blockchain."

Sandbox for security tokens

CoinDesk: “France’s Financial Markets Authority (AMF) has proposed that all of Europe adopt a regulatory "sandbox" to support the emerging security token industry.

The “Digital Lab” would run for three years, the watchdog said in a March 6 legal analysis, exempting projects from financial regulations such as the MiFID and CSDR that AMF’s analysis deemed incompatible with the blockchain sector’s growth.”

Questions? For more in-depth information visit our website. For press-related questions please reach out via info@dusk.network, for business related enquiries please contact business@dusk.network.