

# Business plan for



# MULTY

— Cryptocurrency and assets open-source wallet

This document provides a detailed business plan based on the methodologies developed by a decentralized Rocket DAO expert community.

January 2019

# Table of contents

- Multy company overview .....03
- Important financial metrics (forecast) .....04
- Multy Roadmap .....05
- Product .....06
- Business model .....09
- Market .....11
- Team leaders .....16
- Technology .....18
- Financial model .....28
- Legal .....40
- Risks .....42
- PR & Marketing .....48
- Resources & Assets .....49



## Multy

Multy is an open-source multisignature wallet for Bitcoin and Ethereum cryptocurrencies and ERC20 tokens.

[www.multy.io](http://www.multy.io)

### Product

MVP released

Multy is a new generation cryptocurrency wallet which turns payments into pure pleasure with the help of:

1. Air payments without requesting Internet connection, sharing geo-location, any personal data;
2. Contact list with wallet numbers of all those whom you have made transactions to;
3. Currency converter letting you set the transaction's amount and see balance in fiat ;
4. Multisignature for joint capital control;
5. Highest security level: Multy doesn't store any personal information;
6. Simplicity: setting up a wallet takes only two taps with only one seed phrase for all crypto-assets;
7. Privacy: all private keys are encrypted on the owner's phone;
8. A browser for decentralized applications implemented within our mobile application.

### Founders

Team size: 9



**Vadim Makovsky**

CEO, Android Developer



**Vasily Nemkov**

CTO



**Pavel Klybik**

C++ / Go Developer



**Alexandr Prokopchuk**

Lead iOS Developer



Round  
**Seed**

Equity  
**10%**

Capital s

Business type  
**B2B, B2C**

Headquarters  
**Minsk, Belarus**

Seeking  
**1 000 000 \$**  
Legal registration  
**Minsk, Belarus**



Investments

**Pre-seed - 40 BTC from Cyber Fund in November, 2017 (\$800k at that moment)**

Geographic focus:

**The USA, Europe, Canada; less on post-Soviet region.**



### Problem

Of cryptocurrency users: evident lack of secure, convenient and multi-functional wallets protecting users personal data and providing the best experience transferring assets.

Of vendors: complicated and expensive access to cryptocurrency users.

### Solution

Multy is a mobile cryptocurrency wallet that solves the problem of users' data and assets safety while providing a user-friendly and intuitive interface and experience for the community.

We care about security, so if anyone tampers with your device, we delete all sensitive data permanently.

### Business model

Monetization hypotheses of the application:

- In-wallet exchange commissions;
- Multisignature setups;
- Donations from the wallet's users;
- DApps partnerships and integrations;
- Partnership programs with other market players.

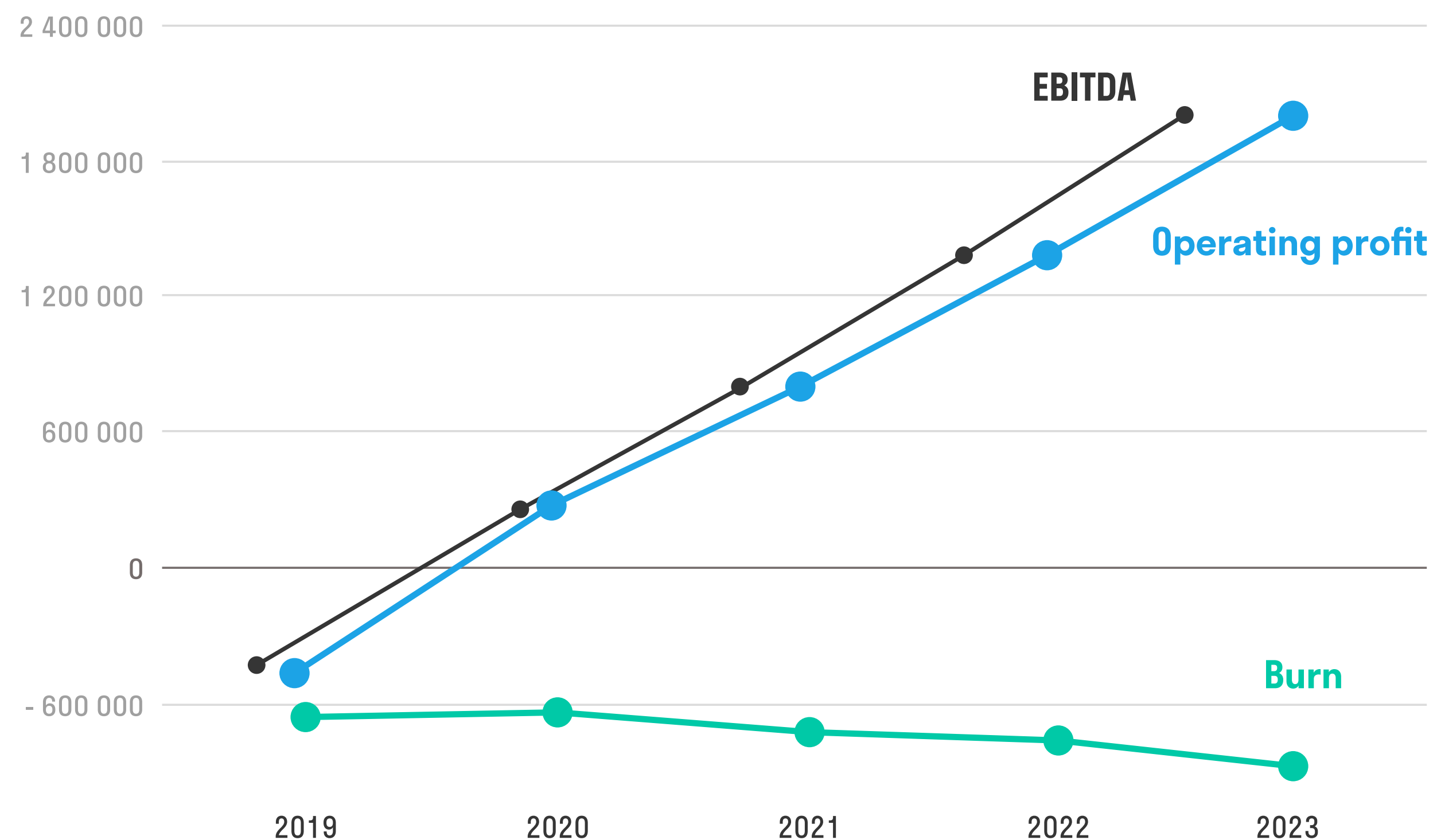
### Market

The market is young but a fast-growing one with the number of blockchain wallets users reaching 29 mln today.

This is a globally scalable market. The USA, Northern Europe, Asia, and post-Soviet area are of our primary interest.



# Important financial metrics (forecast in U.S. dollars)



## As at the end of 2019:

Revenue total = 253 039 \$  
Gross profit = 134 421 \$  
Profit margin = 53 %  
Operating profit = - 367 513 \$  
EBITDA = -373 302 \$  
EBITDA margin total = -148 %  
COS = (-)118 617 \$  
CAPEX = (-)35 400 \$  
OPEX = (-)399 702 \$  
Personnel = (-)220 800 \$  
Burn = (-)650 130 \$  
G&A expenses = (-)139 434 \$  
Selling expenses = (-)362 500 \$  
WACC = 17 %  
ARPU = 2,66 \$  
Average CAC = 1-1.5 \$  
App active users = 663 369  
Total installs = 2 211 230





# Roadmap for 2019



\*Segwit, or Segregated witness - is the process by which the block size limit on a blockchain is increased by removing signature data from Bitcoin transactions.

## Jobs-to-be-done problems

Developing Multy we set a goal **to make any kind of interactions with cryptocurrency easy and intuitive for ordinary people**. Our solution can be used even by a granny.

Multy is a mobile cryptocurrency wallet solving the problem of **users' data and assets security** while providing a **user-friendly and convenient interface** and experience for the community. We care about security, so if anyone tampers with your device, we delete all sensitive data permanently.

Why is it a truly safe solution? We oppose dishonest activities observed in the cryptocurrency market with the help of decentralization. Decentralization successfully solves the problem of secure data storage which is an ideology Multy initially adheres to.

## Relevance of the problem

Before we started an active development of Multy we had conducted a profound practical research of the existing Android and iOS solutions for cryptocurrency wallets in order to examine their strong and weak points and to evaluate key competitors.

We downloaded about 20 mobile applications from Google Play and App Store and tested all of them, this way we found out a great number of problems including an inconvenient mechanism of transferring crypto from one wallet to another, non-obviousness of the important buttons and their functions within the application.

The existing problem was evident: **users needed an intuitive UI/UX which is very easy to understand and to handle with.**

## Alternative solutions

There were and still are competitive solutions on the market, but in fact, none of them actually solve the problem of the secure user experience completely well.

## Product stage

Current product stage: **Product is bought** (small number of customers).

## Lifecycle stage

**MVP is released.** Fusible studies of MVP are completed.



## Innovation protection

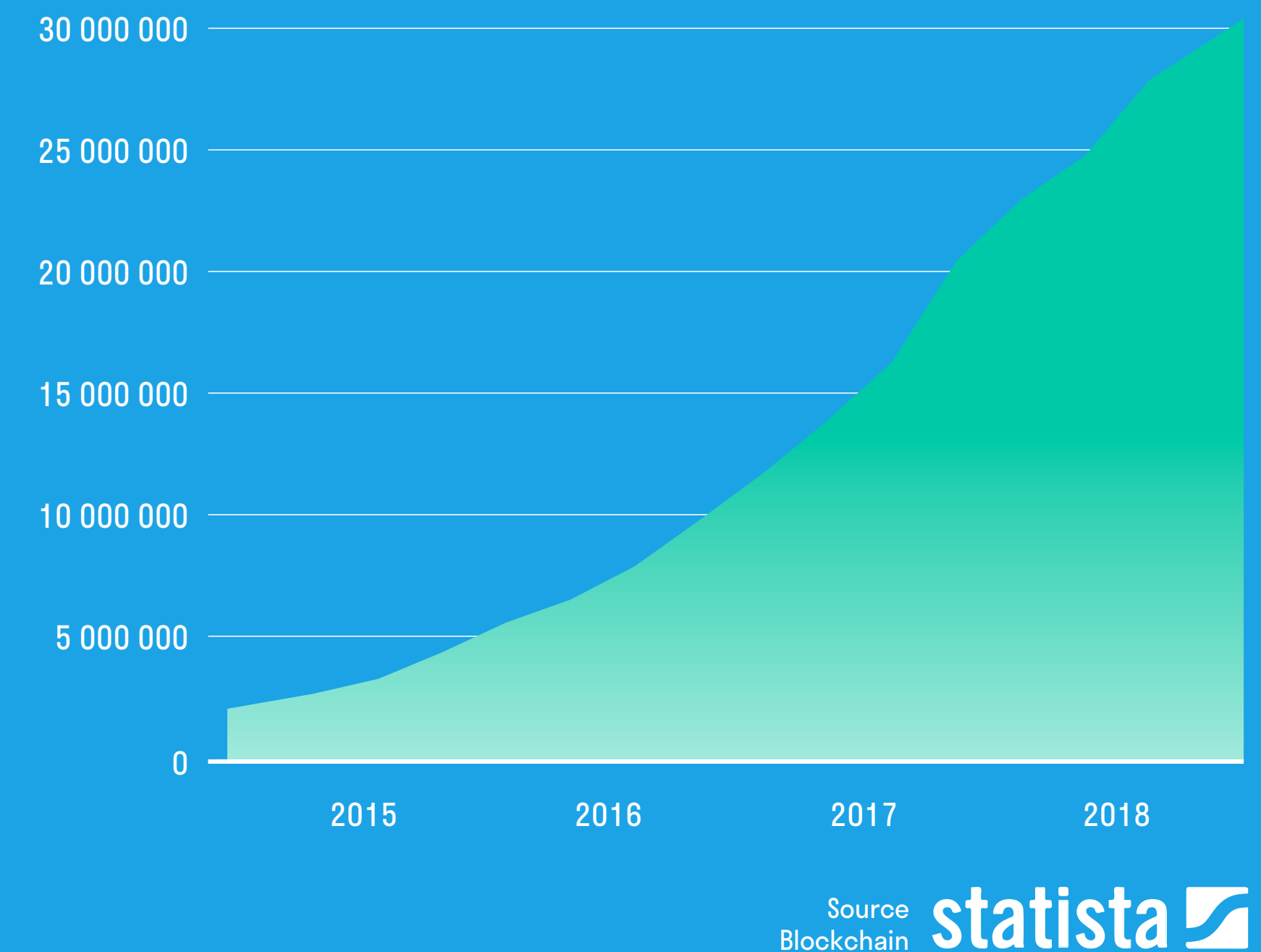
One of the security measures we undertake to protect Multy from competitors involves **stack advocacy** which implies strong advantages in technological level of our solution.

Another powerful instrument is the **license** imposed on our open source solution: this one sets strict limits on the commercial use of Multy's code but sets no rules for personal use.

It means that anybody can take the source code, develop his/her own application using our code available on github, launch his/her own server, but the application can meet individual interests only, one isn't allowed to spread this application among other users. And this restriction relates to the whole world, as github is global and we accept this fact.

That is why we chose MIT license limiting sharing of the app duplicates to third parties. Our Multy License is based on the standard licensing procedures and technologies.

Independent resources claim that the number of blockchain wallets users reaches 31 million people today.

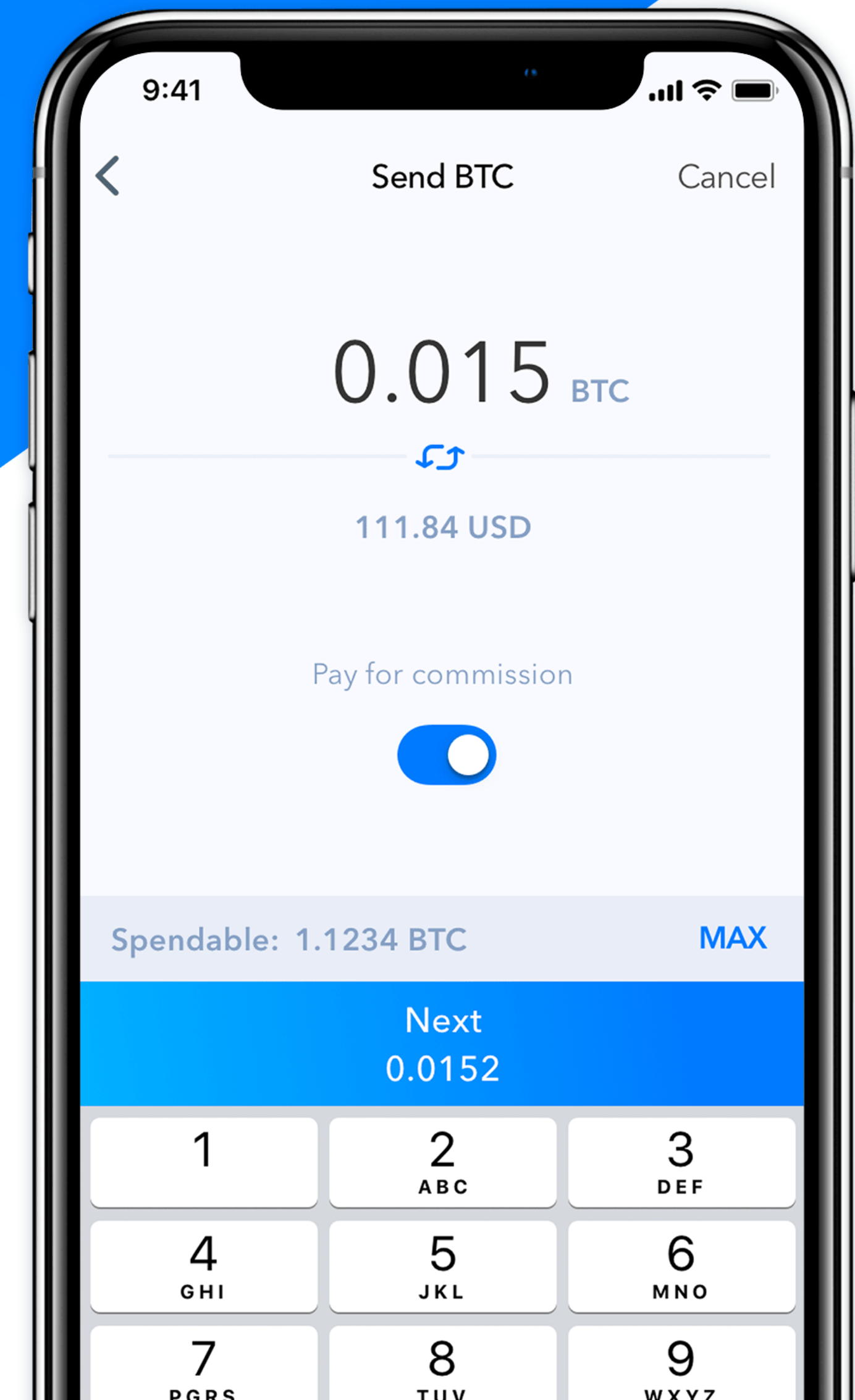


## Achievements

We turned the best on a set of crucial criteria:

1. We have developed **the most secure mobile crypto-wallet** available in the stores;
2. **To understand the vulnerability of the product we spent a great effort and time analyzing and eliminating all the hacking loopholes of the application. This ensured a high level of security for the product.;**
3. We have created an absolutely **unique method for cryptocurrency transfers** without having to disclose geo-location and that is an airdrop payment;
4. Our users are the only ones to know and store their private keys, **each application is encrypted with an absolutely unique key** which enables us to spare app stores this function. Notably, this solution has never been present on the market as other competitors create much less complicated solutions;
5. Multy is **the first Ethereum multisig mobile crypto-wallet** based on the Gnosis smart contracts which are generally accepted and are frequently used.
6. **We created a browser for decentralized applications** within our mobile application. Simply put, we took some key features of Metamask and implemented them in Multy: but in our case, these features may be applied not only to ETH but to other cryptocurrencies as well. This way we ensured that users can use DApps on their smartphones, while Metamask extension only allows to use DApps on desktops.

This solution will guarantee **mass adoption of the our innovative application** and the coverage of the worldwide audience.





# Business model

## Innovation

Not only does Multy enhance and improve existing solutions, but it also **creates brand new interesting and useful features** thanks to the market being so new and growing.

It is a **B2C** product right now, but at the same time it has a very high perspective to become a **C2C** one.

## Third parties

Taking into consideration the fact that we are building an open source project there are many technical solutions we use for our own development, like **blockchains and a variety of libraries** (for Bitcoin node, for Ethereum node; and libraries created for Android and iOS encryption of the inner databases). **Apple Store and Google Play Market** are used as business-oriented third parties.

## Internal logistics

**Users are the only ones to own and possess their assets** while Multy has access to the information about the quantity of these assets, not more. Logistics of the system is infernal. It means that infernal partners are responsible for the logistics of the assets within the application, whereas Multy develops necessary functions to make these operations possible and convenient.

## Clients

In terms of business model and sales perspectives **the main sector we are oriented at is B2B**. Our platform brings the users' attention to the number of ways their cryptocurrency assets could be managed and utilized providing undoubtful revenue opportunities for us and our partners

**Partnerships** for this case imply having a deal with someone who agrees to share with us a specified percentage of his/her revenue generated in cases when their clients spend their money using our wallet. In other words we direct our users to the businesses of our partners and receive cash back for it. This hypothesis is one of the most productive ones.

**Exchange integrated function** will benefit us as well, as we will receive commission for the exchange of BTC to ETH, for example. Another monetization hypothesis describes a proof of stake model. Initially it means that people delegate their money to those who they can trust aiming to get a profit from such an operation.

In fact Multy it now turning into the channel distributing the money of those who take part in the proof of stake directing these money to those who will actually manage the assets. So Multy provides a platform and the tools for this delegation resembling **the broker services mostly**. Users with small cheques give their money to bigger market players letting them manage their money in the way they think will benefit to all parties in the best way. Multy will receive commissions for these transfers from brokers to users.





# Business model

## Competitive protection measures

As it was mentioned before we differ advantageously from our competitors having a **complicated technological stack**, providing our users with **perfect safety solutions** and very convenient interface. Our growth drivers include the two very powerful competitive features of our wallet which include airdrop payments and mobile Metamask.

## Sales channels

**Google Play Market and Apple Store** are primary sales platforms for our product. Advertising networks and bloggers-influencers are efficiently used as well.

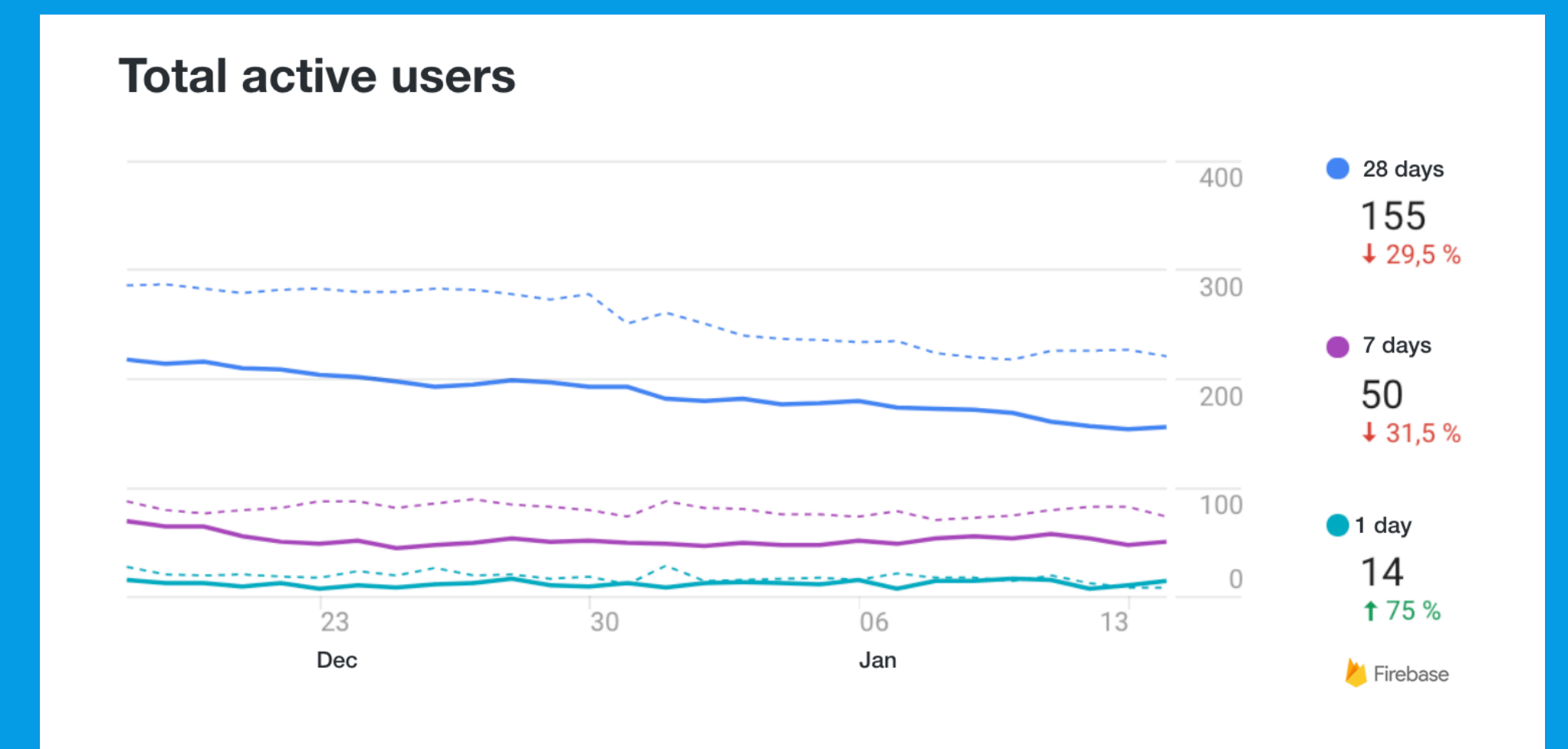
## Price

**Shapeshift and Changelly** (crypto-exchange services) are the third party services which we use and actually sell within our wallet.

## Paying process

We usually provide third-party merchants the right to offer their services within our application. It means that the paying process is **simplified for our partners**. The application itself is free for users.

An average retention rate is 30% (since the launch day).  
Traffic is organic.





## Market geography

The business we are developing can't be a local one. No way. Potential **global market** of all cryptocurrencies is evident, Multy has amazing growth potential.

## Growth rate

The market growth pace is **more than 10%** on a yearly basis.

## Segmentation

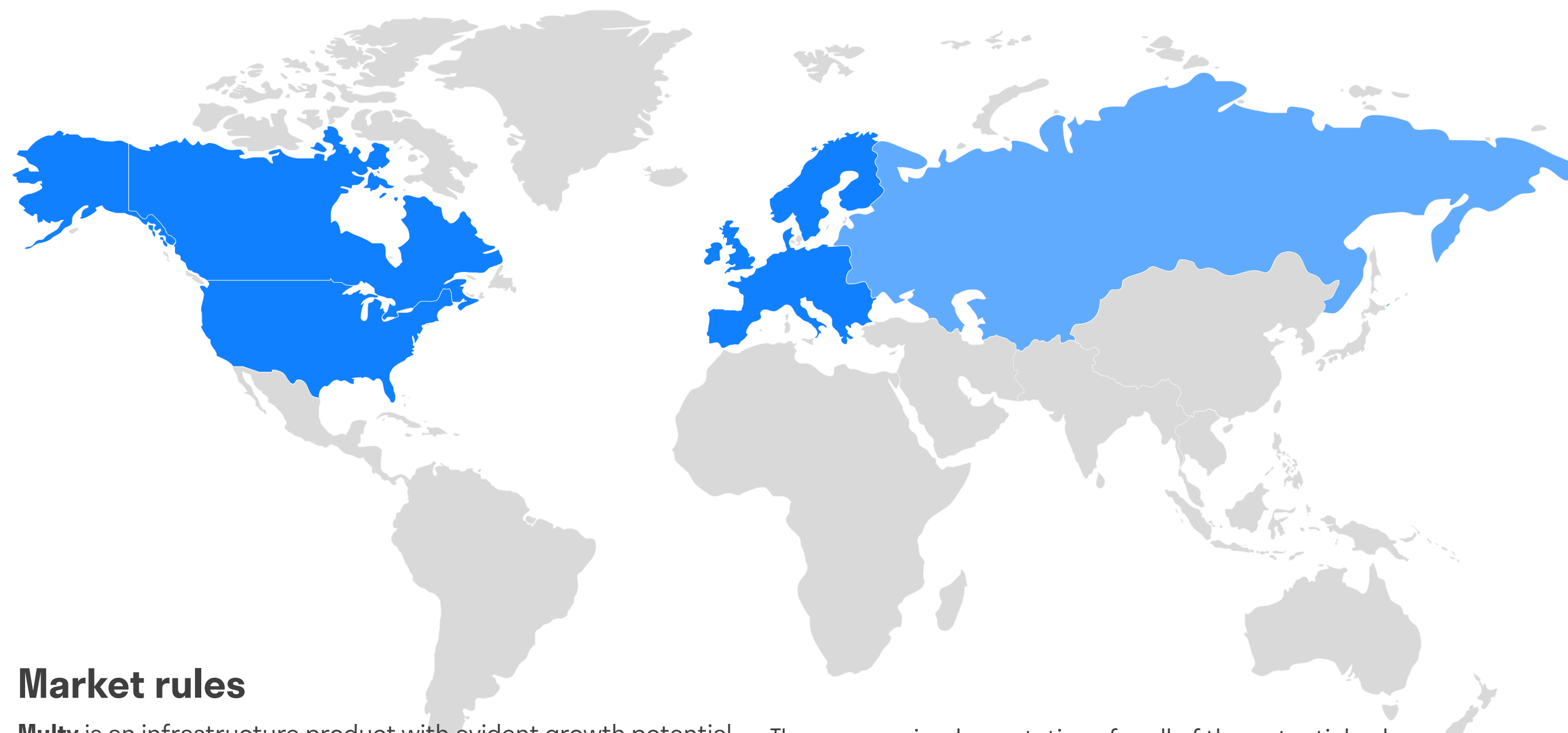
There are **many niches and the sales outlets for them**, nearly 3 or 4 projects can prove this (for example, there are crypto-wallets totally oriented to provide their clients with assets safety, others set different goals). Besides, there are cold and hot wallets. There are many variants of crypto wallets for each of the existing blockchains.

## Market age

Mobile wallet applications market is **young, but a fast growing one**: new wallets appear constantly (one in a month approximately), as well as new blockchains. But still, the market is not established yet.

## Geographic focus is now made on:

**The USA, Europe, Canada; less on post-Soviet region.**



## Market rules

**Multy** is an infrastructure product with evident growth potential. But the truth is that **an existing ecosystem isn't ready to become a well-established market yet**. This is so due to the the lack of the released final products connecting blockchain technology with the reality.

There are no implementations for all of the potential spheres where blockchain could be used yet (only one set of the technological solutions have been fully released already - that is for the trading industry. The rest is now being developed or will not be released at all).



## Target audience

A **man** who is **26-36 years old** living in **the United States of America or Northern Europe**.

Asian region is now being actively investigated.

## Customers' influence

**Users can influence the product**, and Multy's team actually implements some solutions letting users take active participation in the development of the application (for example, votings for new features to be released in the nearest future). But coalitions make no sense.

And what is important, **those who have and use cryptocurrency stay within the application** (that is the team's practical observation since the first release).

Those who don't have crypto delete the wallet consequently.

## Substitutions

Any safety solution for storing and using cryptocurrency apart from wallets are substitutions of the application. **Centralized stock exchanges** with a wide variety of the crypto assets available, but in fact this alternative is the worst one in terms of the security measures needed to deal with crypto.

## Market requirements

What we are actually doing within our team is:

- for **90% technology** and software development;
- for **10% marketing** only. So the only thing we need for business development is quality marketing.



## Target segments

Our target segments include **those who use cryptocurrencies on a daily basis** in small amounts **for e-commerce and DApps** (web 3.0), but trading (including stock exchanges) is excluded from this list as primary interests of the users from this segment do not coincide with Multy's strategy and philosophy. Segments are chosen with regard to the future application's growth.

## Technological barriers

Technological barrier is **not high**.

The reasons for this are as follows:

- the technological stack we are using is a one-range distributed system, and these systems have all been tested and adopted long ago;
- smart contracts require to use plain and simple programming languages;
- blockchains can be developed using Java Script which is a very popular programming language, it means that the entry barrier in the crypto applications market is low for the people with a strong desire and explore the technology.

## Suppliers

Our Suppliers, or those users and businesses we are dependent on are:

- the blockchains and protocols **developers**;
- **market fluctuations** and **people behaviours** do influence the demand on crypto wallets as well;
- **integrating platforms** (like e-commerce platforms) if they make a decision to implement libraries allowing cryptocurrency use for payments;
- **offline retail**: for these cases Multy can be used right now easily and very fast (for any purchases like coffee, clothing for example).
- **Google, Yandex** browsers and search engines.

## Patent protections

We have a license strongly resembling **MIT** which protects us from technology theft. But as we build an open source project, we give access to any Internet user to our code, so anybody can easily copy it.

## Distribution system

**Google Play and Apple Store** are the two main distribution systems we are actively using.



# Market


## Direct competitors

There are three key competitors on the Web 3.0 market (the DApps, to be exact):

**Jaxx, Trust Wallet and imToken.**

Feature	Jaxx	Trust Wallet	imToken	Multy
Opensource	-	+	-	+
Native mobile development	+	+	+	+
Desktop clients	+	-	-	+
Web extension	+	-	-	+
Transaction fee	+	-	-	-
HD Wallet	-	-	-	+
PIN/Fingerprint	-	+	+	+
Contacts	-	-	-	+
Airdrop payments	-	-	-	+
DApp browser	-	+	+	+
Multi crypto-assets	+	-	-	+
Exchange	+	-	-	+



At the same time, there are various **wallets** for each crypto coin in the relevant niches of the segmented market (for Ethereum, Bitcoin and so on).



**Jaxx**

Multi-platform wallet supporting over 70 digital assets and tokens.

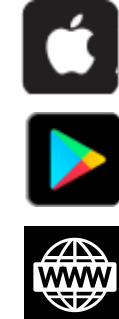

500k+ installs  
3.2 overall rating

**Trust Wallet**

Secure wallet for Ethereum, ERC20, ERC223 & ERC721 tokens.


100k+ installs  
4,7 overall rating

**imToken**

A wallet enabling multi-chain asset management, DApp browsing and secure, private exchange of value.

50k+ installs  
4,4 overall rating





## Access to customers

Mobile applications by default provide **direct access to clients**. For example, application's owner can send pushes to the users in just a few minutes. But we do not practice it.

**Multy stores minimum information about its users.** All access keys belong to their users only. Such measure is necessary for the minimization of the risks connected with the loss of users data in cases if the application's server is hacked. It means that intruders will actually get no new information about Multy's users apart from the one which is already available on the blockchain.

In order to study our audience in terms of geography and some basic metrics we use popular software **Firebase**.

There is another supplier each application is dependent on: Yandex and Google. But in cases these giants eliminate us from their systems we still will be able to distribute our solution to customers.

## New actors

There are several teams creating solutions similar to the Multy's concept, we are talking about blockchains for blockchains. They are **Cosmos Network** (or Internet of Blockchains), **Polkadot**, and **Interledger**.

They are developing blockchains with capacity to transfer cryptocurrencies to other blockchains. It means that having developed a wallet for such a blockchain and perceiving cryptocurrencies as assets one can solve the problem of universality - multi-cryptocurrencies in one place altogether (with the help of peer-to-peer money exchange).

These teams have been developing their technical solutions for several years already, but they are dependent on other blockchains. The chance that they will join the existing crypto-market (for all available crypto assets) is still undetermined, as none of the projects mentioned above have released their implementations.

Another alternative solution worth being mentioned here are the **wallets with atomic swap (crypto-exchange)**. But these wallets have very strict technological limitations as they require hard and timely development of the implementations for each blockchain, for each crypto-pair, only this way they will be able to solve the universality problem. Nothing to say about the necessity to follow all security claims for each case.

**Decentralized stock exchanges** are another type of alternative solution to Multy. But the truth is that if an exchange closes, then the wallets connected with it are deleted as well. Also there are certain obligations imposed on such exchanges by the strict American legislation of SEC which puts more pressure on them.

Multy works with the solutions and technologies that are going to be completely decentralized in the future.





## Team leaders

# Vadim Makovsky

Founder, CEO, Product owner, Lead android developer

**Leader, expert in blockchain technologies and mobile development.**

Key technical and product achievements:

- Proficient mobile developer with more than 5 years experience;
- Took part in the creation, management and development of more than 15 mobile apps (as technical director, android developer and project manager);
- He is a graduate of Imaguru Blockchain Academy - the first Blockchain academy in Belarus;
- Winner of Imaguru Blockchain Hackathon (AppsCrunch team), Datathon and several more hackathons.
- IT entrepreneur with more than 10 years experience;

- Last year he sold his mobile workout application My coach which now has more than 1 000 000 installs;
- Graduate of international startup accelerator TechMinsk;
- Pitching master and expert in business networking;
- Fundraiser.

Youtube links to public speeches at Cyber Fund meetups:

- [Multy against other blockchains.](#)

BlockShow Oscar Berlin 2018:

- [Multy finalist pitch.](#)







## Team leaders

# Vasily Nemkov

Co-founder, CTO, Multy Core developer

### Cross-platform architecture, blockchain expert.

Key relevant characteristics are as follows:

- Vasily has been coding in C/C++, Python for Linux, Windows, Mac (and what not) for more than 15 years;
- Contributed to the development of more than 6 great projects (a graphic editor, VoIP-clients and messengers);
- While working for wargaming.net held a team lead position and contributed to 4 times nodes traffic reduction;
- Worked on Yandex Browser development.

Youtube links to public speeches at:

Cyber Fund meetups

- [Multy's core](#)

- [Multy's ERC20 tokens C++](#)

CoreHard 2017

- [Reflection in C++](#)

C++ CoreHard 2018

- [The core of a cryptocurrency wallet Multy.](#)





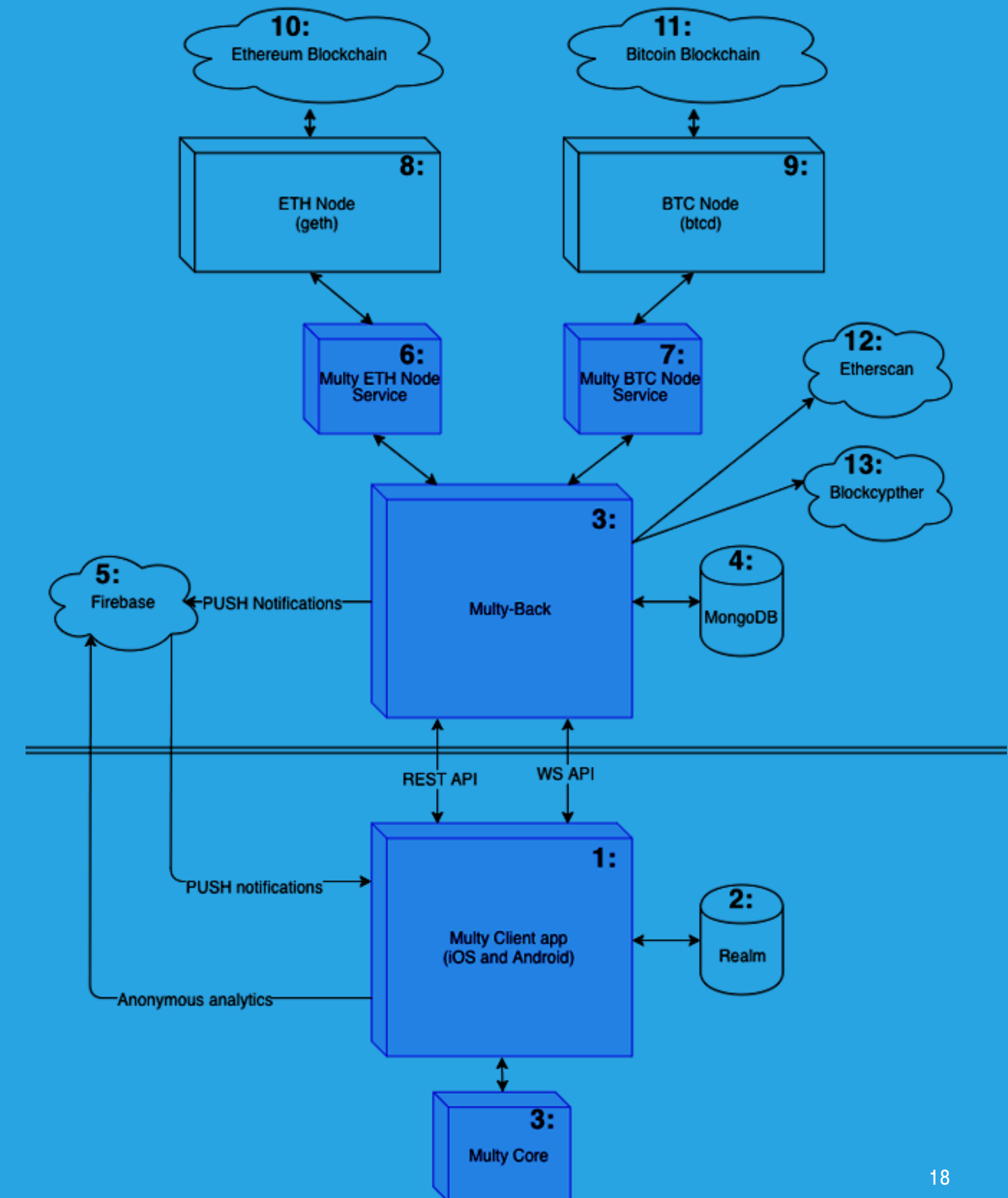
## Algorithm

Key point of the project is to **simplify user access to blockchain** without compromising security of the owned funds.

### That means:

- Native Apps for iOS (Swift) and Android (Java) ensure that it is hard to inject malicious code into or codebase;
- Transactions are made on user device;
- All cryptography is done on user device;
- Private keys and seed phrase never leave the user device;
- Private keys and seed phrase are stored and properly encrypted in a manner that prevents adversary from accessing these even if they obtain a copy of the Data Base;
- Back-end provides a caching layer and stores information that is public anyway - Cryptography is top-notch: we use the same libraries as reference;
- Implementations of Bitcoin (namely, Bitcoin core) and Ethereum (Ethereum-cpp) do for generating transaction signatures, that is libsecp256k1.

## Multy Project Overview



## Algorithm: explanation of the scheme Multy Project Overview

- 1. Multy Client is a Mobile app** (separate applications for iOS and Android) that function in the same way and share same design principles.
  - This is the only component users can interact with.
  - Client provides human-friendly interface to the end-users, allowing them to interact with blockchain in a simple way.
  - Stores all user information in encrypted local database (2). Special attention was given to secure the DB and encryption scheme from being transferred to another mobile device.
  - Creates blockchain-specific transactions with the help of Multy-Core (3)
  - Communicates with Multy-Back (to propagate transactions to the blockchain and access data stored in blockchain).
  - Collects anonymous usage statistics and uploads that to Firebase service (6)
- 2. Realm Database** - a database that stores user private information, such as:
  - Seed phrase
  - Private keys from wallets
  - Wallet balances It was chosen because of good combination of security and performance.
  - See for details:  
  
Secure database research for Android conducted by the team.
- 3. Multy Core** - a cross-platform C++ library:
  - Generates standards-complying seed phrase from entropy;
  - Creates private keys and addresses in blockchain specific manner;
  - Serializes and signs user transactions.
- 4. Multy Back** - back-end service handling user requests and providing simple and consistent interface to multiple blockchains.
  - **Provides Clients** with notifications on important events, such as transaction status change and node mempool state via WebSocker API (for clients currently online) and via Firebase (6) PUSH notifications (for clients that are currently offline)
  - Provides caching layer with MongoDB (5) and stores data that are costly and slow (or even impossible) to obtain from blockchain directly, such as:
    - Balances for UTX0-based blockchains (such as Bitcoin)
    - Incoming/outgoing transaction statuses
    - Existing user wallets and addresses
  - Provides Multisig negotiation protocol
  - Propagates transactions to native blockchain nodes through Multy Node Services: Multy ETH Node Service (7) and Multy BTC Node Service (8)

## Algorithm: explanation of the scheme Multy Project Overview

5. **MongoDB** Stores data supplied by Multy-Back (4).
6. **Firebase** Transfers push notification from Multy-Back (4) to Multy Client (1), stores anonymous usage statistics from Multy Clients.
7. **Multy ETH Node** service - provide consistent interface to the Ethereum blockchain node (9). - Notifies Multy-Back (4) when transaction concerning users of Multy has changed it's status. - Transfers signed transactions from Multy-Back to ETH Node.
8. **Multy BTC Node Service** - as the intermediary, just as Multy ETH Node service, but for Bitcoin blockchain node.
9. **ETH Node** - native Ethereum blockchain full-node, managed by Multy and located on our servers. Participates in Ethereum Blockchain (11) as a regular node. We chose geth as node software due to its robustness and performance.
10. **BTCD Node** - Native Bitcoin blockchain full node, managed by Multy and located on our servers. Participates in Bitcoin Blockchain (12) as regular node.
11. We chose btcd as node software due to extended interface it provides.
12. **Ethereum blockchain**
13. **Bitcoin blockchain**
14. **Etherscan** - third-party API for querying data regarding Ethereum Blockchain that is too costly or impossible to process on node. Used only in case of emergency as a failover measure.
15. **Blockcypher** - third-party API for querying data regarding Bitcoin Blockchain that is too costly or impossible to process on node. Used only in case of emergency as a failover measure.





# Technology

Key developers for each of the architecture levels:



**Vadim Makovsky**

Multy-Client Android developer



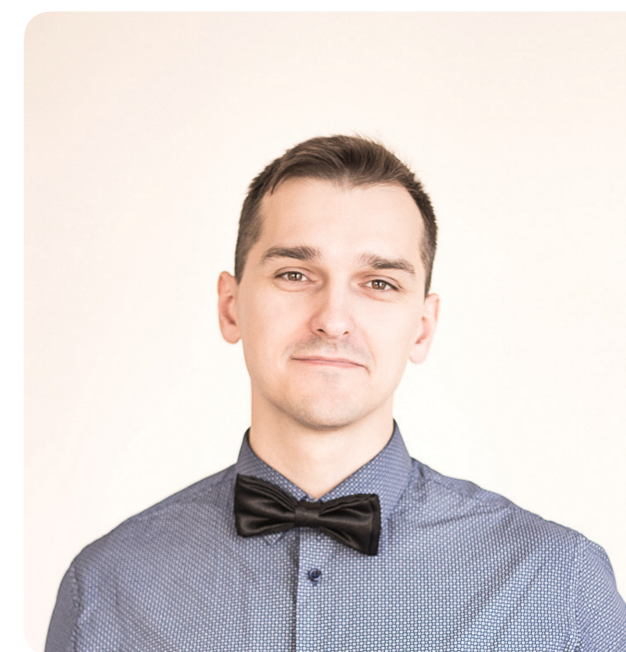
**Alexandr Prokopchuk**

Multy-Client iOS developer



**Pavel Klybik**

C++ / Go developer



**Vasily Nemkov**

Multy-Core developer



## Architecture

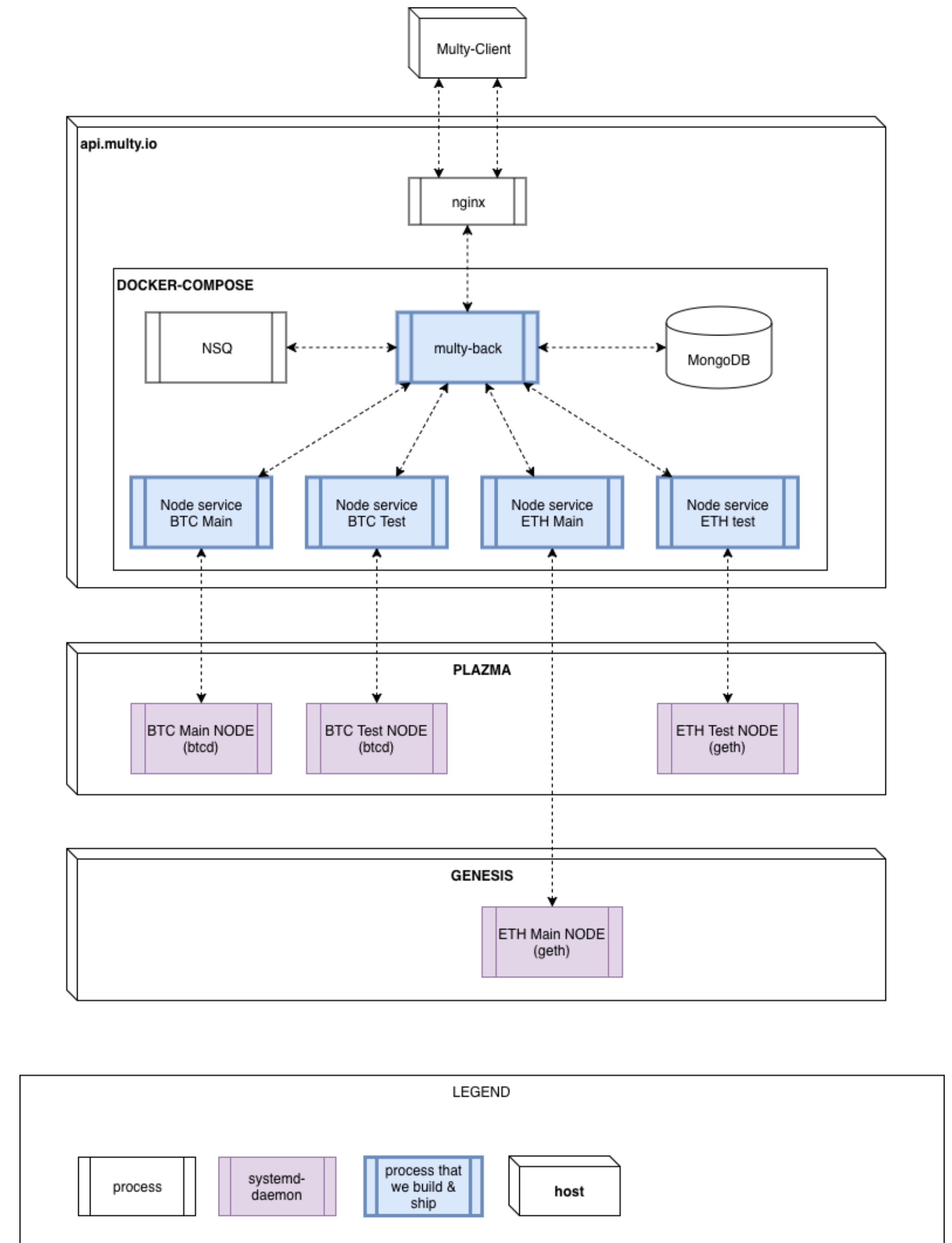
Here are the architecture schemes for both mobile and web solutions.

### Multy back deployment scheme

Our back-end services are run on dedicated hardware, and conceptually consist of following components:

- Nginx - proxies REST and WS requests from clients to Multy-Back, handles SSL connections and certificates.
- Multy-Back - the main piece, handles all business logic. Written in Go due to its high concurrency capabilities, deployment simplicity (executables come as single binary with almost no dependencies):
  - Writes cached data to the database;
  - Proxies transactions to the Nodes thru Node Services;
  - Issues notifications to clients either via WebSockets or Firebase service (not shown here)
  - Manages MultiSig negotiation process.
- MongoDB - caches public blockchain data of the clients to speed up lookup. Was chosen because of good performance and flexibility of JSON documents, allowing us to ship faster.
- BTC node service - talks to the Bitcoin blockchain node (2 instances: mainnet and testnet).
- ETH node service - talks to the Ethereum blockchain node (2 instances: mainnet and testnet).
- Bitcoin node (btcd).
- Bitcoin blockchain FULL node, participates in Bitcoin Blockchain. We do not rent nodes from third-parties, but rather run them on our servers.
- Ethereum node (geth) - Ethereum blockchain FULL node.

**Multy-Back (MB) and Multy-Node-Service (NS)** instances communicate via gRPC. These evolve in parallel and in order to simplify development and deployment are hosted in one github repository. **MB and NSs** are built and deployed as Docker Images by Travis-CI, and run in the single Docker-compose.



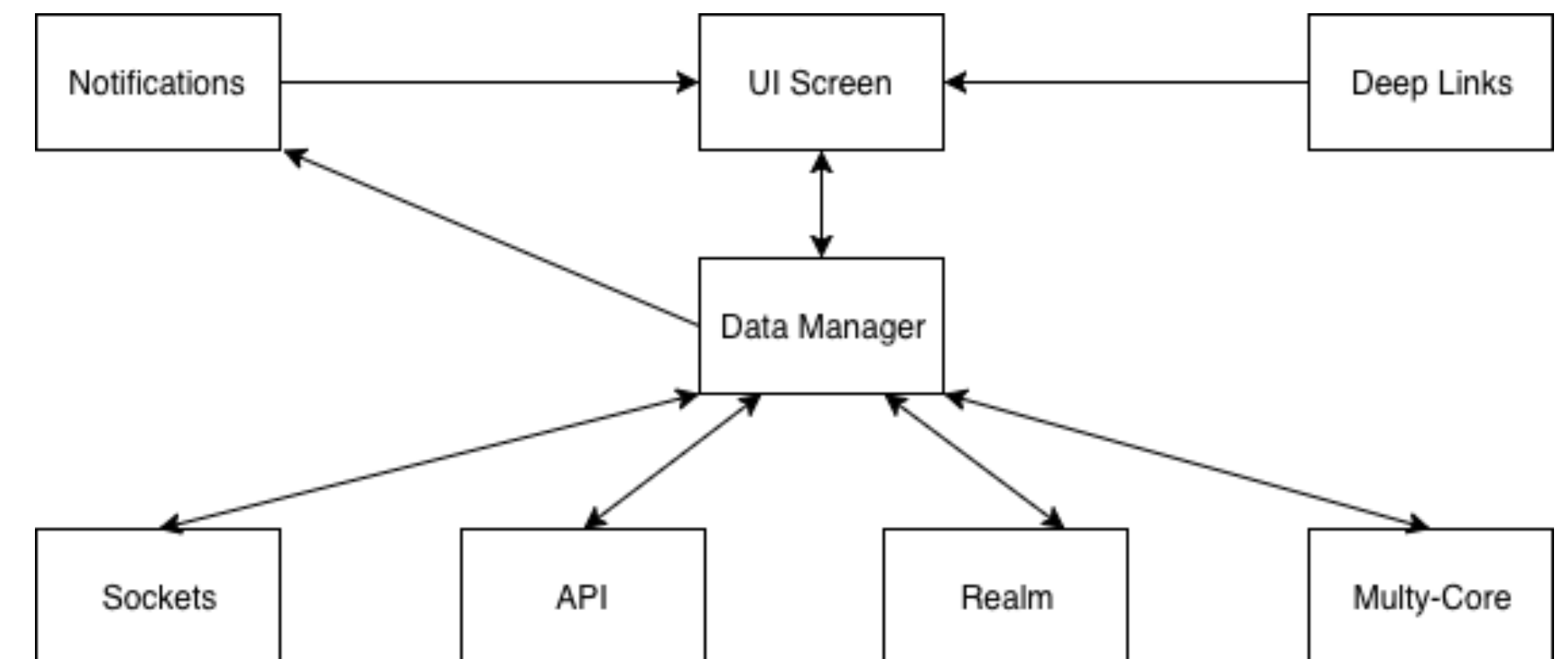


## Algorithm

### Multy iOS overview

- UI Screen - displays information to user, handles input from user. There are many screens in iOS Multy-Client, but each screen can be open in almost any predefined state by the Notifications and DeepLinks modules.
- There is also a special kind of a screen, that hosts WebView to gateway user into DApp world;
- We use MVP architecture;
- Notifications - module that handles PUSH and WebSockets notifications, shows popups and allows to open arbitrary screen by tapping on the popup.
- Deep Links module allows to open almost any screen with a web-link of special kind. If you open that link on mobile client, Multy App is going to be opened OR you will be directed to the App Store page where you can download Multy.

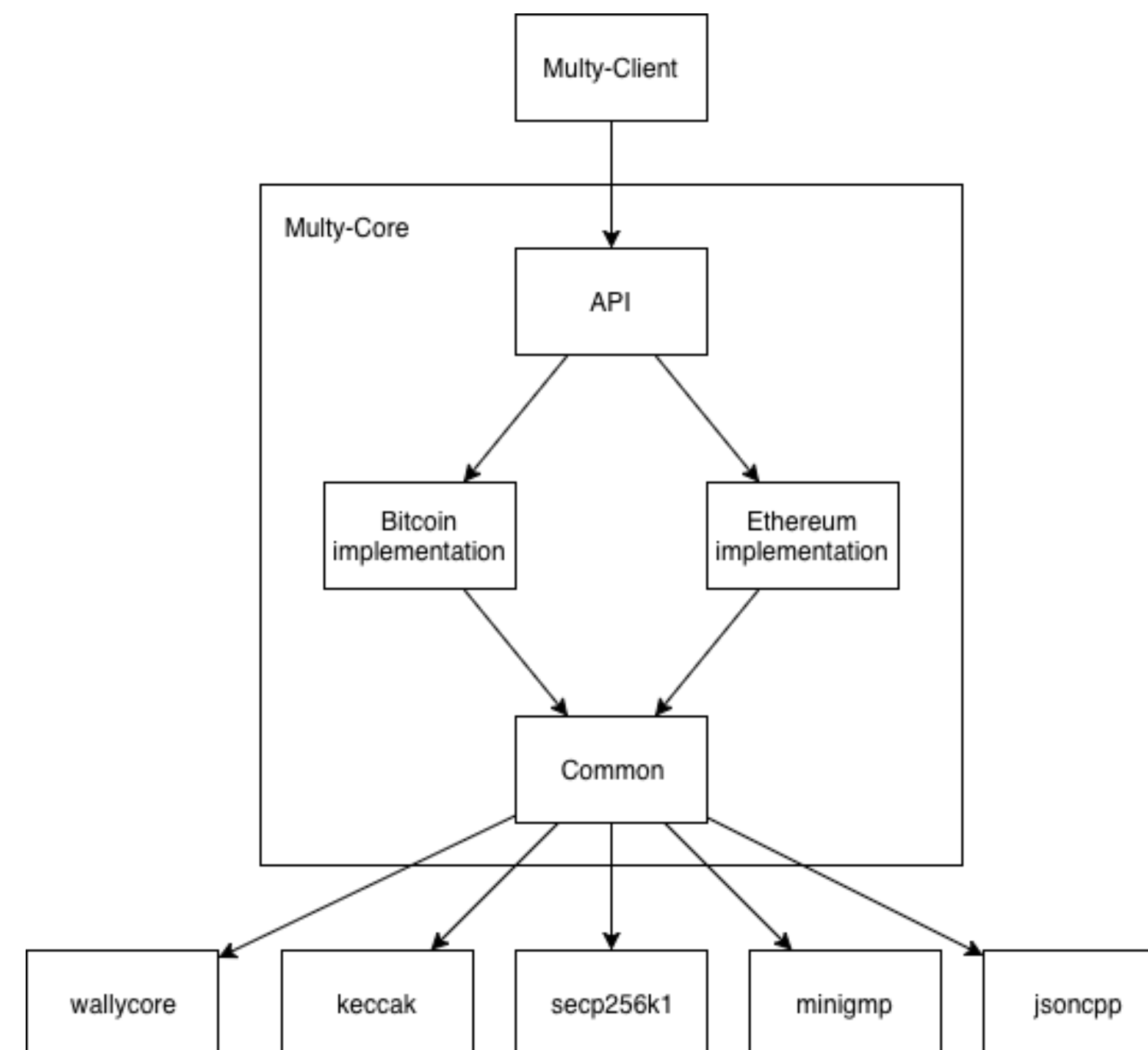
- Data Manager - the most complicated part, handles most of the business logic:
  - Sends requests to Multy-Back (via REST API and WebSockets) and handles responses accordingly, storing result in DB or engaging Notification module if necessary;
  - Interfaces with Multy-Core to generate private keys, and later build a fully serialized and signed transaction using user-provided-data and those stored private keys;
  - Updates data stored in DB according to the user actions on UI and responses from Multy-Back. We use Realm as DB library because it is free, open source, has good performance and convenient to use;
  - Manages DB encryption keys, see for details: Inner-Data-Encryption-(iOS);
  - Manages DB data migration from old schema versions to the new one.



## Algorithm

### Multy Core overview

- API layer - C-like interface, to maximize portability of the library and simplify integration with Java and Swift. Handles and validates data provided by clients, validates output from the bottom-layers sent to clients.
- Blockchain layer - all blockchain-specific logic, like serializing and signing transactions
- Common layer - common code, utilities and wrappers around third-party libraries.
- Third-party dependencies:
  - wallycore - seed phrase generation, deriving BIP44-compliant keys;
  - keccak - hashing library that does SHA3 and Keccak (Ethereum variant of sha3) hashing;
  - secp256k1 - elliptic curve cryptography library, the same as used in Bitcoin and Ethereum;
  - minigmp - library for big integers (values over  $2^{64}$ );
  - jsoncpp - to deserialize client requests and serialize responses from/to JSON strings.

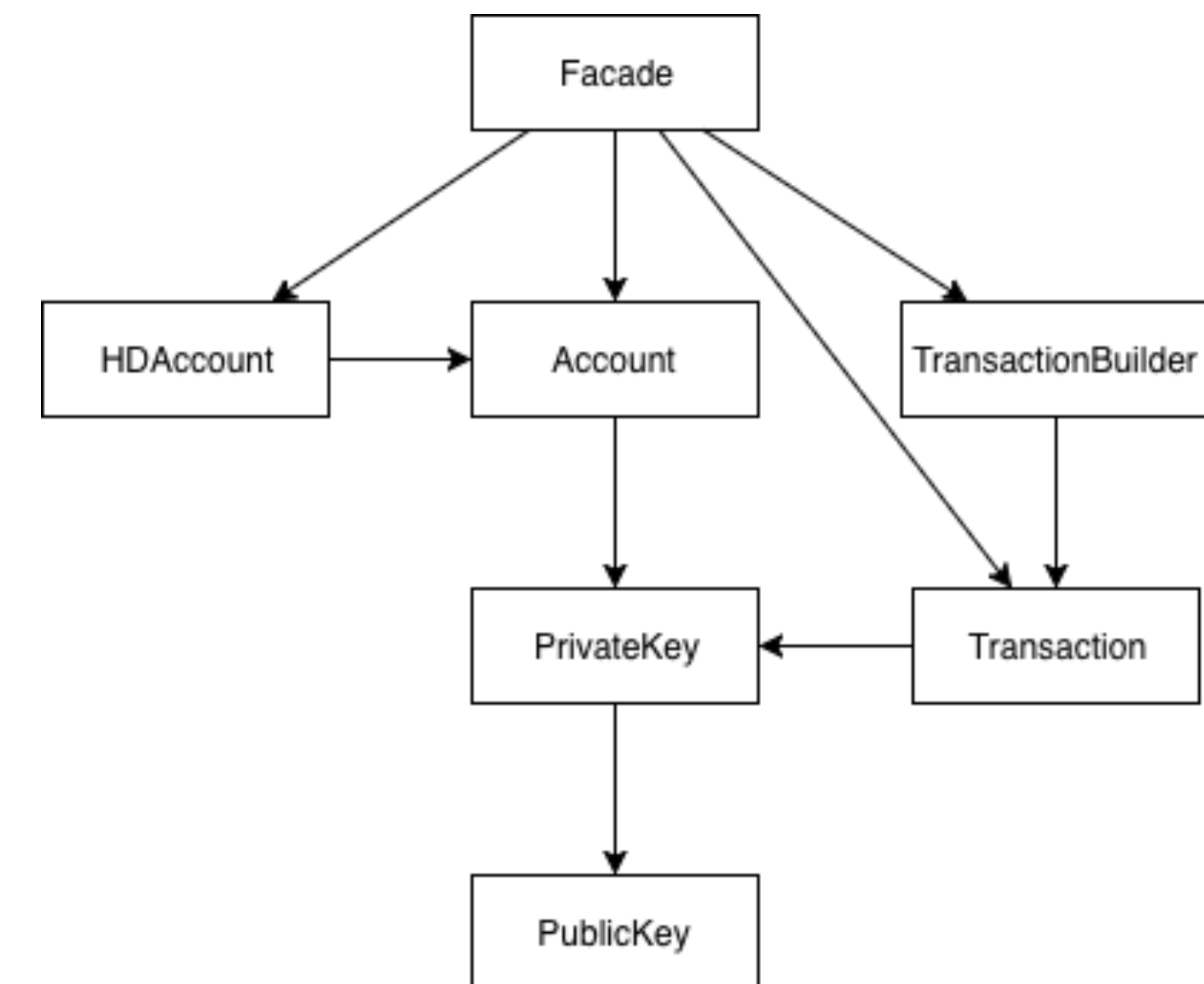


## Algorithm

### Blockchain layer

Where:

- Facade - entry point to the API layer, simple and regular interface ensures that adding new blockchain support is simple.
- HDAccount - controls how Hierarchical Deterministic (HD) wallets are generated for this wallet from root seed phrase in BIP44-complaint way.
- Account - generates private keys and derives account addresses from HD data.
- PrivateKey - signing of arbitrary data and import/export of private keys to user-friendly blockchain-specific format.
- Transaction - serializes and signs transaction with user supplied values to blockchain-specific format.
- TransactionBuilder - array of classes that abstract and simplify transaction creation for Clients through simple and portable JSON API.





# First launch scheme

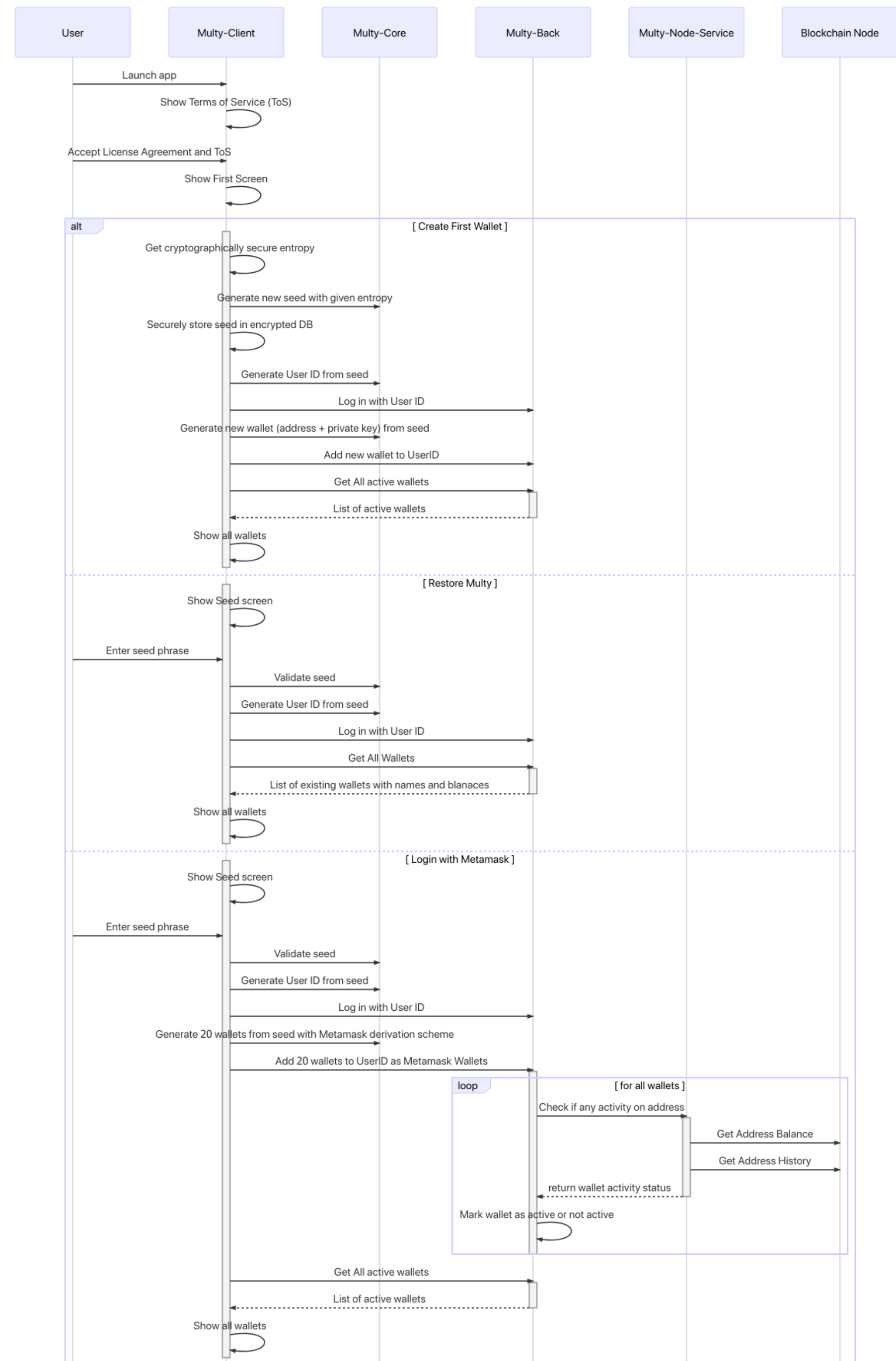
## Integrity

Taking into consideration the first launch scheme, all the use cases are:

- Send transaction;
- Receive transaction;
- View DApp in browser;
- Send a transaction from DApp;
- Create multisig wallet;
- Magic send;
- Magic receive.

Attack vectors:

- Back end;
- Client;
- Communications inbetween;
- Client database file obtained.



## Technologies

Multy-Client and Multy-Core communicate via C-function calls with JSON payload.

Multy-Client and Multy-Back use REST RPC and WS (using Socket-IO).

Multy-Back and Multy-Node-Services use gRPC.

Multy-Node-Service and Blockchain nodes communicate via custom node-specific RPC for both geth and btcd.

Multy back API:

- Rest API
- Socket IO

## Completeness of the solution

We have already shipped both iOS and Android clients.



## Possible areas of performance bottlenecks:

- Client - there isn't many, since client has a very limited number of accounts (typically less than 100) and that number is not growing too much with time.

- Client-Back communication - Back - Communication with single client - Ok due to reasons described above (not too much accounts for a single client).

At the moment, due to DDoS attempt, we have about 2000000 (2 Millions) accounts and wallets created on the back end.

Blockchain - we the block rate is predictable and doesn't depend amount of users that we have. We still parse each and every block to discover transactions fro/to our users.



# Financial model

## Country and product indicators

Type	Country	Income tax	Payroll tax	VAT	Inflation rate	Base risk
Product	Belarus	18%	0%	20%	5,5%	10%

## Monetization hypotheses

- Exchange
- Multisig setups
- Donations
- DApps partnership
- Partner programs

## Market statistics

Forecasted CAC	\$1
Exchange conversion rate	3%
Average Exchange income	\$5
Setup multiSig conversion rate	1%
Average multiSig income	\$2500
Donations conversion rate	1%
Average Donation amount	\$500
Partner programs shares rate	1%
Average Partner programs income	\$1000
DApps incomes rates	\$100
DApps conversion rate	5%



**BITCOIN  
& ETHEREUM  
OPEN SOURCE  
WALLET**

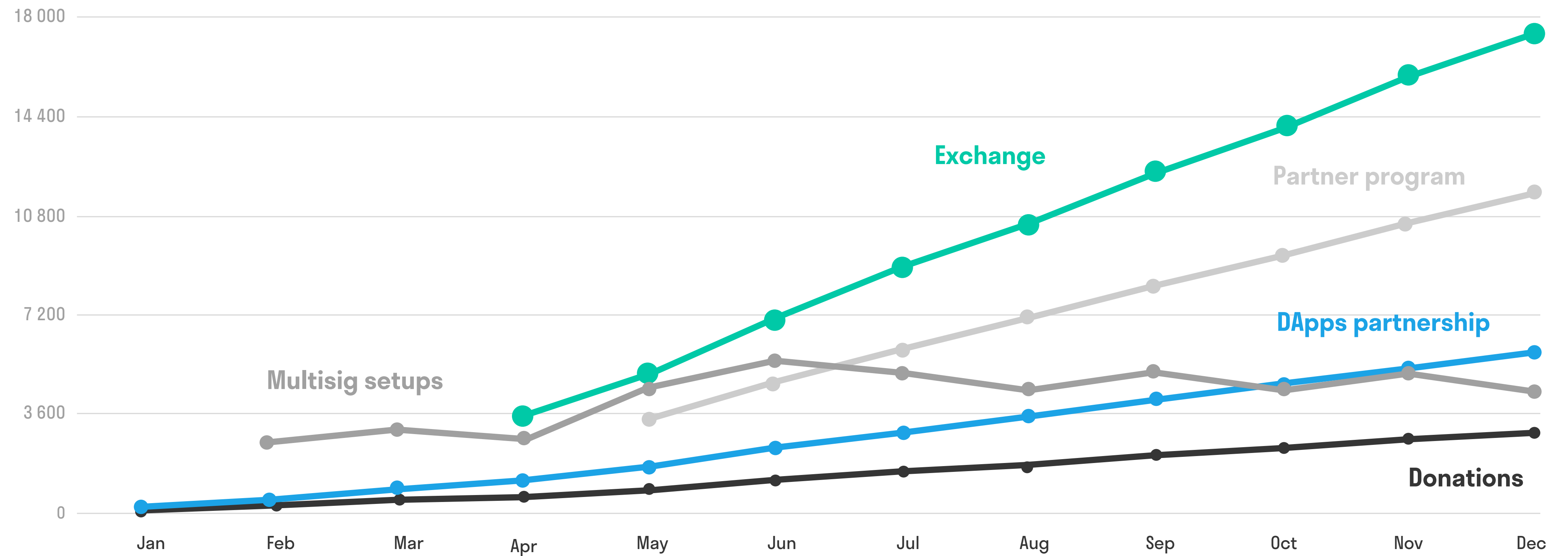






# Financial model

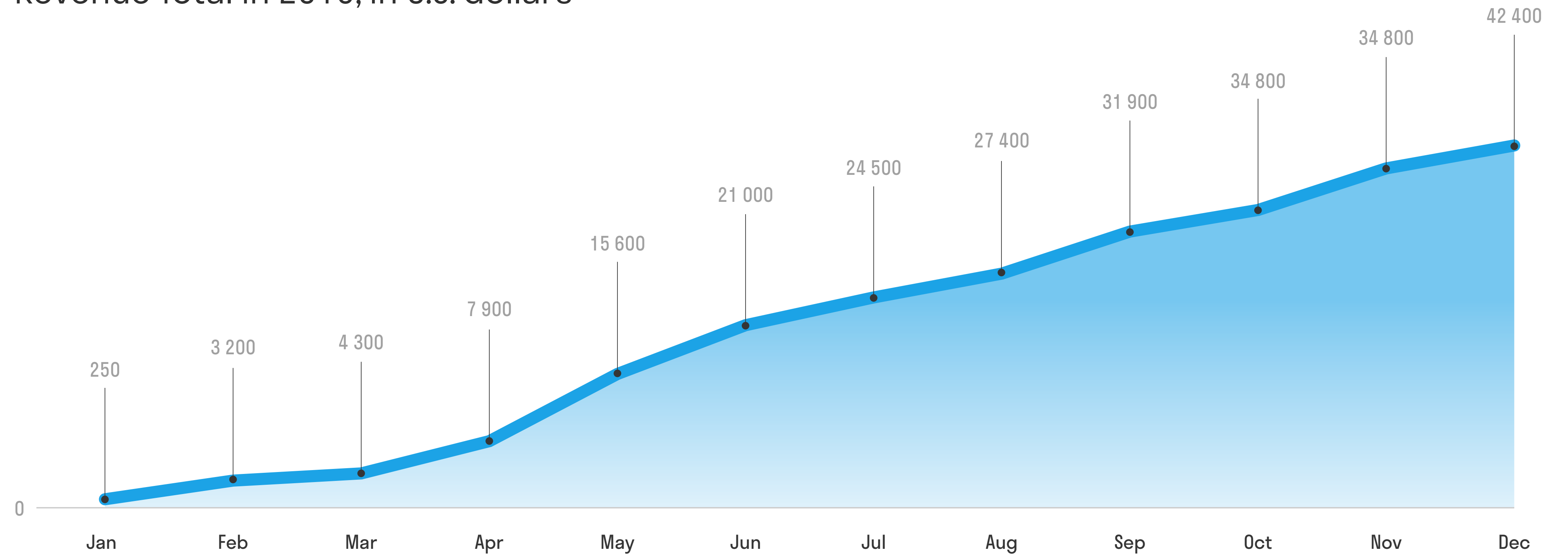
Monetization strategy in 2019, in U.S. dollars





# Financial model

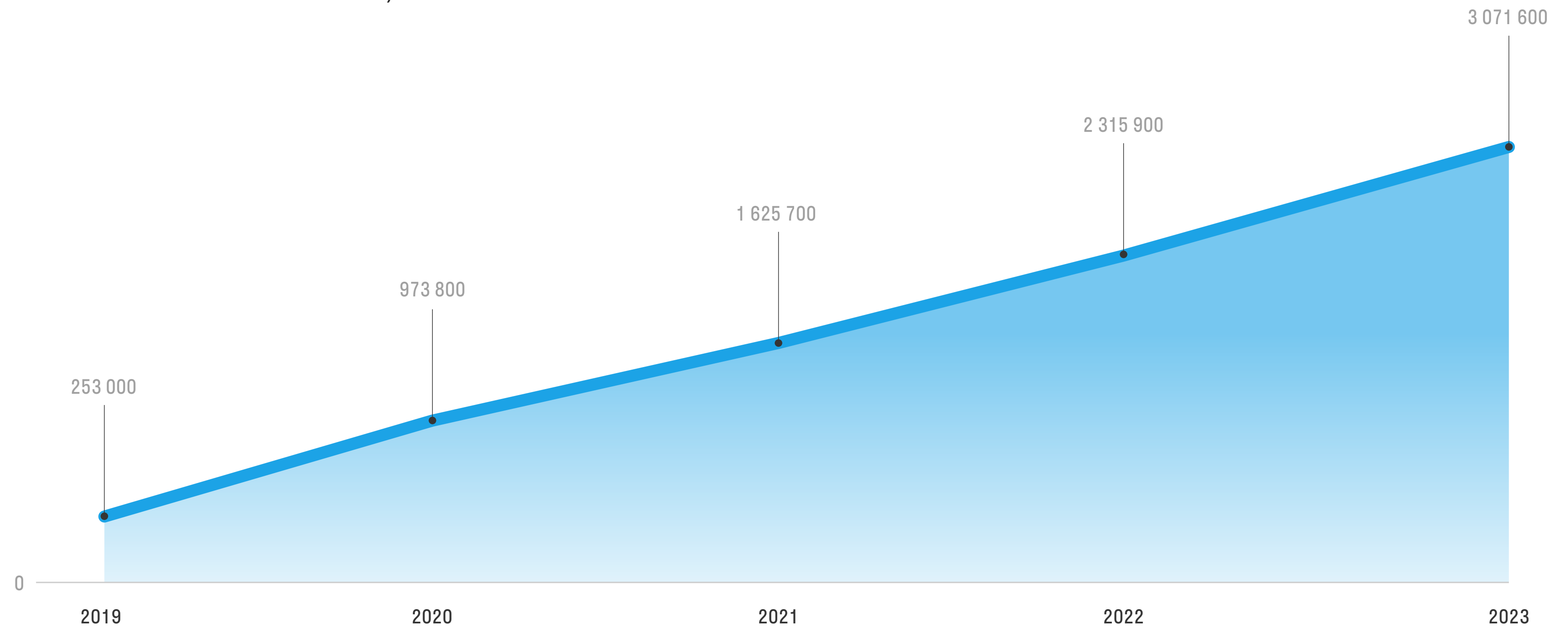
Revenue Total in 2019, in U.S. dollars





# Financial model

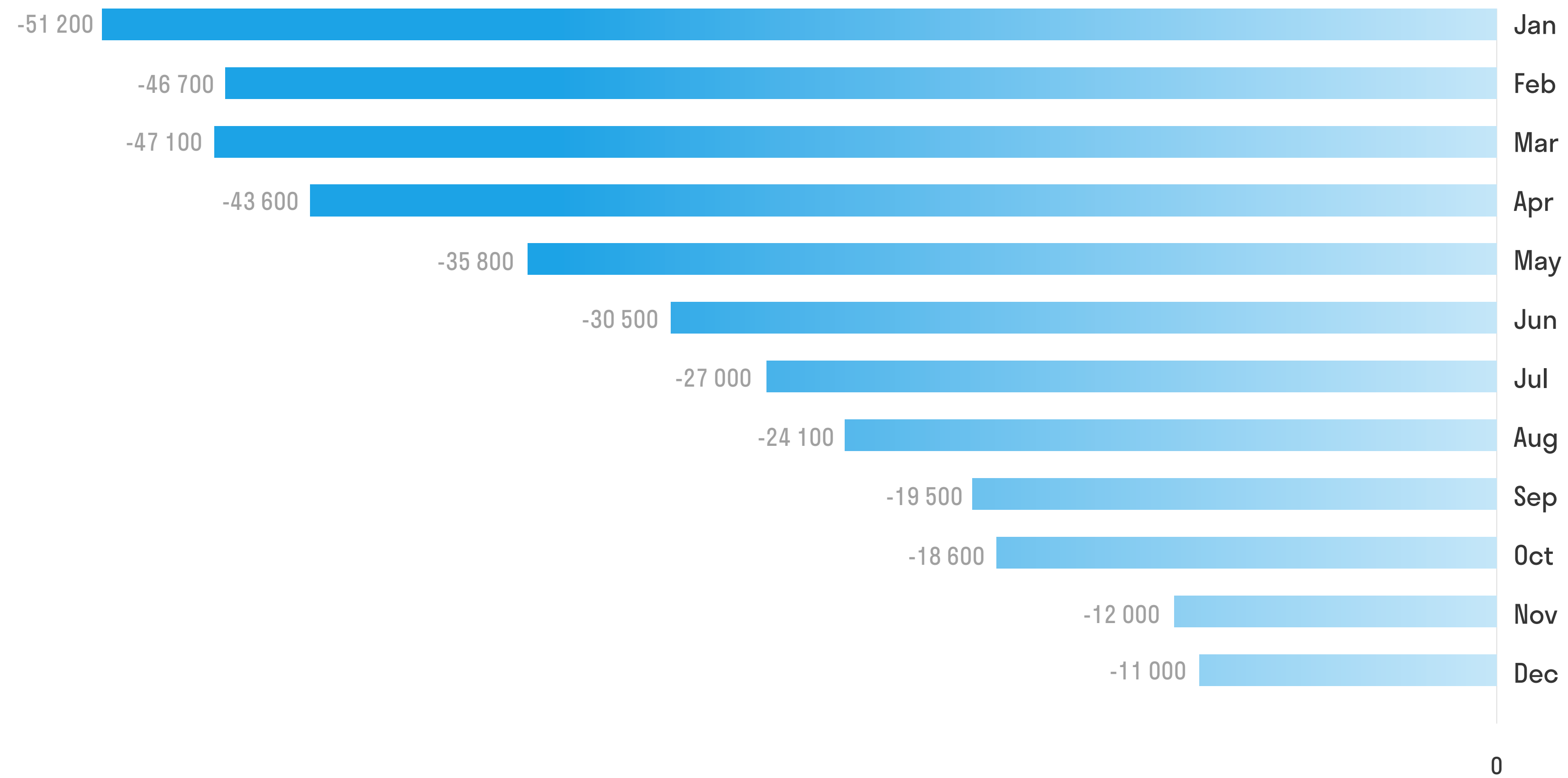
Revenue Total in 2019-2023, in U.S. dollars





# Financial model

Operating profit in 2019, in U.S. dollars

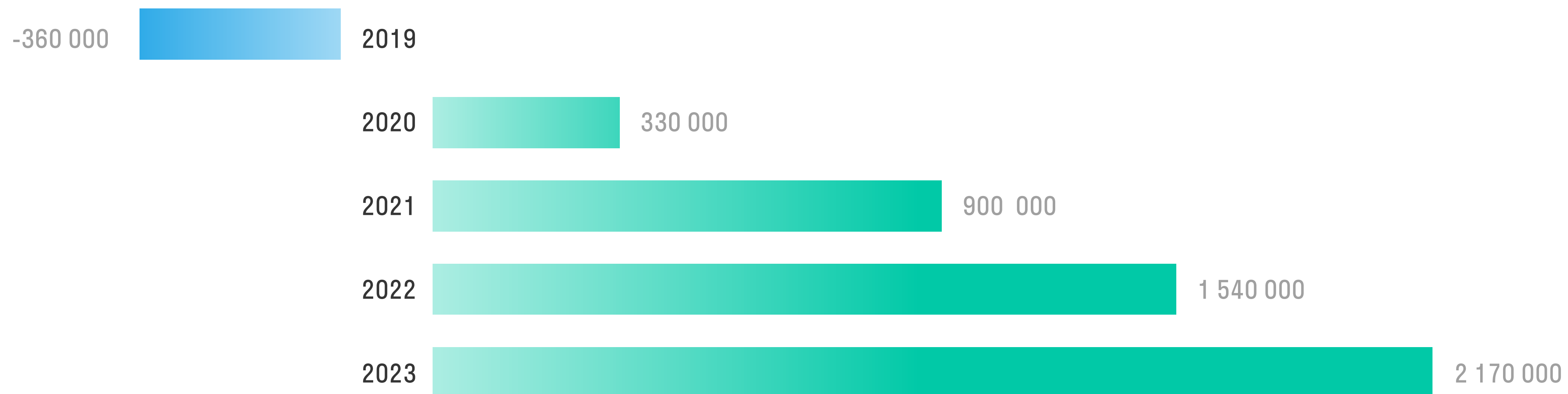






# Financial model

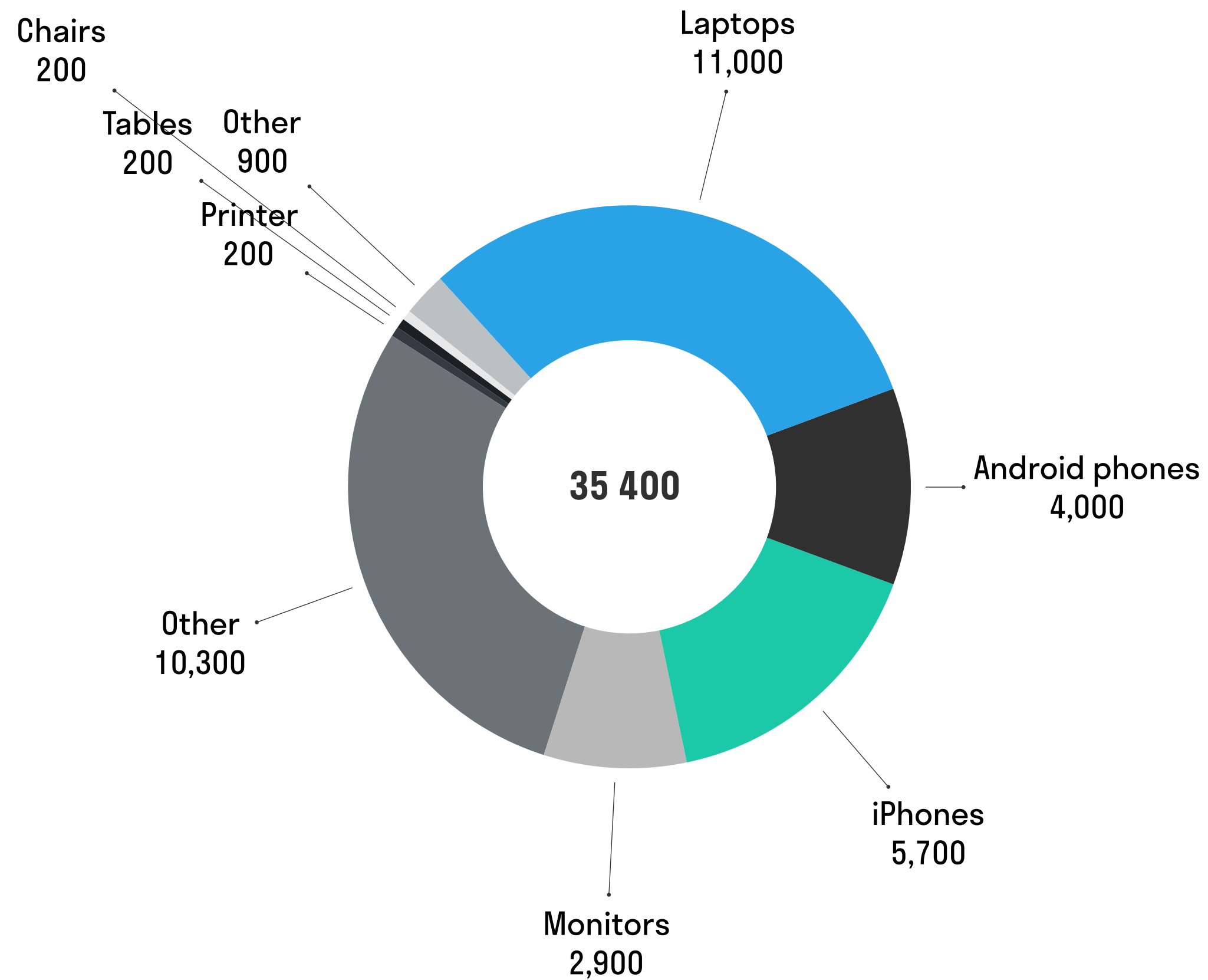
Operating profit in 2019-2023, in U.S. dollars



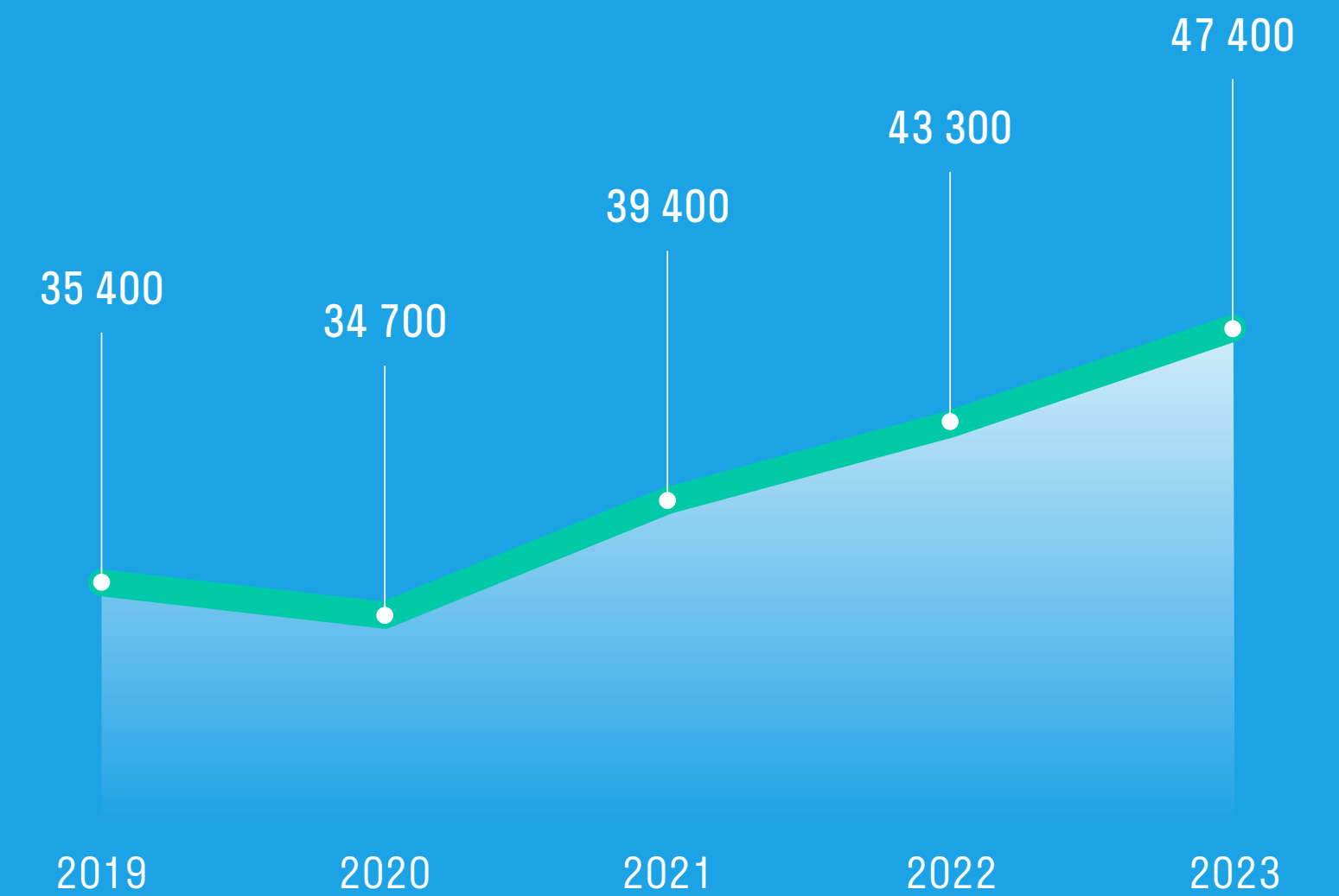


# Financial model

Capital expenditures in 2019, in U.S. dollars



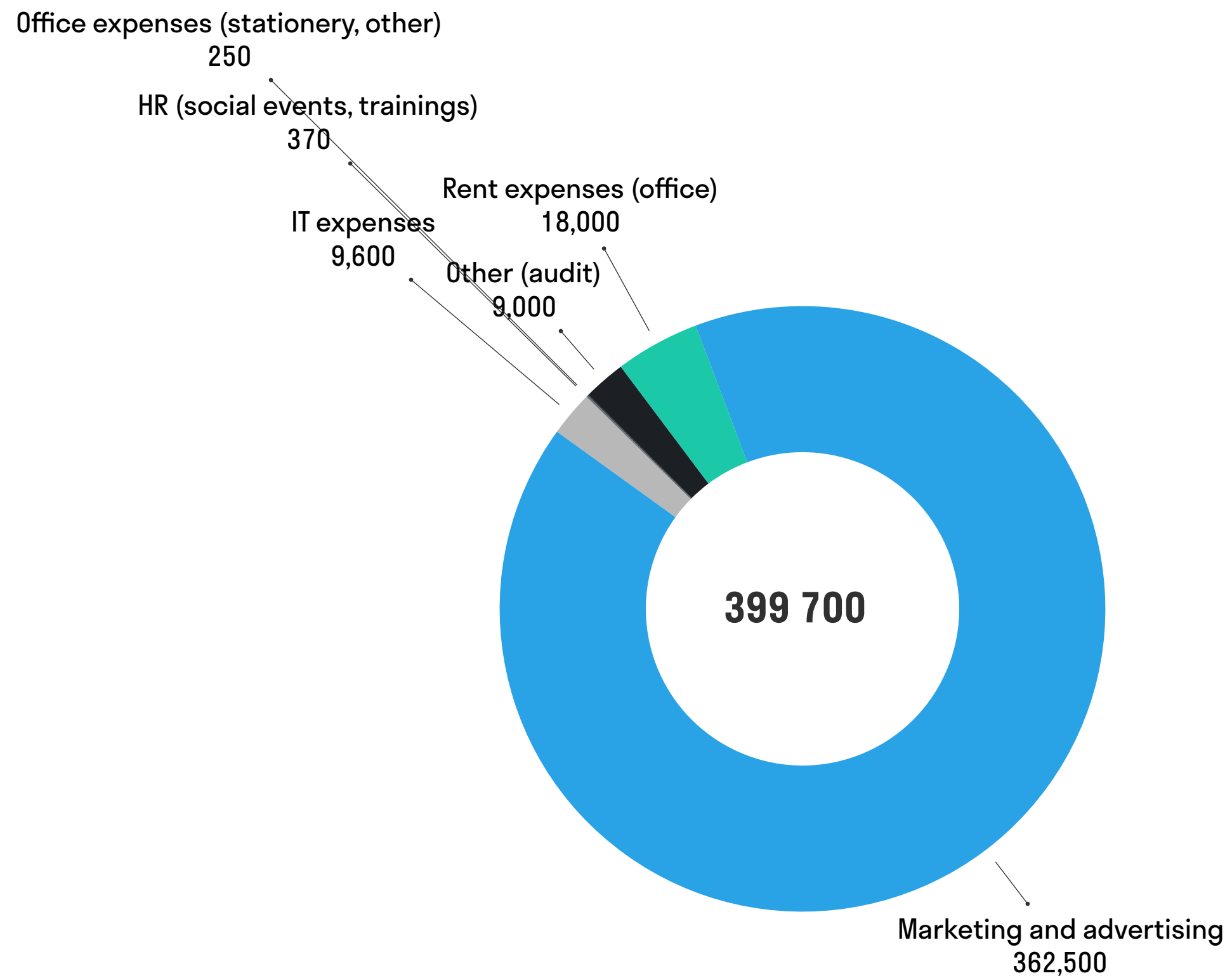
Capital expenditures in 2019-2023, in U.S. dollars





# Financial model

Operational expenditures in 2019, in U.S. dollars



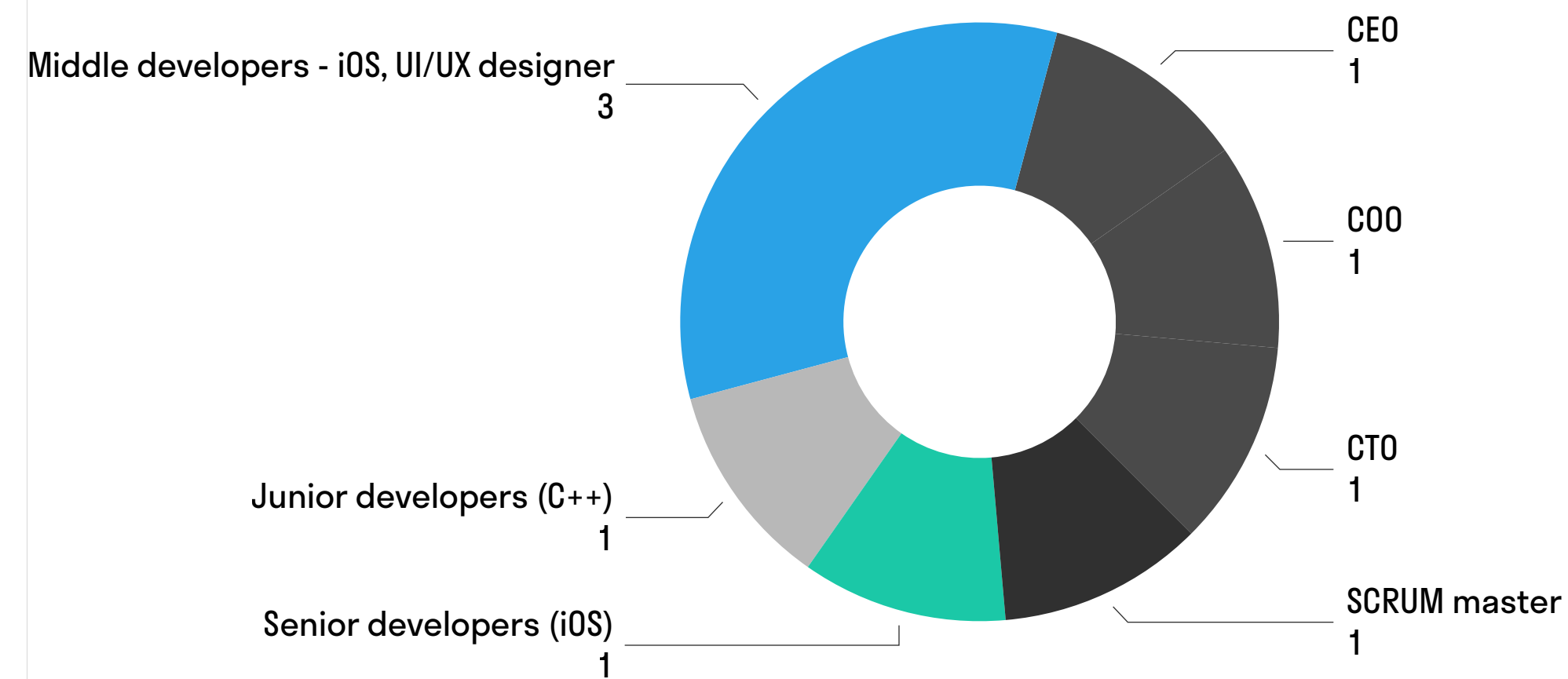
Operational expenditures in 2019-2023, in U.S. dollars



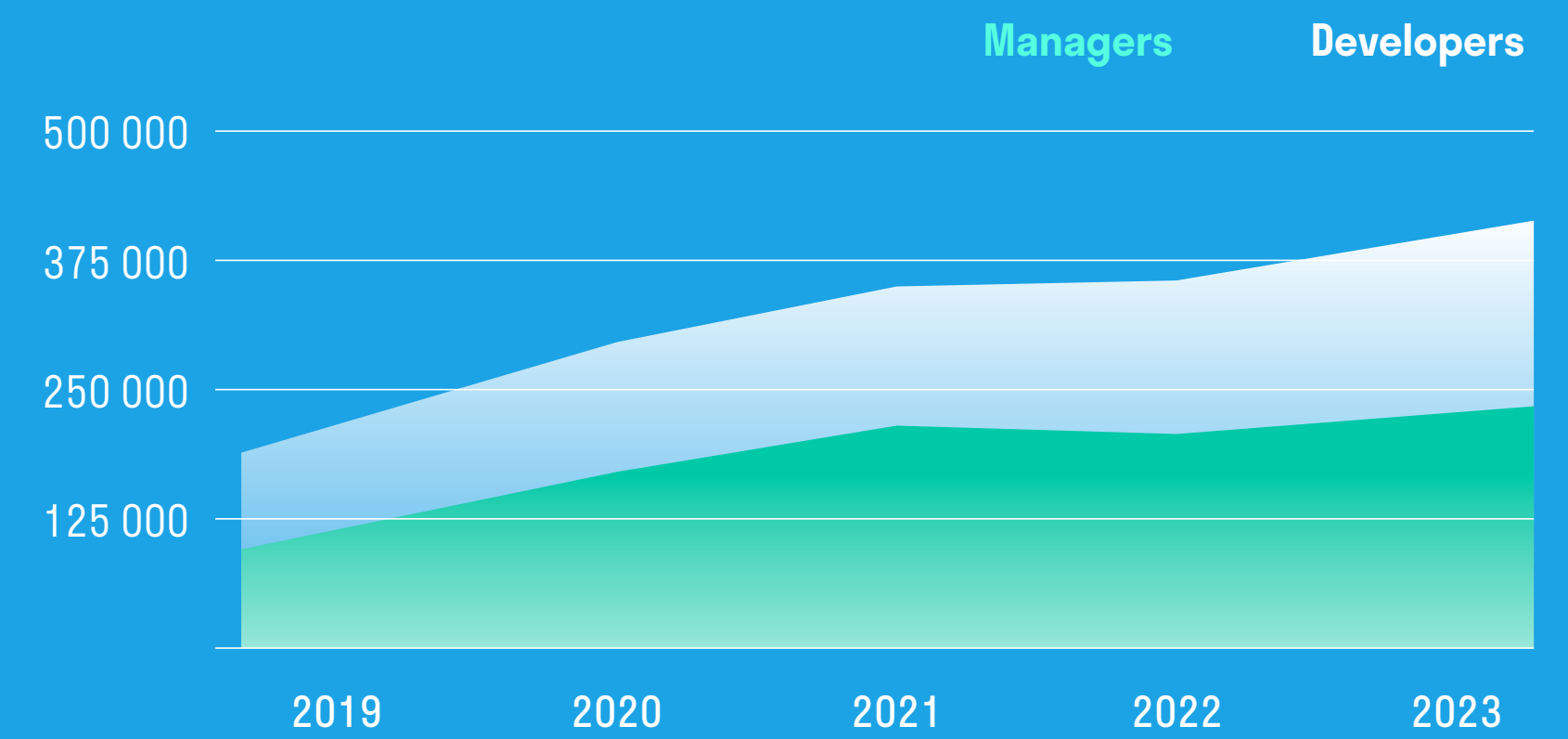


# Financial model

## Team



## Personnel expenses in 2019-2023, in U.S. dollars

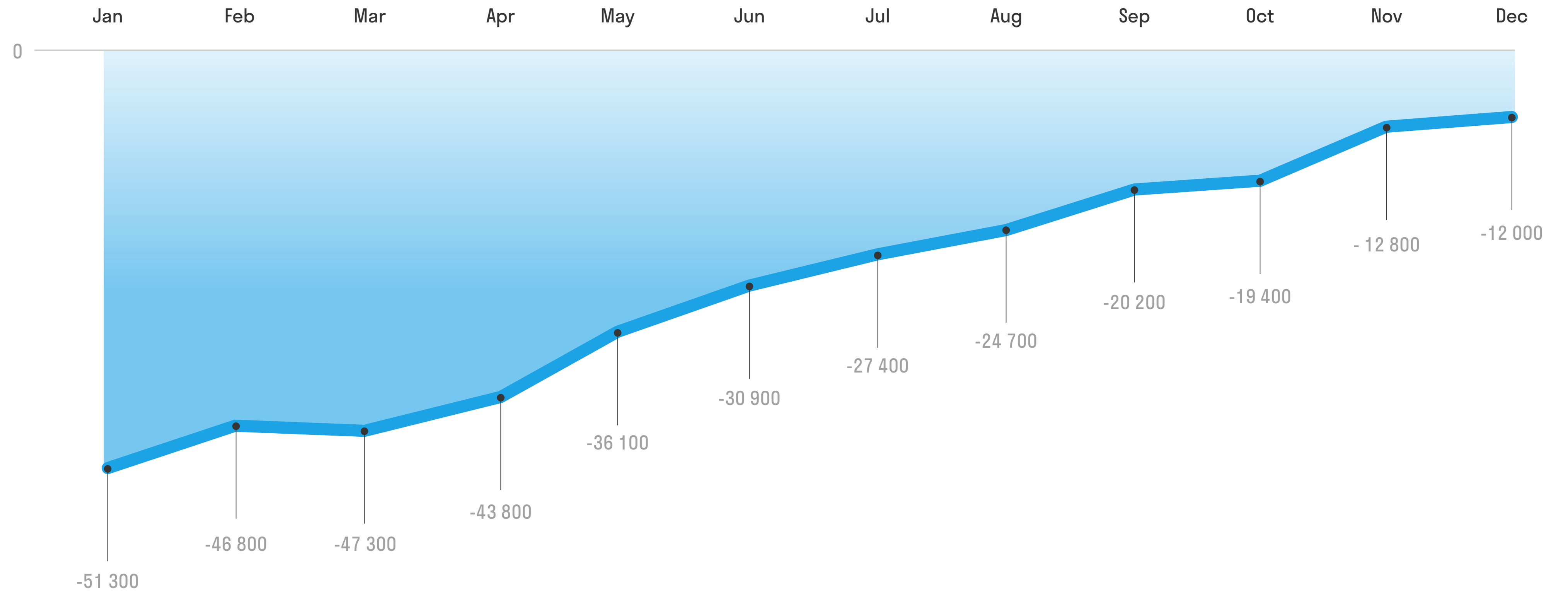






# Financial model

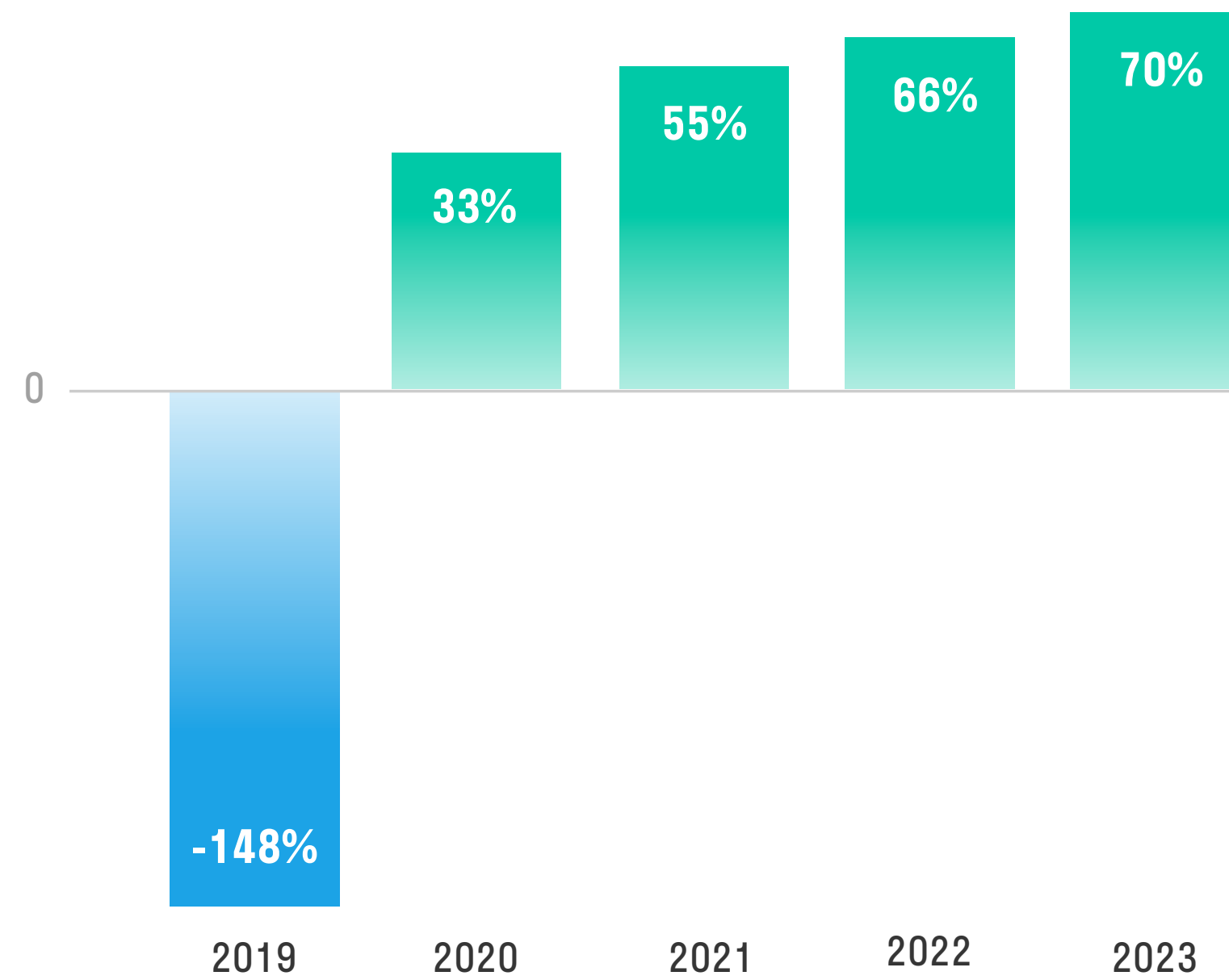
EBITDA in 2019, in U.S. dollars



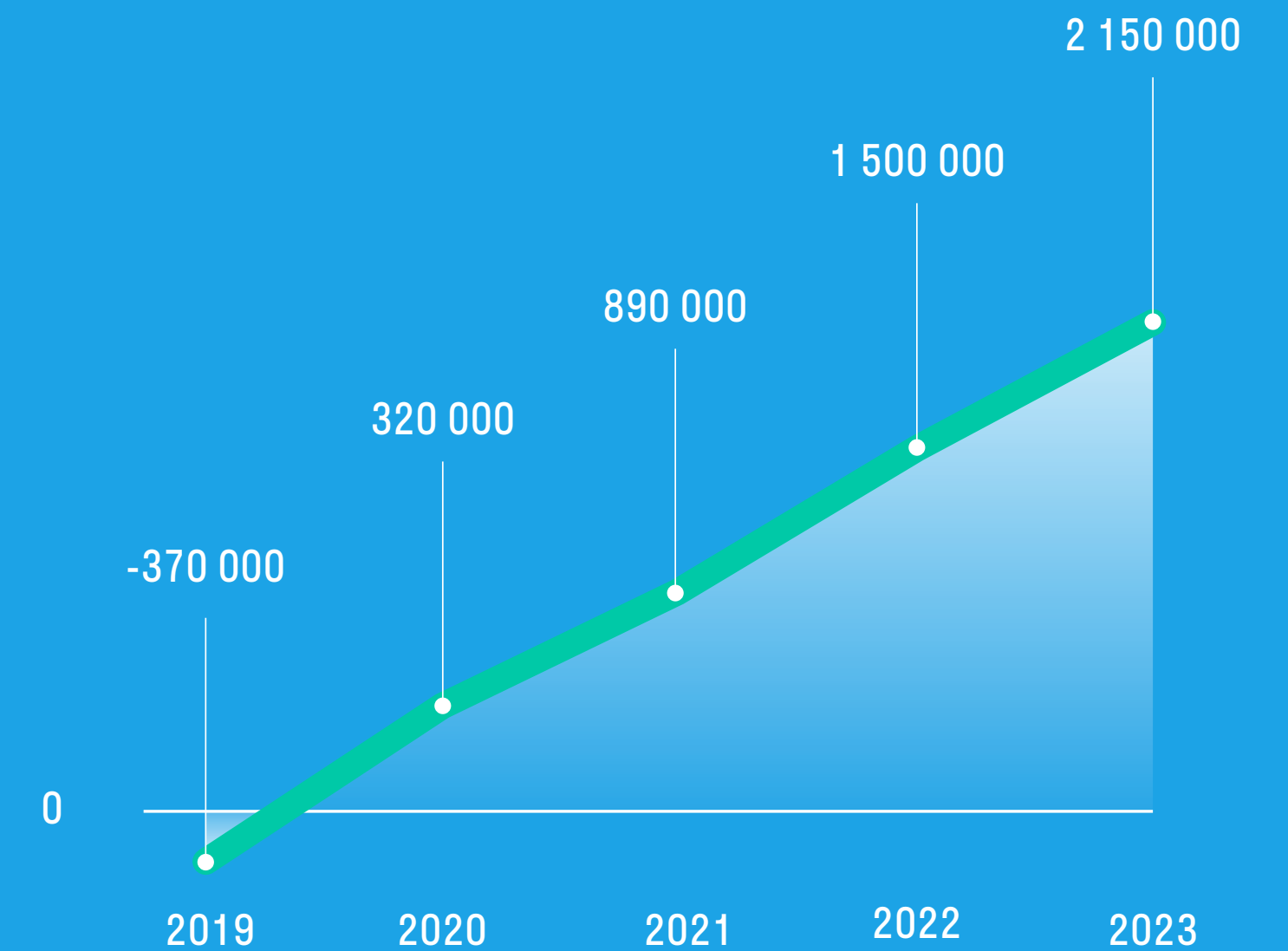


# Financial model

EBITDA in 2019-2023, in U.S. dollars



EBITDA Margin in 2019-2023, in U.S. dollars





# Valuation

## Total for Seed Round **2 304 915 \$**

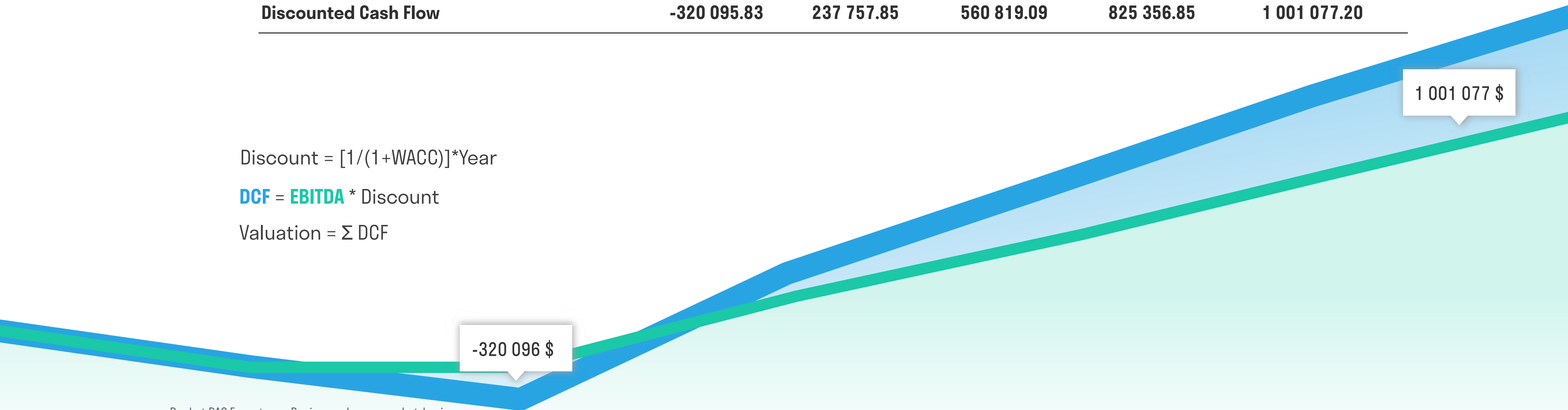
### Income method

	2018	2019	2020	2021	2022	2023
<b>WACC</b>	17%	17%	17%	17%	17%	17%
<b>EBITDA</b>	-373 302.16	-373 302.16	323 367.10	889 537.47	1 526 735.13	2 159 583.47
<b>Discount</b>		0.86	0.74	0.63	0.54	0.46
<b>Discounted Cash Flow</b>		<b>-320 095.83</b>	<b>237 757.85</b>	<b>560 819.09</b>	<b>825 356.85</b>	<b>1 001 077.20</b>

$$\text{Discount} = [1/(1+WACC)]^{\text{Year}}$$

$$\text{DCF} = \text{EBITDA} * \text{Discount}$$

$$\text{Valuation} = \sum \text{DCF}$$





## Civil contracts

We have **typical Employment contracts** which are signed by every team member, the serial number of each agreement is assigned by the Director.

Document management and circulation is outsourced.

## Company charter

De jure Multy operates under **a registered belarusian company (which is a LLC)** founded by 3 partners.

De facto all partnership agreements, responsibilities, equity shares, options portfolio are recorded on blockchain.

## Tax authorities

We are officially registered in Belarus, as any legal entity we are obliged to pay taxes on a regular basis.

## Roles and responsibilities

We **don't have any of the documents prescribing the roles within the team.** That is so because we work under SCRUM methodology. It means that all team members are interchangeable in terms of the functions performed. Formalizing their responsibilities doesn't make any sense.

## Legal registration

We are officially registered as an **LLC Idealnaya rabota.**

## Contractors

As we rent an office we have a **rental agreement** with the landlord.

As our document management is outsourced we have an **agreement signed with an accounting firm.**

## Trade secret

We are developing an open source project that is why we have **no NDA or confidentiality agreements** or agreements setting any limitations on the occupations of the employees as soon as they leave the project.

## Intellectual property

**Everything** developed during the working hours for the benefits of the project **belongs to the company** (this is prescribed in the Employment contracts). Software license agreement is placed on github.



## KYC

**We do not require KYC**, and we hope we will not have to oblige our customers with this procedure in the nearest future, as it will be contrary to our ideology.

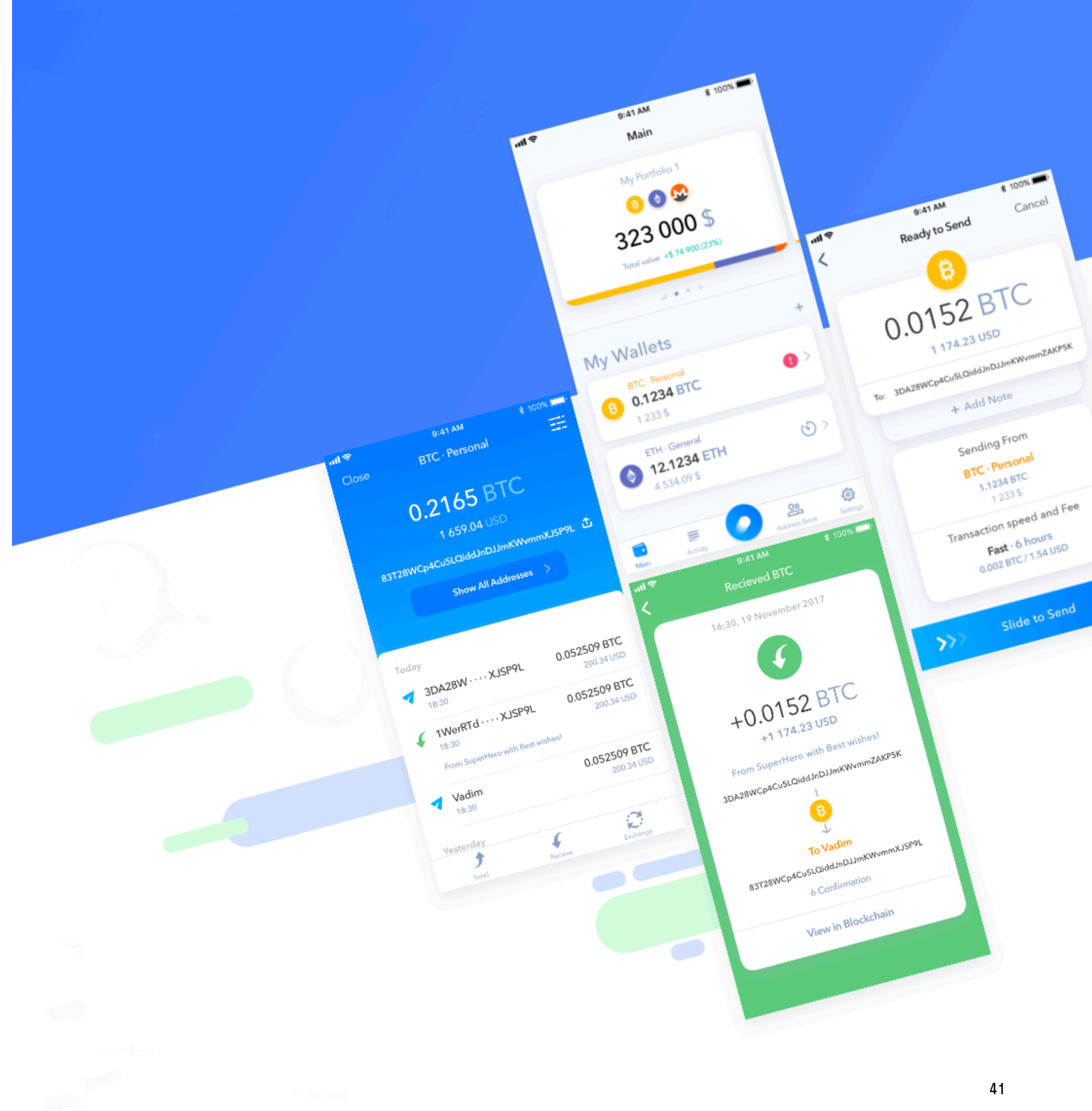
## Personal data protection

We keep as little as possible data about our users, we do not process any data, that is why **we do not fall under GDPR**.

## Terms and Conditions

Terms of use of the application are demonstrated to the user as soon as he/she creates the first wallet in Multy.

Besides, Terms and Conditions of the website use are available on the website footer.





## Safety

### Workplace

We don't have any safety or management quality certificates yet.

Our Director and **COO Alexey Lyakh** is responsible for the safety management system in our company.

**Personal safety kits, fire alarms** are the safety measures provided in our office.

### Location

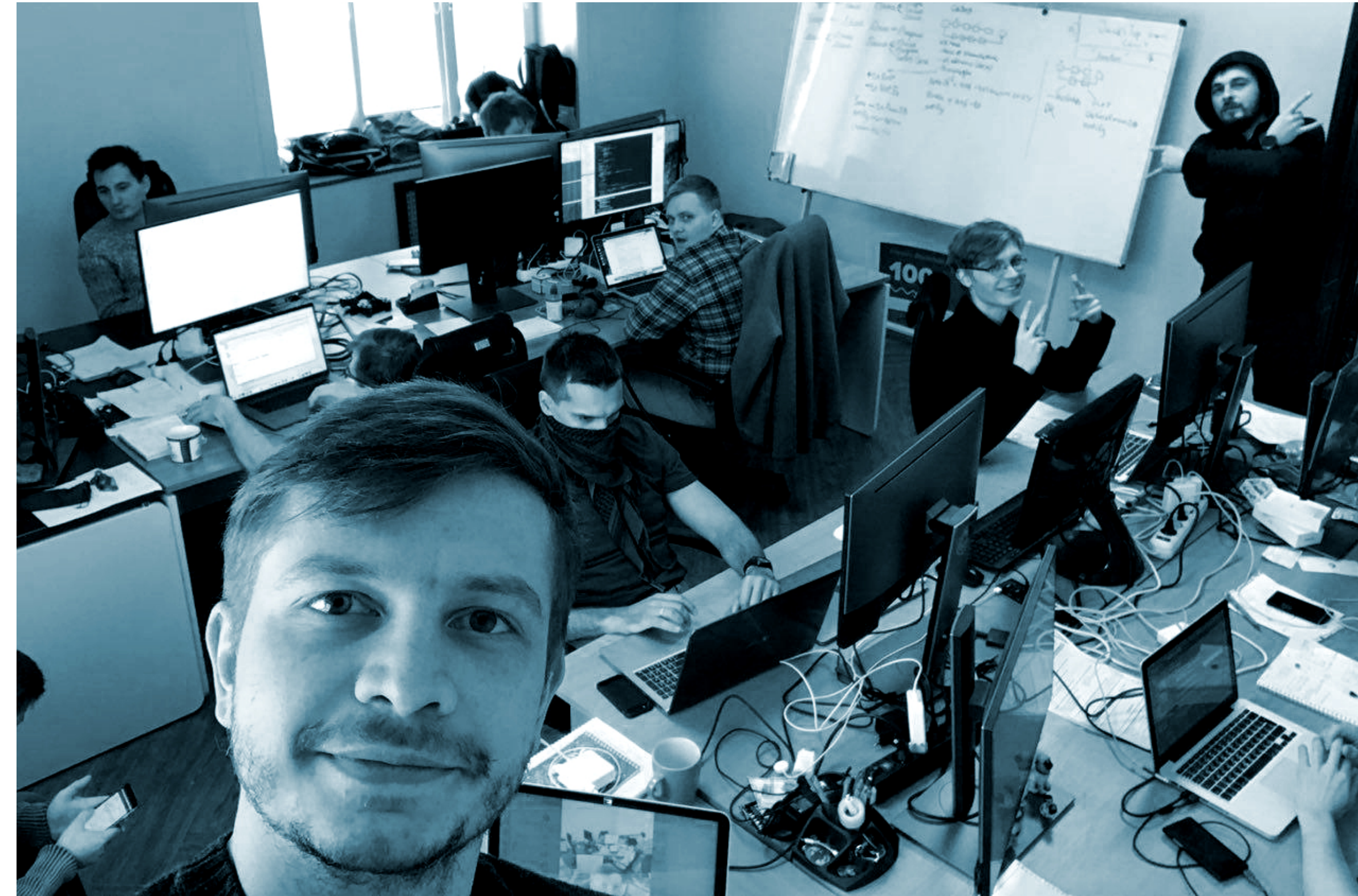
Our office is situated in a residential non-criminal area **5 minutes away from the subway**, **public transportation** has good logistics there.

### Safety rules

All safety rules are specified in the Induction training document and in the **Employment agreement**.

### Medical insurance

We **do not provide** our employees with any kind of medical insurance (but only the one which is required by Belarusian legislation).





## Country specific risk

### Mining

There is **no need to have any specific license** for mining in the Republic of Belarus.

### Smart contracts

It doesn't matter what means are used for the transaction to be made. If it is a smart contract, then the cryptocurrency received is exchanged for fiat money on the stock exchange and filed to the tax authorities. So **smart contracts are accepted** as the source of the companies' transaction data.

### Cryptocurrency

**Cryptopayments are not popular** among local vendors. The point is that financial institutions do not accept these operations yet.

### Crypto-taxation

All the transactions that we ever make are in fiat money. So we fall under **regular taxation norms only**.

As there is no national crypto stock exchange yet, then no extra-taxation can be exposed on such transactions.

### Blockchain startups regulation

**Belarus is among top 10 blockchain friendly countries** of the world. But legal authorities do not use blockchain for their own specific interests yet.

### ICO

There were no successful ICO campaigns registered in Belarus yet.

### Startup registration

First you register as a **regular legal entity**, submit an application to become a **resident of High Technology Park**.

After that you may register as a crypto-company and work with the stock exchange.

### Bank account

**Banks** in our country **do not work with cryptocurrency**.

We work through a stock exchange and transfer fiat money to our bank account.

## HR risk

### HR management

Multy's **CEO Vadim Makovsky** is responsible for all **HR and recruiting tasks** due to the great experience as an IT-entrepreneur.

Besides, any team member may take part in the interview of a potential candidate.

### Hiring stages

Everything depends on the position, personal qualities of a candidate, his/her professional background. Usually it is **screening**, then an **interview with CEO** and some team members, **test tasks** from CTO.

### Probationary period

A probationary period usually lasts for **1-3 months**. It depends. This period is necessary to understand if a person can work collaboratively with the team, display interest in the project, work harder in case something is unknown.

### Training

Any team member can ask to study any relevant course, or to take part in a workshop. As soon as the team agrees we pay for such necessities. The **monthly planned budget for such expenses is \$500**.

But we do not hold any trainings on a regular basis, apart from the ones which include cooperative research of new technologies, for example.

### Office control system

We have got **video surveillance cameras**. Besides, entering the territory of the office and inside the office is admitted only for those who have special chips.

### Salary reviews

We've got a KPI which all team members have to follow. But there is no schedule for salary reviews.

Salary levels are determined by the ability of the project to **attract external funding**.

### Office

We work in an **open-space office** with 2 boardrooms, a canteen (with a refrigerator, coffee machine and a microwave oven) and a lounge zone. There is a parking zone and a gazebo outside. Toilet and bathroom are also available on the floor.

### Equipment

We have all the equipment necessary for comfortable work: tables, swivel office chairs, and even beanbag chairs, **laptops** (Macs released in 2015-2017 years), Dell and Mac **monitors, keyboards** and so on.

Supplementary equipment includes: a Jacuzzi, a fireplace, a tennis table, a chin-up bar, a PlayStation, a balance Board.

### Legislation

Our **director Alexey Lyakh tracks any changes** in the Belarusian legislation on a regular basis and visits relevant conferences dedicated to these matters.



# M Risks

## HR risk

### Performance management

We practice SCRUM methodology per se.  
Everyday morning we hold daily SCRUMs where each team member shares achievements, blocks and plans.

But there is **no prescribed HR policy** in our company yet.

### HR documents

As we do not have any HR manager in our team there is no need for formalized HR documents yet, **everything is agreed orally and prescribed by SCRUM methodology.**

### Team building

We organize **corporate parties** ones a quarter approximately.

The screenshot shows a Jira Backlog for the 'Multy board' project. The interface includes a left sidebar with navigation options like 'Multy board Board', 'Backlog', 'Active sprints', and 'Reports'. The main area displays a list of issues under the heading 'Multy Sprint 29. 17.12-28.12' with 52 issues. Each issue entry includes a title, a priority indicator (green square), an assignee profile picture, an issue ID (e.g., MUL-2123), a status indicator (up/down arrow), and a count (e.g., 3). Some issues are categorized with colored labels like 'Metamask', 'Portfolio', 'CORE JSON API', 'Segwit', and 'BTC'. A 'Start sprint' button is visible in the top right corner of the backlog view.

Issue ID	Assignee	Priority	Status	Count
MUL-2123	[Avatar]	High	Up	3
MUL-2165	[Avatar]	High	Up	3
MUL-2106	[Avatar]	High	Up	1
MUL-2166	[Avatar]	High	Up	3
MUL-545	[Avatar]	High	Up	0
MUL-2111	[Avatar]	High	Up	2
MUL-2116	[Avatar]	High	Up	2
MUL-1932	[Avatar]	High	Up	1
MUL-2179	[Avatar]	High	Up	3
MUL-2184	[Avatar]	High	Up	2
MUL-2056	[Avatar]	High	Up	2
MUL-1847	[Avatar]	High	Up	2
MUL-2060	[Avatar]	High	Down	2
MUL-1941	[Avatar]	High	Up	3
MUL-2057	[Avatar]	High	Up	2
MUL-2114	[Avatar]	High	Up	3
MUL-2130	[Avatar]	High	Up	1
MUL-2115	[Avatar]	High	Up	2



# Risks

## HR risk

### Formalization of duties

All team members are familiar with the **code of conduct** and with the working guide for the developers.

But there are no specific checklists for the enrollment or de-activation procedures.

### Recruitment

We fulfill recruitment ourselves by word of mouth without publishing vacancies on the public head hunting sites. Statistically we have nearly **3-5 candidates for each open position**.

### Corporate culture

We are true adepts of the **SCRUM** methodology and philosophy, we encourage horizontal relations and **unstressed culture**.

### Dinners

We have an arrangement with a **meal delivery service**, however is paid for by each employee and is not passed down to the company.

Still every week we choose one day when we order **corporate-paid pizzas**.

### Working hours

**Every team member logs on the time necessary for each task** assigned to him in the current sprint. At the end of the month Director reviews the metrics.

The overworked time is not extra paid as everybody takes the tasks which he believes he will manage to perform within one sprint in accordance with his competence and comfortable working pace.

### Company's structure

SCRUM methodology supposes a **horizontal hierarchy** and development.

### HR brand

**We are well known** among all crypto enthusiasts as we regularly take part in the relevant event and conferences.

Besides, our CEO Vadim Makovsky is one of the regular lectures at Imaguru Blockchain School. This turns Multy into a **crypto and blockchain expert brand**.

## Operation and financial risk

### CFO

We **don't have** a CFO in our team.

### Lawyers and legal advisors



#### Alexey Lyakh

Our Director and COO is an **in-house lawyer** at the same time.



Besides, in Minsk there is a powerful organization called **Association of the distributed ledger technology**. We have agreements with the members of this organization on legal consultations.

### Risk management policy

We prepare a **SWOT analysis** on a regular basis in order to understand the market trends and the arising threats for the project, this helps us be attentive to the market signals and adjust our strategies to the market needs.

### Internal control

**Jira and github** are the primary performance control systems which we are actively using while organizing all the working processes in our company.

### Financial statements

We prepare financial statements under **Belarusian standards only**. This function is outsourced to Raikiri.

### Business plan

Each month Director makes a review of the planned costs and the actual ones so that to optimize them in the future.

Business plan is constantly reviewed and updated by Multys' CEO Vadim Makovsky.

### Metrics

Being non-profit team at this very moment **we do not track any metrics yet**, apart from costs per month.

As soon as we have the revenue stream we will run all the metrics related to it.





# PR & Marketing

## Landing page

<http://multy.io/>

## Articles and publications

Professional media

- [Cryptoninjas: Bitcoin and Ethereum wallet Multy enables multi-signature for Android and iOS](#)
- [Prnewswire: Multy Crypto Wallet Enables Multisignature Scheme for Android and iOS](#)

We have got several articles in the local startup media about our project:

- [Belbiz: BTC investments from Cyber Fund to Multy startup](#)
- [Belbiz: Multy. Plans for the future](#)

## Dispatching system

We **tested email marketing** techniques as one of the marketing instruments, but in our case it gave **no results**.

## Bounty

As we didn't conduct any ICO campaign yet we **didn't organize any bounty campaign** to support it.



CEO Vadim Makovsky at WebSummit, 2018







# Resources & Assets

## Investment round

We have closed pre-seed (**40 BTC in November, 2017**) and partly seed rounds with investments from Cyber Fund.

So it means that we are at the **Seed round** at the moment.

## Reviews

**Alpha release of our Wallet Multy took place a year ago.**

Reviews are available on app stores where one can download our wallet.

## Team

There are 9 professionals in our team:

- CEO
- CTO
- COO
- SCRUM-master
- 2 iOS developers
- Lead iOS developer
- C++ / Golang backend developer
- UI/UX designer

## Preliminary contracts

We **don't have any**.

## Vendors

Our vendors are - **Google Play Market and Apple Store**. We have signed all necessary agreements with both.

## Marketing research

Unfortunately, we **haven't conducted any high-level research yet**. But we still regularly research the market for any updates and any potential competitors.

At the same time, no budget is planned for such research. But we allocate the budget on marketing occasionally, as and when is necessary.

## Intellectual property

Intellectual property **belongs to the Belorussian LLC Idealnaya rabota** under which Multy is being developed. Trademark is not registered.

License for our software can be found on github.



# Resources & Assets

## Novelty level

Multy is at the fourth novelty level according to the methodology: The implemented **solution has no prototypes**. The idea is brand-new.

## Training budget

**500\$ per month** are allocated for the team for their occasional necessities like courses, extra work shops, tickets to the relevant events and so on.

## R&D budget

**All the investments attracted for the pre-seed round** were used for R&D and development of an application using innovative technologies.

The amount of hours spent on the research is logically lower now, but is a subject to a change should the need be.

## Co-founders share

**17.5%** of the company's equity belongs **to investors**. The rest is owned by the team.

**10% of the equity are reserved for the next round.**

## Tangible assets

All our tangible resources include: monitors, laptops, smartphones, furniture and other elements of equipment.

## Costs of attracting new customers

All the users we have today have been organically generated.

We are about to start an active marketing campaign.

**The forecasted CAC is nearly \$1-1.5.**



# Rocket DAO

Rocket DAO is your **Due Diligence and business plan companion** should you be an innovative **startup** seeking recognition or an **investor** requiring a thorough assessment for the potential investment idea.

Learn more about the project on our website [rocketdao.io](https://rocketdao.io)

Contact us out for more details via [support@rocketdao.io](mailto:support@rocketdao.io)

# Rocket DAO

Uniting startups, investors and experts.

This document provides a detailed business plan based on the methodologies developed by a decentralized Rocket DAO expert community.

January 2019

[rocketdao.io](http://rocketdao.io)