



Telegram

PRIMER

Table of Contents

Introduction	3
Problem Statement	3
Outline of the Vision	4
A Brief History of Telegram	5
Telegram Open Network (TON)	7
TON Blockchain	7
Infinite Sharding Paradigm	7
Instant Hypercube Routing	8
Proof-of-Stake Approach	8
2-D Distributed Ledgers	8
TON Platform	8
TON Storage	8
TON Proxy	9
TON Services	9
TON DNS	9
TON Payments	9
Telegram Messenger-TON Integration	10
Light Wallet	10
External Secure IDs	11
Ecosystem	12
Bot Platform	12
Groups and Channels	12
Digital Content and Physical Goods	12
A Gateway to Decentralized Services	13
Uses of TON as a Cryptocurrency	13
Roadmap	14
Token Distribution	15
Use of Funds	17
Governance	18
Team	19
Founders	19
Other Notable Team Members	20



Introduction

Cryptocurrencies and other blockchain-based technologies have the potential to make the world more secure and self-governed. However, to this day, no consensus-backed currency has been able to appeal to the mass market and reach mainstream adoption.

This paper outlines a vision for a new cryptocurrency and an ecosystem capable of meeting the needs of hundreds of millions of consumers, including 200 million Telegram users.



Launching in 2018, this cryptocurrency will be based on multi-blockchain Proof-of-Stake system — TON (*Telegram Open Network, after 2021 The Open Network*) — designed to host a new generation of cryptocurrencies and decentralized applications.

The protocol and other components of TON are described in detail in the Technical White Paper, while this document focuses on a general overview of the proposed technology and its uses.

Problem Statement

Bitcoin has established itself as the «digital gold», and Ethereum has proved to be an efficient platform for token crowd sales. However, there is no current standard cryptocurrency used for the regular exchange of value in the daily lives of ordinary people. The blockchain ecosystem needs a decentralized counterpart to everyday money — a truly mass-market cryptocurrency.



Despite their revolutionary potential, existing cryptocurrencies lack the qualities required to attract the mass consumer. There are three main hurdles in today's environments:



The established blockchain networks — Bitcoin and Ethereum — play important roles in the ecosystem, but don't have the capacity to replace VISA or Mastercard. In their current architecture they are limited to a maximum of **only 7 transactions per second for Bitcoin and 15 transactions per second for Ethereum**, resulting in insufficient speeds and higher transaction costs.



Regular users starting to engage with Bitcoin and similar technologies **often get confused** when trying to buy, store, and send their coins.



The market of goods and services that can be bought with cryptocurrencies is limited, and the **demand** for crypto-assets **comes mainly from investors, not consumers**.

The current state of blockchain technology resembles automobile design in 1870: it is promising and praised by enthusiasts, but inefficient and too complicated to appeal to the mass consumer. As a result, no cryptocurrency or decentralized platform has gone truly mainstream, and centralized solutions continue to dominate the market.

Outline of the Vision

Exchanging value should be as easy as exchanging information, and blockchain technology offers the ideal foundation to make this a reality. To reach mainstream adoption, a cryptocurrency — and its underlying blockchain design and ecosystem — requires:



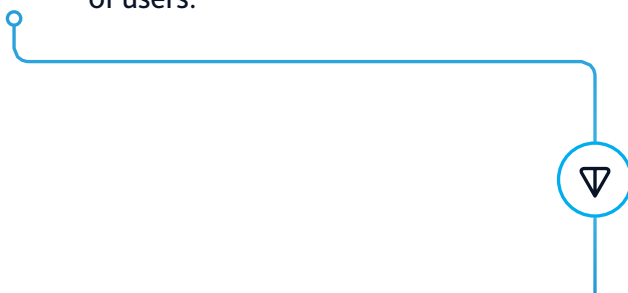
Speed and scalability that allows for processing millions of transactions per second and accommodating hundreds of millions of active users and millions of applications.



Intuitive user interfaces that enable an average user to easily buy, store, and transfer value, as well as use decentralized apps in a natural way.



An engaged user base that serves as the pre-existing critical mass necessary for the ecosystem to grow and eventually become adopted by hundreds of millions of users.





Telegram is uniquely positioned to establish the first mass-market cryptocurrency by providing a platform that combines these properties.

Telegram will use its expertise in encrypted distributed data storage to create TON, a **fast and inherently scalable** multi-blockchain architecture. TON can be regarded as a decentralized supercomputer and value transfer system. By combining minimum transaction time with maximum security, TON can become a VISA/Mastercard alternative for the new decentralized economy.

The Telegram Team will rely on its 10-year experience in building **user-friendly interfaces** for tens of millions to create light wallets, exchanges, and identification services that will allow users to get on board with cryptocurrencies in an intuitive way.

Integrated into Telegram applications, the TON wallet will become the world's most adopted cryptocurrency wallet.

Telegram will leverage its **existing ecosystem** of communities, developers, publishers, payment providers, and merchants to drive demand and value for TON cryptocurrency. A whole new economy saturated with goods and services sold for cryptocurrency will be born — similar to WeChat's fiat-based marketplace, but not confined to a centralized service.

A Brief History of Telegram

Telegram was founded in 2013 by libertarians to preserve freedom through encryption. The project has declared not-for-profit goals and remains independent and self-funded. Like Wikipedia, which for years has been a role model for the Telegram founders¹, Telegram has chosen a .org domain to emphasize its non-commercial status.

The physical infrastructure of Telegram reflects its founders' belief in larger decentralization. Telegram deploys a distributed server infrastructure to synchronize encrypted data across multiple independent server clusters spread across different continents and jurisdictions.

The resulting combination of speed, encryption, and independence attracted millions of users within a few months after the project's launch² in 2013. Telegram kept evolving with an average of 12 major updates a year. By February 2016, it had 100 million monthly active users and was delivering 15 billion messages daily.

1. [Founder of Facebook for Russia donates \\$1M to Wikipedia at DLD.](#)
2. [Why Telegram has become the hottest messaging app in the world.](#)



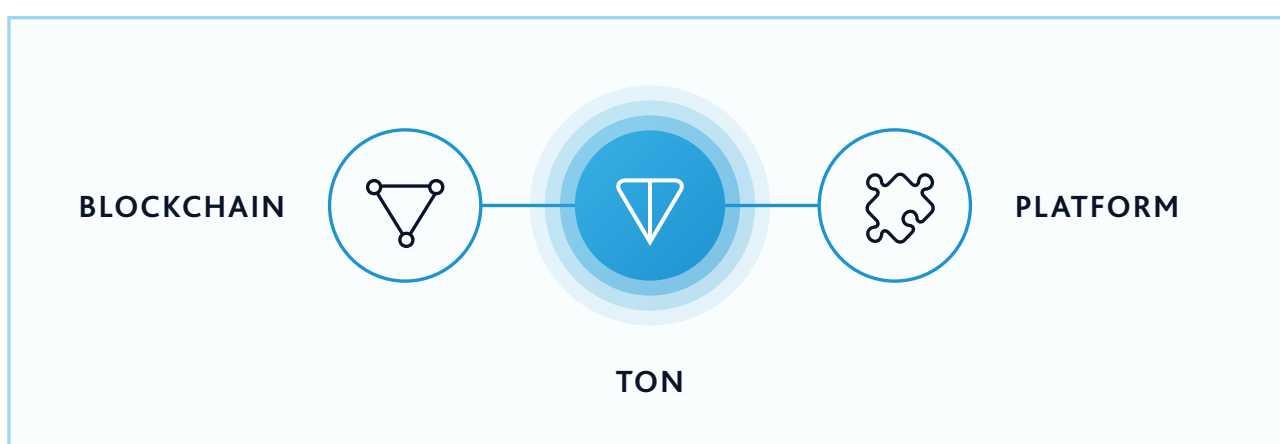
In October 2017, Telegram reached 170 million monthly users, delivering 70 billion messages every day.³ At least 500 000 new users join Telegram daily. At this rate, the service is expected to hit **200 million monthly users in Q1 2018**. These users can provide the required critical mass to push cryptocurrencies towards widespread adoption. ▾

3. Push notifications delivered on iOS and Android devices daily.



Telegram Open Network (TON)

Because taking cryptocurrencies mainstream in 2018 would not be possible using the existing blockchain platforms,⁴ Telegram co-founder Dr. Nikolai Durov set out to find a novel solution to meet the speed and scalability required for mass adoption. His research resulted in the design for the Telegram Open Network — a fast and secure blockchain and network project.



TON Blockchain

At the core of the platform is the TON Blockchain — a scalable and flexible blockchain architecture⁵ that consists of a master chain and up to 2^{92} accompanying blockchains. Below are some notable design choices that allow the TON Blockchain to process millions of transactions per second.

Infinite Sharding Paradigm

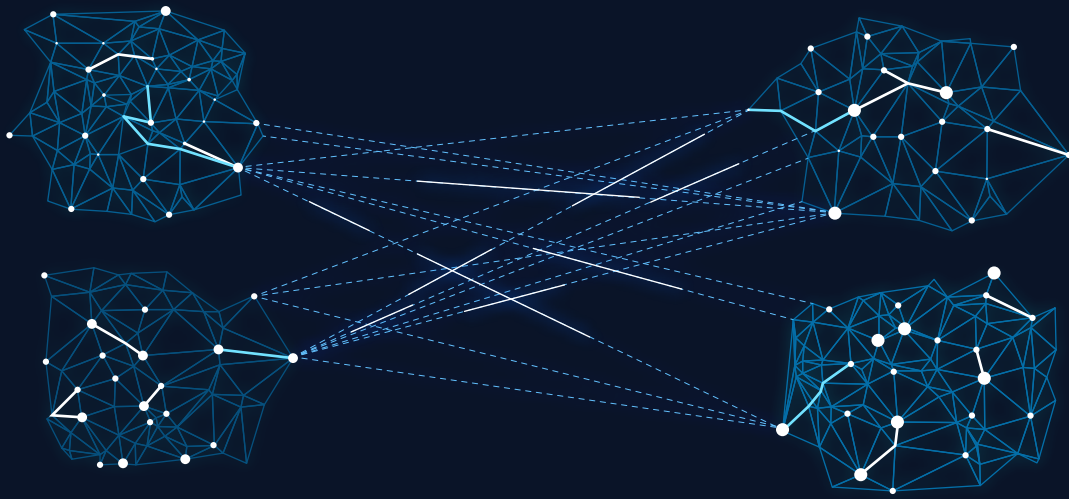
To achieve scalability, TON has built-in support for sharding: TON blockchains can automatically split and merge to accommodate changes in load. This means that new blocks are always generated quickly and the absence of long queues helps keep transaction costs low, even if some of the services using the platform become massively popular.

See «Infinite Sharding Paradigm», 2.1.2.

4. See sections 2.8 and 2.9 in the Technical White Paper for a comparison of blockchain projects.

5. See section 2 in the Technical White Paper.





Instant Hypercube Routing

TON blockchains use smart routing mechanisms to ensure that transactions between any two blockchains will always be processed swiftly, regardless of the size of the system. The time needed to pass information between TON blockchains grows logarithmically with their number, so scaling to even millions of chains will allow them all to communicate at top speed.

See «Hypercube Routing» and «Instant Hypercube Routing», 2.1.4, 2.4.19, 2.4.20.



Proof-of-Stake Approach

TON uses a Proof-of-Stake approach in which processing nodes («validators») deposit stakes to guarantee their dependability and reach consensus through a variant of the Byzantine Fault Tolerant protocol. This allows TON to focus the computing power of its nodes on handling transactions and smart contracts, further increasing speed and efficiency.

See «Proof-Of-Stake Approach», 2.1.16, 2.6.



2-D Distributed Ledgers

TON can «grow» new valid blocks on top of any blocks that were proven to be incorrect to avoid unnecessary forks. This self-healing mechanism saves resources and guarantees that valid transactions will not be discarded due to unrelated errors.

See «Account chains», 2.1.1, 2.1.17.





TON Platform

As a multi-blockchain project, TON requires sophisticated network protocols — such as the TON P2P Network used to access the TON blockchains⁶ — that can be reused to give a significant boost in flexibility to the platform. The following components are scheduled to be released after the TON Blockchain core and will further increase the potential uses of the TON infrastructure.

TON Storage

TON Storage is a distributed file-storage technology, accessible through the TON P2P Network and available for storing arbitrary files, with torrent-like access technology and smart contracts used to enforce availability. This component not only enables storage services akin to a distributed Dropbox, but also paves the way for more complex decentralized apps that require storing large amounts of data, such as Youtube — or Telegram.

See «TON Storage», 4.1.8 and «Is it possible to upload Facebook into blockchain?» 2.9.13.

TON Proxy

TON Proxy is a network proxy/anonymizer layer used to hide the identity and IP addresses of TON nodes. Similar to I²P (Invisible Internet Project), this layer can be used to create decentralized VPN services and blockchain-based TOR alternatives to achieve anonymity and protect online privacy. In conjunction with the TON P2P Network and TON DNS, TON Proxy can make any service, including Telegram, effectively immune to censorship.

See «TON Proxy», 3.1.6, 4.1.6.

6. See «TON Networking», Section 3 of the technical whitepaper.





TON Services

TON Services provides a platform for third-party services of any kind that enables smartphone-like friendly interfaces for decentralized apps and smart contracts, as well as a World Wide Web-like decentralized browsing experience.

See «TON Services and Applications», 4.



TON DNS

TON DNS is a service for assigning human-readable names to accounts, smart contracts, services, and network nodes. With TON DNS, accessing decentralized services can be similar to viewing a website on the World Wide Web.


See «TON DNS», 4.3.1, 4.3.2, 4.3.3.



TON Payments

TON Payments is a platform for micropayments and a micropayment channel network. It can be used for instant off-chain value transfers between users, bots, and other services. Safeguards built into the system ensure that these transfers are as secure as on-chain transactions.

See «TON Payments», Lightning-style off-chain transactions, 5.

All these services can be integrated with third-party messaging and social networking applications, uniting the centralized and the decentralized worlds. 



Telegram Messenger-TON Integration

Telegram-TON integration will provide a clear path to cryptocurrencies for millions of people. Telegram Messenger will not only serve as an example of the possibilities offered by integrating with TON, but will also add unique features to the TON platform, leveraging Telegram's massive user base and developed ecosystem.

Light Wallet

The TON architecture supports light clients that can run on mobile devices without consuming significant resources. TON light wallets will be built into Telegram applications, allowing millions of users to store their funds securely in the TON blockchain. The wallet owners will be the sole holders of the corresponding encryption keys.

See «Merkle proofs», 2.3.11; «Light wallet and TON entity explorer..», 4.3.19.

Telegram mobile and desktop applications with integrated wallets will also double as TON clients, enabling secure transfers of value within the TON blockchain and interaction with TON smart contracts and applications. Telegram will offer streamlined interfaces for sending value to contacts and paying for purchases in TON.

See «TON DNS use cases», 4.3.2; «Light wallet and TON entity explorer..», 4.3.19; TON Payments, 5.

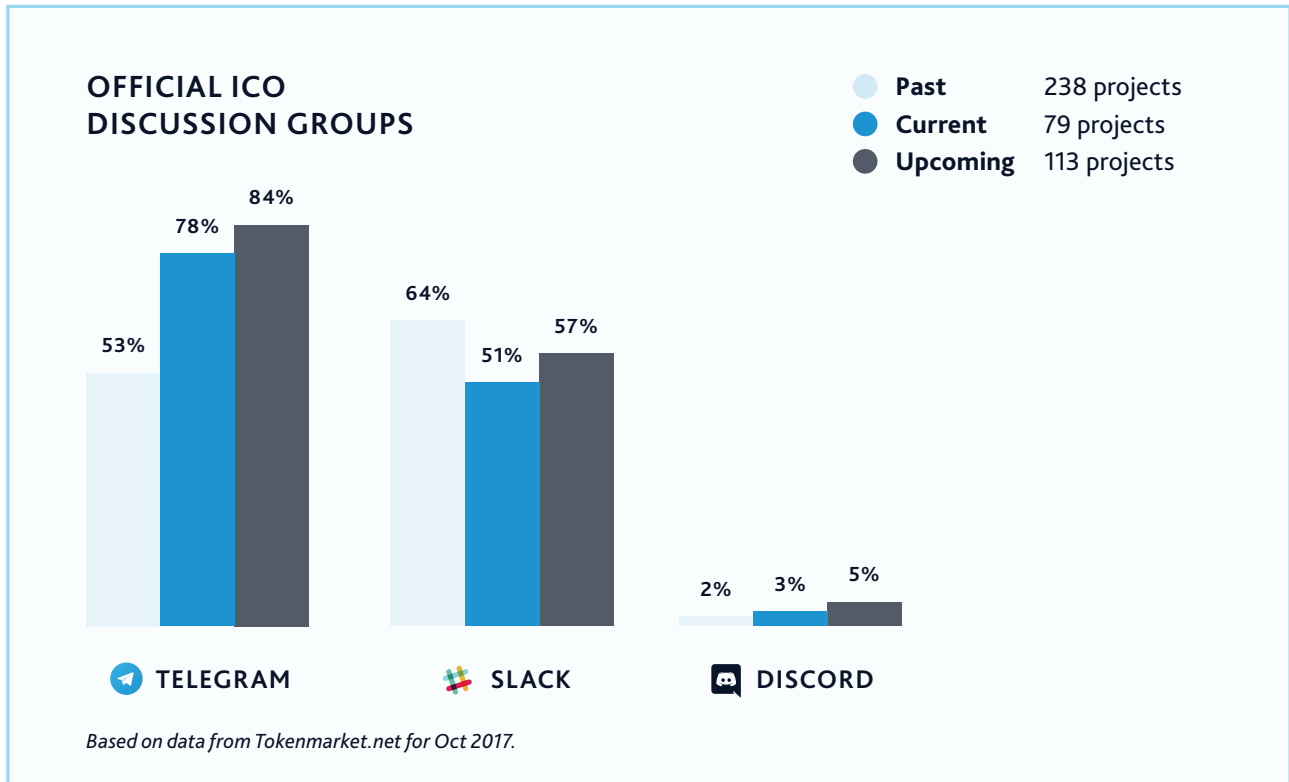
Integrated into Telegram applications, the TON-Telegram wallet will instantly become the world's most adopted cryptocurrency wallet.

The TON coins exchanged by Telegram users will be called «Grams» and denoted by the TON triangular symbol or the 💎 gem emoji. The Gram will serve as the principal currency for the in-app economy on Telegram, and, like any other cryptocurrency, will be available for external use.



External Secure IDs

According to Tokenmarket, 84 percent of blockchain-based projects have an active Telegram community, more than all other chat applications combined.⁷ Forbes and other media outlets have called Telegram the «cryptocurrency world's preferred messaging app» and «as ubiquitous to the cryptocurrency world as Snapchat is to a teenager».⁸



Because the majority of actors in the new digital economy already have active Telegram accounts, it is natural for Telegram to offer a secure universal ID. After passing KYC-AML on Telegram once, users will get a virtual passport to log into services that require user verification, thereby eliminating a major point of friction for anyone engaging with crypto-assets.

All private data (such as passport scans) will eventually be stored end-to-end encrypted with a key known only to the owners. Telegram's distributed servers (and later the TON Blockchain) will have no access to this information, but will instead store a hash of the value to be able to confirm that the data was verified when the user obtained their secure ID. Third parties will be able to add further verifications to these virtual passports.

7. Data from Tokenmarket, as of October 2017.

8. [Russia Fines Cryptocurrency World's Preferred Messaging App, Telegram.](#)



Ecosystem

Telegram's existing ecosystem will offer simple ways of buying the TON coins (Grams), and a range of services to spend them on, driving demand and fundamental value for the cryptocurrency.



Bot Platform

As of October 2017, more than 800 000 unique third-party bots are regularly used by 52 million Telegram users. These bots can already accept credit card payments from users in 200 countries via eight providers connected to the Telegram Payments Platform.⁹ In the future, by using their verified IDs in conjunction with bots that accept credit cards, Telegram users will be able to buy and **exchange cryptocurrencies** in a frictionless and legally compliant way.

Telegram will provide a unified entry point for users willing to connect with bots that offer exchange services, effectively creating a competitive market.



Groups and Channels

The Telegram ecosystem includes millions of public group chats reaching up to 30 000 members and broadcast channels, the largest of which have several million subscribers. Telegram's public broadcast channels generate over 30 billion views by 80 million users each month. Creators of large channels currently try to monetize them by posting advertisements or promoting other channels and groups. However, they presently lack the necessary tools to formalize their transactions with advertisers.

To fix this, Telegram will launch a TON-based **ad exchange** where parties interested in promoting their projects can connect with the relevant channel owners and negotiate a price in a transparent and fully automated way. All accompanying transactions will be made in Grams on a per-view or per-click basis, with the necessary statistics and guarantees provided to all parties.



Digital Content and Physical Goods

Bots, channels, and groups provide a ready market for paid content and subscription services. Users will be able to support publishers and content creators by making donations or paying for exclusive access. Bots can act as virtual storefronts and accept orders for the delivery of physical goods. Telegram's in-app economy will supply the TON market with a wide range of goods and services that can be obtained with TON coins.

9. Bot API Payments: <https://core.telegram.org/bots/payments>.





A Gateway to Decentralized Services

Telegram will offer a searchable registry of decentralized services from its applications, providing a list of the most popular apps, as well as recommendations based on the user's history of choices. These steps can make Telegram a gateway to blockchain-based projects for the masses — similar to how Google Play and the App Store currently work for centralized applications. ▾

Uses of TON as a Cryptocurrency

In addition to payments for all digital and physical assets sold by individual merchants within the Telegram ecosystem and on other projects integrated with TON, the TON coins (Grams) will be used as:

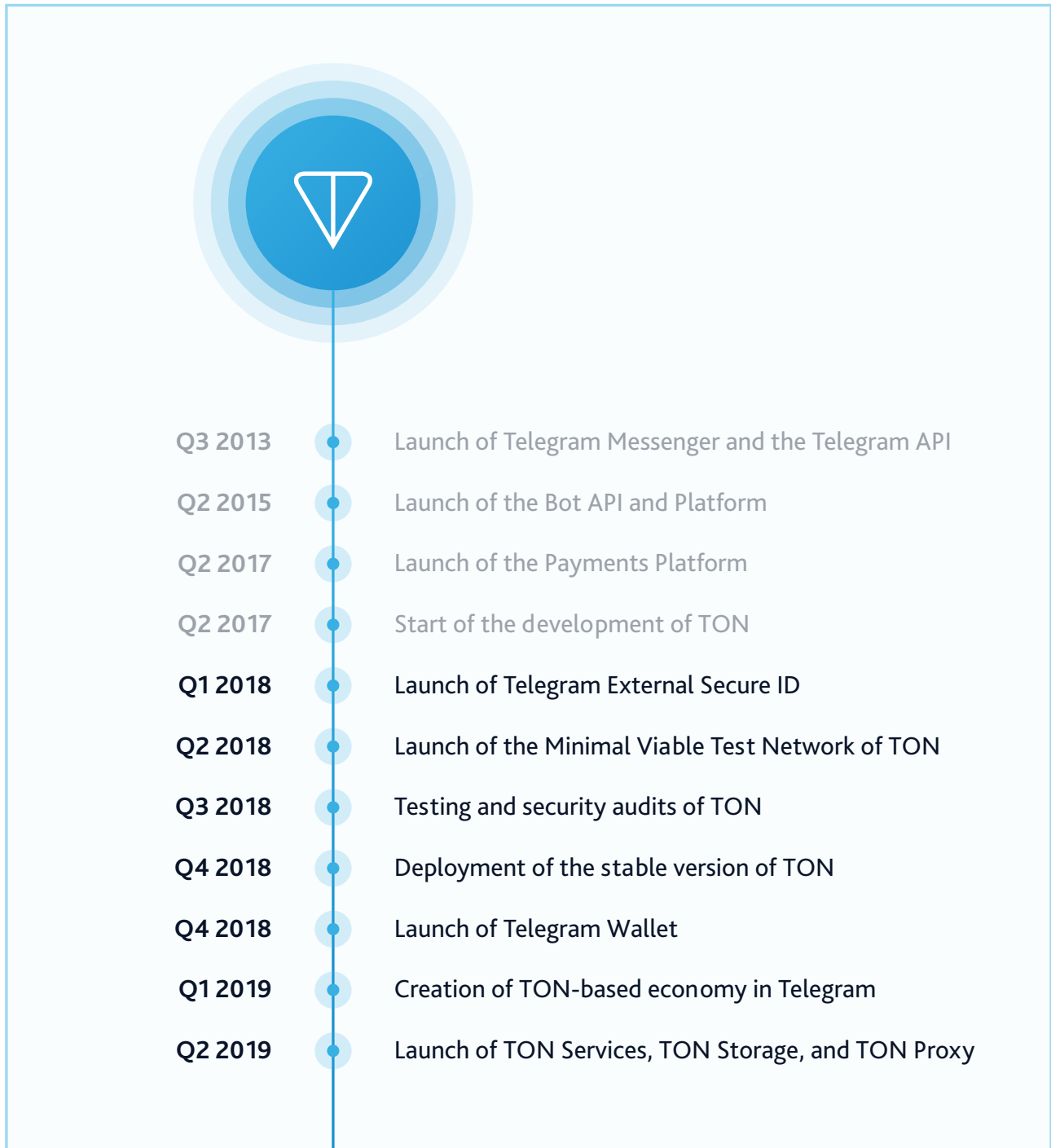
- › Commission («gas») paid to TON nodes («validators») for processing transactions and smart contracts;
- › Stakes deposited by validators to be eligible to validate transactions and generate new blocks and coins;
- › Capital lent out to validators in exchange for a share of their reward;
- › Voting power required to support or oppose changes in the parameters of the protocol;
- › Payment for services provided by apps built on the platform (TON Services);
- › Payment for storing data securely in a decentralized way (TON Storage);
- › Payment for registering blockchain-based domain names (TON DNS) and hosting TON-sites (TON WWW);
- › Payment for hiding identity and IP addresses (TON Proxy);
- › Payment for bypassing censorship imposed by local ISPs (TON Proxy).

All of these services can be free for the users since the application owners may choose to cover the corresponding fees, and adopt a freemium or an advertisement-based business model. ▾



Roadmap

The TON and Telegram technical roadmaps include the following milestones:

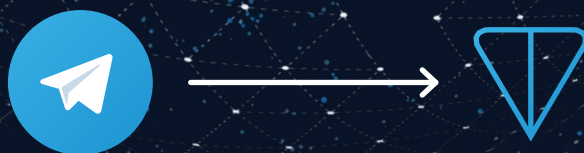


Telegram will also continue shipping monthly product updates that are not related to TON. ▾



Token Distribution

To obtain the resources required to make TON a reality, Telegram is launching a token sale in Q1 2018. The token sale will likely use a SAFT¹⁰ to be converted 1:1 to native TON tokens (Grams) after the deployment of the TON Blockchain in Q4 2018.



The total supply of native TON tokens (Grams) will equal 5 billion.

After the TON Blockchain is fully deployed, the annual inflation rate derived from the fundamental parameters of TON is projected at two percent. This inflation represents a payment made by all members of the community to the validators for keeping the system functional.

See «Validators», 2.6.1, «Original supply, mining rewards and inflation», A.3.

Four percent of the supply (200 million Grams) will be reserved for the development team with a 4-year vesting period. During the initial stage of active TON development, at least 52 percent of the entire supply will be retained by the TON Reserve to protect the nascent cryptocurrency from speculative trading and to maintain flexibility at the early stages of the evolution of the system. The remaining 44 percent (2.2 billion Grams) can be sold in accordance with the formula below:

$$p_n := 0.1 \times (1 + 10^{-9})^n \text{ USD}$$

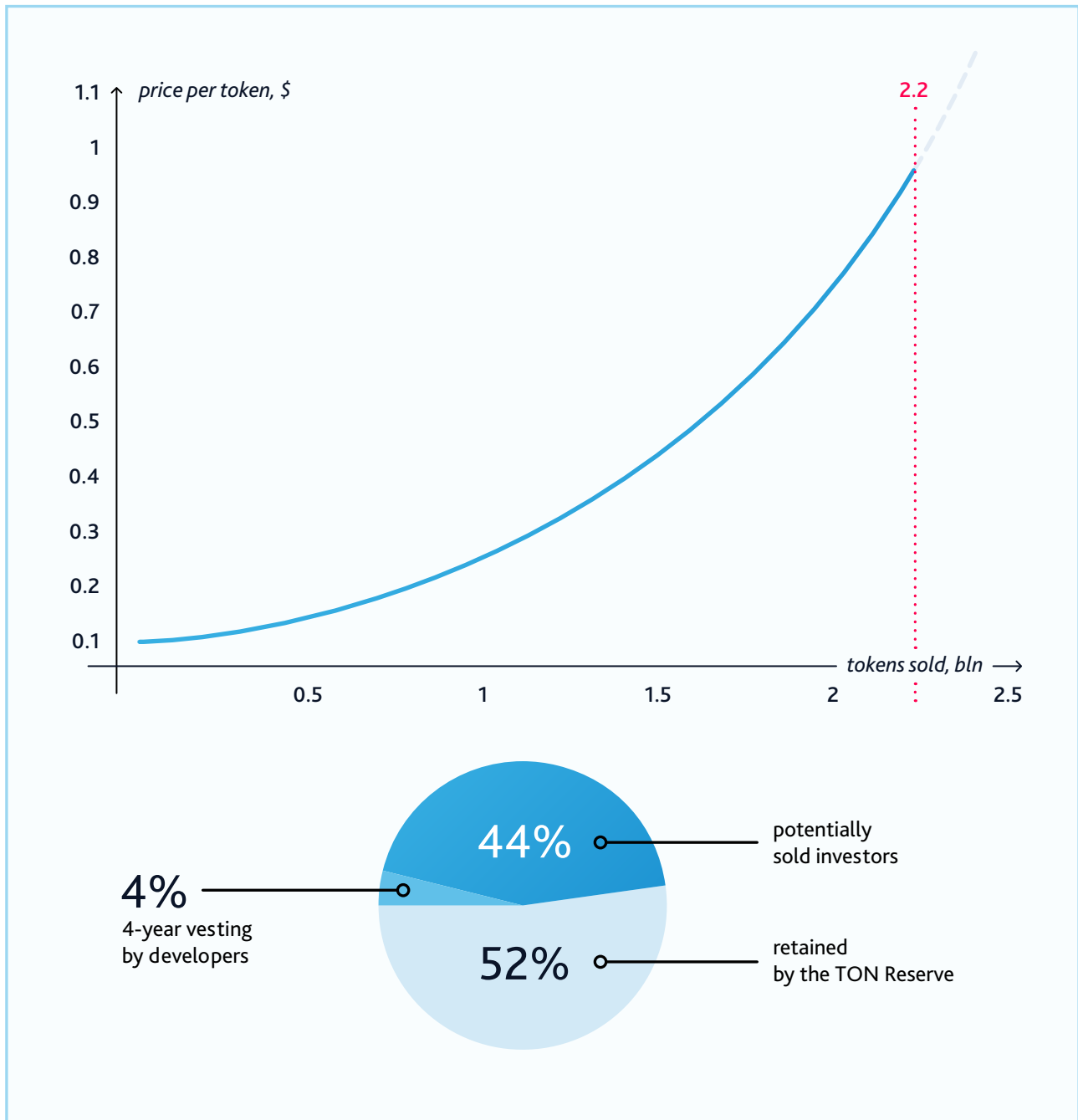
The price of the first token to be sold will be approximately 0.1 USD, with and each successive token will be priced one billionth higher than the previous one. As a result, the additional supply

10. See the [SAFT Project](#).



coming from the TON Reserve will always be more expensive than the price paid by any of the existing buyers.¹¹ This structure should allow the market to define the fair price and volume for the token sale.

A bulk pre-sale of TON tokens to a group of institutional investors for a fiat currency is possible under the average price per token or higher, depending on the vesting period and the volume of the transaction. ▽



11. See section A.4 in the Technical White Paper, «Original price of Grams».



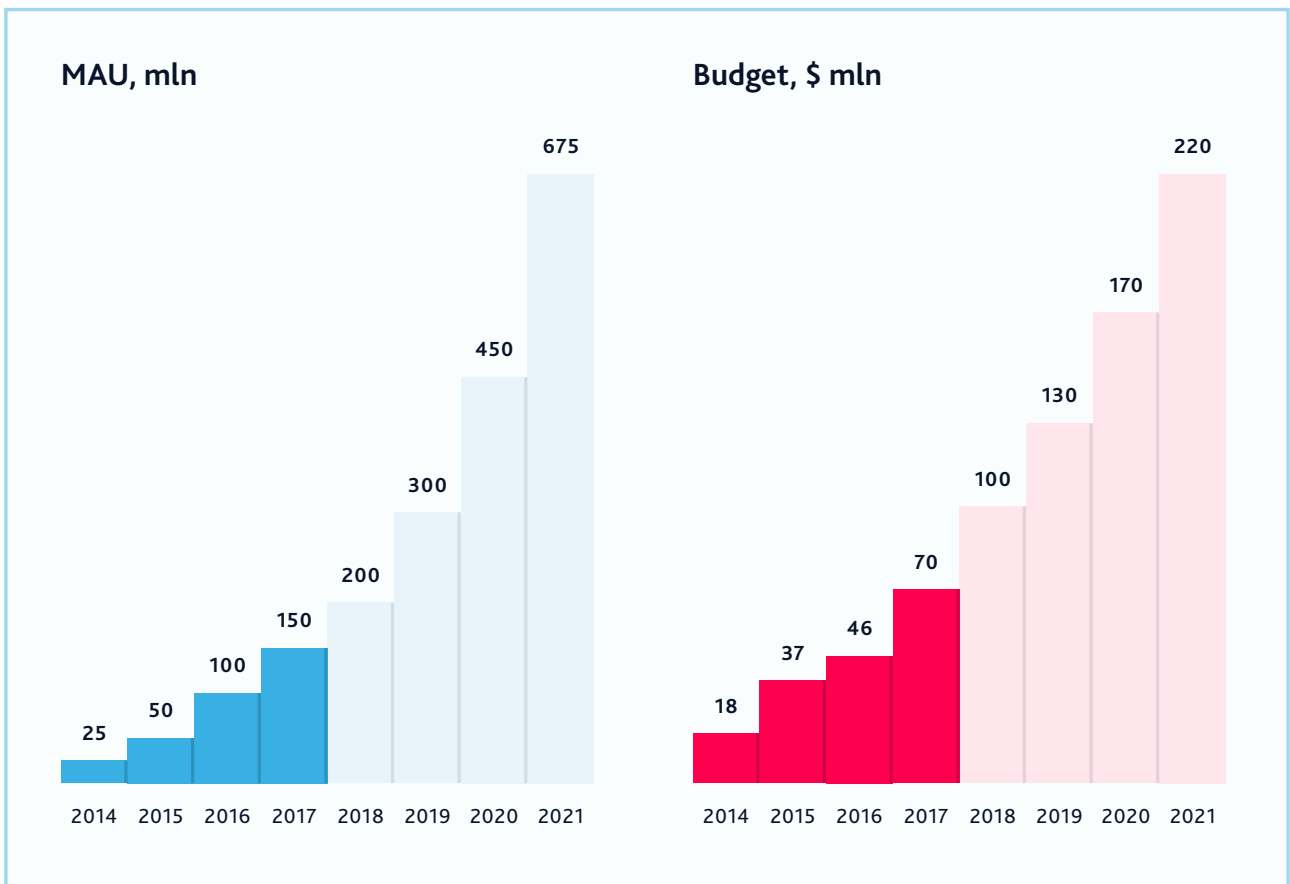
Use of Funds

Funds raised during the Telegram ICO will be used for the development of Telegram and TON and for the ongoing expenses required to support the growth of the ecosystem.

More than 80 percent of collected funds will be spent on equipment, bandwidth, colocation, and user verification costs. The rest will be allocated for wages, offices, and legal and consulting services.



The annual budget of Telegram in 2017 amounted to \$70 million, out of which \$62 million were spent on equipment, bandwidth, colocation, and user verification costs. Telegram's spending is projected at \$400 million in the next three years (approximately \$100 million in 2018, \$130 million in 2019, and \$170 million in 2020). A total spending of about \$620 million to support continuing organic user growth should allow Telegram to reach one billion active users by January 1, 2022. [▼](#)



Governance

The founders of Telegram will be responsible for the efficient use of funds resulting from any sale of tokens from the TON Reserve. Over time, all responsibilities related to TON and its Reserve will be transferred to the TON Foundation, a not-for-profit organization.

By 2021 the initial TON vision and architecture will have been implemented and deployed. TON will then let go of the «Telegram» element in its name and become «The Open Network».

From then on, the continuous evolution of the TON Blockchain will be maintained by the TON Foundation.


Telegram will serve as a launch pad for TON, ensuring its technological superiority and widespread adoption on the initial stages, but the future of TON is in the hands of the global open-source community. ▾

Telegram Open Network → The Open Network



Team

Telegram has a world-class team of 15 developers that were selected from thousands of contenders over the last ten years. To become part of the team, each of its current members had either to win in the world's top programming contests or to take the first place in one of the nationwide multi-level coding competitions held by the founder of Telegram.

Core team members have ten years of experience in building scalable projects for tens of millions of users. Before building Telegram, they created  VK, the largest Europe-based social network with more than **100 million active users**, which still enjoys a dominating share in its local markets.

The Telegram backend team, which has an unparalleled ratio of **winners of worldwide coding competitions**, specializes in creating secure data storage engines for distributed server infrastructures. All networking, cryptographic, and database engine software running on thousands of Telegram servers is custom-built by these developers.

Founders



Dr. Nikolai Durov

Phd (Bonn University), Phd (Saint-Petersburg State University)

- › 2013-present: Co-founder, CTO, Architect, Lead C/C++ Engineer at Telegram. Built MProto and Telegram's distributed data storage engines;
- › 2006-2013: Co-founder, CTO, Architect, Lead C/C++ Engineer at VK. Built data storage and networking software.

Awards

- › Absolute World Champion in Programming (2000, 2001) — one of ten people in history to win the ACM International Collegiate Programming Contest twice;
- › Gold Medals in International Mathematical Olympiads (1996, 1997, 1998);
- › Gold and Silver Medals in International Olympiads in Informatics (1995, 1996, 1997, 1998).

Nikolai is a renowned mathematician and a world-class programmer, uniquely combined in one person. At the age of 8 Nikolai already solved cubic equations.¹² He started coding

12. Nikolai was invited to demonstrate this skill on the main TV channel of Italy, where the Durovs lived at the time.



at 9, and by 13 he built a full-fledged operating system for Intel 80386 microprocessors in x86 assembly language. While spending summers in Siberia without access to a computer, 11-year old Nikolay filled hundreds of pages with x86 assembly code, creating programs such as a Forth interpreter entirely on paper. As a CTO and guru in distributed systems, he scaled VK and then Telegram to tens of millions of daily users. In 2014 Nikolai became interested in Bitcoin and related technologies. His research on these topics culminated in TON's Technical White Paper, where he summarized the advancements of blockchain technology and proposed a novel architecture for scalable decentralized ledgers.



Pavel Durov

- › 2013-present: Co-founder, CEO, Product Manager at Telegram;
- › 2006-2013: Co-founder, CEO, Product Manager, Lead Developer at VK.

Awards

- › The most promising Northern European leader under 30 (2014);¹³
- › Young Global Leader by the World Economic Forum (2017).¹⁴

Pavel first gained international recognition for founding VK, which under his leadership commanded a 70 percent market share in Russia, Ukraine and Belorussia, eclipsing Facebook and other competing social networks. An outspoken libertarian, he published free market manifestos urging the Russian government to deregulate and decentralize the country's economy. Pavel was forced to sell VK and leave Russia in 2014 after a clash with the government over his users' privacy and freedom of speech.

Pavel started coding at 10, and at 11 he already created his first multiplayer strategy game. As a teenager, he built popular online communication tools for fellow students. At 21 he single-handedly coded the first version of VK. Pavel founded Telegram and became interested in cryptocurrencies in 2013, when he spent \$1.5 million of his savings on Bitcoin that he holds to this day.

13. [VKontakte's Founder Pavel Durov the Most Promising Northern European Leader Under the Age of 30.](#)

14. [Young Global Leader, Class of 2017.](#)



Other Notable Team Members



Aliaksei Levin

- › 2013-present: C/C++ Engineer at Telegram. Developed distributed data storage engines, client cross-platform libraries, and the bot API;
- › 2010-2013: C/C++ Engineer at VK. Built data storage engines and created the custom programming language KPHP for high-level backend developers.

Awards

- › Gold Medal, ACM International Programming Contest World Finals (2011);
- › Silver Medal, ACM International Programming Contest World Finals (2010);
- › First Prize, International Mathematics Competition for University Students (2009);
- › Gold Medal, First Place, International Mathematical Olympiad (2005);
- › Silver Medal, International Mathematical Olympiad (2004).



Vitalik Valtman

- › 2013-present: C/C++ Engineer at Telegram. Developed networking and data storage engines;
- › 2010-2013: C/C++ Engineer at VK. Developed networking and data storage engines.

Awards

- › Silver Medal, ACM International Programming Contest World Finals (2006);
- › 4th place, Top Coder Open;
- › 4th place, Top Coder Collegiate Contest.



Arseny Smirnov

- › 2013-present: C/C++ Engineer at Telegram. Developed server data storage engines, client cross-platform libraries, and bot API;
- › 2010-2013: C/C++ Engineer at VK. Developed data storage engines and created the custom programming language KPHP for high-level backend developers.

Awards

- › Gold Medal, ACM International Programming Contest World Finals (2011);
- › Silver Medal, ACM International Programming Contest World Finals (2010).





John

- › 2014-present: Client C++ Engineer at Telegram. Single-handedly built Telegram Desktop;
- › 2007-2013: Lead backend/frontend Engineer at VK after winning a nationwide contest in JS.



Igor

- › 2014-present: Lead Backend Engineer at Telegram. Built the entire Telegram API for client apps;
- › 2007-2013: Lead backend/frontend Engineer at VK after winning a nationwide contest in JS.



DrKlo

- › 2014-present: Android Engineer at Telegram after winning a nationwide contest in Android Java. Built Telegram for Android;
- › 2012-2013: iOS Engineer at VK after winning a nationwide contest in Objective C.



Peter

- › 2014-present: iOS/Swift Engineer at Telegram. Built Telegram for iOS (Objective C). Built Telegram Beta for iOS (Swift);
- › 2012-2013: iOS Engineer at VK after winning a nationwide contest in Objective C.



Grisha

- › 2016-present: Cross Platform Developer at Telegram. Builds voice calls;
- › 2010-2016: Android Engineer at VK after winning a nationwide contest in Java for Android. Single-handedly built the VK app for Android.



Kolar

- › 2014-present: Backend/Frontend Engineer at Telegram. Built the Instant View Platform, the Translations Platform, telegra.ph, telesco.pe, etc.;
- › 2010-2013: Lead backend/frontend Engineer at VK after winning a nationwide contest in JS.



Ilya

- › 2013-present: iOS/Swift Engineer at Telegram after several winning a nationwide contest in Objective C. Built multiple features for Telegram iOS.



Igor

- › 2013-present: Infrastructure Architect at Telegram. Scaled Telegram to tens of thousands of servers;
- › 2008-2013: Senior System Engineer. Scaled VK to tens of thousands of servers.

