

Building Censorship-resistant P2P Network for Parallel Computing

Pandora Project Blueprint

Strictly confidential, not for distribution

v. 1.0.0

February 4, 2018

Abstract

The paper gives a brief introduction into the vision, design, economic model and workflow for building Pandora Boxchain: a scalable censorship-resistant network for parallel computing on top of Prometheus consensus protocol. The paper is subjected for professional investors and cryptoeconomics enthusiasts

Keywords: censorship resistance, decentralisation, distributed systems, artificial intelligence, machine learning, smart contracts, quantum computing, game theory, cryptoeconomics, economic incentives, blockchain, distributed ledgers, parallel computing, privacy

Disclaimer

The document in whole or in any of its parts in no way represents an investment advice, an agreement of any type, a promise of future benefits earned due to the efforts of third party(ies), and is not obligatory or binding to its authors and all the involved parties. The authors of the document and/or governing bodies of the project in no way form a partnership with personal responsibilities or give any obligations or promises.

The document is strictly private and not for a public distribution or distribution to any other parties. The text above is a draft of the thoughts on the matter, some preliminary plans subjected for further discussion and possible corrections/changes.

Contents

1	Project Overview	5
2	Project Vision	7
2.1	Initiatives	7
2.2	Teams	8
2.3	Foundation	10
3	Project Details	11
3.1	Technology, its applications and ecosystem	11
3.2	Current progress	14
3.3	Roadmap	18
3.3.1	Streams	18
3.3.2	Feature sets	18
3.3.3	Epochs and launch phases	19
3.3.4	Future vision	23
3.4	Key people, partners and advisors	23
3.5	Network governance	29
4	Economic Model, Finance and Legal Information	30
4.1	Economic model	30
4.2	Token economics	30
4.3	Token distribution and vesting	32
4.4	Current financial statement	34
4.5	Financial contributions	35
4.6	Budgeting	35
4.7	Current valuation	37
4.8	Grants, investments and business spin-offs	39
4.9	Legal	42
4.10	Risks and Competition	43

List of Tables

1	Deliveries and assets	15
2	Roadmap and milestones	21
3	Key people	24
4	Project teams	26
5	Partnerships	27
6	Advisers, advocates, peer reviewers and outside contributors .	28
7	Financial statement	34
8	Budget for 2018	35

List of Figures

1	Technological stack	11
2	Development streams, epochs and major releases	20
3	Initial token distribution	33
4	Legal entities and financing	40

1. Project Overview

Project goal: research and develop a technology, launch a network based on that technology and contribute to building an ecosystem around the technology that will serve the main goal of performing censorship-resistant decentralised parallel computing (all these parts here and after are called the Project).

By “**censorship resistance**” we mean inability of any strong network member, economic or political subject or even their coalition to affect in a willed or unwilled manner the rules and the way the network operates (including privacy of the data, data flows, monetary flows, transactions, ownership, computation performance etc).

By “**decentralised**” we mean that network will not have a single point of failure and will not be governed by some singular authority/authorities or subjects taking centralized decisions.

By “**parallel computing**” we mean any computations that can be split into arbitrary parts and be computed in parallel in a way that will not affect the final result of computations. First of all, these include all modern forms of artificial intelligence, also future quantum computing etc.

The closest analogy on the topic can be given by Bitcoin: it is a technology and a network that allows censorship-resistant decentralised money issuing and transacting. The impact of the system appeared to be huge since it solved the core problems with the modern monetary systems: censorship of the transactions, centralisation (and constant inflation) of money issuing, trust to third-party, ability to alienate funds by third-parties (governments, banks and so forth).

In the same way we expect our technology and the network to solve the same problems with computing: creating free market for different forms of parallel computing (including artificial intelligence) that can’t be operated centrally or by any intermediaries (“men in the middle”); a market that can’t be regulated, banned or «turned off»; creating free and private medium of exchange for data, algorithms (or, “artificial intelligences”) and computation results. This medium will be censorship-resistant, allowing radical developments in the area of artificial intelligence (for instance in such fields as extending life expectancy, creating artificial forms of life, new types of materials, faster private space exploration, autonomous weapons etc), quantum computing and many others. Decentralised approach and free market will solve the main risks with artificial intelligence on one hand (and this will

attract users to the system) and create stable growing economies that will be much less prone to declines or crises than contemporary economies (see manifesto.ai for the details). Moreover, the ecosystem will become the hosting environment for a new type of “robots/AI economy”, that is estimated to outgrow the human economics in an exponential manner.

Having said that, it is important to note that the technology and network themselves will have “embedded economics” – a natural and required part that is crucial for the creation of the censorship-resistant decentralised system, which can be formally verified and proven to have the stated qualities. These economics also provide an incentive to fund the overall Project: funds will be taken on the terms of SAFT agreement and will be converted into a utility token that drives that economics – and with the increase of the size of the economics the usefulness and value of the token will increase because of its limited supply (you can take Bitcoin as a very simple approach to the matter).

We expect that over a period of time the network will be extended to host more generic and efficient version of “smart contracts” and, additionally to that, the network token will have a potential to become the world’s leading cryptocurrency. This will be due to the fact that the underlying consensus algorithm driving the network can be formally proven to be more censorship-resistant and efficient than bitcoin or smart-contract hosting blockchains (including those that are only being developed today) and since the whole network will be attached to the bitcoin network from its origin (via “sidechain” technology and SegWit-compliance) at some point the value of the bitcoin may shift into our more efficient system.

In terms of artificial intelligence, we aim for the technology to provide a huge impact and due to its nature and design become a hosting medium for an AI development, rise of generic and super/post-human AI, including self-evolving autonomous forms or different kinds of AI and human intelligence integrations. Due to the quality of competition embedded in the network (free market) and multi-agency of the system (decentralisation), this will be an anti-fragile and less risky environment than any form of centrally governed or regulated progress in the field could become.

All of these facts make us believe that the probable network capitalisation over the course of decade(s) will supersede multi-trillion barrier and then become even bigger by some orders of magnitude, since most of the exponentially growing human and post-human economics and computing (including AI, robots and quantum computations) will be run on top of the system in

a way they are run on top of the Internet these days.

2. Project Vision

To achieve this ambitious goal a **number of initiatives** will be performed by a set of geographically diverse **expert teams and companies** strategically (and sometimes operationally) governed by **Pandora Foundation** according to well defined **governance principles**. Hereinafter we explain each of the terms shown in bold.

2.1. Initiatives

As was defined in project goals, we aim to (1) research and (2) develop the technology, (3) launch the network based on that technology and (4) contribute to building the ecosystem around the technology. These are the four main initiatives that will be held under auspices of the Pandora Foundation.

Research. Investigation of the previous work in the field and subsequent scientific research and formal (mathematical) proofs for the ability of the consensus protocol to resist attacks and achieve different forms of censorship-resistance. Research will be held in the three main directions: game theory (proving that fair play is a Nash-equilibrium strategy for the rational players in the network), byzantine fault tolerance (proving that the system can resist more than $p\%$ of byzantine faulty (i.e. “lying”) nodes even in cases of their economically-irrational behaviour) and dynamic systems (studying complete phase space of possible behaviours and its attractors, that can allow to prove that some certain negative strategies are impossible under any type of behaviour).

Develop the technology. The results of research under the first initiative described above will be implemented in form of code prototypes and, then, working products under the second initiative. This will include at least the complete software stack required for the operation of the network (blockchain, consensus and transaction layers, computing layer, client apps etc), and will be accompanied and extended by the software produced in the ecosystem (see below). The resulting products must have the highest quality and must be formally verified and be proven to behave according to the original scientific models.

Launch the network. Bring the products to the market, launch them publicly and support the launch with proper PR campaigns. Bring the token to the exchanges, bootstrap economics, provide initial computing/mining resources to support network operations over the initial period of time.

Contribute to building the ecosystem. This will include:

- 1) providing grants to nonprofit entities (like research labs) doing research, creating products or building awareness of the problems (such as the importance of the free AI market) that can benefit the network;
- 2) investing into the businesses that develop products that will be a part of the ecosystem;
- 3) investing into AI-related and other startups that will consume the network functionality and pay later for the network services;
- 4) providing grants for early adopters of the technology for including the network into their business processes;
- 5) building partnerships and enterprise alliances around the network and technology;

All together these should help with building network adoption and usage upon launch, which will be a critical issue directly affecting the network market capitalisation

2.2. Teams

According to the initiatives there will be four sets of teams:

Research teams. Teams in the research group will be selected from existing world-known academical bodies with proven track of scientific record using grant system (we will use IOHK and organisation of academical groups underneath it as example).

Technology development teams responsible for developing technology, products and launching the network. The developers teams will be formed from two main sources: by hiring high-skilled world-best developers to the core team and by subcontracting teams/companies with

proven experience and record track to develop specific parts of the solution/products (like client software etc) according to the given technical specifications and formal description. This model follows the best practices used in such projects as Cardano & IOHK, which, we believe, is one of the best managed blockchain projects on the market.

Network development teams responsible for public and business relations related to the network launch, including: marketing, press, PR, government relations, building partnerships, alliances, reaching agreements with exchanges on listing tokens and so on. . .

Business teams. These are the teams running different for profit and non profit projects mentioned in the “*Contribute to building the ecosystem*” within the “Initiatives” section. They will be overseen from a product perspective by a small core team inside Pandora foundation and from a financial perspective by an Administration and Legal Team (see below on Core Teams).

Each set of the teams will have one **Core Team** – a part of the Pandora Foundation, which will lead and govern the overall progress. Also, Pandora Foundation will have a dedicated **Administration and Legal Core Team**, that will be responsible for Financial, managing Legals, possible Government relations etc. This team will also manage and outsource parts of these tasks to a dedicated third-party lawyer and accounting companies and will prepare and structure information and updates for **funders** and **auditors**.

Upon network launch, with its gradual adoptions, the team integration will become more and more ephemeral, and Core Teams and Administrative Team will become dissolved at some point of time, brining the network to the fully decentralised state (an event called hereinafter **Dissolvement**). Separate teams from outside of Foundation will have an opportunity to become separate business or nonprofit parts of the network ecosystem and will have internal incentives to continue to operate for the overall benefit of the network. All unspent funds at this stage will be spent on buyback of the tokens on exchanges; all bought-back tokens and unspent tokens from pre-mine will be burned. These two actions will help to increase the value of the tokens and will result in benefit of all token holders at that moment of time.

Founders team plays a special role in the Project and Foundation management, especially at the initial stages of the project. The following 8 persons are the founders of the project: Maxim Orlovsky, Sabina Sachachtinsk-

agia, Olga Ukolova, Andrey Sobol, Vitaliy Bulychov, Andriy Khavryuchenko, M. and A. (everyone but the last two, who do not yet want publicity, appear on the project's website pandoraboxchain.ai).

2.3. Foundation

Is a virtual unit (that may be legally registered lately in form of non-profit foundation, for-profit company or their combination, see “Legals” section) that in no way represents an unlimited responsibility partnership. Foundation's responsibility and goodwill is to achieve the goals of the project and overwatch the project initiatives. While the Foundation as a virtual unit may receive financial contributions and can spend them to achieve its goals, it's responsibility is limited by the tokens provided according to some financial contribution agreement like SAFT or similar, which will be negotiated separately.

Foundation is and will be continued to be governed by the Board of Directors, consisting of five people from the number of the project Founders. The Board of Directors makes decisions on the following topics:

- budget and spendings;
- funding and accepting financial contributions;
- appointing responsible persons for specific project directions and initiatives and delegating them;
- legals (agreements, creation/updates/dissolvement of legal entities etc).

Directors who are in power to make decisions in the project are: Maxim, Sabina, Olga, Andrey and Vitaliy (see Founders section). They also have the right to change the number of directors by three votes out of five. However, as of now, there are no plans to increase the number of directors in the near future.

According to the conditions of their participation, the other three founders are not actively involved in the project, they do not vote and they do not make decisions. They receive monthly information update about the progress of the project.

Matters that require voting are decided by the directors by the principle of a simple majority (3/5). In case of an equal distribution of votes (if the amount of directors will change to an even number or if someone abstains from voting), the deciding vote goes to Maxim Orlovsky.

More specific or smaller matters in the ordinary course of the project are taken by those who are responsible for the relevant field of activity. The

project's resources are to be spend in accordance with the budget and are to be signed by any three of the five signatures of multi-sig.

3. Project Details

3.1. Technology, its applications and ecosystem

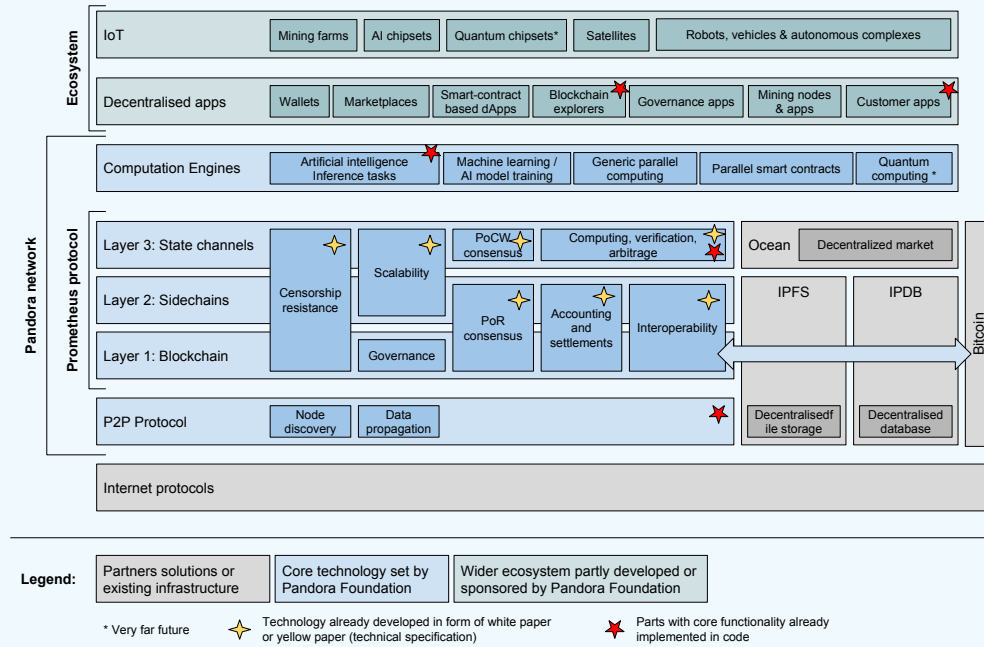


Figure 1: Technological stack of the Pandora Network

From a technical point of view the network will be built as an implementation of **Prometheus consensus** protocol (blockchain) as it is described in the appropriate sections of the Prometheus white paper [?] and yellow paper [?]. It will be interoperable with **Bitcoin**, other SegWit-compatible public blockchains (**Litecoin** etc), **Polkadot** [?] and **Cosmos network** [10]. The network will also utilise other existing decentralised networks such as **IPFS** [?], **IPDB** [?], **Ocean protocol** [?] for implementing different types of its functionality at the application level (decentralised file storage, decentralised database and decentralised market for data and algorithms).

Business cases for the network will be based on the computation engines layer (see Fig. 1). It will be presented by different types of computing that will be gradually added to the network according to the roadmap (see Section 3.3 below). At this stage we see five main engines, but this list can be extended with further research: two types of artificial intelligence tasks (“machine learning”, to be more precise), generic parallel computing, smart contracts and, at some future point (when technologies will be ready for mass hardware production), quantum computing.

Artificial intelligence. There are two main computing types related to the field of artificial intelligence: the actual *machine learning* (making some computing system to “learn” from the data or itself) resulting in a trained (i.e. learned) *model* and so-called “*inference*”: an application of some pre-trained machine learning model to analyse a set of data (like in image recognition tasks etc). To be brief, we will simply call the former **training** and the latter **inference**. Pandora network would be able to run both types of jobs, but with different workflows and computation engines. Initially, only inference will be supported, with training added at a later stage (see Roadmap section for details).

Generic parallel computing. Pandora Network will be capable of running any generic computation on the types of data which can be split into independent pieces and calculated separately. This case is quite similar to the usage of trained machine learning models, however instead of the model network nodes run specific program code applied to different batches of the data in parallel manner.

Parallel smart contracts. Since the introduction of smart contract concept by Nick Szabo in 1994 [...], the most of efforts was spent on building quasi-decentralised blockchain-based environments for executing generic and specific forms of smart contracts. Quasi-decentralised nature of this solution is related to the fact that the same code is executed on each of the network nodes on the same virtual machine, creating single point of failure for the censorship and a very low scalability (the fact was quite prominently demonstrated by the recent Ethereum network hacks, forks and congestion). Instead in case of using parallelisable smart contracts only small part of all computations will be performed by more than one node, reducing total load for network from $O(n*c)$ to $O(c)$, where n is a number of computing nodes in network and c is an amount

of computations in all smart contracts. Some initial attempts have been already made on the topic of the true decentralisation of smart contract execution: Plasma [...], TrueBit [...], RChain [...]. However all of these initiatives are lacking proper censorship-resistance consensus layer and have no formally verified models for proving the correctness of contract execution. Since Prometheus consensus protocol underlying Pandora network is perfect for solving these issues, it is quite natural to build the next generation of parallelised provable censorship-resistant smart contracts on top of it. We plan to run this initiative under auspices of Pandora Foundation after the initial work on the Artificial Intelligence and Generic parallel computing is completed.

Quantum computing. Today we are still quite far from the consumer-ready quantum computing. However recent advances of IBM, Intel and other companies give promise that quantum-enabled processors (quite expensive though) will reach the market during the next decade. This will instantly render quantum computing as a “weapon” that will be accessible only to few. According to the ideology of Pandora Foundation and the free market, we believe that this may create some global risks of different kinds (we will write on this topic in more details elsewhere) and need to be counteracted with the creation of economic incentives for chip producers to provide quantum computing capacities to a broad public in a censorship-resistant manner. Pandora network and Prometheus consensus protocol provide a perfect ground for the task: in case of quantum computing, owners of quantum chips will be able to sell their computing powers to the broad public, which can develop quantum computing models (alike to AI models) and order computations using them on some specific data sets.

On top of computation engines layer, a specific type of decentralised applications and IoT/hardware solutions (shown on the Fig. 1) for solving particular business needs will be built by the broader public/community. We call this part the **Ecosystem**. Pandora Foundation will participate and support initial efforts in building the first blocks of the ecosystem since this will be required to spread the adoption of Pandora network for the real-world business cases. Particular types of support are described in the section “Grants, investments and business spin-offs”. Among others this will include providing grants and investing into nonprofits, startups and companies that will

provide computing resources (“mining”), develop efficient chips for particular computation types (AI / quantum computing “ASICs”), focus on developing new self-evolving AI and robotic technologies (which will consume network computing resource at a large scale) and even space satellites that will help to keep network globally operating and resistant to physical types of censorship.

3.2. Current progress

The general technological progress is visually marked on the Fig. 1, where we have shown parts of the whole system that are already partially implemented or described in details in technological and scientific documentation. Briefly, at the current stage the project has achieved the following milestones:

1. Developed censorship-resistant Prometheus consensus and published it in form of different scientific, technological and generic papers, including formal proofs of Nash equilibrium for the top level of consensus.
2. Developed proof of concept lately followed by a full test net running federated AI inference tasks in a distributed network with consensus made on Ethereum smart contracts
3. Secured funds necessary for the launch of the first production network
4. Gathered and organised core teams for the research and technology development, partially built core team for the network development
5. Built strong network of expertise and advisors
6. Established technological partnership network with blockchain- and decentralisation-related projects
7. Presented materials and participated in a number of conferences and events worldwide, built a large network of connections to experts in the field of blockchain tech, bitcoin, ethereum etc.
8. Built social media presence and initial community around the project
9. Developed brand, marketing materials (online, printed), accumulated a number of high-valued domain names related to the project.

The detailed outlook of the current milestones and achievements is given in the Table [1](#).

Table 1: Main delivered results and assets by the project at the current stage

Deliverable / Asset	Field	Type	Date	Done	Description
Initial financial contribution	Funds	Finance	Aug	100%	See section Current financial statement
Pandora White Paper v 1.0	Technology research	Generic paper	Jul	100%	Initial document describing the project
Pandora White Paper v 2.0	Technology research	Generic paper	Dec	100%	This document
Prometheus White Paper	Technology research	Generic paper	Nov	100%	Detailed technological description of the consensus protocol
Prometheus Yellow Paper	Technology research	Scientific paper	Jan 2018	40%	Formal mathematical description of the consensus protocol
Pyrrrha Yellow Paper	Technology research	Tech. specification	Aug	100%	Technical specification for the testnet on Ethereum smart contracts and the PoCW consensus (part of Prometheus)
Proof of Computing work	Scientific research, formal verification	Scientific paper	Sep	95%	Scientific work proving Nash equilibrium for the PoCW consensus

Table 1: Main delivered results and assets by the project at the current stage

Deliverable / Asset	Field	Type	Date	Done	Description
Epimetheus Consensus	Software development	Proof of concept	Jun	100%	Smart contracts and worker node code for the initial “proof of concept” version of the system (called Epimetheus)
Epimetheus Worker Node	Software development	Proof of concept	Jun	100%	
Pyrrrha Consensus	Software development	Testnet	Dec	100%, audited	Components of testnet version running federated
Pyrrrha Worker Node	Software development	Testnet	Dec	100%, under audit	AI inference tasks in a distributed network with consensus made on
Pyrrrha Explorer	Software development	Testnet	Dec	100%	Ethereum smart contracts
Pyrrrha Client App	Software development	Testnet	Dec	100%	
Operational Testnet	Infrastructure	Testnet	Dec	100%	
P2P network layer	Software development	Proof of concept	Jan	50%	Network layer (see Fig. 1) libraries for the Prometheus consensus
Pandora Project Website	Marketing	Website	Sep	100%	Pandoraboxchain.ai , initial and second versions

Table 1: Main delivered results and assets by the project at the current stage

Deliverable / Asset	Field	Type	Date	Done	Description
Pandora Branding	Marketing	Prints	Oct	100%	Logo, business cards, banners, t-shirts etc
Social media presence	PR	Community management		ongoing	
Presentations	PR	Community management		ongoing	
Advisory board	PR	Community management		ongoing	See section “People, partners, advisors”
Key partnerships	Ecosystem	–		ongoing	
Building core teams	Execution	Science and development	Jan	90%	
Key domain names	PR	Asset	Nov	100%	whitepaper.ai yellowpaper.ai manifesto.ai pandora.network pandora.foundation

3.3. Roadmap

Research, development and testnet/mainnet launch/update tasks will be carried in **streams** developing different parts of well-defined **feature sets** in **stages**. The release plan will split the whole process into **epochs** (or, network versions), each of which will be a kind of hard- or soft-fork. At this moment of the project we see four main streams developing 12 main feature set blocks which will be gradually launched over 7 epochs. Main PR and other external events (start of mining/issuing of token, listing token on exchanges) will be attached to the epoch changes.

3.3.1. Streams

Streams allow to split the work between different teams (scientific, engineering, business – see Table 4) and organise a proper development processes and communications. There will be four main streams:

Core research & engineering: research on the technologies and methods that allow to achieve project goals, formal verification of the found models, technological specifications.

Core technology & development: implementing mission-critical parts of the system in code and ensuring their quality and compliance to the original formal models.

Applied development: implementation of the applied parts, computing engines and their variants.

Ecosystem: building client apps, associated technologies, businesses, marketing & PR campaigns.

3.3.2. Feature sets

Feature sets are blocks of network functionality that will be developed and launched in different epochs / releases (see below). Feature sets in their development will go through the streams defined above: initially from the research, that to core development and finally to the applied development and building ecosystem of apps around them.

Computing channels implementing ability to compute different types of models in parallel decentralised manner, including realisation of proof of cognitive work consensus (**PoCW**), that verifies results of computation and provides two-staged arbitrage (see Prometheus white paper for more details [...]).

Blockchain implementing the bottom part of Prometheus consensus (proof of reputation, **PoR**, see Prometheus white paper for more details [...]).

Governance as a set of technologies and features enabling network/protocol changes and upgrades.

Transactional privacy , enabling private PAN token transfers.

Data/computing privacy (Lethe), enabling computations on the private protected data or using private protected models. This will also protect the privacy for the results of computation.

Machine learning (training) as a first part of the AI computing engine.

AI inference as the second part of the AI computing engine, including federated learning models.

Data streaming: support to compute not only static existing data sets, but also real-time data streamed from some source.

Interoperability including support for sidechain technology, SegWit compatibility, Polkadot parachain technology and Cosmos sidechain with Tendermint consensus.

Generic parallel computing – computation engine as described in Technology section.

Parallel smart contracts – the third type of computing engines supporting new level of smart contracts. Will include virtual machine (*Styx*) and smart contract language (*Haron*) with formally defined semantics, syntax and formal verification of the code. Language which will be probably based on existing efficient models (RhoLang [...], Plutus [...]).

Quantum computing (at some point in future)

3.3.3. Epochs and launch phases

All epochs can be grouped into three supersets. The first one, named after Epimetheus (less clever brother of Prometheus), if a proof of concept historical version launched in Jul 2017. The second and third supersets contain three epochs each, the former are named after the daughters of Pandora, the latter – after three main places of the Greek mythology, going deeper

and deeper from the common humanity. The second superset will gradually implement core Prometheus consensus running basic AI inference tasks with governance, interoperability and transactional privacy feature sets. The last, third planned superset of epochs will go deeper into machine learning, data/computing zero-knowledge privacy, generic parallel computing, smart contracts and, finally, when the time comes – quantum computations.

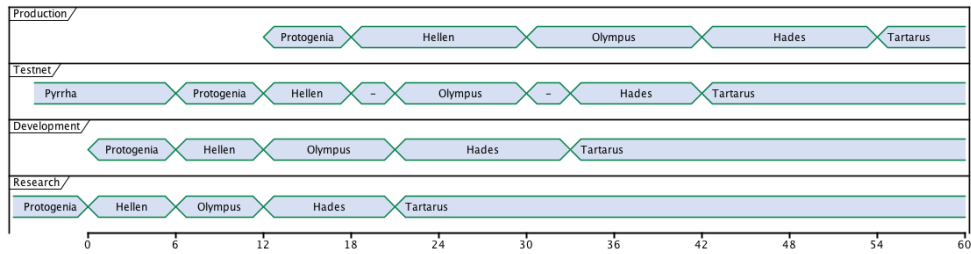


Figure 2: Development streams, epochs and major releases¹

Roadmap contains a core milestone: the start of the production network **mining** (i.e. issuing of new tokens for the proved computing job performed by the miners – worker nodes) which must happen nearly at the same time as the listing of the token on the main exchanges (since both miners and clients will need the ability to buy tokens, so as to use them as the working node’s stake and pay for the computing, correspondingly). We expect both of the events to happen simultaneously with the launch of Protogenia network at some point in Q4 2018. This will be preceded by the test net version of the same functionality required to avoid any problems with the release. The code will be carefully audited by professional audit companies, and, to the most possible extent, formally verified to correspond to original models developed by the scientific team. We will also tightly work with possible mining partners to enable sufficient computing capacity available for the market at the launch, as well as with business and scientific partners to ensure both existence of demand for computations and availability of AI models on the decentralised market. These are the parts of the ecosystem development tasks for the Pandora Foundation and they have been given corresponding budgeting (see Budget section) from the planned second financial contribution round. Following exchange listing all necessary funding

¹Axis X displays time in months since the 1 Jan 2018.

Table 2: Project roadmap with epochs and milestones

Epoch	Feature sets	Launch date		Other related events (ecosystem)
		Testnet	Mainnet	
Epimetheus	Proof of concept: distributed AI computing using blockchain technology	2017 Jul	–	First financial contributions
Superset “Pandora daughters”: gradual consensus and blockchain implementation				
Pyrrha	Initial testnet: federated computing using pre-trained AI models	2017 Dec	–	Second financial contributions
Protogenia	Prometheus computing channels: (on top of bitcoin and lightning network) PoCW consensus, AI inference	2018 Q2	2018 Q4	Mining; exchange listing (with main net); decentralised market
Hellen	Prometheus sidechains: (on top of bitcoin main chain) transactional privacy; governance	2018 Q4	2019 Q2	Start of chips production; client dApps and different software

Table 2: Project roadmap with epochs and milestones

Epoch	Feature sets	Launch date		Other related events (ecosystem)
		Testnet	Mainnet	
Superset “Going deeper into the rabbit hole”: from new computing engines to a world infrastructure and post-human economics				
Olympus	Complete Prometheus implementation: full PoCW+PoR consensus stack; data streams; AI model training; support for interoperability	2019 Q3	2019 Q4	Robotics
Hades	Computing engines advancements: generic parallel computing; data/computing zero-knowledge privacy	2020 Q3	2021 Q2	Self-evolving AI
Tartarus	Smart contracts & quantum: parallel smart contracts; at some point in the future – quantum computations	2021 Q2	2022 Q2	Space satellites

for the further development of the system and ecosystem will come from the Foundation tokens sold on the exchange.

3.3.4. Future vision

Decentralising machine learning and AI industry could not only enhance the market by making it open and free, but would significantly speed up the development of more efficient forms of AI due to availability of nicer data sets and possibility of ROI for ML research.

Furthermore, blockchain hybridization with AI might give some unexpected long-term synergetic side effects, like bitcoin didn't just resolve the double-spending problem, but by inventing blockchain it created the basis for massive disruption in distant industries. For introduction one may read this [Medium article](#), look at [Slideshare presentation](#) and [YouTube presentation video](#).

We imagine that in the future Pandora Boxchain computation resource could be used not only by a human/business clients, but also by other AI agents, creating new machine learning models, collecting data, and evolving themselves further and further, in a decentralized unstoppable environment. At the same time AI agents are incentivised to play a "trading game": a non-zero-sum cooperative strategy rendering them not aliens to humans, but cooperative partners, the same way that humans can cooperate with non-human legal entities (companies etc).

From this large perspective we have chosen the name "Pandora" for our project because it was the first woman created by Zeus to punish humans for the intelligence given to them by Prometheus. We call it "boxchain" as an allegory for Pandora's Box, since we believe that the success of the project might trigger a sequence of events leading to the appearance of generic forms of AI on our planet, a new type of intelligence. We also highly appreciate female intelligence and gender equivalence and that's why have selected Pandora for the name of our project and Prometheus as the name of consensus protocol underlying it.

3.4. Key people, partners and advisors

Overall the team has 3 PhD (neuroscience, game theory, dynamical systems, chemistry); multiparadigm lead developers (ex-CTO of Satoshi Fund), seasonal businessmen, experts in the field of artificial intelligence and machine learning, blockchain, cryptography etc.

Table 3: Key people participating in the Project

Name, surname	Role	Expertise	Responsi- bilities	Profile
Dr Maxim Orlovsky	Founder, Director	AI, neuroscience, data science, complexity science, computer science, business	vision, science, architecture, public presentation	PhD, MD, Director at Bitcoin Foundation Ukraine, Soros Prize laureate, multiple scientific awards
Sabina Sach- tachtinskagia	Founder, Director	economics, game theory, governance	science, compliance, finance	PhD candidate and researcher in Athens University of Economics and Business; BICA Labs
Andrey Sobol	Founder, Director	blockchain, economics, decentralised systems, technology	technology, infrastruc- ture, research, IT security	ex-CTO of Satoshi Fund
Andrey Khavryuchenko	Founder, Adviser, Peer reviewer	blockchain, decentralised systems, business, technology	ecosystem, audit	Member of Dash Core, owner & founder of 42 Coffee Cups

Table 3: Key people participating in the Project

Name, surname	Role	Expertise	Responsi- bilities	Profile
Olga Ukolova	Founder, Director	agile software development, biotechnol- ogy, brain- computer interfaces, AI, quality assurance	operations, management, HR,	MD, seasonal operations & quality assurance director, researcher at BICA Labs
Vitaly Bulychov	Founder, Director	business, investments, blockchain technology	networking, project development, community, PR	Certification Committee Board Member at The Financial Commission , Blockchain researcher and investor since 2012
Dr Olexander Ivanov	Researcher	nonlinear science, game theory, computer science, data science, AI, multiagent systems, technology	science, research, technology	University of Groningen
Julian Konchunas	Researcher, Core dev	software architecture	technology, research	Ubisoft ex-team lead

In total there are 21 people involved in the project execution, with 12 of them to be working full time since January 2018.

At this moment Project is performed by the teams presented in the Table 4.

Table 4: Existing project teams

Team	Responsibilities	Key fields of expertise	Size and lead	Since
Board of Directors	– overall management – legal – finance	– business – finance – IT security	6 part time	Jul
Science & technological research	– consensus formal verification – PoS algorithms – governance modelling – white, yellow papers and tech specs	– computer science – game theory – distributed systems – cryptography – dynamic systems – data science	4 full time 3 part time Dr Maxim Orlovsky, Sabina Sachtachtinskagia	Aug
Testnet development	Development and launch of the testnet	– Ethereum – Web tech – Python – DevOps	5 full time ² 4 part time Andrey Sobol	Jun
Mainnet development	Start with test implementations of different parts of Prometheus specs	– Rust – Haskell – Web tech – QA	4 full time ² Dr Maxim Orlovsky	Dec
Apps development	Develop initial ecosystem of web and mobile apps	– Web tech – Mobile	3 full time ² Olga Ukolova	Dec
Design & branding	– brandbook – t-shirts, stickers, business cards – websites for pandora and ecosystem	– web design – print design – web development	1 full time 1 part time ² Olga Ukolova	Sep

Table 4: Existing project teams

Team	Responsibilities	Key fields of expertise	Size and lead	Since
Project development	<ul style="list-style-type: none"> – conferences & events – community management – fundraising 	<ul style="list-style-type: none"> – business – SMM – PR – events 	2 full time 2 part time ² Vitaly Bulychov	Sep

The project has already built a strong networking and partnership around the technology, that include a number of technological partners, advisors, advocates, peer reviewers, outside collaborators and an initial community. Details on this are given in Tables 4 and 5. In September 2017, Pandora project has also become a strategic partner with the Ocean protocol, in building a decentralised market for big data and AI models.

Table 5: Existing project partners

Partner	Country	Field
IPDB & Ocean Protocol	Germany	Technological partner
Parity Technologies	Germany	Technological partner
Cryptovalley Association	Switzerland	Adoption advocates, networking
CyberFund	Blockchain	Adoption advocates
Bitcoin Foundation Ukraine	Ukraine	Adoption advocates
Microsoft	Ukraine	Technological partner
IBM Research	Czech	Technological partner
Wachsman PR	USA	PR
Saenko & Kharenko	Ukraine	Lawyers
Baer & Karrer	Switzerland	Lawyers

A number of advisors, advocates are working together with Pandora on different aspects of research, technology and building public awareness. They are briefly described in the Table 6.

²people are shared between teams

Table 6: Project advisers, advocates, peer reviewers and outside contributors

Name, Surname	Company or project	Role	Field of expertise
Dr Aliaksei Rubanau	Exosphere	Adviser	AI, Space
Dr Andre Karpištšenko	Planet OS	Adviser	AI, Big Data
Alex Shelkovnikov	Semantic Capital	Informal adviser	Business, Networking
Dr Alex Vasylchenko	Sofitto, GridSingularity	Adviser	Bitcoin, Blockchain, Engineering
Bruce Pon	BigChainDB, Ocean Protocol	Informal adviser	Business, Networking
David Knott	Plasma, Omise Go	Peer reviewer	Blockchain, Business
Dr Dimitri De Jonghe	BigChainDB, Ocean Protocol	Contributor & peer reviewer	Blockchain
Dmitry Starodubcev	Cyber Fund, Golos	Peer reviewer, Informal adviser	Blockchain
Dr Giacomo Zucco	BHB Network	Peer reviewer, Informal adviser	Bitcoin, Censorship resistance
Konstantin Lomashuk	Cyber Fund, Golos	Peer reviewer, Informal adviser	Blockchain
Dr Pavel Kravchenko	Distributed Lab	Peer reviewer	Blockchain, Cryptography
Robert Bent	TrueBit	Peer reviewer	Parallel computing
Prof Roman Olyinykov	IOHK	Peer reviewer, Adviser	Consensus, Cryptography

Table 6: Project advisers, advocates, peer reviewers and outside contributors

Name, Surname	Company or project	Role	Field of expertise
Dr Sergei Lonshakov	AIRA Lab	Peer reviewer	AI & Robotics
Tim Daubenschütz	BigChainDB, Ocean Protocol	Peer reviewer	Blockchain
Dr Trent McConaghy	BigChainDB, Ocean Protocol	Adviser (preliminary)	AI, Blockchain
Valery Litvin	Cyber Fund	Peer reviewer	Blockchain

3.5. Network governance

No one specifically manages the network (blockchain) and can neither single-handedly change its functionality, nor “disconnect” it. The Foundation and its subsidiaries will manage and oversee the development of the open source code that nodes can either accept or not accept, resulting in potential fork.

Neither the Foundation, nor the founders, nor developers personally take any responsibility for the work of the network and underlying consensus.

De facto, network management can be viewed from different angles:

1) Everyday work of the network. The network will be automated and decentralized. It can be said that the network is based on the computing work of nodes and on consensus that distributes the reward for the work. No one, including the Founders, can interfere with the normal operation of the network, including changing anything or disconnecting it: it is not possible from the technical perspective.

2) Network protection. If the results of the calculations of two nodes diverge, the consensus is determined collectively by a nodes with high reputation with a special pre-agreed fault-tolerant and censorship-resistant algorithms which are the part of the consensus itself. As it is embedded in the protocol this represents the mechanism to protect the network from attacks. In the early years, most likely that the Founders (as private individuals, not as Foundation) will own most of the nodes with high reputation and stake, because founders own tokens and will actively, honestly mine and gain reputation. Gradually, the total number of nodes will increase and the proportion

of nodes owned by founders will decrease accordingly. It should be noted that the right to resolve the disputes of the nodes and thus protect the network from attacks does not bring any dividends apart from ordinary payment for arbitration, and does not directly give the opportunity to decide anything in other areas.

3) Who determines the future of the network? The Foundation can ask the network nodes to upgrade to a new version, but any person in the world can do the same as the project is open source. Thus, the Foundation does not manage the network directly, although it is very likely that network participants will listen to the good ideas that Foundation will offer, follow it to improved versions, and use the code that it develops.

4. Economic Model, Finance and Legal Information

4.1. Economic model

The project is not structured as a business, thus it does not provide any business model, margin on some services etc. It is not operated by any legal entities due to its decentralised nature. While our initiatives (described above) will include a number of businesses, they will all be a part of the ecosystem around the core project technology and main network, and their total value may be by orders of magnitude lower than the network capitalisation or value of the pre-mined tokens (see below). Moreover, the main goal of such businesses will be to increase the value of the main network by driving its adoption, so they will be secondary to the network itself.

All the work performed by the non profits will be released to the public domain under open source licenses (preferably MIT; others if required by the used software) and in form of scientific papers (preferably high-impact peer-reviewed scientific journals) with OpenAccess.

4.2. Token economics

Pandora network connects, as a distributed platform, several huge, evolving markets: computer computation, data and algorithms. Pandora tokens (PANs) are utility tokens that act as the internal “currency” of the network to be used in all transactions on the platform. These tokens have the Pandora network’s qualities of being uncensorable and inalienable, which means that there exists no external force like network administration, government, etc. that would have the technical capability to take the PAN tokens from their owner, or to freeze them, or to inflate them, or to “tax” them, or to

discriminate the owners in the network based on their nationality, wealth, beliefs or any other characteristic. The only way to engage tokens in any activity is for the owners to sign it with their private key.

Mining and pre-mine. Pandora tokens are (a) pre-issued at the network launch (see section Token distribution for the details) and (b) issued over the period of 20 years via so-called “**mining**” process. With the total supply cap of 10 millions of tokens that can be issued in the future, 50% of the supply is pre-mined (category A) and 50% will be mined over the 20 years with logarithmic rate decrease over the time. The distribution of mined tokens will be the following: the most will be received by the worker nodes providing resources for computing tasks; some part will be allocated for the highly-reputable nodes signing blocks in the root and transactional chains with proof of reputation consensus (see Prometheus white paper for the details [...]) and the last part will be allocated to the researchers in the field of AI proportional to their scientific impact measured with h-index. The exact proportion between these beneficiaries will be defined elsewhere after necessary economical and mathematical modelling in order to obtain robust and sustainable solution with proper Nash equilibrium for non-byzantine behaviours of the network participants.

The users of the token in the network include two broad categories.

1. The buyers of network services. PANs are required by the clients who need to buy computation, data and algorithms. This is probably the largest category of token users. At the initial stages it will include corporations, businesses of all sizes, research institutions. Since data gathering develops rapidly, even small businesses and individual entrepreneurs and professionals have been given the opportunity to gather potentially beneficial data from themselves, the clients who visit their websites or even use their services offline. All these data is ready to be analyzed, but the market still lacks the affordable tools for that, which our platform provides. The market for algorithms that analyze data has various applications. For example, a major application is machine learning and the Pandora platform is designed to be very suitable for A.I. entities training. In the near future, buyers of Pandora network services

are expected to include not only companies and individuals, but also “artificial” individuals - e.g. simple automated A.I.s that participate in the IoT (Internet of Things) and then more complex “specialized” A.I.s - until the platform hopefully has the honor to provide services for a swarm of “general” A.I.s. (see Future vision section for more details).

2. The sellers of network services. The users who offer services to the network and expect to receive rewards for them, also need tokens to enable their participation. In particular, they need to deposit a collateral “stake” that ensures that they have the proper economic incentives. The sellers of computations, also known as network nodes (“miners”) would need to deposit relatively big token stakes, that enter an Escrow “smart” contract (part of the consensus protocol), to be forfeit if cheating behavior is detected by the network protocol. On the other hand, the sellers of algorithms and data would also need stakes, but much smaller, only to ensure that they do not spam the network with massive bad offers and are not involved in plagiarism. Thus, through the use of stakes, the security of the network is increased by economic incentivization of the desirable behavior.

Finally, since PAN tokens have some state-of-the-art economic and blockchain qualities, we do not exclude the possibility that demand for tokens will exist even outside of the scope of the immediate network use. There could be interesting possible uses that are not limited to speculation motives, to “portfolio diversification” by funds and to storing tokens for future use. It is hard to predict all possible uses of PAN tokens, but the history of e.g. “colored” Bitcoins shows that the ecosystem that develops around any major project often involves its main “currency” for extended use.

4.3. Token distribution and vesting

The tokens that Pandora network is to use are limited to 5,000,000 tokens issued initially (current total supply) and additional 5,000,000 tokens to be mined over the next 20 years.

Distribution of tokens to be issued is shown on the chart above. 30% of tokens will go to Founders to form economic incentives to launch the

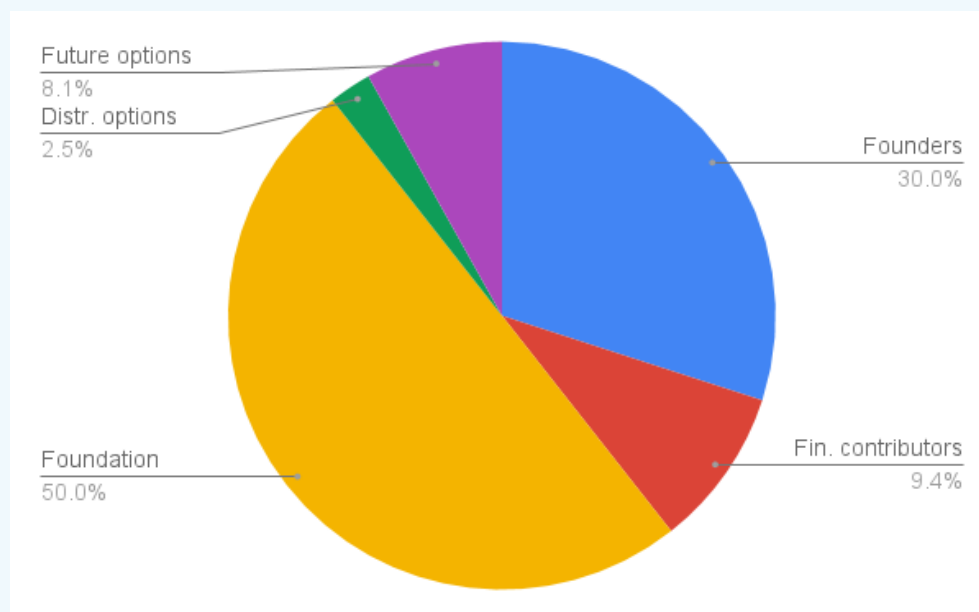


Figure 3: Initial token distribution

project and for the contribution to the project vision and know-how. Additional 10.61% are reserved as “options” for key future employees or other major contributors (e.g. world-class expert consultants) to be involved in the project. Of them, 2.5% were assigned to existing major contributors, while 8.1% are reserved for future use.

The remaining 59.39% of total current supply are to be used for funding of the project. During the first closed round of funding in July of 2017, 9.39% of total current supply was distributed (469’536 tokens) and an equivalent total of 469’536 CHF was received from 4 contributors. Another 13.32% is to be distributed in the second (this) closed round. The remaining 36.68% will be donated to the Foundation that will gradually spend them on a grants and sell them on exchanges once the network goes to production stage, and will use the proceeds for non-profit activities: to develop, scale and market the network, to grow its ecosystem etc.

The vesting terms are the same for everyone who receives tokens before they are sold on exchanges, that is for founders, option-holders and financial contributors in closed rounds. Those tokens cannot be sold for a year and a half plus additional six months of a cliff period starting from the receive of the funds from each of the contributors. However, those tokens can be used

Table 7: Financial statement on cash at disposal of the Project

Ticker	Coin & network	Amount	Rate to CHF ³	Value, CHF
BTC	Bitcoin	80.2868	17'326.30 ⁴	1'391'073.18
LTC	Litecoin	458.1	340.36 ⁴	155'918.92
DASH	DASH	121.6	1'133.81 ⁵	137'871.30
BTG	Bitcoin Gold	92.3	316.92 ⁴	29'251.72
GBYTE	GBytes: Byteball	4.457	610.37 ⁶	2'720.42
Total				1'716'835.54

for offering mining services to the network once it launches, and the mining rewards received will not have any vesting period.

4.4. Current financial statement

From the formal point of view, so far all the tangible assets at the disposal of the project were contributed solely by the founders of the project in the form of donations of cryptocurrencies. Donators are enthusiasts of the blockchain with a long record of accomplishments and are not interested in formalities, so the closed round of financing is the internal affair of the team, the transactions of individuals among themselves. Hence, an equivalent of 469'536 CHF total was received in July of 2017, on the first closed round of financial contributions.

The Project so far had a slow burning rate (less than 30,000 CHF monthly), since we were centered on research and general design of the system without much work for the development. Expenditures are going to increase starting December, as we have completed formation of the initial development teams and the amount of people in the project have increased nearly threefold.

Due to rise of cryptocurrency prices, the fiat value of the funds has increased since the initial contribution. As of 20 December 2017, the Project's funds portfolio consisted of a number of cryptocurrencies as shown in Table 7.

³Rate for the 20 Dec 00:00; cross-conversion from USD rates by 1:1 which corresponds to the rate on the 20th Dec

⁴Bitfinex

⁵Bittrex

⁶byte-ball.com with cross-conversion vs GBYTE

4.5. Financial contributions

Aforementioned project initiatives require funds, so there will be an option for the financial contribution to the project. We will probably propose a SAFT agreement: an exchange of contributed funds on the promise of ownership of the future utility tokens that will be used by the contributing party for the purpose of participation in a decentralized parallel computing framework. Additionally to the funds available for the Project (see Current financial statement above) the Project seeks for a financial contributions in the total amount of 5 millions CHF. Contributed funds will be spent according to the rules described in the following Budgeting section.

4.6. Budgeting

Approximate budget for the 2018 year is given in the Table 8.

Table 8: Budget for 2018

Budget article	Expenditure, CHF
Administrative	
Directors salaries	240'000
Legal (including relocation)	60'000
Offices	72'000
Hosting	24'000
Other infrastructure	24'000
Legal entities	114'000
Accounting	48'000
Total Admin	582'000
Research	
Core team	194'000
Game theory team	116'400
BFT team	77'600
Dynamic systems team	116'400
Cryptography team	77'600
Consensus team	77'600
Publications	145'500
Conferences	32'980
Literature & software	9'700
Total Research	847'780

Table 8: Budget for 2018

Budget article	Expenditure, CHF
Development	
Core team	116'400
Ethereum team	58'200
Prometheus team	116'400
Web app team	82'450
Mobile team	116'400
ML team	97'000
Devops	58'200
Audit & Bounties	77'600
Servers	38'800
Total Development	761'450
PR & Marketing	
Core team salaries	72'750
Visiting conferences	150'000
Organising conferences	60'000
Hackathons	40'000
SMM	97'000
PR Agencies	242'500
Media	48'000
Printing	12'000
Branding & Design	30'000
Enterprise relations	388'000
Exchanges	200'000
Total PR & Marketing	1'340'250
Ecosystem	
Grants to adopters	50'500
Software project investments	126'250
Startup venture funding	126'250
Mining	101'000
Total Ecosystem	404'000
GRAND TOTAL	3'935'480

The rest of the funds (around CHF 2.7M, if we take into account the current balance of the project) will constitute a contingency & reserve fund required to maintain necessary liquidity during cryptocurrency price decreases and secure different *force major* events related to cryptocurrency, AI and big data regulations requiring some additional spending on the legal, immigration or personal security protection – or delays in product launch and stock exchange listings (for instance, due to a new regulations).

This budget for 2018 will allow Pandora Foundation:

- to launch a first version of productive main network using own consensus (Prometheus) with AI-based computing;
- bring the token to public exchanges;
- build initial technology adoption and awareness.

After that, over the course of 2019-2022 Pandora will be focused on the following tasks:

- extending functionality of the AI computing (training, homomorphic encryption);
- adding new supported types of parallel computing;
- extending ecosystem of applications and services around the network

These activities will be funded by gradually selling the remaining stake of Pandora tokens owned by the Foundation on the open exchanges. Since tokens will be sold when funds are needed and not all at once, they will likely not be sold undervalued, therefore very substantial funding is likely to be raised.

Once the network will reach feature-completeness and ecosystem will be sufficiently evolved for a broad adoption the Foundation will become dissolved, bringing the network to the fully decentralised state (an event called **Dissolvement**). All unspent funds at the stage of Dissolvement will be spent on a buy-back of the tokens on exchanges; all bought-back tokens and unspent tokens from pre-mine will be burned. These two actions will help to increase the value of the tokens and will result in benefit of all token holders at that moment of time.

4.7. *Current valuation*

Estimation of the current valuation of the Project presents certain challenges because of the unprecedented scope and novelty of the task undertaken. Venture industry does not have established yet some widely accepted valuation practices for the public blockchains before they are listed on exchanges. The Project endeavours to create a game-changing way for any in-

interested party to transact autonomously within the platform, use and trade freely and privately the most valuable goods of the modern and future world: information (data), R&D (algorithms) and computing power, especially in the fields of Artificial Intelligence and Quantum Computing which are going to boost in size of their economy by many orders of magnitude in the following decade. By its nature, the project is designed to embed the most advanced parts of the technological sector into a new, direct economy without middlemen and unwanted supervision. Therefore, when fully fledged, the possible future valuation of the project once it got widely adopted should be counted in multi-trillion figures and would have its own economics comparable in size to those of the global economy itself.

At the same time, the current state of the Project is yet relatively modest and very undervalued compared to what it can be in foreseeable future, e.g. upon the network launch. In brief, the Project has gone all the way from being an idea in May to a proof of working concept that it was during round 1 in July, to being a well designed, researched and documented project, embedded in code with public testnet launching on the 1st of Jan 2018. Scientific and technological deliverables have been produced, initial teams and people with core expertise are gathered, and a degree of networking and community awareness has been achieved. For full details on the current state of the Project, see the section “Current research & development progress” and Table 1. This progress plus the available project equity (see Table 7) justifies the proposed valuation of CHF 50 millions. This still leaves the Project quite undervalued comparing to other projects that are on the same or earlier stages of development. While there is no project of similar to ours scope and scale on the market, we could use Golem Network as a sample: a project that covers one of our target markets (although not being a direct competitor since it lacks consensus layer and is built on top of Ethereum network and existing technologies without much of technological innovations). Its current market valuation (market cap) is around CHF 400 millions, although its own roadmap shows it being years away from the launch and has a very basic white paper without much of the technological details. Looking at many other blockchain projects, even those without big ambitions, we see similarly high numbers – and way higher for blockchains that promise game-changing results, like Cardano which got to over 15 billions valuation within days after the launch of a very early version of mainnet.

The proposed valuation of the future tokens of the network is CHF 37.5 millions (that includes CHF 1.7 millions of the available project cash) gives

a x7.5 multiplier to the initial valuation at the first round. This valuation is well below industry market norms not just for the whole project valuation but even for the size of funds raised on the typical game-changing ICO of much smaller size and technological advancements. We accept it however in order to avoid the distraction of the public coin offering that would shift our attention from the core development to an advertising targeting creation of hype. Therefore, instead of following the ICO path, we expect that faster and smarter private, closed-round financial contribution will provide the layer to get higher, by orders of multitude, valuation on the open round that will follow after the main production network will be launched.

Additionally, the for-profit part of different business initiatives that are created around the network (see the next Section 4.8 for details) is valued in 13.688.923 CHF (except remaining tokens at the dispose of Foundation) and includes available cash and raised funds that will be used for the network development. Thus, the proposed current joint valuation of both the future network tokens (non-profit) and for-profit ecosystem is 51.188.923 CHF.

4.8. Grants, investments and business spin-offs

We have already mentioned elsewhere that the mission of the Foundation is to launch the Pandora network *and* support its progressive adoption, increasing capitalization of the network. In the previous sections we have described technological vision, roadmap, economical models and operations structure that is required to fulfill the first part of the mission: launching Pandora network. As for the second part, the Foundation will use a number of tools to achieve its goal, keeping in mind also the need to protect the interests of financial contributors of the project:

- providing grants to nonprofit entities (like research labs) doing research, creating products or building awareness of the problems (like the importance of the free AI market) that can benefit the network;
- investing into the businesses that develop products that will be a part of the ecosystem;
- investing into AI-related and other startups that will consume the network functionality and pay later for the network services;
- providing grants for early adopters of the technology for including the network into their business processes;

- building partnerships and enterprise alliances around the network and technology.

Basically, all these approaches fall into one of two categories: **grants** and **investments**. The general workflow for the process is shown on the Fig. 4.

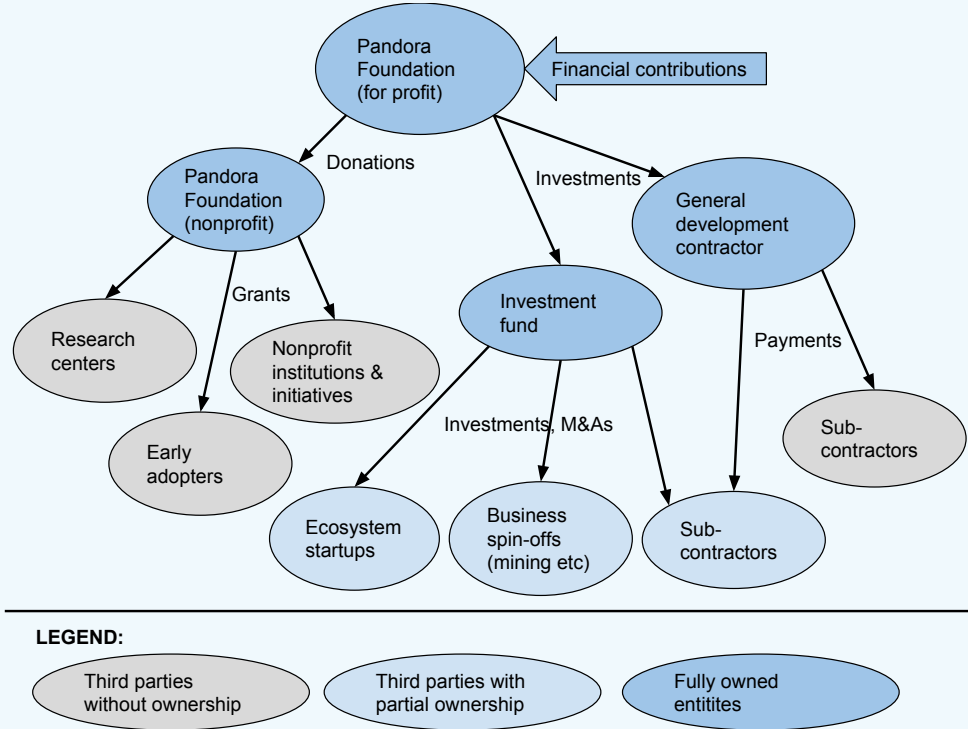


Figure 4: Structure of possible legal entities and financial flows required for the realisation of the project

All financial contributions that comes in exchange for tokens are done into a single entity at the top of hierarchy (Root entity) that will, probably, have a form of for-profit company. In return, this entity will issue a promise for the future tokens (SAFT agreement). PAN tokens themselves do not provide any voting rights or share in the future profits of any of the for-profit entities which may be a part of Pandora business ecosystem (there is no profit in Pandora Network itself).

Additionally there is an option to invest into the working capital of the for-profit companies at different levels in exchange for their equity (not PAN tokens). Having said that, it still worth mentioning that the primary goal of

the whole structure is to work not for the financial returns of its shareholders, but for the increase in the network capitalisation for the Pandora network, and thus we do not set returns for the investments by Root entity as a priority or main decision-taking criteria; rather, such additional financial return from such investments will be a nice supplement rather than a dedicated venture fund business. To emphasize this once again, the financial contributions to the project are not an investments into any kind of a business or venture fund; it may result in some returns aside from the token price increase, but this is not put as a goal. The goal is to stimulate increasing adoption of the features of Pandora network and the growth of the ecosystem around it.

Possible business ventures that may be supported (in form of investment) or acquired by the project may be of the following types (not limiting to them):

Software development houses, creating software products and tools for the network

Startups AI, quantum computing and other breaking technology startups that will benefit from the functionality of Pandora network and will create a demand on its services

Vendors Robotics, autonomous vehicles (including weapons)

Hardware Hardware/chip producers for AI, quantum computing etc

Space industry companies and startups helping to bring the network global accessibility and connectivity, as well as mining/computing facilities to an orbit

Mining/computing power farm producers and data centers

Apart of the funds taken from the Foundation and its financial contributions aforementioned business spin-offs and startups may attract additional capital from third-party investors and thus the Pandora Project may have a role of a non-sole or even minority owner.

Aside from the investments the Root entity will have a majority-owned general development contractor which will orchestrate the whole network implementation/software development process by a number of subcontractors that may or may not be co-owned with the project members. The selection of subcontractors will be done in an open and transparent way: they either

should be an entities organised by the Project or existing companies with a proven professional track record.

The final part will be related to grants given towards public nonprofit, academic and business projects for the necessary professional research work, building of the public awareness and early adoption of the Pandora technologies into their business processes/models. These companies will be selected by the same principle as stated above for the subcontractors.

Decisions on the investments, donations, grants and payments will be taken by the management of the appropriate entities; at the Root level – by the Board of Directors with the simple majority. Other financial contributors will have an advisory voice.

The whole structure of the legal entities is preliminary and may be changed after careful examination with the legal advisers (the list of partnered legal advisors is given in Table 4). However, notwithstanding the legal form, the structure will be serving the defined purposes and cash flow lines as described above, so this would not change the incentivisation of the Founders and financial contributors to the project.

4.9. Legal

The most likely corporate structure of the Project (pending more legal consultations) includes a non-profit organisation that acts as a public coordinator for the Project and manages those activities that do not generate profit, and a for-profit company or set of companies that are involved in profit-generating activities (see also Fig. 4).

It should be noted that non-profit entity requires stricter compliance and therefore its location needs to be chosen very carefully. Following closely the recent developments in legal and regulatory framework, it appears that some jurisdictions stand out for their consistent support and friendliness to blockchain and cryptocurrencies, as well as big data and A.I. Primarily, cantonal regulators in Zug, Switzerland tend to offer semi-formal consultations pre-incorporation and municipal-level support after the incorporation. Formation of a Swiss Foundation is currently the standard and widely acknowledged way for managing the creation of a blockchain platform. We are in contact with leading Swiss law firms, primarily Baer & Karrer, and await the publication of the amendments to the Swiss regulatory framework, expected in January. Other potentially suitable locations for a non-profit organisation include Liechtenstein, Luxembourg and Malta.

The for-profit company or set of companies have much more flexibility in location for incorporation and may be based in Hong Kong, Switzerland, Malta or Cyprus (for operational units, ecosystem of startups and business spin-offs).

4.10. Risks and Competition

We see the following risks or uncertainties for the Project:

Cryptocurrency price volatility risk. Since a substantial portion of the funds is to be held as cryptocurrency (primarily Bitcoin and a few other select currencies of sufficient capitalization), a downward shift in their price could have an adverse impact on Project’s liquid position. The protection against this risk is diversification: holding a portfolio of high-quality cryptocurrencies (including some with negative correlation between them and Bitcoin) and also a sufficient fiat balance (e.g. CHF) for operational expenses.

Blockchain and cryptography regulatory risks. There exists much uncertainty about the forthcoming regulation of crypto-projects worldwide. In particular, SEC shows a tendency towards characterization of tokens as securities by default. Therefore, it becomes crucial to have a premier legal team and to choose a blockchain-friendly and consistent jurisdiction for incorporation. See the section “Legal” above for details.

A.I. regulatory risks , namely potential restriction of research for “ethical reasons” or imposing any sort of censorship. Such risks would likely take time to materialize, since there is no common framework about A.I. ethics yet. After the network launch, and especially after the Dissolution event, such regulations would not directly affect the Project, since it is open source, decentralized, uncensorable, non-jurisdictional and not run by a particular legal entity or physical persons, but only by anonymous nodes. The initial developers would not be pressed to comply with regulation, as they would have no legal or actual ability to change the rules of the network.

Political uncertainty. The overall tendency for the increase of government surveillance and control over assets, for more bureaucracy and for populist solutions, may pose a threat to decentralized activities as a whole, and especially to activities that have the capacity to disrupt the current

state of affairs. Such political risks are not readily calculable at this moment, especially since different countries fail to coordinate and do not act in accord. As a side note, the Project is built to outmaneuver political risks by providing by-design censorship-resistant environment for transactions.

Execution risks . One of the highest risks for the project is the ability of the team and involved companies to deliver the desired product that will be able to work robustly, securely reach its aims and get adopted by a growing community of users. Taking into account the size of ambitions of the project this risk clearly exists, however it's being mitigated by the main three factors: (1) clear roadmap with staged delivery of the project features; (2) big attention to peer reviewing, formal verification, code audit and quality assurance testing of the resulting software and (3) project policies to hire and work with the world-best expertise, starting from the scientific and research areas, and up to the development. The project team already consists of many cross-disciplinary scientists, engineers, developers and businessmen with the proven track success record and expertise covering all necessary fields (please refer section Team for the more details). We already have 4 PhD in the core team plus 9 PhD as peer-reviewers, contributors and advisers to the project, with international recognition in the fields of blockchain technology, cryptography, artificial intelligence, computer science. As from the operational perspective we will use best practices to manage and coordinate different teams and streams of the development, directly exchanging experience and taking samples from the successes and failures of the previous large blockchain projects (Ethereum, Cardano etc).

Competitive risks for the first epochs of the project (specific for AI computing) are analysed below; for competition analysis of other network feature sets (consensus layer, censorship resistance, parallel computing) one may refer to the section Previous work of Prometheus white paper [?].

Below are analysed some major sectors that can be seen as competitors to the Project

Large corporations Computational services offered by large corporations, e.g. Amazon. These services could hardly be seen as competitors to

the Project for several reasons. Firstly, they offer bundled services that have a limited scope, not being a free market for algorithms, computations and data. Secondly, despite their big scale, they are burdened with costly expenses, such as management, accounting, compliance, leasing costs etc. and additionally they need to operate with a profit for their shareholders. Therefore, they need a substantial margin. On the contrary, the Project operates without expenses, with automated rules, benefiting from decentralized leasing of hardware and electricity, data and algorithms, wherever they are cheaper worldwide. The Project operates with zero profit margin, for the benefit of all those who hold and use its tokens, achieving highly competitive prices for services that it offers.

GPU miners The Project's network initially will use GPU in AI-related computations, therefore it is important to consider the opportunity cost of using these GPU resources for other cryptoprojects mining, instead of leasing them to the network. The major cryptocurrencies that use these resources are Ethereum, Ethereum Classic and Bitcoin Gold. It has been announced that Ethereum is switching to PoS during the following year, thus if it happens then GPU resources are expected to become more abundant, so the Project is expected to have an additional influx of nodes willing to rent their hardware to the Project. It should be noted that the Project offers to its miners useful computational tasks on the progress of A.I. and not just on electricity waste like other currencies that compete for GPU resources.

Blockchain projects Decentralized A.I. and computing blockchain projects. It appears that direct competition in the field is still absent. There are several projects that are worth mentioning on the intersection of A.I. and blockchain fields, somewhat similar to the Project, but with important differentiations that place them in a different niche. These are [OpenMined](#), [Singularity.NET](#), Neuromation and some other local startups. **OpenMined** creates blockchain-based private neural network model training with homomorphic encryption of the data. The project has very vertical niche and needs to solve many mathematical difficulties on the way towards reaching its goal. Pandora may as well use this technology once it will be developed (since its open-sourced), embed it into AI training engine and leverage on it. So this project is to be seen

as an important cooperator rather than competitor. **Singularty.NET** is a recent ICO by Hanson Robotics producing humanoid robots. They are pro-censorship for AI models, so this puts them into a completely different position on the market as compared to our project. **Neuro-mation** specialises in training neural networks with simulated data, which, again, is very vertical niche of the market and lies outside the scope of our project. What is important, though, is that all mentioned projects do not have their own consensus protocol and blockchain, instead they try to operate on top of the Ethereum network. This creates very high third-party risks for those projects and significantly reduces their sustainable market advantage.

Additionally to possible competitors, a number of big data/AI blockchain-related projects can be seen primarily as partners and as a part of the ecosystem rather than as competitors. First of all this is **Ocean Protocol** that provides foundation for building decentralised markets for big data and machine learning models. Pandora Project already has become strategic partners with the Ocean Protocol, which will allow us to boost the speed of the development of the dApps for the clients.

References

- [1] The specs for libp2p and associated submodules. <https://github.com/libp2p/specs>.
- [2] Webassembly. <http://webassembly.org/>, 2016.
- [3] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timon, and P. Wuille. Enabling blockchain innovations with pegged sidechains. 2014.
- [4] K. Bennett, C. Grothoff, T. Horozov, I. Patrascu, and T. Stef. Gnunet-a truly anonymous networking infrastructure. In *In: Proc. Privacy Enhancing Technologies Workshop (PET)*. Citeseer, 2002.
- [5] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn. Corda: An introduction. <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf>, 2016.
- [6] V. Buterin. Ethereum: A next-generation smart contract and decentralized application platform. <https://github.com/ethereum/wiki/wiki/White-Paper>, 2013.
- [7] V. Buterin. Serenity poc2. 2016.
- [8] N. community. Whitepaper: Nxt. <http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt>, 2013.
- [9] C. Copeland and H. Zhong. Tangaroa: a byzantine fault tolerant raft. http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf, 2016.
- [10] E. B. Jae Kwon. Cosmos: A network of distributed ledgers. <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md>, 2016.
- [11] J. Kwon. Tendermint: Consensus without mining. <http://tendermint.com/docs/tendermint.pdf>, 2014.
- [12] D. Larimer. Bitshares. <http://docs.bitshares.org/bitshares/history.html>, 2013.

- [13] P. Maymounkov and D. Mazières. Kademlia: A peer-to-peer information system based on the xor metric. In *IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems*, pages 53–65, 2002.
- [14] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song. The honey badger of bft protocols. Technical report, Cryptology ePrint Archive 2016/199, 2016.
- [15] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, 2008.
- [16] D. Ongaro and J. Ousterhout. In search of an understandable consensus algorithm. In *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, pages 305–319, 2014.
- [17] Parity. Parity ethereum client. <https://parity.io>, 2016.
- [18] S. Popov. The tangle. https://www.iotatoken.com/IOTA_Whitepaper.pdf, 2016.
- [19] Y. Qian. Randao. <https://github.com/randao/randao>, 2015.
- [20] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474. IEEE, 2014.
- [21] P. Snow, B. Deery, J. Lu, D. Johnston, and P. Kirb. Factom: Business processes secured by immutable audit trails on the blockchain. https://raw.githubusercontent.com/FactomProject/FactomDocs/master/Factom_Whitepaper.pdf, 2014.
- [22] G. Wood. Devp2p wire protocol. <https://github.com/ethereum/wiki/wiki/libp2p-Whitepaper>, 2014.
- [23] G. Wood. Ethereum: a secure decentralised generalised transaction ledger. <http://gavwood.com/paper.pdf>, 2014.
- [24] G. Wood. Yellow paper committee. <https://github.com/gavofyork/curly-engine>, 2016.