# Tezos

The self-amending cryptographic ledger

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS

# EXECUTIVE SUMMARY

## Tezos is a decentralized blockchain that governs itself by establishing a true digital commonwealth.

What's more, Tezos was built to facilitate formal verification, a technique which boosts the security of the most sensitive or financially weighted smart contracts by mathematically proving the correctness of the code governing transactions.

The Tezos blockchain will underpin secure, decentralized applications and smart contracts while avoiding some of the political and technological problems which earlier efforts such as Bitcoin and Ethereum have faced. Tezos was built on the belief that a deep commitment to security, formal verification, and governance that gives stakeholders the power to make protocol decisions is the formula for earning trust and generating widespread adoption on the blockchain.

This document provides a comprehensive overview of Tezos, its applications and benefits, the developers involved in the project, the upcoming Tezos fundraiser (sometimes loosely called "ICO" or "crowdsale"), the Tezos Foundation and the goals the Foundation hopes to achieve.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS

tezos.com

# THE HISTORY OF THE TEZOS BLOCK-CHAIN

Work on Tezos began in 2014 by its founding development team, whose academic experience spans from philosophy to physics, mathematics and computer science, along with professional experience that includes positions at Goldman Sachs, Morgan Stanley, The Wall Street Journal, and Accenture. They recognized that decentralized blockchains share the same challenges that exist in any commons (the name economists give to a resource shared by several people), specifically that challenges around governance and maintenance often lead to stagnation, shortages, and political deadlock.

In the case of pioneers like Bitcoin and Ethereum, those challenges have manifested themselves in situations that put too much power in the hands of core development teams or miners. In other words, first-generation blockchains have become subject to a form of centralization that their developers sought to avoid.

During three years of development, the Tezos team sought to address the need for decentralized innovation in protocol design and emphasized the importance of formal verification in its software design philosophy.

**December 2013** - Gordon Mohr suggests NomicCoin on Twitter

**January 2014** - Independent formulation of this idea by L.M. Goodman

**March 2014** - Tezos development begins self-funded

**August 2014** - Tezos Position Paper is released

**September 2014** - Tezos White Paper is released

**January 2015** - Zooko becomes an advisor to Tezos

**August 2015** - Bitcoin XT proposed, the "block-size debate" begins putting governance on the front stage

**June 2016** - The DAO is hacked, a hard-fork of Ethereum is soon decided by the Ethereum Foundation

**June 2016** - The pre-fork Ethereum chain becomes Ethereum Classic and splits the network

**June 2016** - Andrew Miller joins as an advisor

**September 2016** - Arthur Breitman presents Tezos as StrangeLoop

**September 2016** - Polychain Capital and several individuals back Tezos to help scale up development

**February 2017** - Emin Gün Sirer joins as a technical advisor in an official capacity

**May 2017** - Tezos Foundation launches in Switzerland

**Summer 2017** - Tezos network launches


1 HISTORY

2 **PRINCIPLES**

3 PEOPLE

4 FUNDRAISER

5 PLANNING

6 GOALS




# THE PRINCIPLES OF THE TEZOS BLOCKCHAIN

## 2.1 GOVERNANCE

While all blockchains offer financial incentives for maintaining consensus on their ledgers, no blockchain has a robust on-chain mechanism to seamlessly amend the rules governing its protocol and explicitly fund protocol development. As a result, first generation blockchains tend to empower, de facto, centralized core development teams or miners to formulate design choices.

Tezos takes a fundamentally different approach by **creating governance rules for stakeholders to approve of protocol upgrades that are then automatically deployed on the network.** When a developer proposes a protocol upgrade, they can attach an invoice to be paid out to their address upon approval and inclusion of their upgrade. This approach provides a strong incentive to contribute efforts towards core development of the Tezos blockchain and further decentralizes the maintenance of the network. It compensates developers with tokens that have immediate value rather than forcing them to seek corporate sponsorships, foundation salaries, or work for Internet fame alone.

Tezos instantiates new technical innovations but can also enforce types of constitutionalism through the use of formal proofs to mathematically verify that key properties are upheld over time. By allowing stakeholders to coordinate on-chain, the network also allows for the creation of bounties to implement specific features or discover bugs. Collectively, the network maintains the decentralized aspect of blockchains while introducing a mechanism to enable collective decision making. Tezos tokens not only power smart contracts in the network, but also allow votes on protocol amendments. The initial Tezos rollout is simple by design, but its self-amending nature means that the rules governing the network can be improved over time.

## 2.2 CORRECTNESS

Blockchains underpin billions of dollars of value with relatively small codebases, which puts them in the sweet spot for formal verification, a powerful technique that mathematically proves the correctness of computer programs. Formal verification has been used in the aerospace industry, in medical devices, and other instances where the stakes are too high to fail.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



### 2.2.1 OCAML IMPLEMENTATION

Formally verifying a complex piece of software is a sizable task, so the development team sought to simplify it as much as possible. To that end, we implemented Tezos in OCaml, a functional programming language that has been developed and maintained by the INRIA since 1996 (and itself based on earlier efforts). Its speed is comparable to that of C++ and it generally features among the fastest programming languages in benchmark testing. More importantly, OCaml is strongly typed and offers an impressive type inference system. Its expressive syntax and semantics, including powerful pattern matching and higher-order modules, make it easy to concisely and correctly describe the type of logic underpinning blockchain-based protocols. OCaml's semantic is fairly rigorous and a very large subset has been formalized, which removes any ambiguity as to what is the intended behavior of amendments. In addition, Coq, one of the most advanced proof-checking software tools, is able to extract OCaml code from proofs. As Tezos matures, it will be possible to automatically extract key parts of the protocol's code from mathematical proofs of correctness.

### 2.2.2 MICHELSON

The correctness of smart contracts running on the Tezos blockchain is almost as important as that of the core protocol itself. Smart contract bugs can taint the reputation of the platform they operate on. To mitigate that risk, the development team designed our smart contract language with correctness and formal verification in mind.

Michelson is statically typed and purely functional. This design largely eliminates large classes of bugs such as the DAO reentrancy bug or the Solidity ABI vulnerability discovered by the Golem project. The language itself looks like a mix between Forth and Lisp and a reference is available **here**. The Tezos development team has already successfully proven the correctness of Michelson contracts in Coq, including the multisig contract.

More information about these design choices are found in the Tezos **position paper** and **white paper**.

Formally verifying a complex piece of software is a sizable task, so the development team sought to simplify it as much as possible.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



## 2.3 PROOF OF STAKE

In its initial incarnation, Tezos is launching with a delegated proof-of-stake consensus algorithm. This choice of consensus algorithm is amendable, on-chain, by the stakeholders. In principle, a proof-of-work consensus or even a federated consensus could take its place. However, the development team expects proof-of-stake to be an important part of the Tezos culture and thinks it will remain the primary consensus method.

Tezos' delegated proof-of-stake system works by letting every stakeholder designate one or several delegates of their choice to create blocks and validate transactions on their behalf. The higher the stake delegated to a given validator, the more often will they be called upon to create blocks. **Though the Tezos system is delegated, every token holder can participate as a delegate regardless of the amount they hold.**

The network issues newly minted tokens as a reward to validators for the service they provide to the network. These rewards will create *nominal* inflation; **holders are free to be their own delegate if they so desire and thus to avoid any dilution.** It likely that large delegates will offer to share some of their profits in a bid to attract more stakes.

The computing requirements to become a validator are relatively lightweight (a few hundred watts at most) but a robust, high-speed Internet connection is required. Running a proof-of-stake node also requires more operational security than running a mining operation as it involves signing blocks with a private key on a machine connected to the Internet. This risk can be mitigated by the use of secure hardware components, as found in devices like the Trezor or the Ledger Nano S.

The development team expects proof-of-stake to be an important part of the Tezos culture and thinks it will remain the primary consensus method.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



# PEOPLE AND ORGANIZATIONS INVOLVED WITH TEZOS

## 3.1 DYNAMIC LEDGER SOLUTIONS

The Tezos blockchain is primarily being developed by Dynamic Ledger Solutions, Inc. (“DLS”) a US-based company co-founded by Kathleen and Arthur Breitman.

Arthur was born in France and educated at École Polytechnique in math, physics, and computer science. He then went on to a career in quantitative finance, including positions at Goldman Sachs and Morgan Stanley. Kathleen holds a BA from Cornell University and worked at The Wall Street Journal, Bridgewater Associates, Accenture, and R3 prior to Tezos.

Kathleen met Arthur at a crypto-anarchist meetup in New York in 2010 and they’ve been together ever since.

## 3.2 THE DEVELOPMENT TEAM

Tezos is a small team. The philosophy behind the Tezos project dictates that the core team should not be the only contributors to the Tezos project. That being said, the original team will obviously play a critical role in growing and improving the network in its infancy.

There are currently ten core developers: Arthur Breitman, Benjamin Canou, Çağdaş Bozman, Pierre Chambart, Grégoire Henry, Mohamed Iguernlala, Fabrice Le Fessant, Alain Mebsout, Vincent Bernardoff, and Guillem Rieu.

Our development team is primarily located in Paris, France and has been working on the Tezos ledger through a partnership with OCamlPro, a software company with deep OCaml expertise founded by Fabrice Le Fessant. Most of our developers have Ph.Ds in Computer Science and expertise in programming language theory.

1 HISTORY
2 PRINCIPLES
3 **PEOPLE**
4 FUNDRAISER
5 PLANNING
6 GOALS



## 3.3 THE TEZOS FOUNDATION

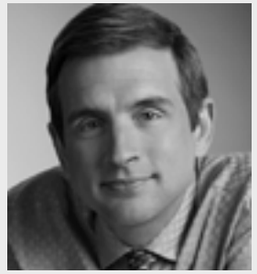
Tezos' founders thought it that it would be beneficial for the the Tezos Network if a non-profit foundation could guide its early steps and complement the decentralized nature of its governance model. The Tezos Foundation is an independent Swiss entity whose goal is to promote and foster the use of the Tezos blockchain, its technology and its ongoing development.

Since the early days of the Tezos network are critical, the Tezos foundation will retain a veto power over protocol upgrades for a period of one year from minting the Genesis block. However, the Foundation does not and will not have any privileged power in proposing protocol upgrades. Any protocol upgrade proposed by the Foundation will need to be vetted and agreed upon by the stakeholders just as any other proposal would.

The members of the Foundation council are Johann Gevers, Diego Ponz, and Guido Schmitz-Krummacher. Johann Gevers is one of the founders of the Cryptovalley ecosystem in Zug, Switzerland, as well as the CEO of **Monetas**, a digital payments company based in Zug. Diego Ponz is a computer scientist and entrepreneur with an expertise in combinatorial optimization. Guido Schmitz-Krummacher is a businessman in the Zug area.

## 3.4 ADVISORS

Tezos advisors currently include:



### Zooko Wilcox

*Computer scientist and the leader of the ZCash project.*

Additionally, Zooko is the designer of multiple network protocols and a member of the development team of ZRTP and the BLAKE2 cryptographic hash function.

### Emin Gün Sirer

*Associate Professor at Cornell University.*

Gün's research spans operating systems, networking, and distributed systems. He is a Co-Director of the Initiative for Cryptocurrencies and Contracts (IC3) at Cornell. Emin has made enormous contributions to the Bitcoin community through his work on vaults and selfish mining techniques.

### Andrew Miller

*Assistant Professor at the University of Illinois, Urbana-Champaign in Computer Engineering and Computer Science.*

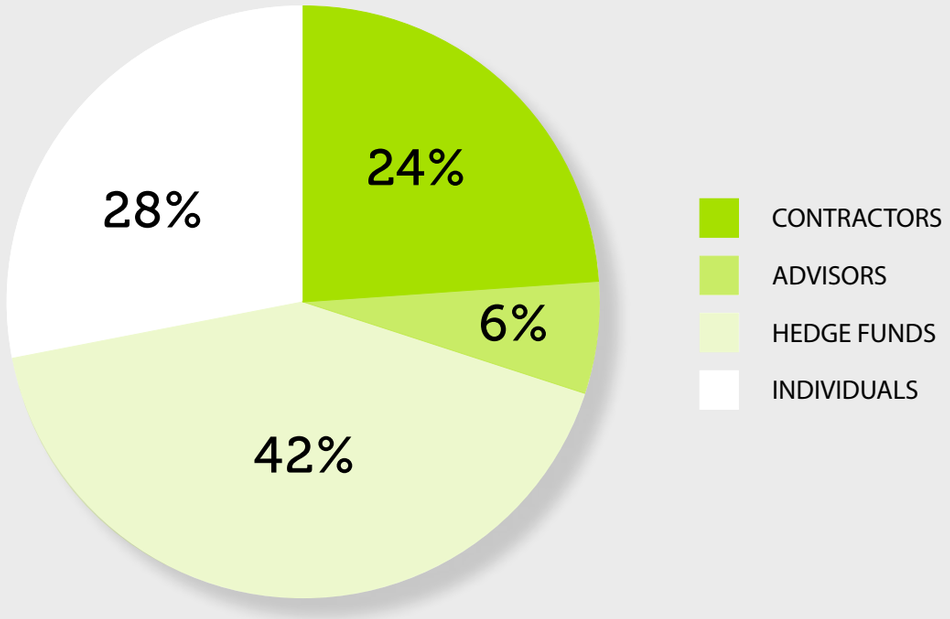
Andrew is also an Associate Director of the Initiative for Cryptocurrencies and Contracts (IC3) at Cornell and an advisor to the ZCash project. His research interests are broadly in computer security, and focused on the design of secure decentralized systems and cryptocurrencies.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS

## 3.5 EARLY BACKERS

In order to fund the last phases of Tezos' development, the DLS team received backing from ten entities from September 2016 through March 2017. Three of these entities were hedge funds with a specific focus on tokens. The other seven backers were high net-worth individuals, or federations thereof, many of whom were also LPs of the hedge funds. Total early funding amounts to $612,000.  In order to value the early participants in this project, the Tezos Foundation will recommend an allocation of XTZ tokens equivalent to $893,200.77 in contributions (corresponding to a 31.48% discount). No single backer represented more than 33% of the total amount.

DLS chose these backers strategically, with an emphasis on people and entities who were philosophically in-line with our uncapped fundraising structure and are long-term believers in the Tezos protocol, either based on their technical expertise or familiarity with the founding team.



1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS

# FUNDRAISER

**The Switzerland-based Tezos Foundation will oversee a fundraiser on July 1, 2017.**

**It will recommend a token allocation in the Tezos genesis block based on contributions in bitcoins and Ethers** (Please refer to the legal document that will be issued by the Foundation for more details.)

The Foundation will receive and manage all contributions on a special website: **https://crowdfund.tezos.com** and through Bitcoin Suisse AG, a Swiss exchange that has successfully managed several fundraisers.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



## 4.1 SCHEDULE

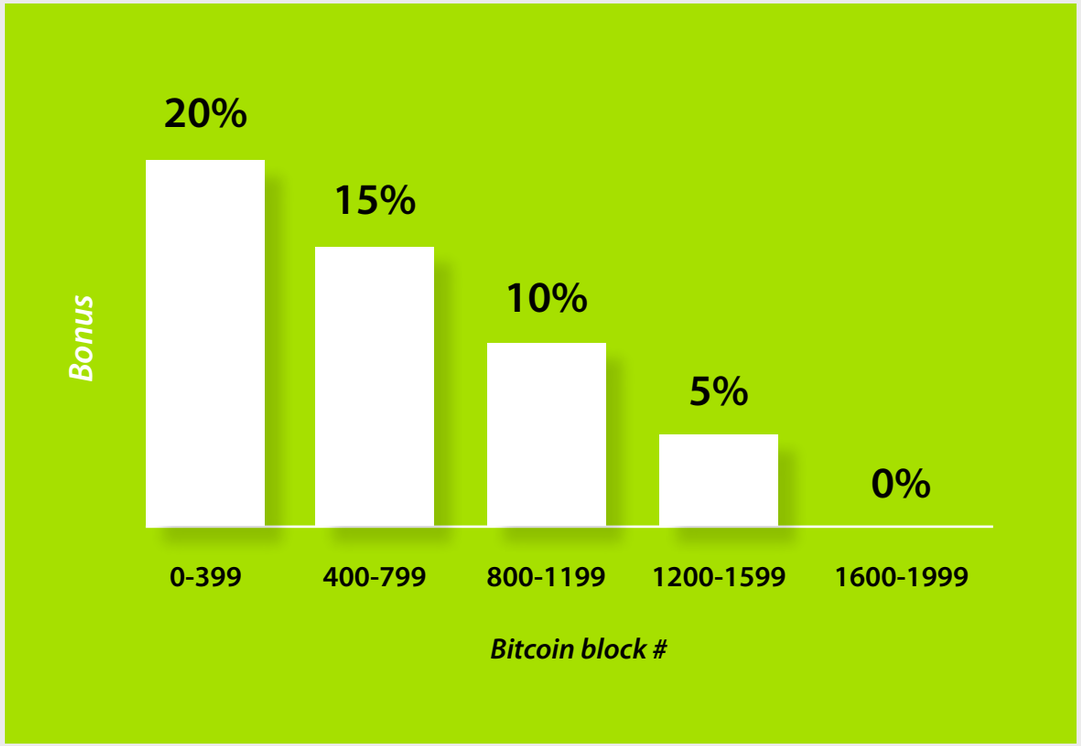
Following the example set by the Ethereum Foundation, there is no cap on the amount of contributions that will be accepted by the Foundation. This is done in order to ensure that participation is not limited only to insiders or the "fast-fingered". The Tezos development team believes that an un-capped fundraiser will promote a widespread distribution of the tokens, a necessary prerequisite to launching a robust network.

Though the amount of Tezzies allocated is denominated in bitcoins, contributions may be made in ethers, that will be implicitely converted at the prevailing rate on a best effort basis. Contributions may also be made through Bitcoin Suisse AG who accepts fiat currencies and other electronic tokens and will participate in the fundraiser on behalf of its customers.

The fundraiser will last for a period of 2,000 Bitcoin blocks. Throughout this period, a contribution of one bitcoin (1 XBT) will lead to an allocation of five-thousand tezzies (5,000 XTZ) plus a time dependent bonus. This bonus is meant to incentivize contributors not to delay their participation. The bonus starts at 20%, meaning that a contribution of 1 XBT will yield an allocation of 5,000 X (1 + 20%) = 6,000 XTZ and decreases progressively to 0% over 5 periods lasting 400 Bitcoin blocks each.

The average time between Bitcoin blocks is approximately 10 minutes, thus the fundraiser is expected to last approximately two weeks, and each period of 400 blocks roughly two days and eighteen hours.

The Foundation will manage the proceeds of the fundraiser and sell contributions progressively throughout the fundraising period in order to reduce the risk inherent in holding cryptographic tokens.



1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS

tezos.com

## 4.2 RECOMMENDED ALLOCATION

**The foundation will recommend allocation based on the following pools:**

### Pool A

**The fundraiser**

Pool A will represent the contributions made during the fundraiser and be allocated at a rate of **5,000 XTZ / XBT** plus a bonus depending on the time at which the contribution is made.

**5,000 XTZ / XBT + up to 20% bonus**

### Pool B

**Early backers**

As mentioned above, DLS accepted a small amount of backing to fund development, representing $893,201 in promises. These backers are thus being allocated a specific number of tokens based on the initial price (bonus included), **not a fixed percentage of the issued tokens.**

**$893,201 worth + 20% bonus**

### Pool C

**Advisors, PR, and development team bonuses**

Bonuses totalling $317,000 will be granted to the development team in addition to their regular compensation. An additional $75,000 will be granted to advisors, and $30,000 worth of tokens to a communications consulting firm.

**$422,000 worth + 20% early bonus**

### Pool D

**10% to the Foundation, vesting over four years**

An amount equivalent to one eighth of the tokens allocated in pools A, B, and C will be allocated to the Foundation. This pool will represent **10% of the total number of tokens issued during the fundraiser**. The foundation's priorities are listed below, in Section 4. **These tokens will vest over a period of 4 years.**

**10% over 4 years**

### Pool E

**10% for acquisition of DLS, vesting over four years**

An amount equivalent to 1/8 of the tokens allocated in pools A, B, and C will be reserved by the Foundation as part of its acquisition of shares of DLS (subject to approval by the Swiss supervisory authority for foundations). **These tokens will vest over a period of 4 years** and also represent 10% of the total amount of tokens issued.

**10% over 4 years**

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



# FOUNDATION PLANNING

→ A detailed layout based on different fundraising scenarios can be found in **THE TABLE**.

The Tezos Foundation will manage the contributions according to its purpose. Initially, the Foundation will budget from four to six years, depending on the amount raised. After this period, the Foundation will phase itself out unless the community votes to keep it in existence through funding via tokens.

The Foundation will have the discretion to pay for services it believes will benefit the promotion of the Tezos protocol, either in tokens or another currency. This section outlines initial team believes the Foundation should value, as well as the estimated costs for servicing each priority based on the proceeds of a fundraiser.

## 5.1 ENGINEERING

The primary task of the Foundation is to ensure the functionality of the network. To this end, the Foundation will, at a minimum, retain the original development team at the current annual cost of $900,000. This will cover maintenance, as well as some integrations and proposals. Over four years, this will cost the Foundation $3.6 million.

DLS partnered with OCamlPro, a company based in Paris with deep expertise in OCaml. Most of the developers working on Tezos have PhDs in formal verification and programming language theory.

## 5.2 RESEARCH

The Tezos protocol currently benefits from research in the formal verification and programming language communities at no cost. The initial development team of Tezos has a strong philosophical commitment to formal verification and a keen interest in researching new consensus algorithms for blockchains. The Foundation will look to fund research in this area with its endowment from the fundraiser.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



## 5.3 LEGAL SERVICES

Currently, Doug Barnes works on behalf of Dynamic Ledger Solutions, the company developing Tezos, through **Barnes Legal**. In addition to his legal qualifications, Doug was also involved in the cypherpunk movement in the early 90s. The Swiss law firm **MME** represents the Tezos Foundation and will continue to do so after the token generation event.

## 5.4 COMMUNICATIONS AND MARKETING

Currently, DLS retains communications consultancy to support its marketing efforts. As stated in the original Tezos whitepaper, DLS believes that the advocacy and marketing of protocols are integral to gaining greater acceptance of them from a wide community.

The Foundation exists to drive an ecosystem around the Tezos protocol. Similar projects have seen extraordinary success from running meetups across the world. The Foundation will target New York, Tokyo, and Paris for events and meetups.

In the spirit of community building, the Foundation will also provide a forum attached to the **www.tezos.com** domain that can facilitate debate on proposals. This isn't meant to be the only forum for discussion and posts will be moderated to weed out abusive actors. Though the Tezos community will converge on a place to discuss proposals, it makes sense for the Foundation to spend a modest amount to create and moderate a potential option.

## 5.5 BUSINESS DEVELOPMENT

Non-engineering Tezos protocol efforts entail managing potential partnerships, marketing, financial transactions, and business operations broadly construed. It will soon be necessary to solicit more business development people to interface with non-technical stakeholders, as well as help manage Tezos vendors and contractors.

“

The Foundation exists to drive an ecosystem around the Tezos protocol. It will target New York, Tokyo, and Paris for events and meetups.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



# LONG-TERM GOALS

Though our philosophy and governance model constrains how prescriptive the Foundation and the initial team can act, we thought it was worth documenting the types of things the Foundation will work to realize within the Tezos community.

## 6.1 COMMUNITY GOALS

Since Tezos has a built-in governance mechanism, its protocol can evolve and incorporate new innovations over time. In other words, stakeholders can make and enforce decisions about changes to the network using the network itself.

All protocol changes should go through the Tezos internal governance mechanism when possible. If a person or party introduces a change via a hard fork, but that change could easily have been instigated inside of Tezos, the network should reject that change and treat it as illegitimate.

However, some decisions will inevitably arise at a level that cannot be fully addressed within the network. The founding team would like to have a certain ethos govern the network. Namely, they believe the central goal of the governance mechanism is to protect the interest of each token holder, irrespective of their stake, in their capacity as a token holder.

Generally speaking, this would mean favoring decisions that tend toward increasing the value of the tokens. Not only does this directly benefit token holders, but it also acts as a proxy for the most desirable properties, such as security, fairness, or usefulness.
The ideal Tezos community would be intellectually rigorous without sacrificing pragmatism and inclusive without tolerating belligerence. There would be a focus on experimentation, testing, and folding in the most useful and innovative technical tools for the community to use. The Foundation does not endorse or look to facilitate any immoral behavior such as fraud or the instigation of violence on other beings or entities.

Tezos should be comprised of a community of serious thinkers, focused on preparing the most effective upgrades to increase the utility of the Tezos token. The network will reward these proposals by issuing them new tokens upon acceptance, creating a robust pecuniary incentive.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS

tezos.com

## 6.2 DEVELOPMENT GOALS

The development goals of Tezos follow five axes: security, scaling, privacy, usability, and features. The development team will pursue all five goals somewhat in parallel but not with the same priority.


### 6.2.1 SECURITY

Tezos is built on a fresh code base. This let the development team control every aspect of the initial design and benefit from the advanced safety features of OCaml, but it also means that the system hasn't been battle-tested yet. Both Bitcoin and Ethereum successfully recovered from critical bugs in their code base, but such crises should be avoided as much as humanly possible. Therefore, the development team's primary focus will be to continuously work to improve the resilience of the network to DDOS attacks or malicious fork. Every other effort on the ledger is for naught if the core team fails to properly secure the network. Concretely, they will:

- ***Keep increasing the test coverage of the code base***
- ***Develop formal proofs of correctness for the most sensitive parts of the code***
- ***Submit security upgrades to the protocol as needed***
- ***Improve the randomness generation protocol with public verifiable secret sharing***
- ***Release security upgrades to the block creation software***
- ***Produce recommendations for operational security of block validators***

### 6.2.2 SCALING

The Tezos proof-of-stake algorithm affords us better scalability and transaction throughput that can be achieved with Bitcoin style proof-of-work. However, the initial parameters are set very conservatively in order to let us assess its performance in the real world and allow the ecosystem of validators to grow. Once the ledger accumulates real world experience, the development team will work towards cranking up the transaction throughput by:

- ***Increasing the block size***
- ***Lowering the block time interval***
- ***Packing transactions more efficiently***

Note that the consequences of increasing the blocks' size in proof-of-stake are very different from the consequences of increasing the block size in a Nakamoto proof-of-work systems. In Nakamoto proof-of-work any increase in block size gives a slight advantage to centralized miners. This is because proof-of-work requires the block propagation and validation time to be very small compared to the block interval. In synchronous proof-of-stake protocols like Tezos', it only needs to be smaller than the block interval.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



### 6.2.3 PRIVACY

Privacy preserving transactions and smart contracts are a key feature of modern blockchains. Not only are they a security requirement, they ensure censorship resistance much more effectively than any tweaking of the consensus algorithm.

However no solution is perfect yet. Ring signatures, as used in Monero, can still leak some information about senders. Zcash makes an impressive use of zero-knowledge proofs to provide full, information theoretic, anonymity, but the risk – however remote – of undetected hyperinflation in the event of a bug in the proof circuit makes some users uncomfortable.

Our initial plan is to strike a compromise and integrate Zcash's proof circuit in the protocol, but restrict its operations to a special token issued on the Tezos blockchain. This token will be convertible 1 to 1 with Tezos tokens, but the chain will keep track of how many tokens have been converted so that undetected inflation in the privacy preserving token cannot spill over onto the main token. Users who trust the security of the privacy preserving token will have full use of its functionality while those who don't will remain protected as long as they do not make use of the privacy feature. This mechanism replicates the economic behavior of a side chain, but on a single ledger.

In the long run, the team intends to replace all operations on the blockchain with zero-knowledge proofs. Instead of downloading an entire blockchain a client will be able to download a single proof attesting that the entire blockchain has been validated starting from the genesis hash. However, to that end, they will likely make use of STARKs, zero knowledge proofs similar to SNARKs but which do not require a trusted setup.

### 6.2.4 USABILITY

Initially, the Foundation team's primary task will be to build robust, scalable, and secure infrastructure. However, the development team also needs to make it an attractive platform. In particular, they will:

- ***Develop light client libraries in most popular programming languages to help developers integrate with the Tezos network.***
- ***Develop an IDE to facilitate development and formal verification in Michelson.***
- ***Develop a certified compiler for a high-level language that will compile down to Michelson.***

“

Initially, the Foundation team's primary task will be to build robust, scalable, and secure infrastructure.

1 HISTORY
2 PRINCIPLES
3 PEOPLE
4 FUNDRAISER
5 PLANNING
6 GOALS



### 6.2.5 FEATURES

"Features" are decentralized applications supported at the protocol level. In Ethereum, the prevailing trend is to deploy these "DApps" through App Coins, a way for developers to build specially marked tokens to power applications on an existing network which can be converted in-and-out of the main network token.

While Tezos permits the creation of App Coins, we do not focus on them. If an application is particularly valuable to the network, we believe it should be folded into the protocol. Though we do not know exactly yet which features will be voted into the protocol level by the network, some applications seem to have widespread appeal in similar projects: prediction markets, DNS systems, on-chain node identity, debt networks (à la Stellar), decentralized exchanges, file storage, and cloud computing. More exotic or specialized applications, such as the Numéraire project, are probably better fits for App Coins as they have less explicitly general appeal.

Unproven systems ought to innovate at the leaves, while tried-and-true features ought to have a way to make the network more valuable by integrating at the protocol level. This is not purely for the sake of creating more valuable networks but also for ensuring consistency of execution.

## 6.3 RESEARCH GOALS

The initial development team's research goals represent longer term developments or ideas to push out of the lab and deploy.

### 6.3.1 ZERO-KNOWLEDGE PROOFS OF KNOWLEDGE

Right now, the Tezos development team is fascinated with a new development in zero-knowledge proofs: STARKs. Unlike SNARKs, STARKs do not require a trusted setup. They also rely on simpler mathematics and are more efficient to compute. However, the proof time of STARKs is still cumbersome.

### 6.3.2 PROOF-OF-STAKE

The team is interested in researching different proof-of-stake consensus algorithms offering stronger guarantees and scalability. This is a burgeoning field and interesting proposals such as Ouroboros, Algorand, Honey Badger and Snow White have been appearing at higher frequency.

### 6.3.3 INCENTIVE COMPATIBLE GOVERNANCE

Moving beyond technology, the Foundation will also try to sponsor research focusing on decentralized governance and incentive structures.

tezos.com

## IF THE FOUNDATION IS ENDOWED WITH...

Note: all amounts in $1,000

| | CURRENT | $6,000+ | $12,000+ | $20,000+ | MOONSHOT | MARS-SHOT |
|---|---|---|---|---|---|---|
| **Engineering** | Continue development with our current team. | Push work on v2 by the foundation. Attempt a secondary issuance in conjunction with the release of the new version. | Directly hire additional talent from ETH Zurich for full-time code maintenance in Switzerland. | Grow the team with other experienced, academically oriented engineers. | Hire talented teams of engineers and designers to build direct consumer applications through strategic acquisition of tech companies. | Deploy and silo several teams of engineers to build different candidates for upgrades. Evaluate empirically the best proposals and merge them. |
| **Headcount** | 6 | 6 | 10 | 15 | | |
| **Yearly rate** | $900 | $900 | $1,500 | $2,250 | | |
| **Research** | Continue our use of PhD candidates to work on formal verification. | Keep our current approach, strategically engage the formal verification community. | Contract a team of academics to research and help build v2 consensus algorithm, followed by research on zk-STARKs. | In addition, join the IC3 team as a sponsor. | Offer competitive salaries to attract experts on formal verification to work exclusively on the protocol. Set up an institution a la IC3 in Europe. | Sponsor a leading computer science department with endowed professorships and extensive grants to graduate students in the field of formal verification. |
| **Yearly rate** | $0 | $0 | $300 | $700 | | |
| **Communications & Marketing** | Continue working with our communications consultancy. | Continue working with our communications consultancy. | Host an annual developer conference in Europe and retain current communications consultancy. | Conduct three annual developer conferences (EU, US, Asia), retain current communications consultancy, run ad campaigns. | Sponsor an online magazine to cover major debates. Pay to publish a hash of the Tezos blockchain in a reputable outlet like the Financial Times or The New York times (à la Guardtime). | Acquire mainstream print and TV media outlets to promote and defend the use of cryptographic ledger in society. |
| **Yearly rate** | $120 | $120 | $370 | $1,000 | | |
| **Legal Services** | After the fundraiser, the Foundation will pay for its own legal expenses through MME. | Retain our counsel and start exploring, as a failsafe, alternative legal structures or advocacy for the Foundation beyond the Swiss Cryptovalley. | Retain our counsel and start exploring, as a failsafe, alternative legal structures or advocacy for the Foundation beyond the Swiss Cryptovalley. | Retain our counsel and start exploring, as a failsafe, alternative legal structures or advocacy for the Foundation beyond the Swiss Cryptovalley. | Lobby municipalities and local governments to use formally verified smart contracts as a form of binding legal contract. | Fund efforts to digitize and map transaction logic from traditional legal prose to a Tezos language. |
| **Yearly rate** | $100 | $250 | $250 | $250 | | |
| **Business Development** | Kathleen Breitman manages all non-technical efforts. | Hire one strong former management consultant to assist in interfacing with vendors and service providers. | Hire two seasoned former management consultants and a community manager to engage with token holders. | Hire a blend of junior & senior business development talent, as well as a business development person in China and a community manager. | Purchase a banking license and deploy the Tezos blockchain as a backbone for business operations. Experiment with automation using a blockchain for basic processes. | Negotiate with a small nation-state the recognition of Tezos as one of their official state currencies, which would immediately give Tezos favorable treatment in terms of financial regulation. Attempt negotiations to purchase or lease sovereign land. |
| **Yearly rate** | $0 | $250 | $450 | $750 | | |
| **Education** | | Produce a series of online Michelson tutorials with videos and exercises. | Produce in addition an OCaml MOOC geared towards increasing our potential developer base. | Also run a quaterly Tezos school focusing on protocol development in OCaml and smart contracts. | Offer student grants for conducting projects related to the Tezos ecosystem and subsidize OCaml education in universities. | Run a development school with emphasis on functional programming and safe smart contract construction. |
| **Yearly rate** | $0 | $50 | $125 | $350 | | |
| **Annual Rate** | **$1,120** | **$1,570** | **$2,995** | **$5,600** | **$10,000 - 15,000** | **$20,000 and above** |

# Contact

**contact**@tezos.com