



**envited**  
E C O S Y S T E M

# TEZOS DEEP DIVE DECK 2.0

(UPDATED NOVEMBER 2021)

# Tezos – the Blockchain Solution to Your Real-World Problem!

created by [Niko Hildebrand](#) on behalf of [asc\(s e.V.\)](#)

This work is subject to  
the [Attribution 4.0](#)  
[International Creative](#)  
[Commons License](#)



# Content

## The Tezos Deep Dive Deck:



1. [The value proposition](#)
2. [What is blockchain and why do you need it?](#)
3. [Why are public blockchains the future?](#)
4. [Tezos: Interesting aspects of the technology](#)
5. [Tezos: Amendment history](#)
6. [Tezos: Ecosystem overview](#)
7. [Tezos: Application examples](#)
8. [Blockchain MythBusters](#)
9. [References](#)

# OUR PROMISE

## What you will learn from this slide deck...



You will...



...gain an understanding of what **blockchain** is, how the technology works and what it is good for!



...learn about the difference between **private** and **public blockchains** and why we think that public chains are the future!



...fall in love with **Tezos** for its superior and upgradeable technology and its great and open community!



...gather knowledge about important blockchain-related concepts such as **SSIs** and **NFTs** and their place with Tezos.



...see a **blueprint** of how to build **industrial applications** on top of Tezos, streamline consortia and interact with the community.



...enjoy a series of **mythbusters** about common misconceptions in the blockchain and crypto space!

# YOU

## Let us tell you something about yourself...



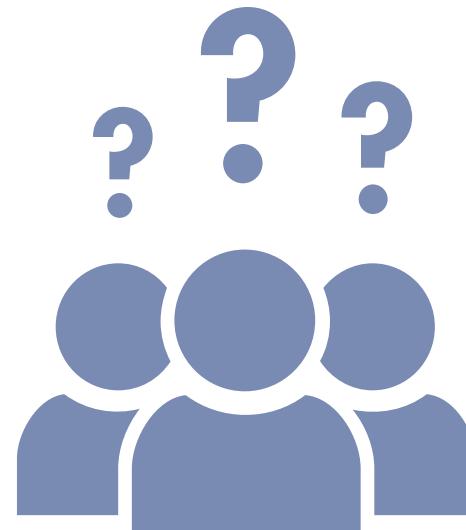
You are  
**technologically affine**

You are well-respected and  
**your opinion counts**  
in your organization

You probably have at least  
**a basic understanding** of what a blockchain is...

Your superiors **manage** things,  
but they never really get to the bottom of them...

Maybe you work  
in the "**old economy**"...



Your superiors may have heard  
of blockchain during the **hype**...

## ...and what your problem might be...

Your organization operates in an **environment**, that is characterized by...

...a **diverse ecosystem**...

...**diverging incentives**...

...a need for **coopetition**...

...a long and fragmented  
**multi-tier supply chain**...

...strict **regulatory requirements**...



You face **business challenges**,  
that are characterized by...

...**(self-) certification** requirements...

...a lack of **trust**...

...expensive **intermediaries**...

...**auditability**...

...an obligation to provide **proof** of something  
– e.g. conducted validation...

...lacking market **transparency**...

...a need for **privacy**...

...the need for tamper-proof **immutable documentation**...

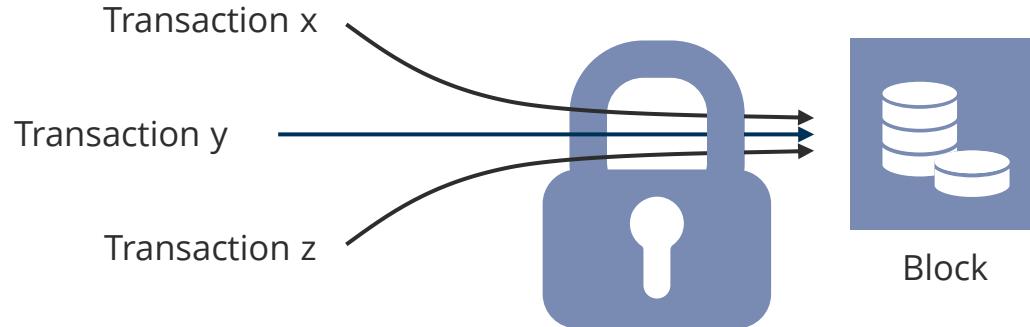
# YOUR PROBLEM



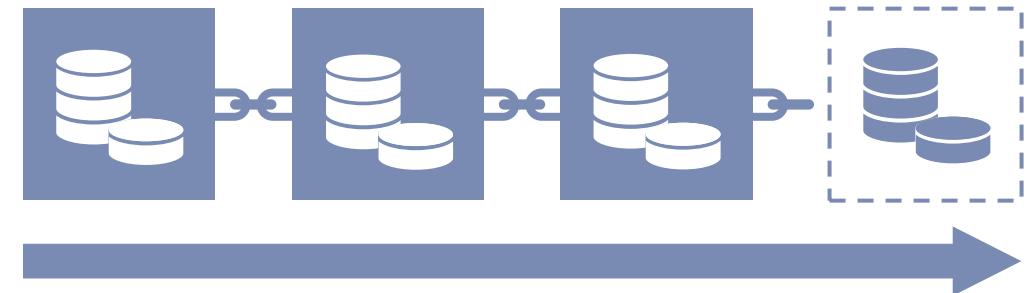
# WHY BLOCKCHAIN?

## Just a quick reminder - what exactly is a blockchain?

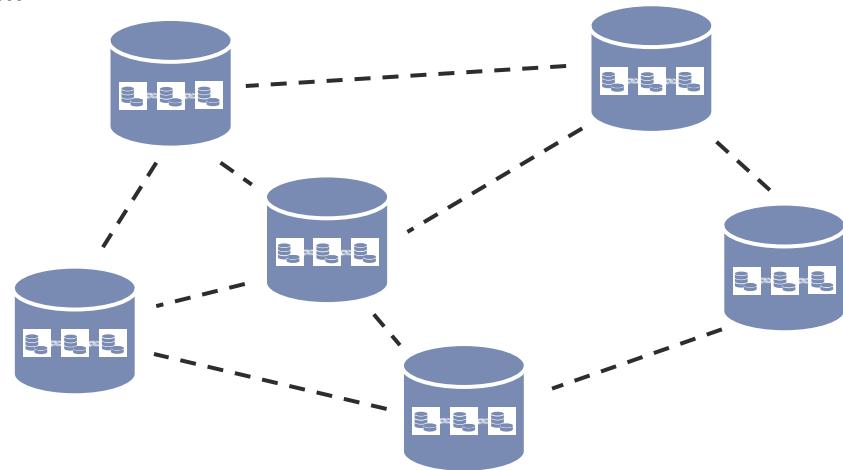
A blockchain is a data structure that groups data (e.g. transactions) into immutable containers called blocks...



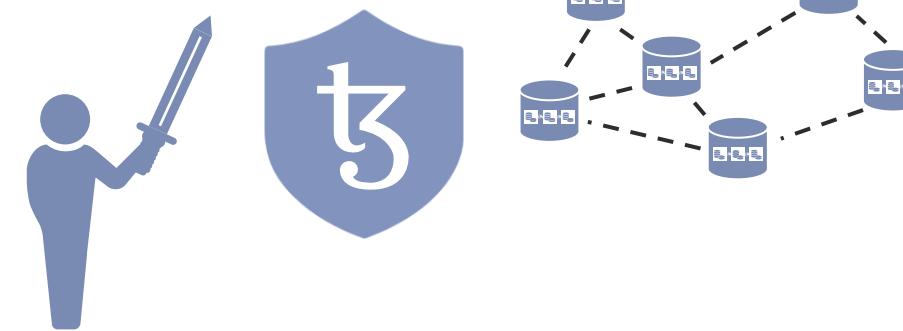
...chains them together in an order-preserving way that only allows appending (but not deleting or editing)...



...is replicated limitless times in a distributed (peer-to-peer) network...



...and maintained by a protocol that aligns participants' incentives in a way that provides protection against fraud and malicious attacks!



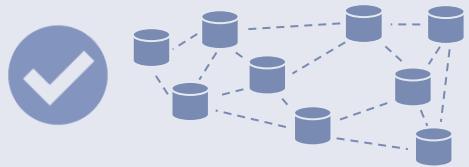
# Why blockchain could be a building block for your problem's solution...



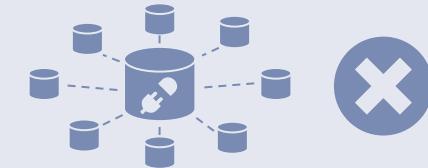
Blockchains are **shared** and **immutable** data stores that provide **trust** in **trustless environments**!



They allow to **save costs** and **increase process efficiency** through **disintermediation**.



They are operated by **distributed peer-to-peer networks** which makes them very **reliable** as there is **no single point of failure**.



They can be used to provide **transparent documentation** with **selective privacy** enabling **traceability** and **auditability**.

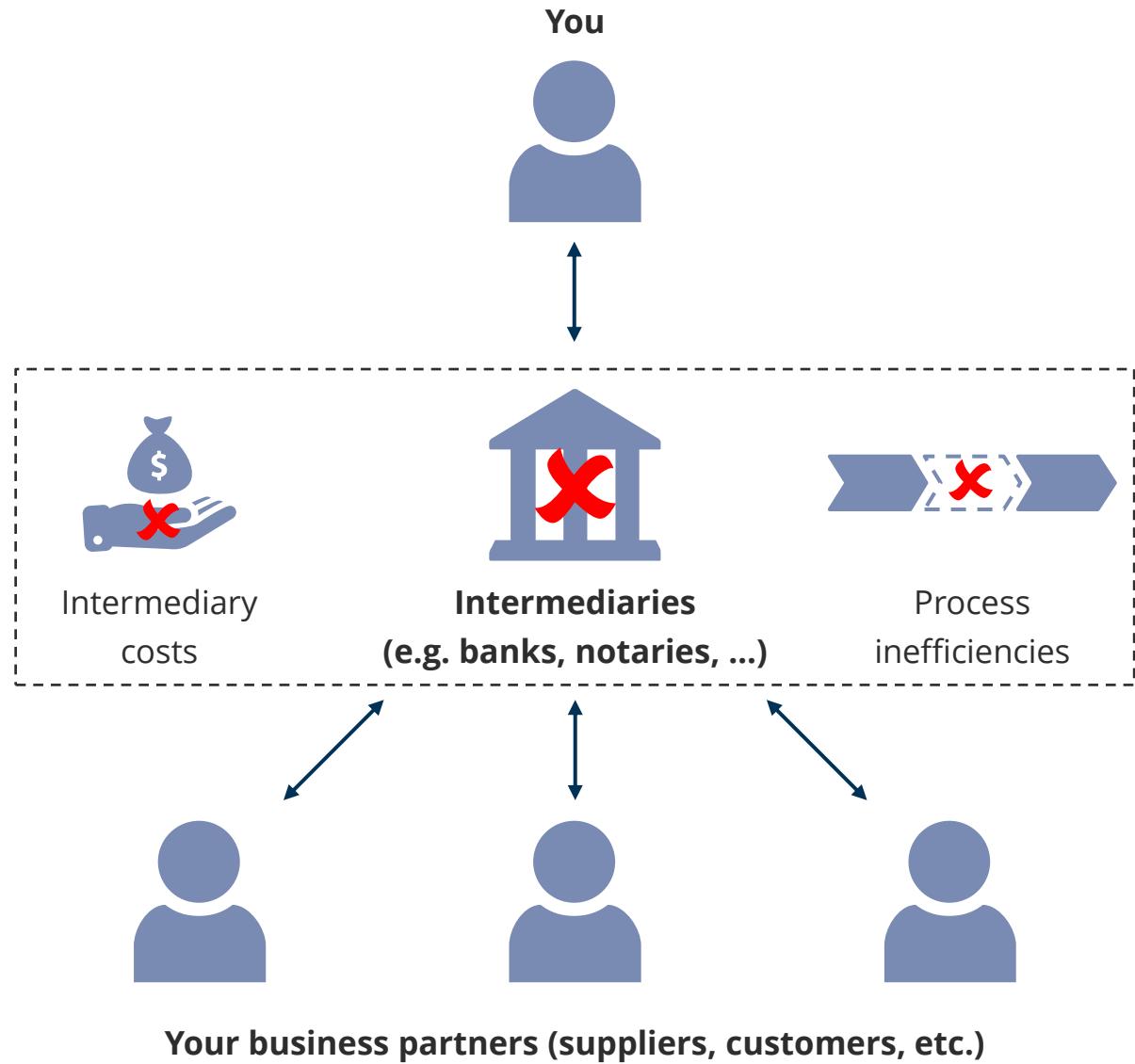


Their combination of immutability and **accessibility** enables **revocable certificates**.



# Why blockchain could be a building block for your problem's solution: Disintermediation

- **Transactions** require two or more parties to fulfill their part of the deal.
- In **physical transactions**, little **trust** is needed since goods and/or money are exchanged (almost) **simultaneously**.
- In contrast, **nonphysical transactions** are theoretically prone to **fraud** as the exchange of goods and/or money happens **sequentially**.
- The traditional solution to this problem is the use of a **trusted third party** – a so called **intermediary** – who operates between the transacting parties:
  - ▶ If the other party doesn't fulfill their part of the deal, the intermediary does not release your contribution to the transaction to that party.
  - ▶ All transacting parties can trust the intermediary because he has a strong economic incentive to act honestly as his entire business model depends on his **reputation**.
- Intermediaries cause additional **process costs** (as they need to be paid for their services) as well as **process inefficiencies** in form of additional process steps and times.
- Blockchain technology allows transacting parties to **directly interact** with each other by **shifting the required trust** from the intermediary to the technology – or rather the network maintaining the blockchain – and thus saves costs and allows to realize process potentials. The removal of intermediaries is called **disintermediation**.

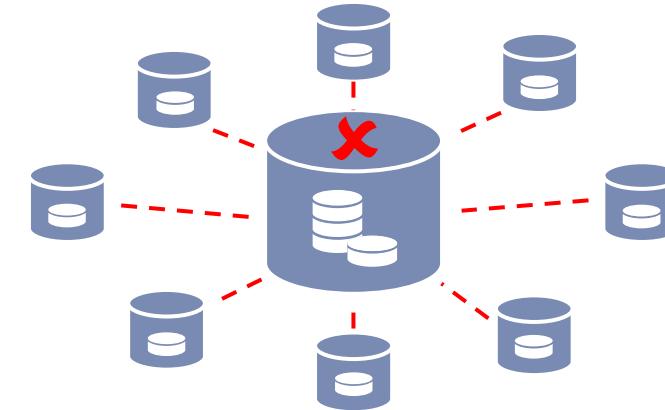


# Why blockchain could be a building block for your problem's solution: No single point of failure

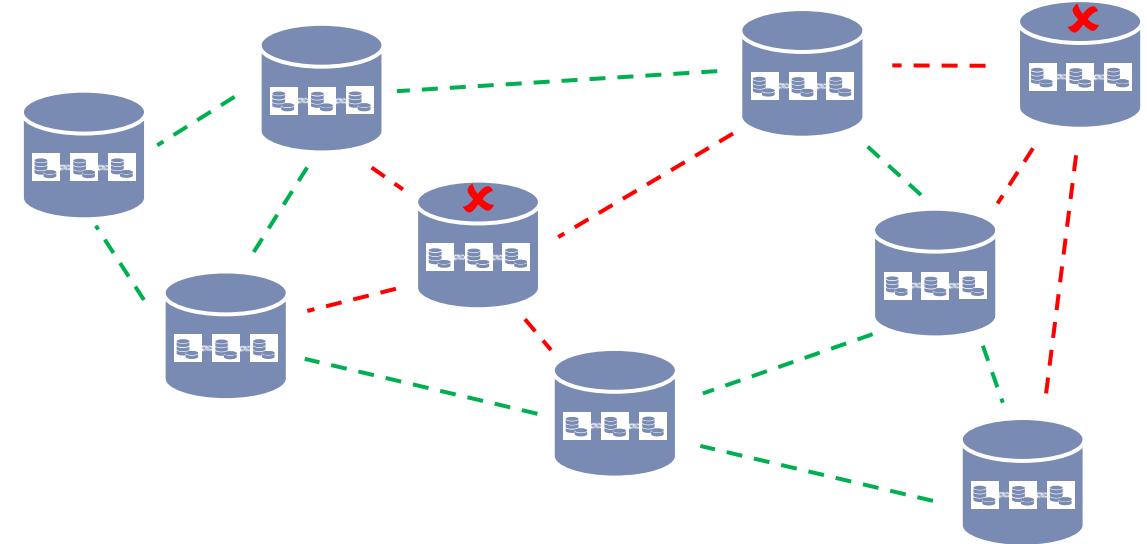


- In **centralized networks**, participants are not directly linked to one another but connect via a central network resource that serves as a **data hub**.
- You may know this pattern from **logistics**, where such set-ups are called **hub-and-spoke networks** and the hub serves as a turnover point where goods from various origins are **consolidated** before jointly transported to their destinations.
- While comparatively efficient in various ways, centralized networks have a fatal **weakness**: if the hub fails, the whole network breaks down, which is why there is a **single point of failure**.
- In contrast, **distributed networks** are characterized by direct point-to-point (or **peer-to-peer**) connections between network participants.
- There is no direct connection from every participant to every other participant, but since every participant maintains **multiple connections**, data interchanged between two arbitrary points can be relayed via a multitude of routes.
- Distributed networks are thus much **more resilient** against system breakdowns and data loss as they can even compensate the simultaneous failure of multiple nodes.
- As blockchains are maintained by a distributed (peer-to-peer) network where every peer holds a **complete copy of the blockchain's current state**, the system has no single point of failure.

## Centralized networks with a single point of failure:



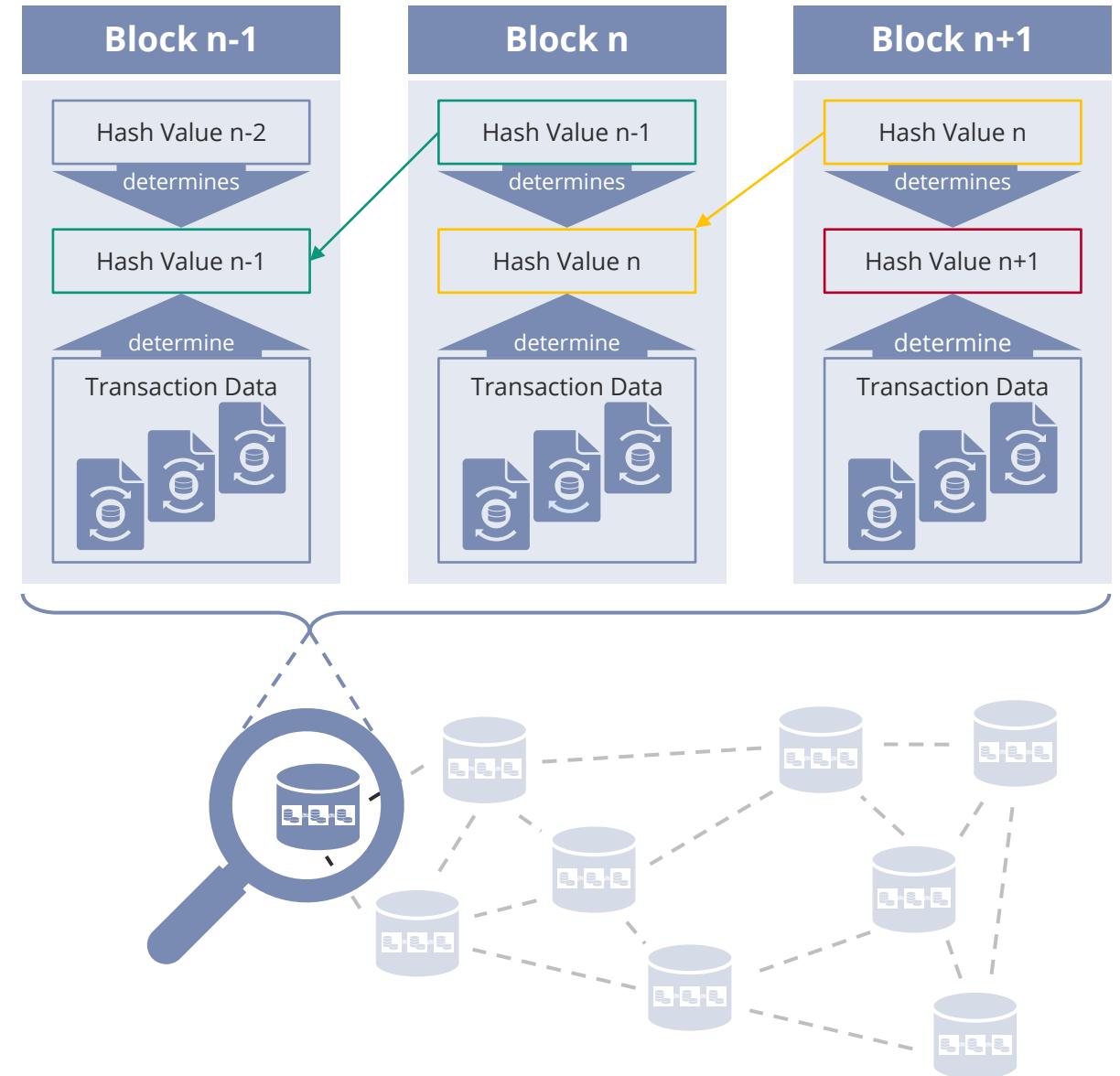
## Distributed networks with no single point of failure:



# Why blockchain could be a building block for your problem's solution: Immutability/Traceability

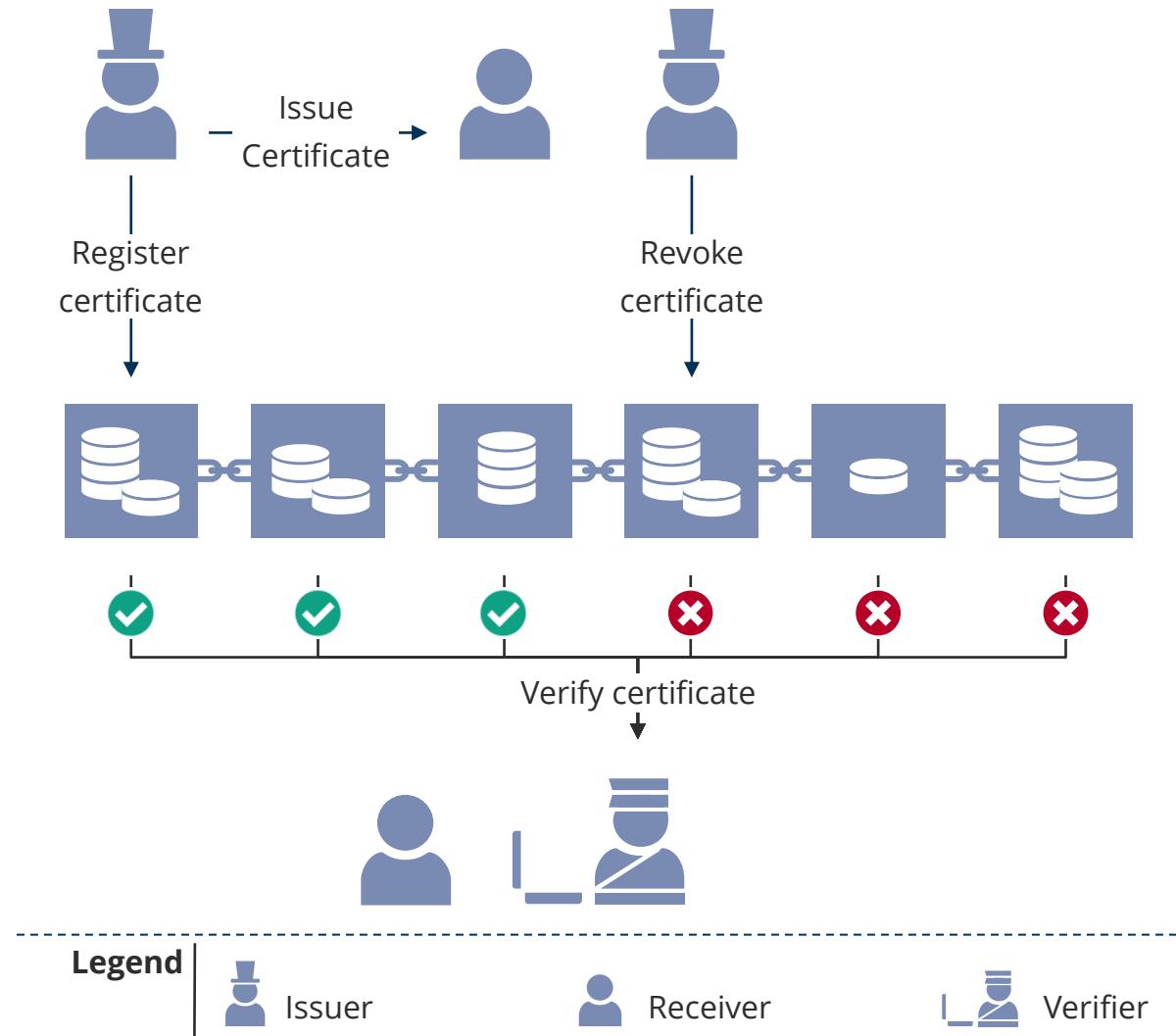


- As the name indicates, a blockchain is a **data structure** that essentially **groups data into blocks** (e.g. transaction data) which are **chained together** in a way that preserves **chronological order** and **prevents editing** (i.e. manipulating) any data that has entered the blockchain:
  - Blocks are **timestamped** and new blocks of data are always **appended** at the end ("head") of the chain.
  - A **hash function** creates a concise representation of the block's data called **hash value** often described as the **fingerprint** of the data as it identifies the data and changes drastically if the input is modified in the slightest way.
  - The **hash value of the previous block** is always included in the calculation of the current block's hash value, thereby **linking** the blocks. If data in a previous block were manipulated, this would change its hash representation and thus **breaking the chain**.
- Replicating** this special kind of database across the nodes of a **Peer-2-Peer-Network** (P2P-Network) and finding **consensus** on its "right" state in an attack resistant way makes the blockchain a practically **immutable ledger**.
- Blockchain solutions are therefore destined for applications that require immutability for **traceability/auditability** reasons.
- These are typically found in environments in which **high values are exchanged** i.a. with **strict regulatory requirements** and **complex multi-agent ecosystems**.



# Why blockchain could be a building block for your problem's solution: Revocable certificates

- As an immutable, independent and public ledger, a blockchain enables **revocable certificates and credentials**.
- For certificates to have a value, they must be **trustworthy**.
- In particular, it must be (almost) **impossible to forge or edit** the certificate **even for its issuer**.
- If a credential changes, the existing certificate has to be **revoked** (i.e. declared invalid) and – if applicable – a new certificate has to be issued.
- The blockchain's immutability makes certificates **forgery resistant** and – in case of public blockchains – its accessibility enables it to serve as a **revocation registry**.
- To avoid making **sensitive information** publicly available, the certificate issuer can hand out the certificate to its recipient and just **register a hash-representation** (a representation, that is unambiguously linked to the original data but is neither human readable nor allows a reproduction of the original data) on the blockchain.
- The recipient can present his human readable version of the certificate to any verifier, who can produce the hash-representation and match it with the one found on the blockchain to **verify its authenticity and validity**.
- To revoke a certificate, the issuer **references** the hash and adds the information that it's invalid – any future verification then fails.

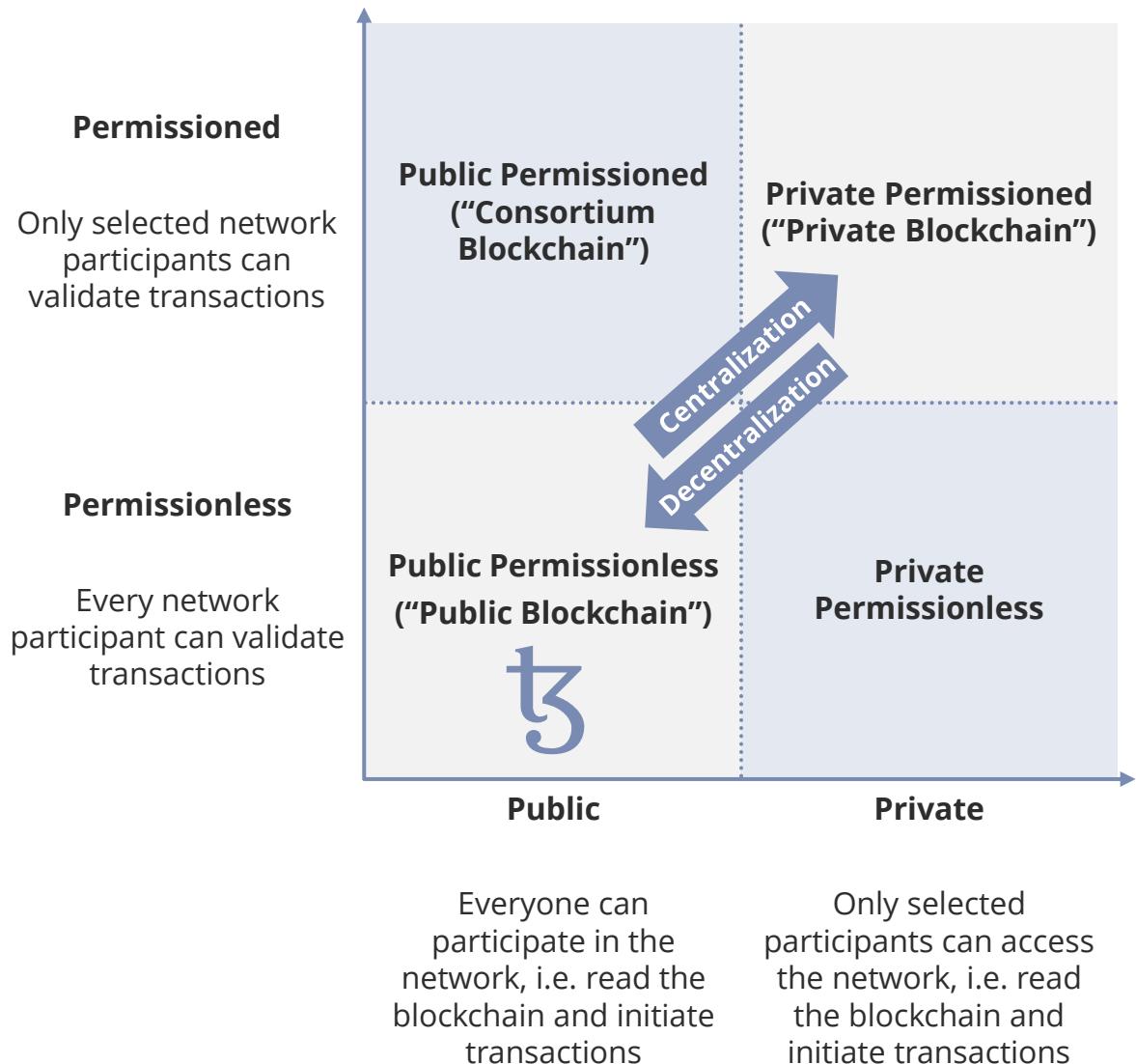




# WHY PUBLIC BLOCKCHAIN?

# Just a quick reminder - what exactly is a PUBLIC blockchain?

- Although every blockchain protocol may have its unique features, there are four **archetypes** that allow a **basic classification** along two binary dimensions:
- The **public vs. private dimension** determines, whether the network is in general open for everyone (→ public) and thus who can **read the blockchain** and **initiate transactions** or whether its access is restricted (→ private).
- The **permissioned vs. permissionless dimension** determines, if every network participant (as allowed by the public vs. private dimension) can take part in the **validation of transactions** (→ permissionless) or if transaction validation is restricted to a selected subset (→ permissioned).
- Public permissionless types are also called "**public blockchains**", private permissioned set-ups are called "**private blockchains**" and public permissioned combinations are known as "**consortium blockchains**".
- While all types may have their **use cases** (e.g. private permissionless for voting), private and permissioned blockchains are more centralized (in the sense that they are less decentralized) and thus provide a lower level of security against various attack vectors while being "less immutable".
- Tezos** is a public and permissionless blockchain that is open to everyone and only requires bakers (i.e. validators) to hold a minimum **stake** (i.e. number of tokens).

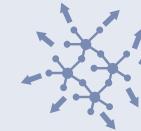


# Why public blockchains are the future...

PRIVATE



PUBLIC



**The benefits of closed networks are limited** – today's internet applications wouldn't be possible if we only had intranets!



The **fixed costs of maintaining your own network** are higher than **(variably) paying for using an existing one**, overall costs for numerous small networks are higher than for one large network!



Public blockchains **tap into the wisdom of the crowds** and their **intrinsic motivation**, while private blockchains are solely developed by paid and thus extrinsic motivated people.



Public blockchains provide much **higher immutability/security against manipulation** through stronger decentralization!

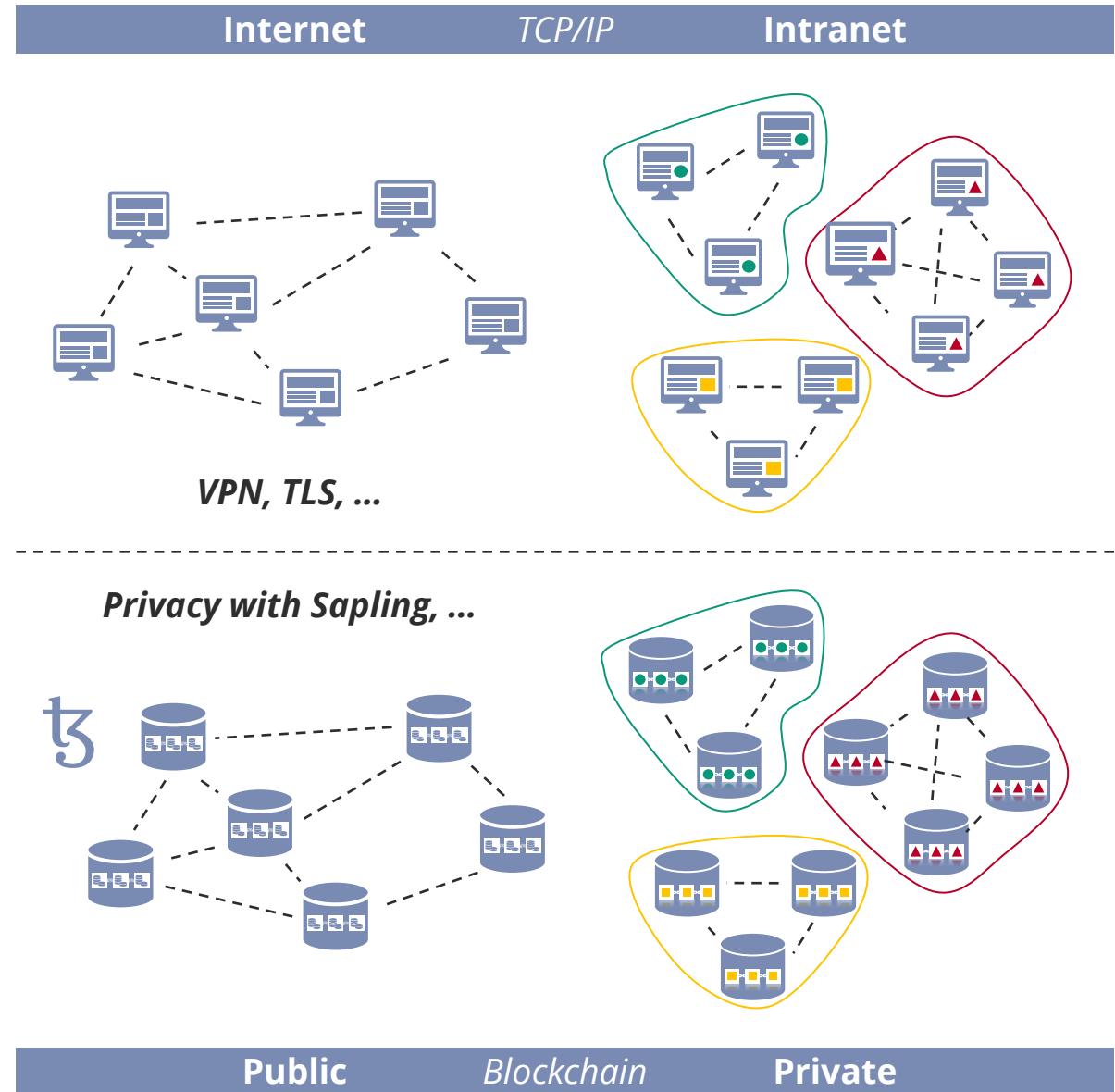


Alleged USPs of private blockchains (like privacy, scalability) erode with current and further technological developments (e.g. implemented: privacy with Sapling, under way: Tenderbake, layer 2 optimistic rollups)



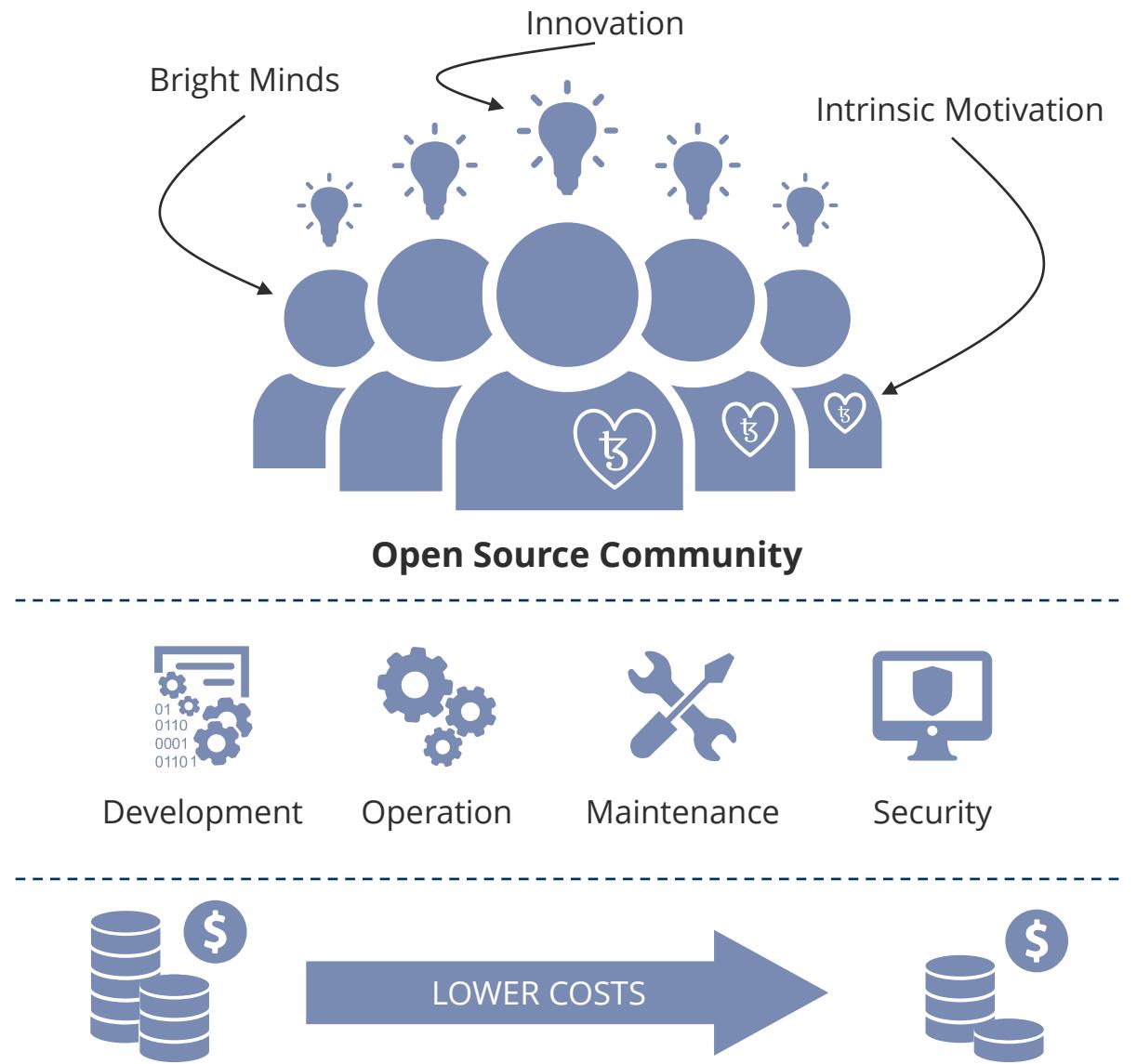
# Why public blockchains are the future: The internet analogy

- In economic theory, there is a big chapter about **network effects**. It covers everything from **decreasing marginal costs** through **economies of scale** to **increased individual utility** with growing network size.
- Imagine a telephone network that consists of only two endpoints. Its users' **benefits would be very limited** as they could only call the other endpoint but no one else (for selected use cases – say the “red telephones” between the Pentagon and the Kremlin during the Cuba Crisis – there could still be significant utility).
- Now imagine a protocol such as TCP/IP that – in contrast to telephones, which are limited to synchronous verbal communication – allows a **multitude of applications** such as websites, e-mail, tube video sites, IP telephony, etc.) and the effect multiplies.
- You can employ the protocol in a private environment which gets you an **intranet**, or in a public network which we call the **internet**. From which use can you extract the most value?
- While private enclaves are still necessary e.g. for company internal applications, they now tend to be built as parts of the internet that are shielded from the public through **additional privacy and security mechanisms** such as **VPNs, TLS**, etc. with only critical infrastructure remaining truly self-sufficient networks.
- With blockchains, it is exact the same: a private blockchain may be adequate for a very specific use case, but **public blockchains will generate much more value in the long run**.



# Why public blockchains are the future: The power of open source technology

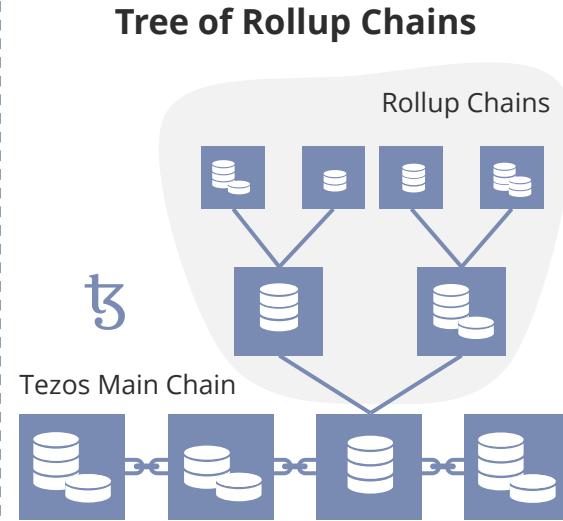
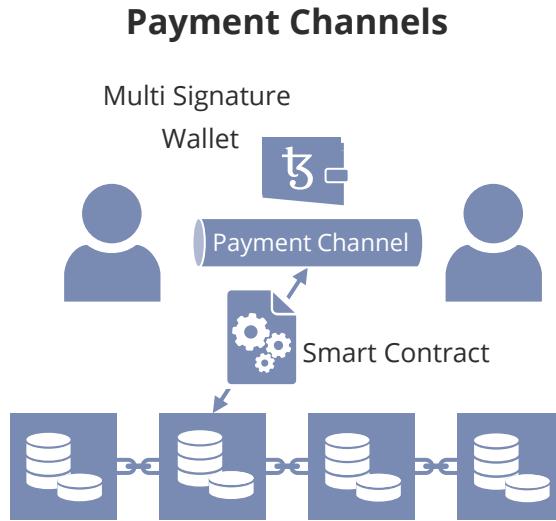
- In addition to “classical network effects” such as increasing marginal utility and decreasing marginal costs with a growing network, public blockchains unleash **the power of open source technology**.
- They are developed and maintained by **vibrant open source communities** that consist of some of the brightest individuals in their fields.
- Using a public blockchain thus allows you to:
  - ▶ Capture the enormous potential and **innovation capabilities** of **intrinsically motivated** communities.
  - ▶ **Distribute** the burden of **development and maintenance costs** on multiple shoulders.
  - ▶ Profit from **greater software security** because the openly available codebase is not only reviewed by the community itself but also vetted by third parties (like yourself) who wish to build their applications on top of it.
  - ▶ **Concentrate** on your use case, the development of the corresponding **application** and its integration with the blockchain via **interfaces**.
- An important economical aspect, that is not applicable for open source technology in general, but also comes with public blockchains, is that the **costs for operating the blockchain** are carried by the network: **you pay for its use instead of its operation!**



# Why public blockchains are the future: Developments in scaling and privacy technologies

## SCALING TECHNOLOGIES

- **Scalability** is one of the major points of concern of public blockchains.
- However, several so-called **layer 2** solutions (because they add a layer on top of the root blockchain) are currently being developed and tested, in order to solve scalability problems.
- One such concept are **payment channels** (as devised for the **Bitcoin Lightning Network**) between two transacting parties. For example, implemented as zkChannels by Bold Labs on Tezos.
- **Optimistic rollups by Marigold** are a Layer 2 solution validating transactions on behalf of the main chain. They are “optimistic” based on the assumption that validation is correct until proven otherwise.



## PRIVACY TECHNOLOGIES

- Developments in privacy technologies diminish **concerns about confidentiality** on public blockchains.
- **Zero-knowledge proofs** allow to prove a fact without revealing the fact itself, e.g. that a valid transaction has occurred without revealing the transaction (and its details) itself.
- Current protocols are **zkSNARKs** (zero-knowledge succinct non-interactive arguments of knowledge) which require a confidential initial set-up and are used in Zcash's **Sapling** which has been integrated with the [Edo proposal](#).



*The Proof...*

- ...is **complete**: every true claim will convince an honest verifier
- ...is **sound**: a false claim will not convince an honest verifier
- ...reveals **zero knowledge**: the proof does not leak the secret

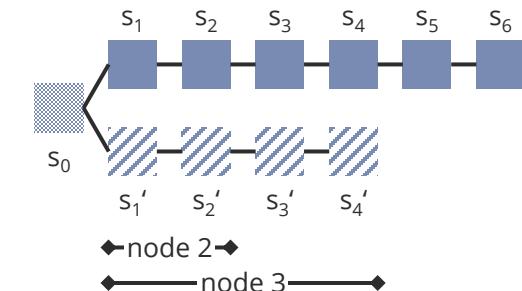
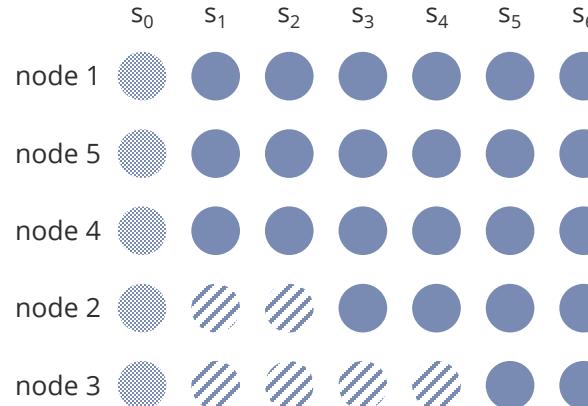
# An excursion to algorithm theory: Why public blockchains require a coin/token

- In order to agree upon “one truth” in the distributed network, a **consensus protocol** is required.
- A consensus algorithm needs to possess the following **properties**:
  - Termination (finality)**: the algorithm terminates
  - Agreement**: all nodes agree on the same value
  - Validity**: the agreed upon value makes sense
- In **fault-tolerant distributed networks**, these properties cannot be achieved simultaneously (FLP impossibility).
- By **abandoning the termination requirement** (finality becomes probabilistic), consensus protocols for blockchains become **semi-algorithms**, resulting in the possibility of multiple “current state” versions of the blockchain across the network that evolve over time.
- In a **Sybil attack** an attacker exploits this by creating fake nodes that convince the network of a wrong version of the “current state”.
- To prevent this, **Sybil control mechanisms** such as **Proof-of-Work (PoW)**, **Proof-of-Stake (PoS)**, ... (PoX) utilize economic incentives to prevent malicious behavior. This is achieved by the use of a coin (crypto currency) by:
  - rewarding honest behavior** (rewards are generated through coin inflation)
  - making non-compliant behavior expensive** (work/coin collateral).

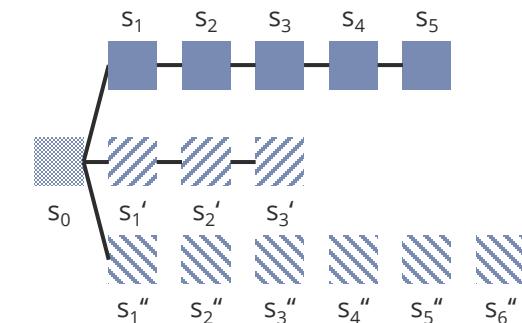
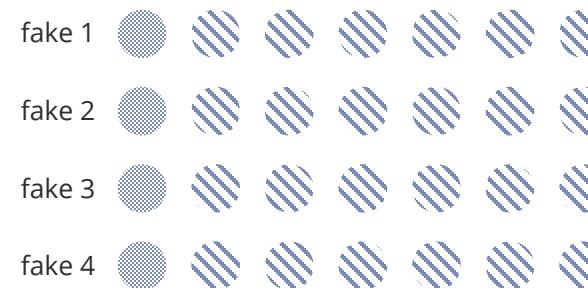
## GOOD TO KNOW

If consensus algorithm Tenderbake is activated, probabilistic finality becomes deterministic finality.

Due to **non-termination**, blockchain states evolve across the network:

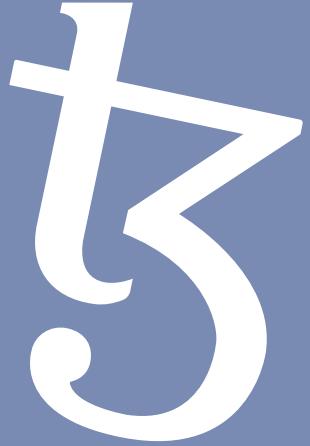


In a **Sybil attack**, fake nodes manipulate the „truth“:



**Sybil control mechanisms** (PoX) prevent this through **economic incentivisation** with a coin:





# WHY TEZOS?

# What is Tezos? - A definition by Arthur Breitman, co-founder of Tezos



"Tezos is a **technology**...

...implemented in a **software project**

...which allows participation in a **peer-to-peer network**

...that produces a **blockchain**

...which maintains a **decentralized ledger**

...instantiating a **cryptocurrency.**"

*Arthur Breitman*



# Why Tezos is the right choice when building your blockchain solution...



Tezos is a **public and permissionless blockchain** and public blockchains are **the future!**



Tezos is **upgradable** through a **proven on-chain governance mechanism** and thus **built to last!**



Tezos employs **Liquid Proof-of-Stake** which is more **scalable** than Proof-of-Work and **does not consume much energy!**



Tezos is **secure** and uses the purpose-built functional language **Michelson** which allows **formal verification of smart contracts!**



Tezos is driven by a **vibrant and active community** with a lot of **academic backing!**



Powerful features like **zkSNARKs for privacy** and a **Layer 2 solution for further scalability**

have been developed and/or are under way!



## Some KPIs: Tezos in numbers...

June 2018

active  
since



> 1,800,000

created  
blocks

~ 400

active  
validators

> 1,900,000

funded  
accounts

~ 5.0%

average  
inflation

> \$ 4.5 B

market  
capitalization

8

successful  
amendments

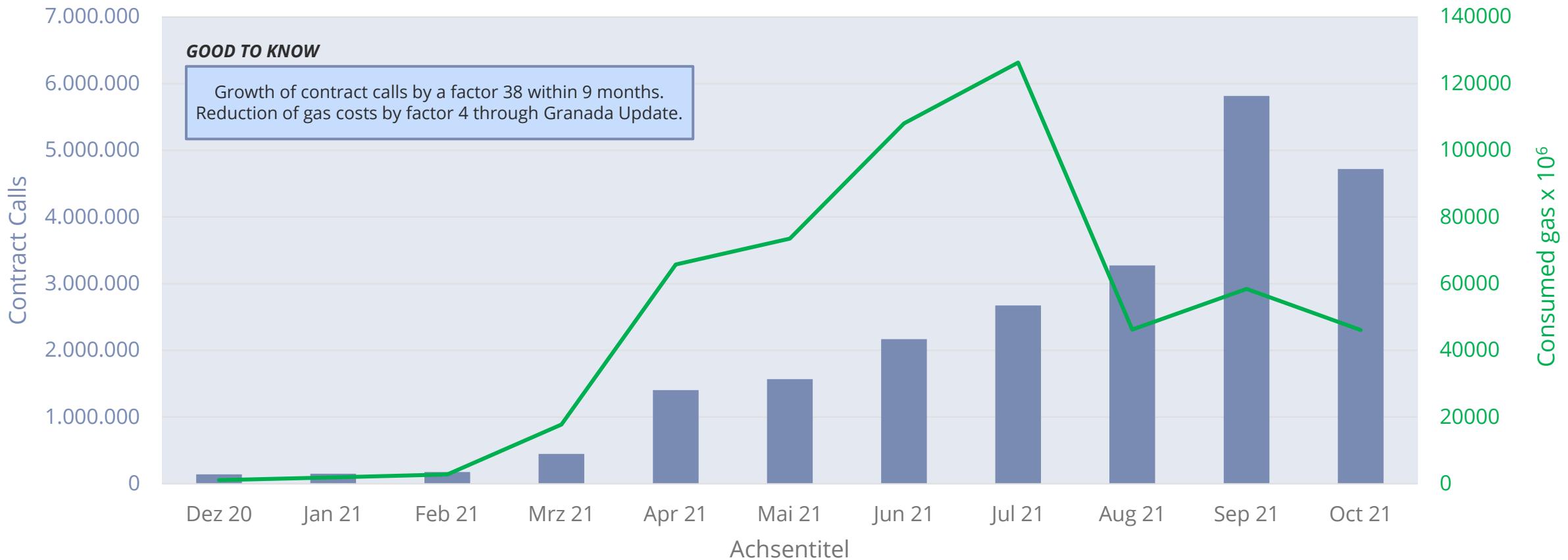
~ 120

transactions  
per second

> 135

active  
projects

## Some KPIs: Growth in Smart Contract Calls



Thanks to a growing number of applications and falling gas fees due to protocol upgrades, there has been a massive and continuing growth in smart contract calls on Tezos in 2021 proving that the chain is very much alive and being used!

# Key Feature: The amendment process/on-chain governance makes Tezos future-proof

## The intrinsic dilemma of blockchains so far:



a structure built to last for eternity

**VS.**

a very young and immature technology



*"everything is set in stone"*



*"technology still advances in quantum leaps"*

So far, every new blockchain project tried to solve one or two “problems” of previous blockchains.  
But nobody is omniscient and there are still major advances in virtually every aspect of the technology.

So by the time a new blockchain goes live, it is already obsolete!

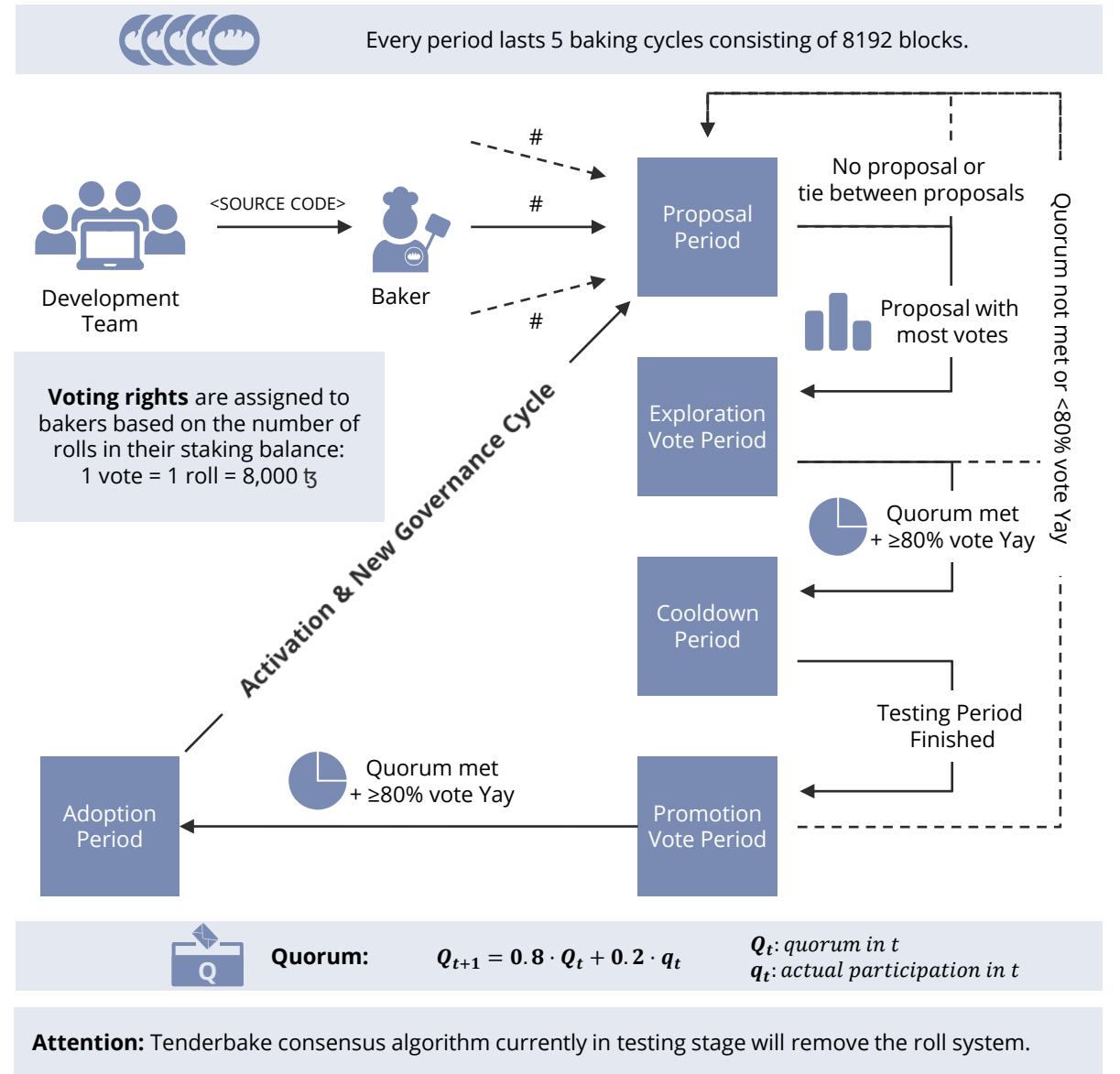
Changes to “classical” blockchains can only be achieved by forks.

Forks do have their *raison d'être*, but are very hard to coordinate in a truly decentralized ecosystem  
and do not favor decisions based on options' merits.

**Tezos** solves this dilemma with a **built-in and proven governance mechanism** that allows **on-chain coordination** leading to **controlled upgrades to the protocol**. The Tezos blockchain can thus **evolve over time** and **adapt the best technological developments from the entire ecosystem!**

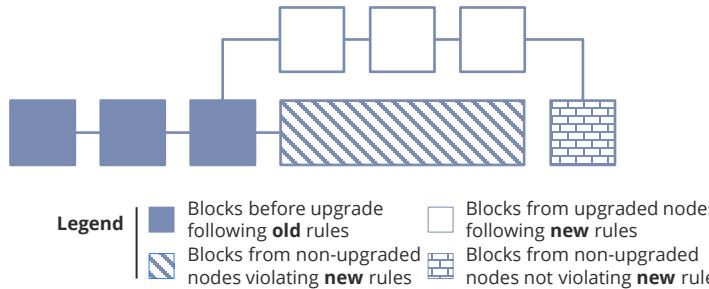
# How the Tezos on-chain governance/amendment process works

- The Tezos **on-chain governance** is implemented in an **amendment process**, that consists of **five major periods**, each of which lasts **five baking cycles** of 8,192 blocks (so 40,960 blocks per period).
- Depending on the votes, each period may end by **forwarding the process to the next period** or by **reverting to the process' outset**.
- During the **Proposal Period**, bakers can submit up to 20 proposals by injecting the **hash** of the amendment's **source code**.
- If there is no proposal or a tie by the end of the period, the process reverts to its start. Otherwise, the proposal with the majority of votes proceeds to the **Exploration Vote Period**.
- Bakers can then vote, whether they wish the previously selected proposal to proceed to the **Cooldown Period**, which happens, if both a dynamically determined **quorum** which is calculated as a function of the previous quorum is met and a **supermajority of initially  $\geq 80\%$**  is reached. Otherwise, the process is reset.
- During the **Cooldown Period**, bakers and community members can and should test the amended protocol (outside the mainnet).
- The **Promotion Vote Period** follows without another vote but is concluded by the final vote of whether the amendment should be adopted. If the quorum is met and a supermajority reached, the amendment will be **activated** on the main chain following the **Adoption Period** that serves as a buffer for the ecosystem to adapt to the new protocol version. Either after the Adoption period or if the proposal is not successful in the Promotion Vote Period, the process starts again with the next **Proposal Period**.

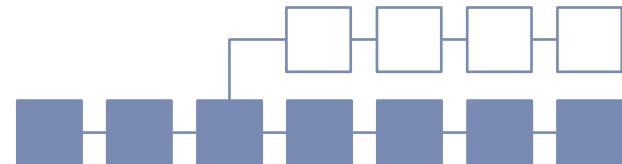


# What is the difference between forks and the on-chain governance?

## Soft Fork



## Hard Fork



## On-Chain Governance



- A **soft fork** is a **backward compatible** change of the protocol adopted by a willing subset of nodes.
- Changes in the protocol **restrict the protocol rules**, so “old” nodes will accept blocks adhering to the new rules.
- Only a subset of blocks created by “old” nodes will be accepted by the network, as some will break the now stricter rules.

- A **hard fork** is a change of the protocol that is **not backwards compatible**.
- Changes in the protocol **allow blocks that were not allowed before**, so “old” nodes will **not** accept blocks adhering to the new rules, effectively splitting the network.
- This **duplicates** the coins, **dividing their value** between the “old” and “new” currency, and nodes will switch to the version they think will be adopted by the majority.

- With the **on-chain governance**, a new version of the protocol is **activated by all nodes**, replacing the previous protocol.
- With the controlled governance mechanism, protocol options are **evaluated based on merits** rather than **herd behavior**.
- A “duplication” of currency is avoided, thereby preserving its value.

There are scenarios/situations in which **forks still make sense** (e.g. emergency bugfixes), but with on-chain governance, they are **not necessary** for protocol evolution, making them very **rare**.



## Key Feature: Liquid Proof-of-Stake makes Tezos secure without wasting energy

### Bitcoin's intrinsic dilemma:



network security

VS.



energy consumption

#### GOOD TO KNOW

196 TWh in November 2021  
<https://digiconomist.net/bitcoin-energy-consumption>

"Bitcoin mining is needed to prevent 51%-attacks"



"Bitcoin mining consumes more energy than Thailand"

If an attacker controlled more than half of the network he would be able to "convince" the network of his "truth".

He could thus reverse transactions by rewriting the blockchain history and **double spend** his money.

This type of attack is called **51%-attack** or **Sybil attack\*** as the attacker creates a lot of fake nodes to gain control.



Bitcoin seeks to prevent 51%-attacks by making them very costly.

This is achieved through the Sybil control mechanism Proof-of-Work (PoW) that requires a Bitcoin miner (i.e. validator) to prove that he invested a lot of work by solving a cryptographic puzzle which consumes a lot of computing power and consequently energy.



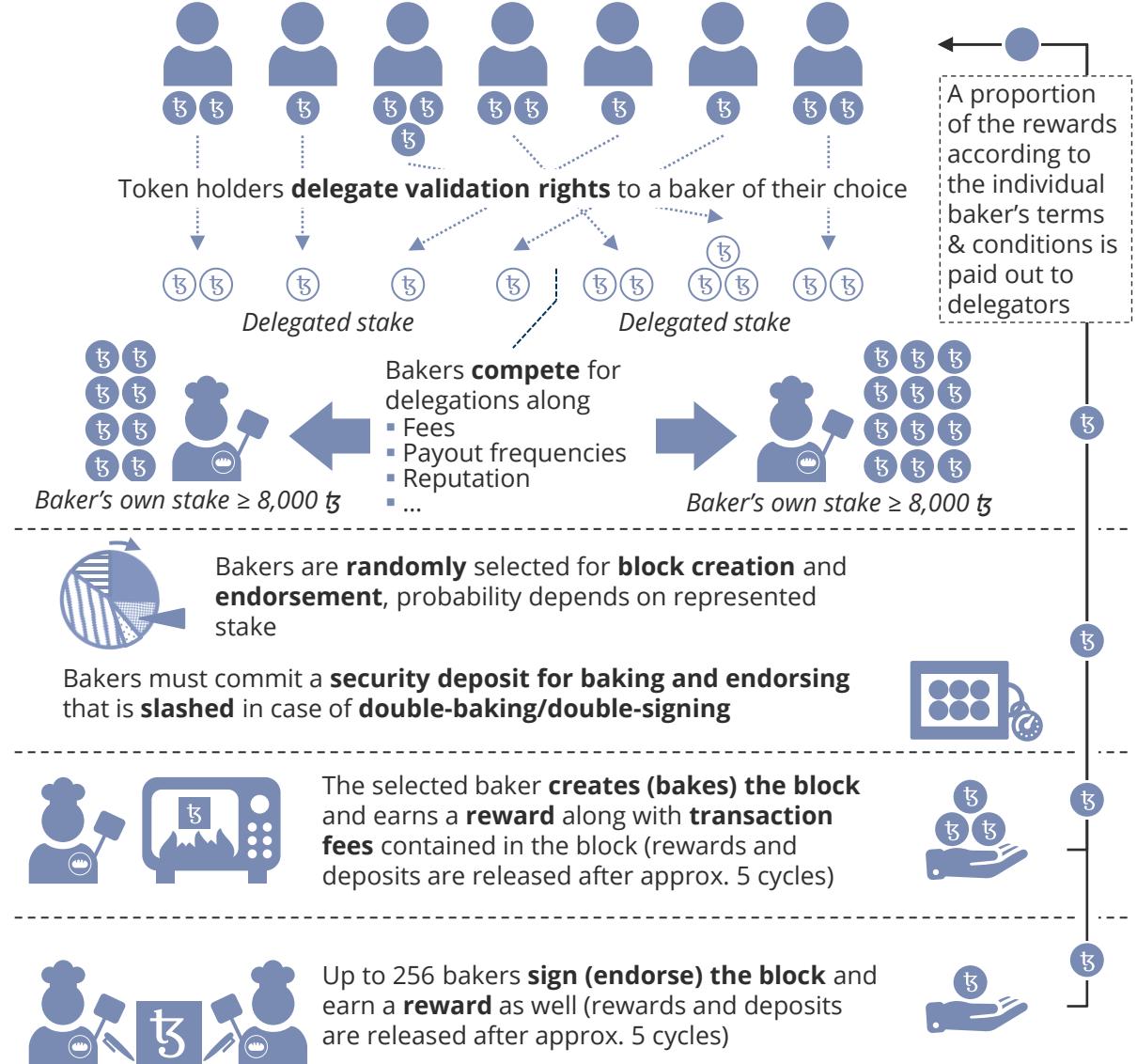
**Tezos** solves this dilemma with a different kind of **Sybil control mechanism** called **Liquid Proof-of-Stake**. Like in PoW, Bakers (i.e. validators) are **extrinsically incentivized** through rewards but energy consumption is avoided by a security deposit, that can be slashed.

# How Liquid Proof-of-Stake (LPoS) works

- The top design priority for **Liquid Proof-of-Stake (LPoS)** is security by true decentralization.
- While a worrying degree of concentration can be observed with mining pools for Bitcoin's **Proof-of-Work** (PoW) and **delegated Proof-of-Stake** (dPoS) as utilized in EOS and Lisk operates with a fixed and limited validator set, Tezos' LPoS strives for **low entry barriers for validators** (called bakers in Tezos).
- Baking requires downloading the baking/endorsing node, holding a **roll** (8,000 t3) as well as **modest computing power** and a **reliable internet connection**.
- Delegation is **optional** for token holders and bakers **compete** for delegations with the proportion of earnings they share with their delegators, their reputation and individual terms & conditions.
- The number of delegations a baker can accept is limited by his self-bond (approx. 10-times its own stake).
- Bakers are **randomly selected** for block creation and endorsement, with a **probability** depending on the **represented stake**. They commit a **security deposit** for block creation and endorsements proportional to the potential gains which can be **slashed** in case of misbehavior.
- The baker receives a **reward** and including **transaction fees** for creating a block as well as for each of the 256 possible endorsements. Rewards and deposits are released after approx. **5 cycles** and delegators are paid their share.

## GOOD TO KNOW

If [Tenderbake](#) is adopted the number of endorsements will change but the overall inflation of 5% will remain.



# Tez - the Tezos coin and its functions



CANNOT BE  
DELEGATED

CAN BE  
DELEGATED

VALIDATION

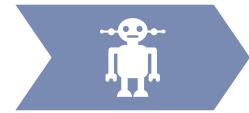
VOTING

FINANCIAL OWNERSHIP



# Key Feature: Formally verifiable smart contracts

## The smart contract dilemma:



process automation

**VS.**

process integrity



*"smart contracts can automate inter-party processes"*



*"is the smart contract doing what it should?"*

Smart contracts are simple **computer programs** that can automatically be executed, when certain conditions are met.

They are **deployed on the blockchain** and thus both accessible and immutable.

Smart contracts can be used to automate the execution of the conditions of legal contracts and thus **automate inter-party processes**.



However, when engaging in a smart contract, there are two problems:

First, smart contracts are programmed by humans and humans make errors, so is the smart contract doing what it should be?  
Second, the smart contract's compiled version deployed on the blockchain is not human readable, so is it doing what its author claims?



**Tezos** solves this dilemma with smart contracts in the custom-made, **formally verifiable language Michelson** and a **certified compiler**. The first **minimizes the probability of errors** as formal correctness can be proven, the latter allows to **analyze the human-comprehensible version**, compiling it oneself using the certified compiler and then comparing the result to the deployed version.

# The main design goals for the Michelson virtual machine were readability, security and efficiency

- **Virtual machines** that allow the **execution of smart contracts** are **attack vectors** for blockchains.
- Bugs caused by smart contracts that are known from other blockchains are:
  - ▶ Overflow (Multiple)
  - ▶ Reentrance bugs (Ethereum DAO hack)
  - ▶ Absence of libraries (Parity)
  - ▶ Combination of imperfect features (Parity)
  - ▶ Honeypots
- All these bugs were possible due to **design failures**. The Michelson VM was **custom-made** to avoid bugs and allow **formal verification** (mathematical proof).
- Next to **security**, the Michelson **design goals** were:
  - ▶ **Readability**: an expressive representation of the smart contract on the blockchain.
  - ▶ **Efficiency**: allowing fast contract execution and making the calculation of gas costs as easy as possible.
- Michelson is a **statically typed stack language** without variables but with **high-level primitives** (arbitrary length integers, maps, sets, lambdas and crypto primitives: hash, check signature).

	EVM	WASM	Michelson
Properties	256 integers	32/64 integers	Infinite precision integers
	No data structures	No data structures	Persistent sets, maps, lists
	Side effects	Side effects	No side effects
	Purpose made	Standard	Purpose made
Platform	Ethereum	Dfinity, EOS	Tezos

EVM

= Ethereum Virtual Machine

WASM

= Web Assembly

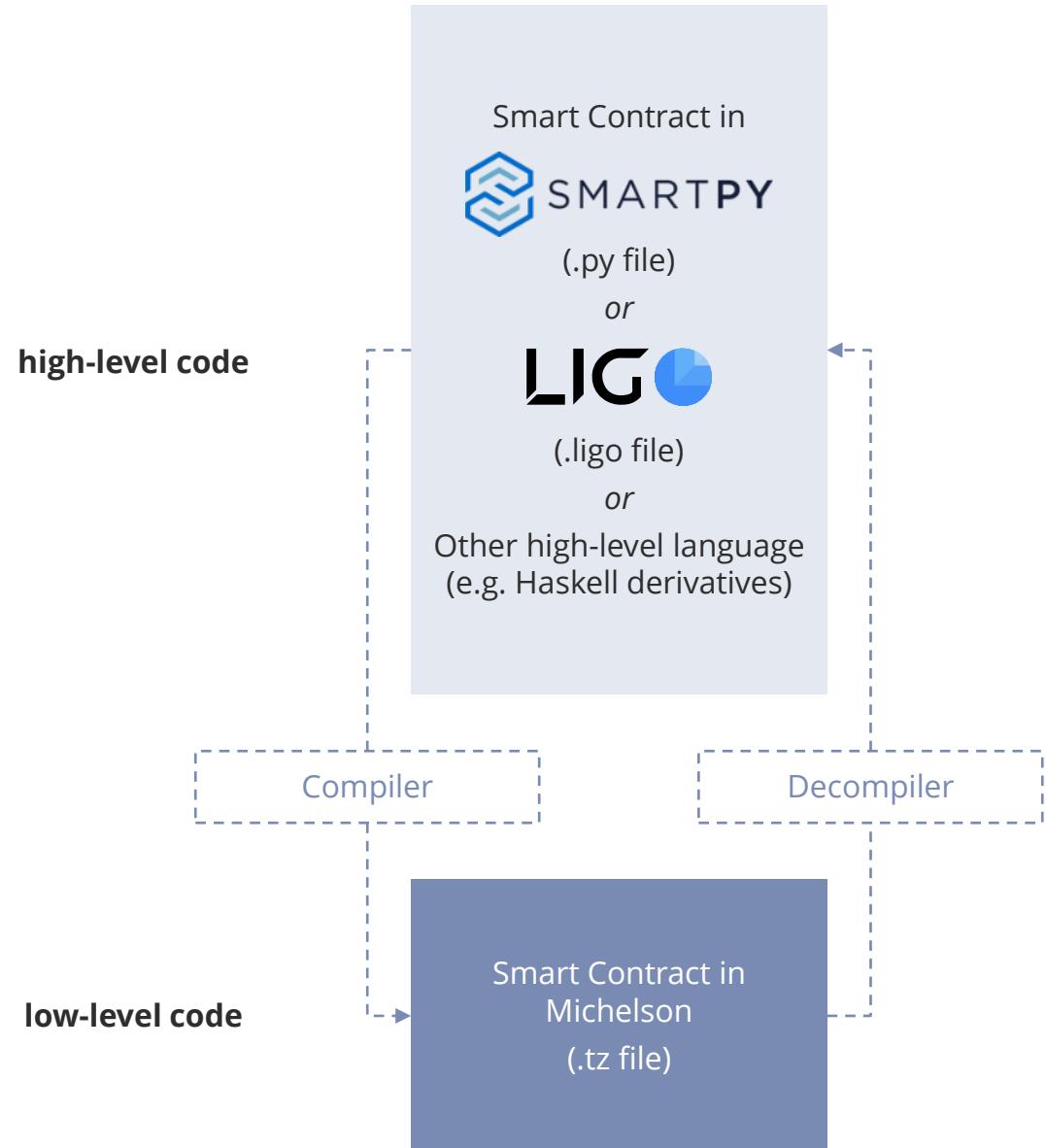
“Business logic, not protein folding.”

Arthur Breitman

(about the purpose of smart contracts in Tezos)

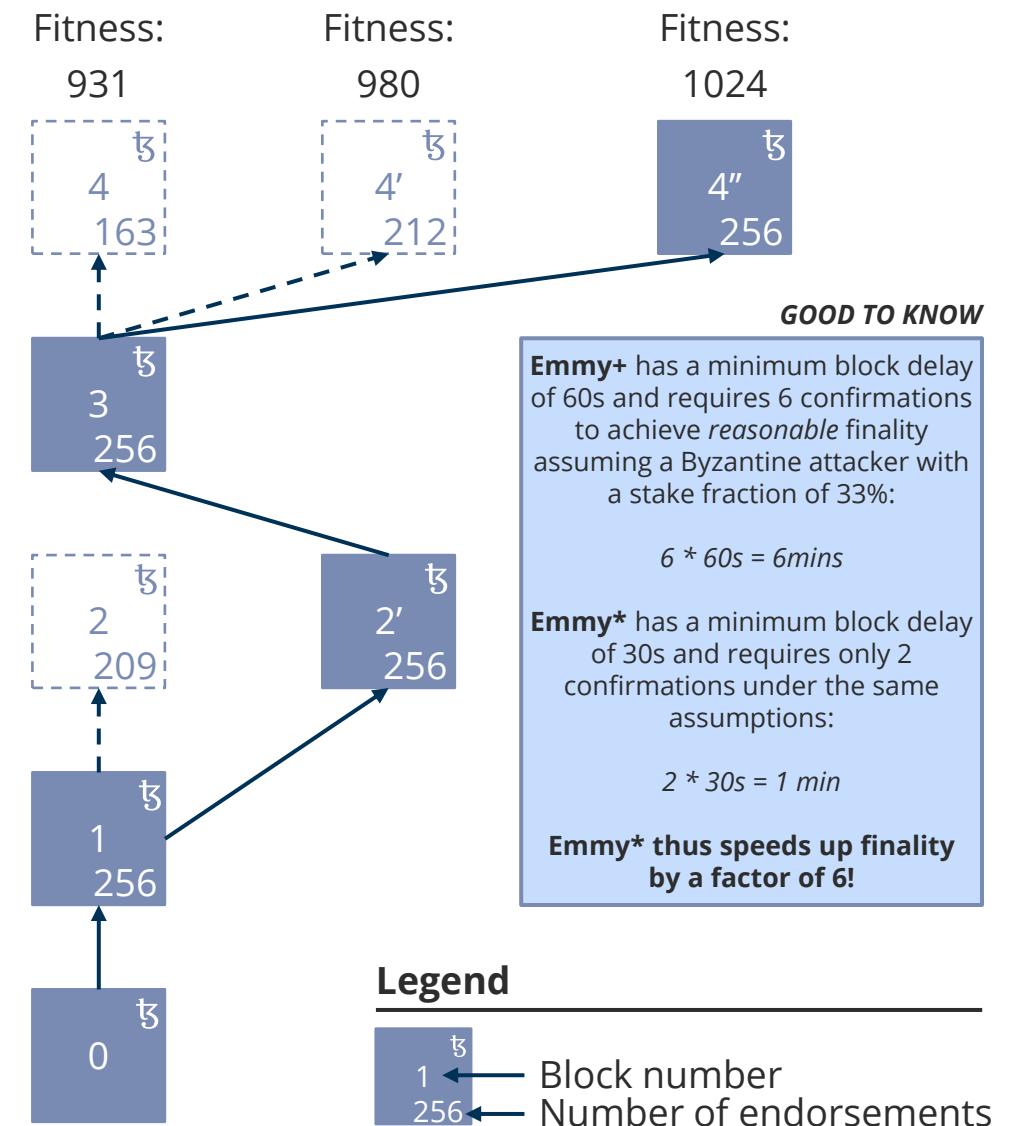
# Smart contracts in high-level languages can be compiled to Michelson

- Michelson is a **compromise** between the design goal of efficiency with respect to gas accounting that would suggest an **assembly-like language** on the one hand and security and readability that would suggest a **high-level functional language** on the other hand.
- There are high-level languages such as **SmartPy**, **LIGO** (and more, e.g. Haskell derivatives) that can be **compiled to Michelson**.
- This allows to program smart contracts in a way that comes **more natural to most programmers**, e.g. LIGO offers different syntaxes that are designed to resemble Pascal (PascaLIGO), Ocaml (CameLIGO) and ReasonML (ReasonLIGO).
- It also allows people who want to engage with a smart contract deployed on Tezos to **read and understand what the contract does** (its “terms”).
- To **verify**, that the deployed contract on the chain and the high-level language contract offered for inspection are indeed **equivalent**, a **certified compiler** can be used: it guarantees that the third party gets the same result when compiling the high-level code and can compare it to the low-level code on the chain.
- Smart contracts in Michelson can be formally verified using test frameworks like **Mi-Cho-Coq** (<https://www.springerprofessional.de/making-tezos-smart-contracts-more-reliable-with-coq/18522634>)



# The Tezos consensus algorithm: Emmy / Emmy+ since Babylon / Emmy\* since Granada

- Because they are closely entwined, **Sybil control mechanisms** like **Proof-of-Work (PoW)** or **Proof-of-Stake (PoS)** are often confused with **consensus algorithms**. However, they are merely **mechanisms to protect the consensus protocol** against **Sybil attacks**.
- The consensus algorithm is needed for the network to **agree upon a “common version of the truth”** (i.e. the right chain). It is mainly characterized by the question of **how the right chain is determined**.
- There are two main types of consensus protocols:
  - Nakamoto Consensus:** the longest/heaviest/fittest chain is the canonical one (probabilistic finality).
  - Byzantine Fault Tolerant Consensus:** the latest block with more than 2/3 of the validator set's signatures is appended (deterministic finality): **Tenderbake**.
- Bitcoin's consensus protocol uses Nakamoto Consensus with the longest chain criterion as the longest chain has consumed the most work – which shows how consensus protocol and Sybil control mechanism are mutually dependent.
- The **Tezos consensus protocol** is called **Emmy** and since the Babylon amendment the refined version **Emmy+** is in place which was replaced with **Emmy\*** (with the goal of providing faster finality without compromising security), with the activation of Granada.
- Emmy\* uses Nakamoto Consensus with the **fittest chain criterion** where **fitness is determined by the number of endorsements** (signatures from endorsing validators) contained in the chain. Up to 256 bakers (validators) can endorse a block (only 32 with Emmy+).





## Consensus on chain state

Achieved through  
consensus mechanism  
**Emmy\***

### Necessary preconditions:

- “Healthy” network, i.e. diverse validator set
- Low entry barriers for new bakers
- Sybil control mechanism (LPoS)

### Implications:

- Secure consensus on canonical chain

## Consensus on technology evolution

Achieved through  
on-chain governance/  
amendment process  
("change management")

### Necessary preconditions:

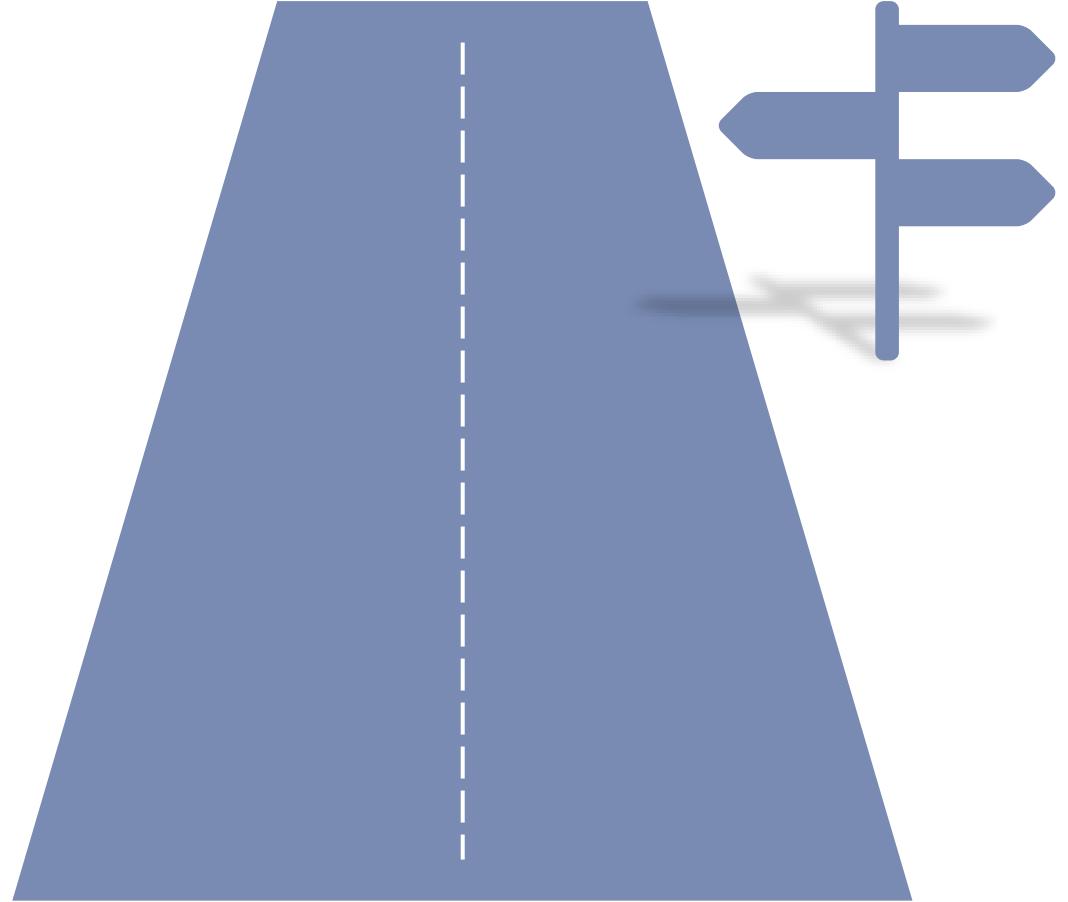
- Tools
- Discussion forums
- Transparency
- Communication
- Participation
- Rigorous test framework

### Implications:

- Community can vote on developments that you do not favor
- Drastic reduction of hard fork probability
- No „asset duplication problem“ through hard forks (see NFTs !)

# Is there a development roadmap for Tezos?

- For people or organizations thinking of **building applications on top of Tezos**, it is of course of interest **which developments can be expected in the future**.
- As Tezos is a **truly decentralized** project, there is **no central governing body** that decides on its development, so there is no **roadmap** as such.
- Developments are implemented through the **amendment process** and thus **governed by the community** through **on-chain governance**.
- However, no development simply materializes out of nowhere. All the greater developments are discussed in the community – good sources are: [Tezos Agora Forum](#), [TZIP](#), [Nomadic Labs Announcements](#)
- Some of the developments that can be expected in the future are:
  - ▶ Introduction of an alternative BFT-style consensus algorithm: **Tenderbake**
  - ▶ Layer 2 scalability solutions with **optimistic rollups**.
  - ▶ **Baking accounts** (to enable bakers to rotate their keys without losing their delegations)
  - ▶ Improvements to the **amendment process itself** (e.g. privacy-preserving amendment procedures)





# TEZOS AMENDMENT HISTORY

# The self-amendment process works: 8 successful amendments and counting... (1/3)

- The self-amendment process through Tezos' on-chain governance **works!**
- So far, there have been **8 amendments** that went live after the proposals successfully ran through the voting process and update number 9 with the letter "I" is already under way.
- Tezos Agora** (agora like the central festival, assembly and marketplace of cities in ancient Greece) allows to:
  - Browse all periods that occurred so far** with respect to proposals, their description, voting outcomes, etc.
  - Discuss current and future proposals in the [Tezos Agora Forum](#).
- One proposal that got voted to the Exploration Period, **Brest A**, did not make it to the Testing Period, reverting the process to Proposal.
- The amendments contain a multitude of changes like new features, housekeeping/bugfixes and performance updates as well as amendments to the existing ruleset, including the amendment process itself.

A	thens	  	05/30/2019 Participation: 84.35 % In Favor: 99.89 % Increase gas limit per block, reduce roll size from 10,000 t3 to 8,000 t3
B	abylon	  	10/18/2019 Participation: 83.46 % In Favor: 84.53 % Emmy+, delegable tz1 addresses, Michelson upgrades, hardened governance
C	arthage	  	03/05/2020 Participation: 72.05 % In Favor: 99.61 % Increase gas limit per block and operation, improve formula for baking and endorsing rewards

Legend		Date of Activation
		KPIs from Promotion Period
		Description of Amendment

## The self-amendment process works: 8 successful amendments and counting... (2/3)

- Until Edo was activated, a **period** within the amendment process took 8 baking **cycles** with a cycle consisting of 4,096 blocks. As blocktime varies slightly but has a lower bound of 1 minute, a period used to take at least 22.76 days or **roughly 3 weeks**.
- Accordingly, a **full iteration of the amendment process** used to take at least 91.02 days or roughly **13 weeks / 3 months**.
- However, the fifth & sixth updates – **Edo** and **Florence** – brought about some significant changes to the amendment process itself:
  - The fifth period called the **Adoption** period was introduced to give bakers, indexers and end users a sufficient time window to update and adapt to the new protocol version. (Edo)
  - Period lengths were reduced from 8 to **5 cycles**, shortening the minimum time between updates to 25 cycles taking at least 71.11 days or roughly **10 weeks / 2.5 months**. (Edo)
  - No test chain is created within the mainnet anymore and the Testing period has been rechristened to **Cooldown** period accordingly. (Florence)

<b>D</b> <b>elphi</b>	 11/12/2020  Participation: 68.49 %  In Favor: 100.00 % Reduce gas costs, reduce storage costs, fix bugs, code cleanup and refactoring, improve Michelson safety
<b>E</b> <b>do</b>	 02/13/2021  Participation: 63.91 %  In Favor: 100.00 % Sapling for privacy preserving transactions, Michelson opcodes, tickets, Adoption period, reduction of periods to 5 cycles
<b>F</b> <b>lorence</b>	 05/11/2021  Participation: 59.61 %  In Favor: 100.00 % Incr. max. operation size to 32kB, reduce gas consumption, intercontract calls depth first, Cooldown period without test chain

Legend	
	<i>Date of Activation</i>
	<i>KPIs from Promotion Period</i>
	<i>Description of Amendment</i>

## The self-amendment process works: 8 successful amendments and counting... (3/3)

- The Tezos community follows the **convention** of naming amendment proposals with **city names** in **alphabetical order**. With the last successfully activated proposal being Hangzhou, the next proposal currently within development is named after a city starting with "I": the test net is called Idiazabalnet.
- The voting mechanism of the Tezos On-Chain Governance reveal the voting behavior of all its participants. There is ongoing research in partnership with INRIA to **introduce privacy preserving voting mechanisms**. More information can be read in: [Possible evolutions of the voting system in Tezos](#).
- The features of the next protocol upgrade are as always not fixed but can be **predicted by participating** in the discussions of the before mentioned social platforms and by analyzing the test networks.
- With the possible introduction of the new consensus algorithm Tenderbake not only **evolution** of the consensus mechanism is shown as with Emmy -> Emmy\* but a **revolution** with the chain from Nakamoto to BFT consensus.

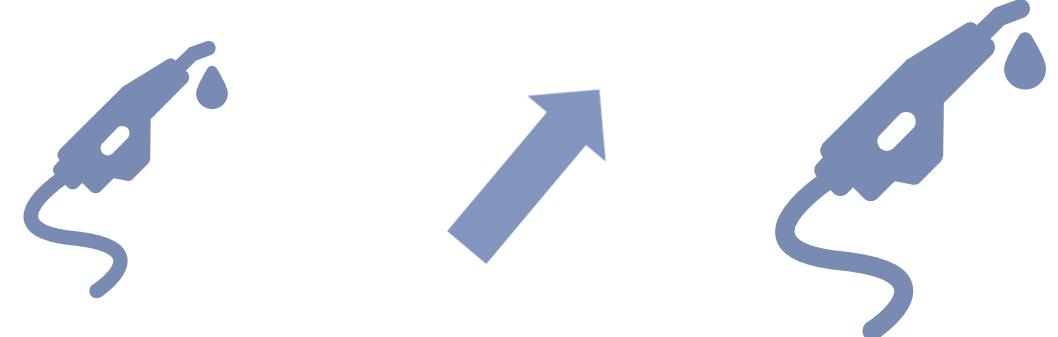
<b>G</b>	<b>ranada</b>	 06/08/2021
	Participation: 68.60 % In Favor: 99.59 %	
	Reduce blocktime to 30s, decrease time to finality by a factor of 6, gas improvements by factor ~ 4, liquidity baking for tzBTC	
<b>H</b>	<b>angzhou</b>	 03/12/2021
	Participation: 67.14 % In Favor: 99.39 %	
	Add timelock opcodes to counter MEV, introduce On-Chain Views, add global constants, add smart contract cache	
<b>I</b>	... ?	 April 2022 ?
	Participation: ? In Favor: ?	
	Tenderbake ?	
<b>Legend</b>		
 Date of Activation		
 KPIs from Promotion Period		
 Description of Amendment		

## Athens – the first amendment to the Tezos protocol

- Athens is the **first successful amendment** to the Tezos protocol through the on-chain governance mechanism.
- The proposal was developed and brought forward by [\*\*Nomadic Labs\*\*](#) in the 10<sup>th</sup> period and activated on 2019-05-30.
- Its main goal was to introduce a sensible yet simple amendment in order to **prove the on-chain governance mechanism's viability**.
- With Athens A and Athens B, two different proposals entered the **Proposal Period**, Athens B proposing a subset of Athens A's changes:
  - ▶ **Athens A:** Increase the gas limit per block and reduce the roll size from 10,000  $\text{tz}$  to 8,000  $\text{tz}$ .
  - ▶ **Athens B:** Increase the gas limit per block.
- **Gas** is a measure for the computation power needed to validate a block, so the increase of the limit allows more computation steps.
- A **roll** is the minimum amount of  $\text{tz}$  a Baker must hold in order to bake (i.e. validate blocks).
- With a majority of 70.3% of votes, Athens A proceeded to the **Exploration Period**, got voted to the **Testing Period** and was finally activated on **2019-05-30** after receiving 99.89% of the votes at a participation rate of 84.35% in the **Promotion Period**.
- Nomadic Labs included a symbolic **invoice** of 100  $\text{tz}$  in their proposal as an example for funding proposal development.



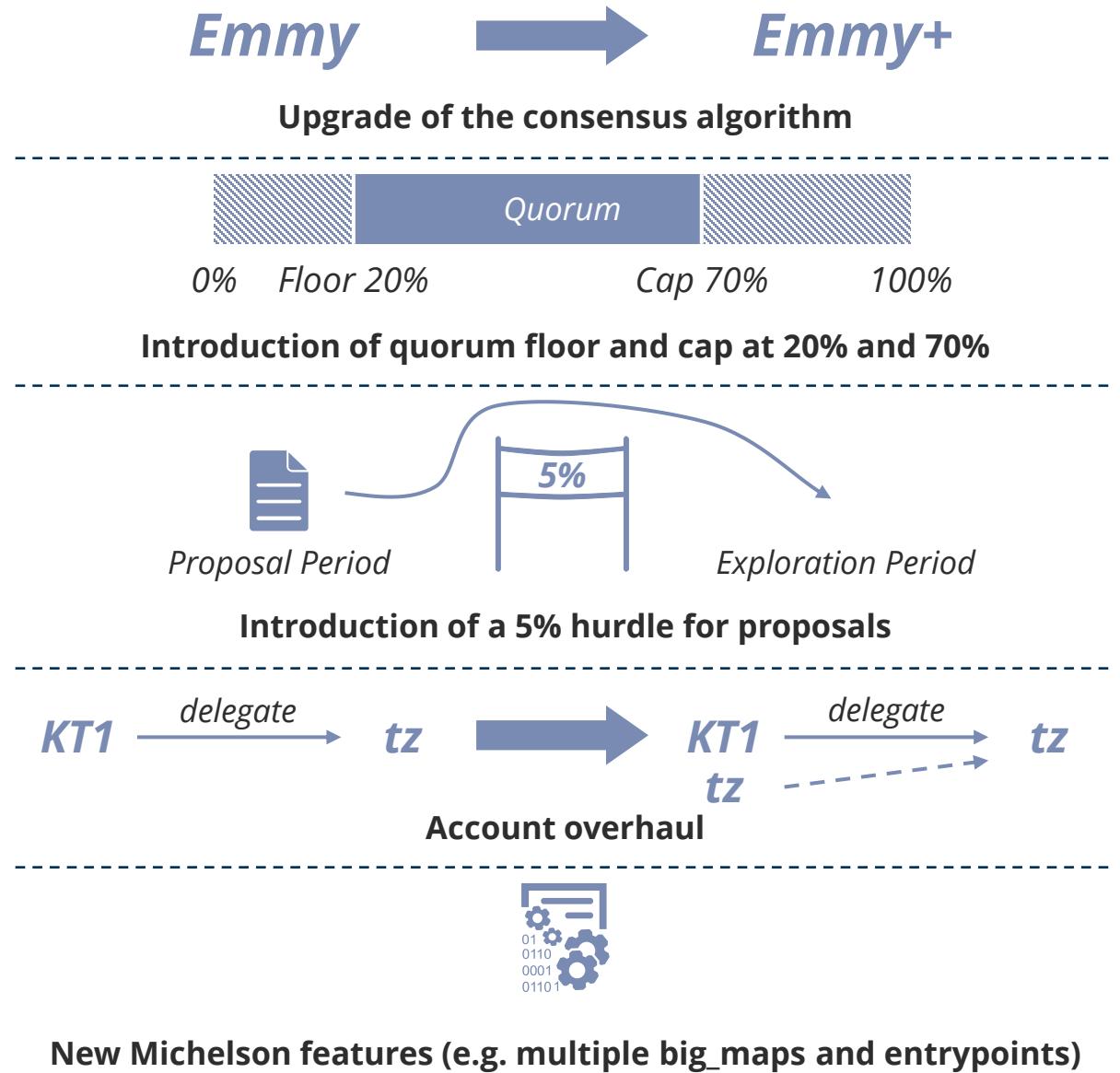
**Reduction of the roll size from 10,000  $\text{tz}$  to 8,000  $\text{tz}$**



**Increase of the gas limit**

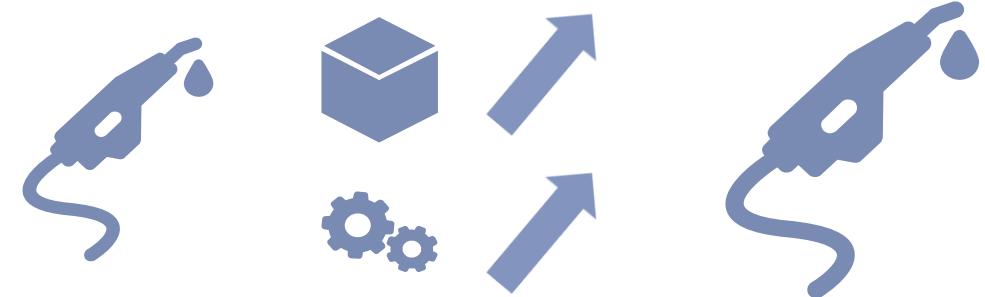
# Babylon – the second amendment to the Tezos protocol

- Babylon is the **second successful amendment** to the Tezos protocol through the on-chain governance mechanism.
- It was the first amendment that introduced a **significant set of new features** and thus proved, that the amendment process not only worked (as shown by Athens) but that **amendments to large parts of the codebase** are feasible.
- Babylon is thus a **cornerstone** for Tezos to become a **blockchain that evolves over time** and **adapts the best technologies** from the entire ecosystem.
- It was jointly developed by [Nomadic Labs](#) and [Cryptium Labs](#) with contributions from [Marigold](#) and invoiced with 500 tz.
- Babylon brought the following changes:
  - ▶ An **upgrade of the consensus algorithm** Emmy to the more robust version **Emmy+**.
  - ▶ A **quorum floor** was set at **20%** and a **quorum cap** at **70%**.
  - ▶ A proposal now requires a **minimum of 5% support** to proceed to the Exploration Period.
  - ▶ Introduction of a clear distinction between **delegable tz1, tz2 and tz3 accounts** and **KT1 accounts for smart contracts**.
  - ▶ **New Michelson features** such as the possibility for multiple **multiple big\_maps** and **entrypoints** to assist smart contract developers and designers of higher-level languages.



## Carthage - the third amendment to the Tezos protocol

- Carthage is the **third successful amendment** to the Tezos protocol through the on-chain governance mechanism and was **activated on 2020-03-05**.
- It was jointly developed by [Nomadic Labs](#) and [Cryptium Labs](#) and did not contain an invoice.
- The proposal was nicknamed the **housekeeping proposal** as it focused on code clean-up, optimizations and minor fixes instead of introducing significant new features.
- Noteworthy changes brought in with Carthage are:
  - ▶ Increase of the **gas limit per operation** from 800,000 to 1,040,000.
  - ▶ Increase of the **gas limit per block** from 8,000,000 to 10,400,000.
  - ▶ Adaption of the **formula for calculating baking and endorsing rewards** to be linear in the number of endorsements (replacing a step function) and to be more resistant to certain types of attacks.
  - ▶ Minor **improvements to Michelson**.



**Increase of the gas limit per operation to 1,040,000**  
**Increase of the gas limit per block to 10,400,000**



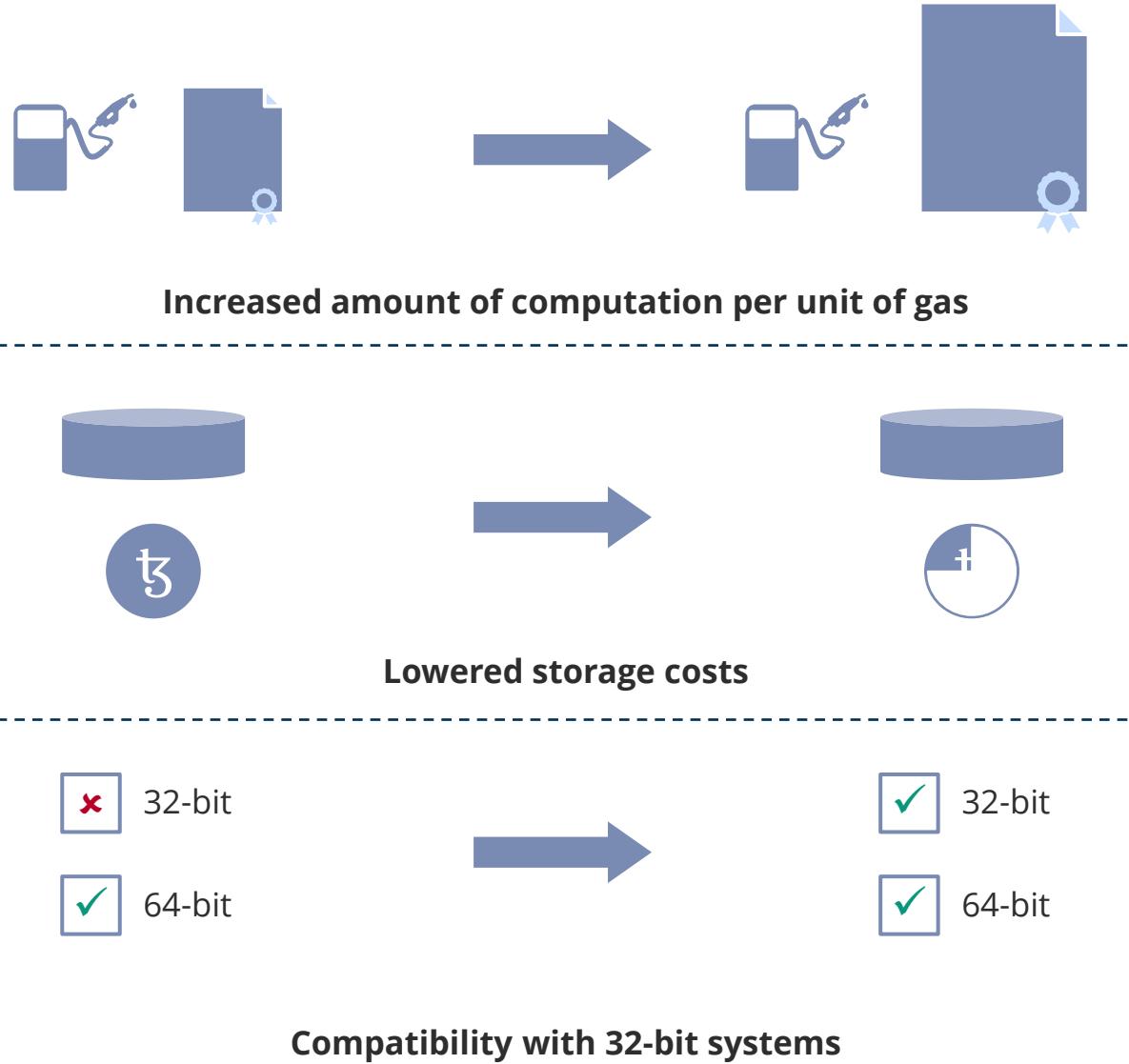
**Adaption of the reward calculation formula**



**Improvements to Michelson**

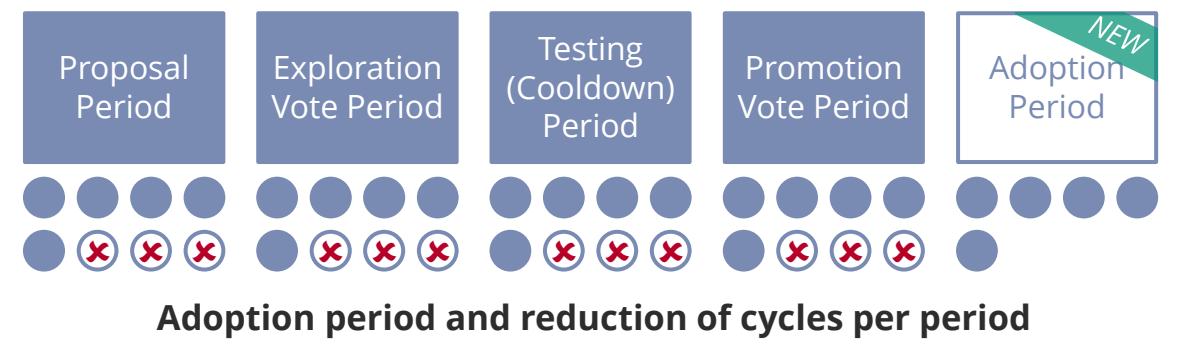
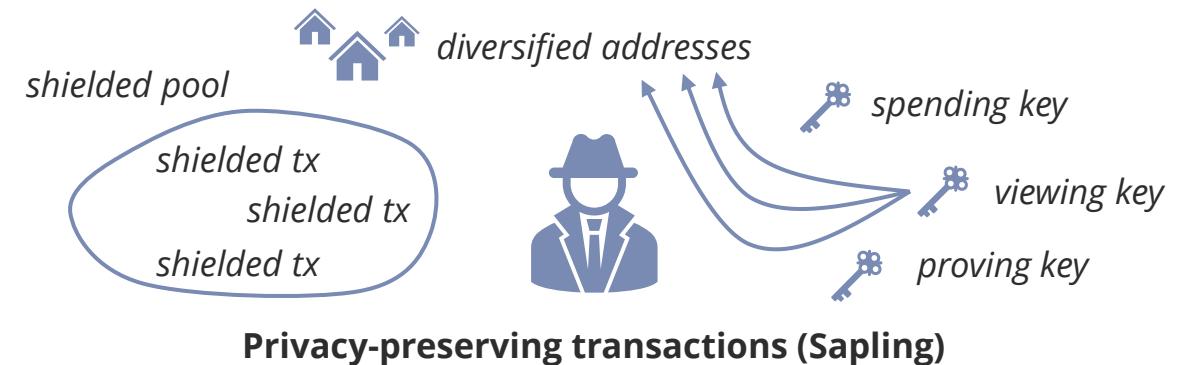
# Delphi – the fourth amendment to the Tezos protocol

- Delphi is the **fourth successful amendment** to the Tezos protocol through the on-chain governance mechanism and was **activated on 2020-11-12**.
- Originally planned as a major feature upgrade, Delphi instead became an **interim protocol proposal** focused on **performance and gas improvements** in order to enable novel applications on Tezos that target areas like DeFi, collectibles, and gaming while features like Sapling, baking accounts, etc. were not ready for deployment.
- It was jointly developed by [Nomadic Labs](#), [Metastate](#), and [Gabriel Alfour](#), did not contain an invoice and was proposed after seven governance periods without proposals.
- Noteworthy changes brought in with Delphi are:
  - ▶ **Gas changes** based on performance improvements **increasing the amount of computation per unit of gas** while maintaining the current gas limits (Tezos' low gas costs have since become a significant competitive advantage when compared to other smart contract platforms like Ethereum and have inspired some [great memes that were rewarded within the CRP](#)).
  - ▶ **Lowered storage costs** (proportional amount of  $\text{tz}$  burned when increasing the size of the data stored in the state) by a factor of 4 from 1  $\text{tz}$  per kB to 0.25  $\text{tz}$  per kB.
  - ▶ **Bugfixes**, most prominent among them the restoration of **compatibility with 32-bit systems**.
  - ▶ General **code cleanup** and **refactoring**



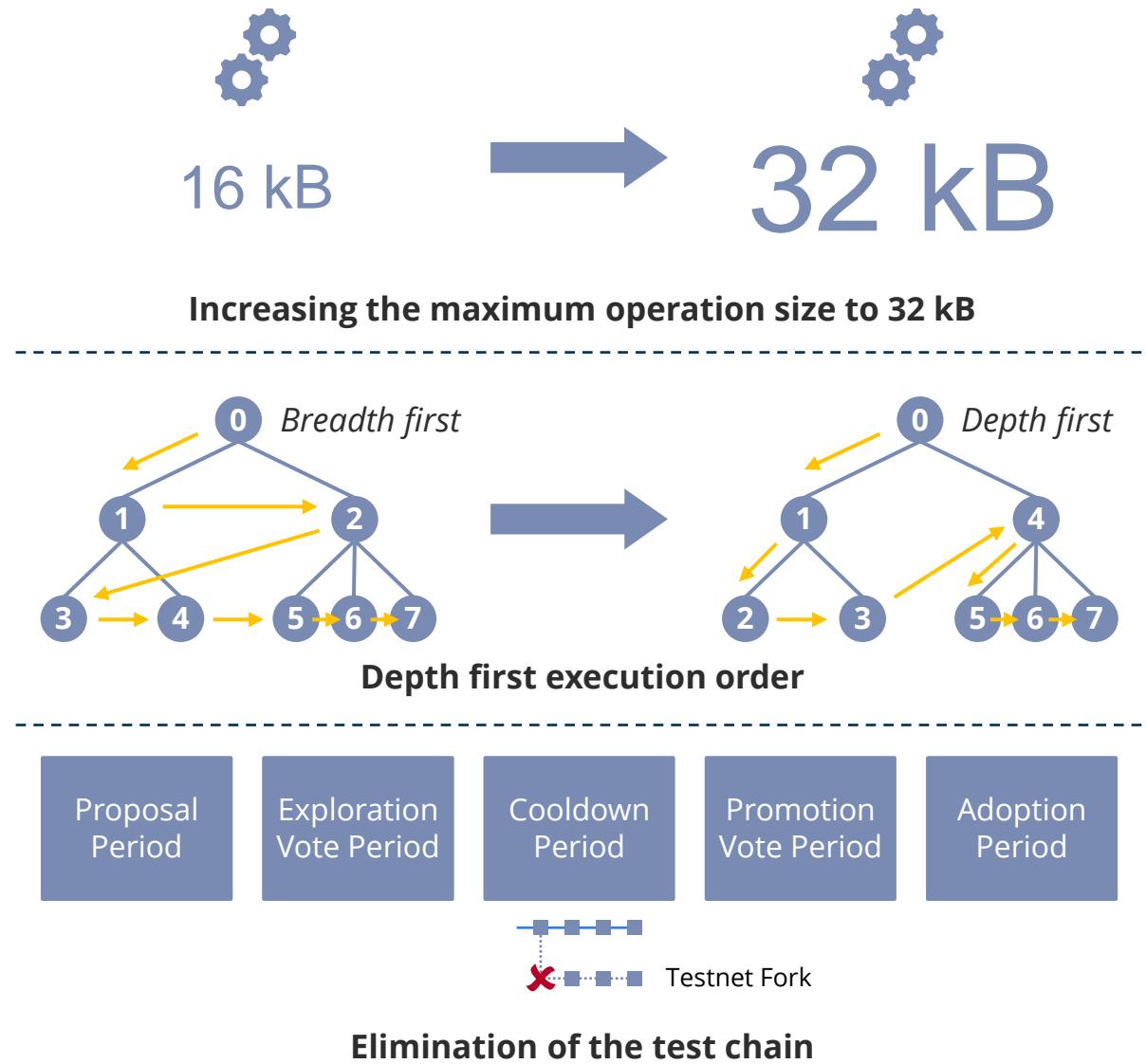
## Edo - the fifth amendment to the Tezos protocol

- Edo is the **fifth successful amendment** to the Tezos protocol through the on-chain governance mechanism and was **activated on 2021-02-13**.
- Edo was packed with new features and an update to the amendment process itself.
- It was jointly developed by [Nomadic Labs](#), [Marigold](#), and [Metastate](#), did not contain an invoice and was proposed in the period directly following the activation of Delphi.
- Noteworthy changes brought in with Edo are:
  - ▶ Integration of **Sapling** to enable **privacy preserving transactions** (protocol enabling privacy preserving transactions of fungible tokens in a decentralised environment) and addition of Michelson opcodes for the pairing-friendly elliptic curve **BLS12-381**.
  - ▶ Introduction of **Tickets** as a mechanism for smart contracts to grant portable permissions to other smart contracts or issue tokens.
  - ▶ Introduction of a fifth period, the **Adoption period**, to the amendment process and **reduction of period lengths from 8 to 5 cycles** (shorting the minimum time for a governance iteration from 32 to 25 cycles while simultaneously providing more time to adopt an update *after* the community's decision on the update is final).
  - ▶ Addition of some new instructions to Michelson, including **LEVEL** to query the level of the current block.



# Florence – the sixth amendment to the Tezos protocol

- Florence is the **sixth successful amendment** to the Tezos protocol through the on-chain governance mechanism and was **activated on 2021-05-11**.
- There were **two versions** of the proposal: One containing **Baking Accounts** and one identical to the first minus the Baking Accounts. The community followed the developers' recommendation in voting for the proposal without Baking Accounts due to some concerns about breaking changes that had not been resolved at the time.
- It was the first update to go through the new Adoption period and jointly developed by [Nomadic Labs](#), [Marigold](#), [DaiLambda](#), [Tarides](#), and the external contractor [Keefer Tyler](#) who was rewarded with the proposal's invoice of 100  $\text{tz}$ .
- Noteworthy changes brought in with Florence are:
  - ▶ Increase of the **maximum operation size from 16 to 32 kB** allowing for more complicated applications by (more than) doubling the maximum size of a smart contract.
  - ▶ Further **gas consumption optimization** to bring down costs even more by increasing efficiency.
  - ▶ **Depth first** execution order for smart contract calls (instead of breadth first) making intercontract calls more intuitive.
  - ▶ **Elimination of the test chain** in the third period of the governance cycle (and rechristening of the period from Testing period to Cooldown period).



## Granada – the seventh amendment to the Tezos protocol

- Granada was the **seventh successful amendment** to the Tezos protocol through the on-chain governance mechanism and was **activated on 2021-08-06**.
- It was jointly developed by [Nomadic Labs](#), [Marigold](#), [TQ](#), [DaiLambda](#), and [Tarides](#).
- Noteworthy changes brought in with Granada:
  - ▶ An overhaul of the current consensus algorithm Emmy+ with **Emmy\*** which will bring down blocktime to approx. 30 s (effectively halving the time between blocks).
  - ▶ **Liquidity baking** as a means to enhance liquidity by piggybacking off the liquidity and global availability of Bitcoin.
  - ▶ Significant **gas improvements** that will further decrease gas consumption by **factors of 3 to 6** and even 8 in some cases.

**Emmy+** → **Emmy\***

~60s blocktime

~30s blocktime

**Upgrade of the consensus algorithm**

**tez**



**tzBTC**

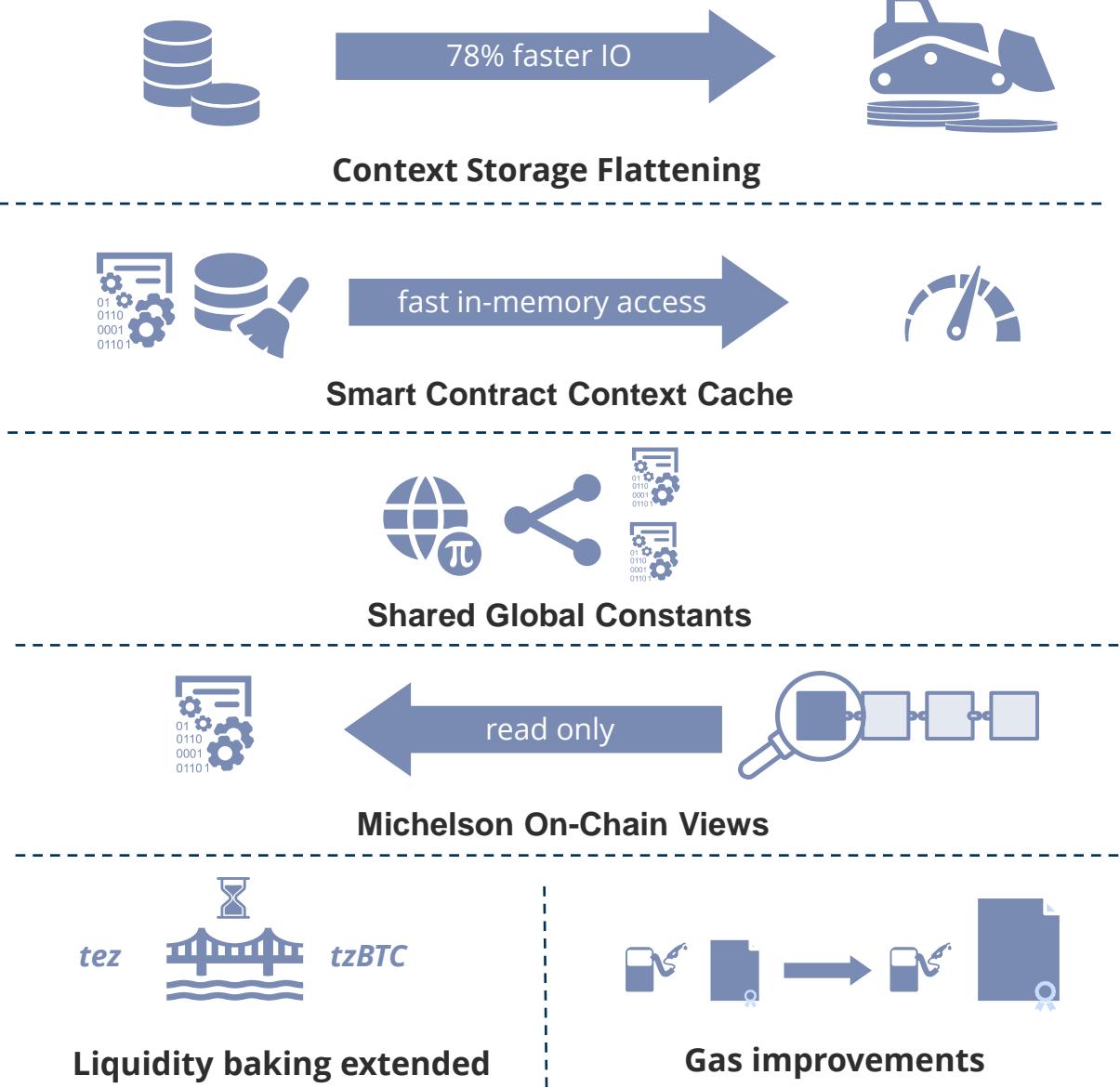
**Liquidity baking**

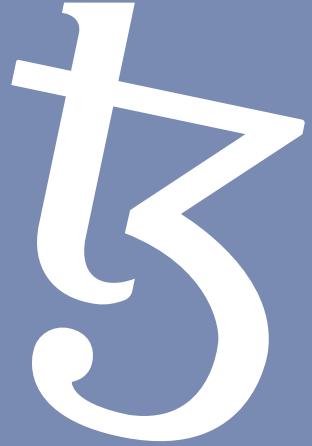


**Gas improvements**

# Hangzhou – the eighth amendment to the Tezos protocol

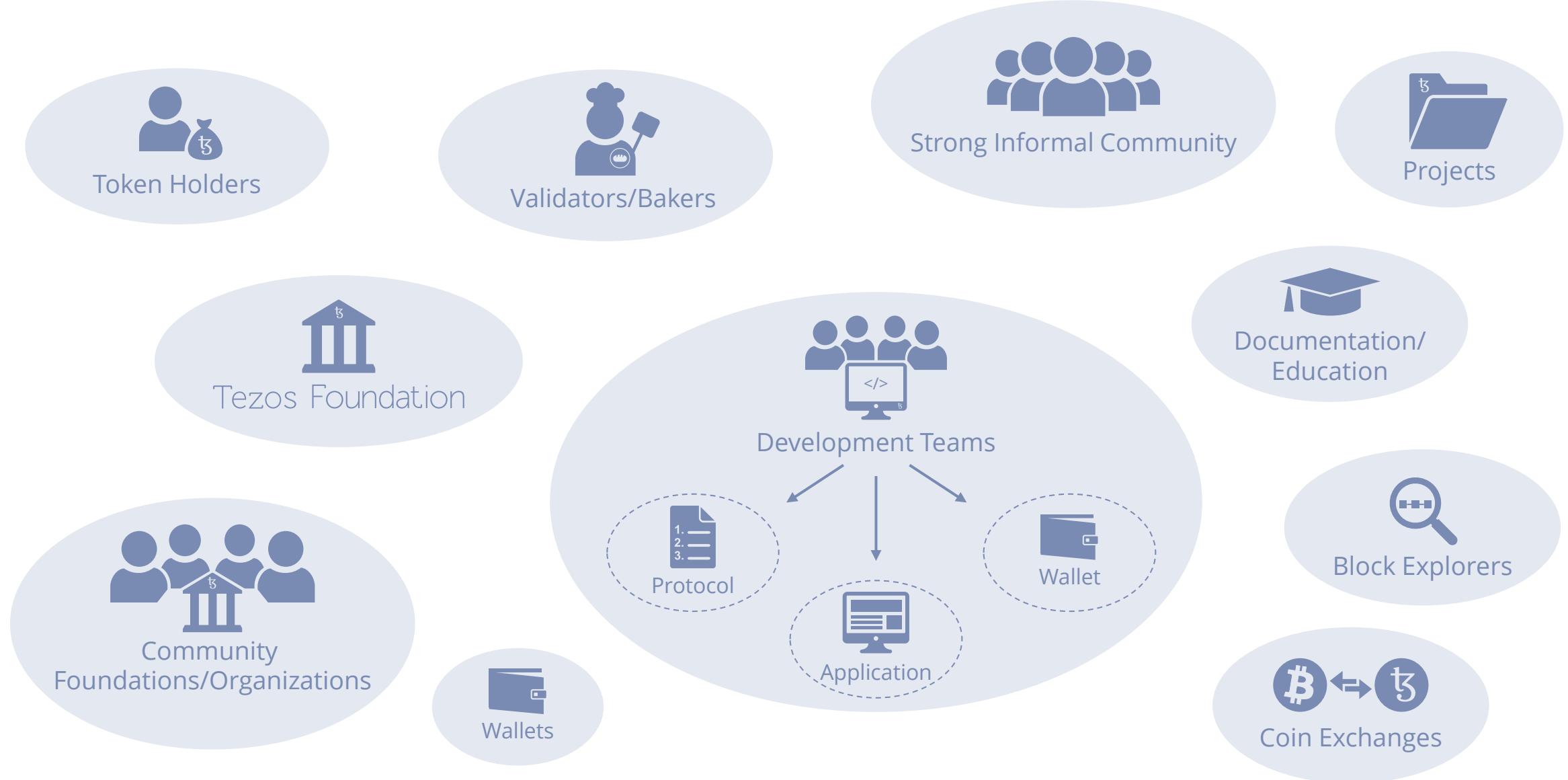
- Hangzhou is the **eighth successful amendment** to the Tezos protocol through the on-chain governance mechanism currently in adoption phase and will be **activated on 2021-12-03**.
- It was jointly developed by [Nomadic Labs](#), [Marigold](#), [DaiLambda](#), [Oxhead Alpha](#) and [Tarides](#).
- Noteworthy [changes](#) that will be brought in with Hangzhou are:
  - ▶ **Liquidity baking** is extended approx. until the end of the next protocol amendment phase.
  - ▶ **Gas improvements** and general gas cost adjustments.
  - ▶ **Context Storage Flattening**: a new, more performant data schema for the ledger state resulting in 78% faster I/O. The explosive growth in overall contract calls and NFTs on Tezos means that the size of context is constantly growing.
  - ▶ **Smart Contract Context Cache**: in-memory context providing fast access to the most recently used values reducing gas consumption.
  - ▶ **Global Constants**: users can use constants to originate larger contracts, as well as share code between them.
  - ▶ **Michelson On-Chain Views**: read-only contract storage access is synchronously available on the stack with a new instruction set.





# TEZOS ECOSYSTEM & HISTORY

# The Tezos ecosystem unraveled: the different roles and actors that constitute Tezos



# What is the Tezos foundation and what is its mission?

## Our Vision



We seek to **empower** persons and entities from all over the world to create a **robust and decentralized digital commonwealth**.

## Our Mission



We believe Tezos will **fuel social, political, and economic innovation** on a global scale. Our core mission is to **support the Tezos protocol and ecosystem** in service of this goal.

## Our Strategy



We **deploy resources** to help **facilitate the advancement of the Tezos protocol and growth of the Tezos ecosystem**.

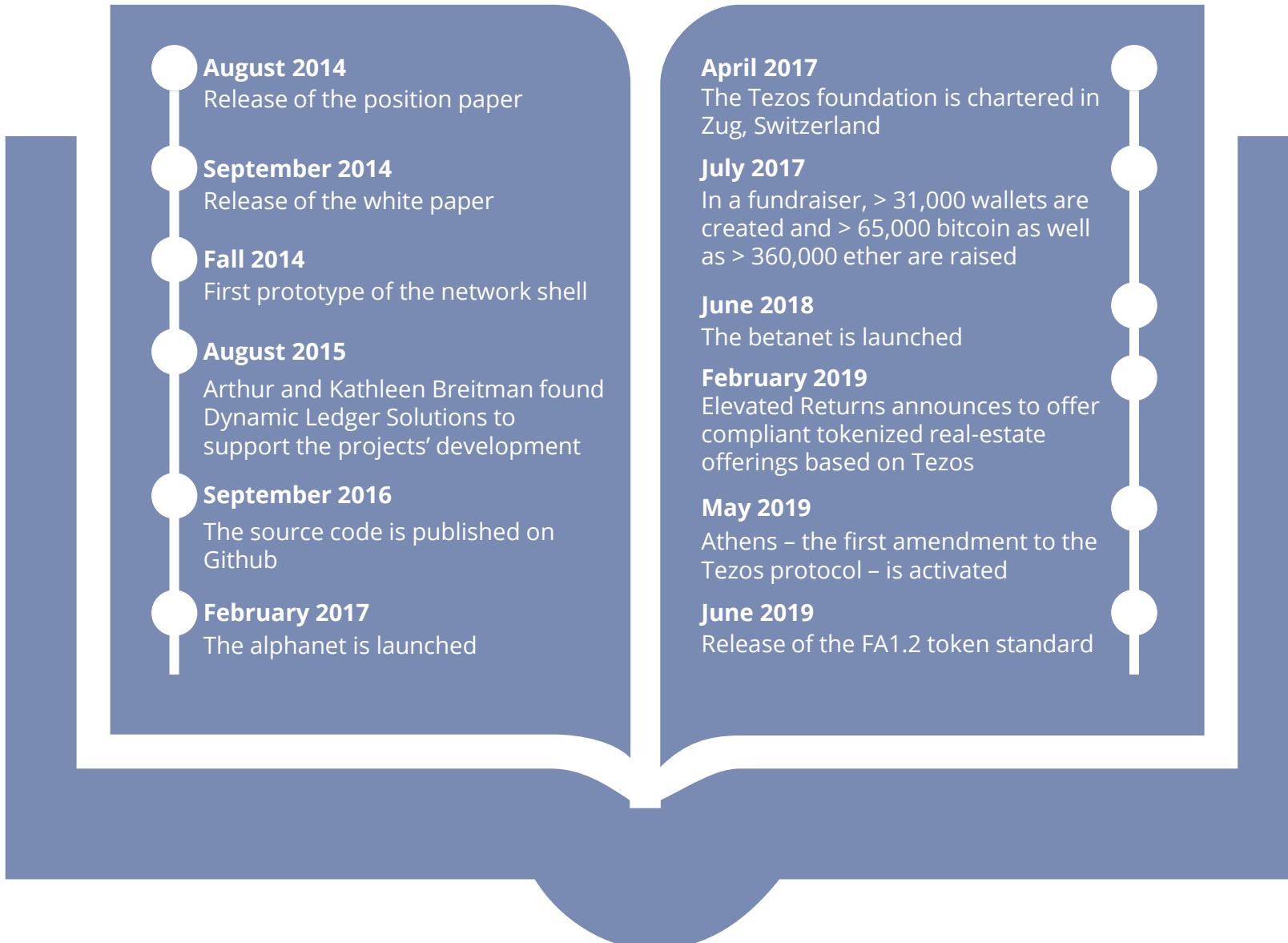
Tezos is a distributed, peer-to-peer, permissionless network. **No single entity owns, manages, or controls "Tezos."** Understanding this paradigm is fundamental to understanding Tezos.

## Tezos Foundation

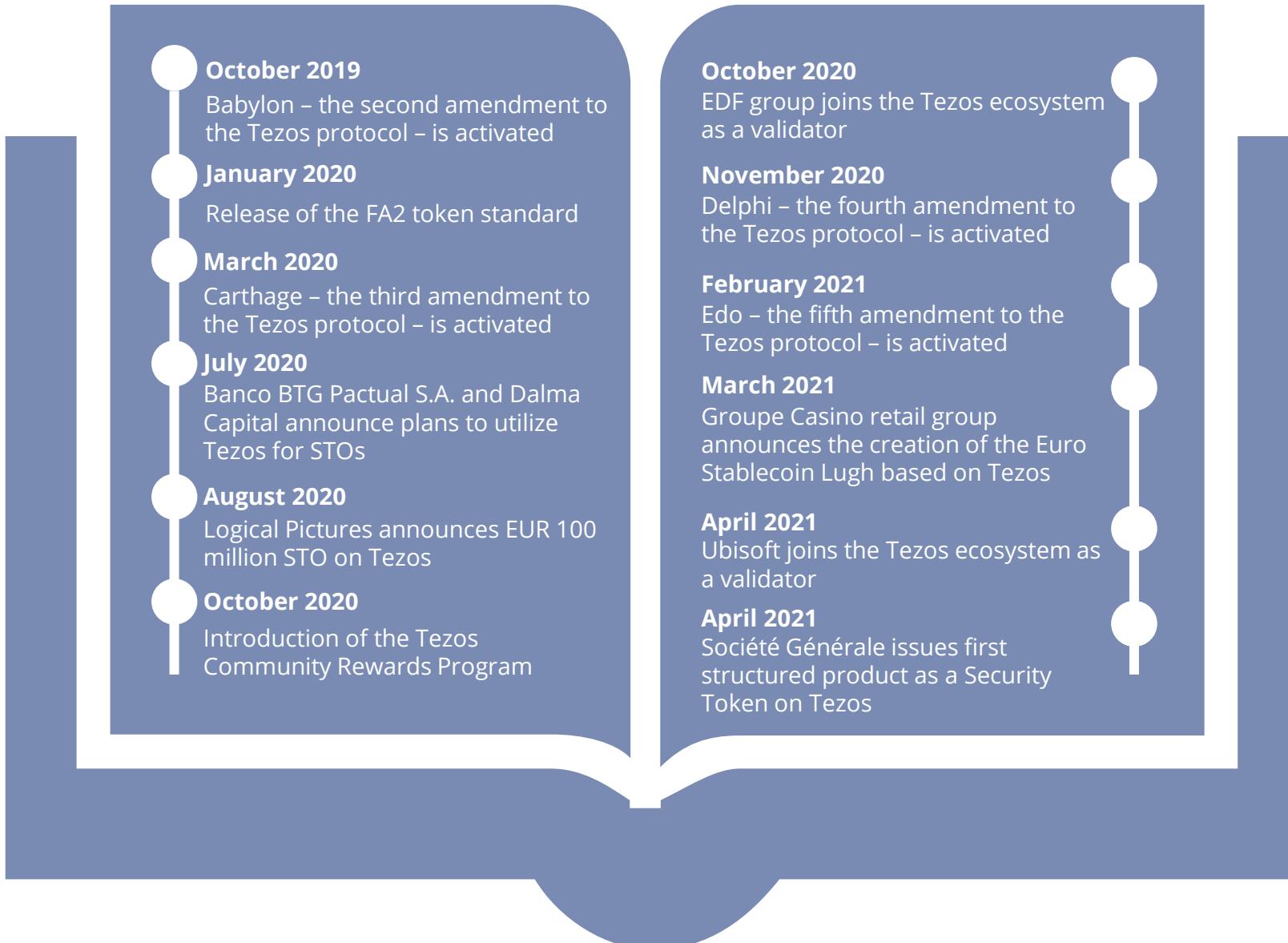
As highlighted in the [\*\*Tezos position paper\*\*](#), the success of any decentralized network is determined by the efforts of a **robust, diverse, and flourishing community**.

Tezos' potential rests in the hands of its **community**, and we have no doubt that the Tezos community is **among the strongest and most exceptional** in the cryptocurrency ecosystem.

# A brief history of Tezos and the Tezos foundation (1/3)



## A brief history of Tezos and the Tezos foundation (2/3)



## A brief history of Tezos and the Tezos foundation (3/3)



# To support the advancement of the Tezos ecosystem, the foundation awards grants



Areas of interest that may be eligible for funding through grants by the Tezos Foundation and information on the evaluation process can be found on the [Tezos Foundation's website](#):

- Process:
  1. Application and initial vetting by contributors from the Tezos ecosystem.
  2. Technical Due Diligence by the Tezos Foundation's Technical Advisory Committee (TAC)
  3. Final Decision by the Executive Committee or the Tezos Foundation Council
  4. Communication of final decision and completion of necessary formalities.
- Areas of Interest:
  - ▶ Baking → [Target List](#)
  - ▶ Developer Experience → [Target List](#)
  - ▶ Education and Training → [Target List](#)
  - ▶ End-User Applications → [Target List](#)
  - ▶ Privacy → [Target List](#)
  - ▶ Security → [Target List](#)
  - ▶ Other

To apply for a grant, use the [Tezos Foundations Grant proposal website](#).

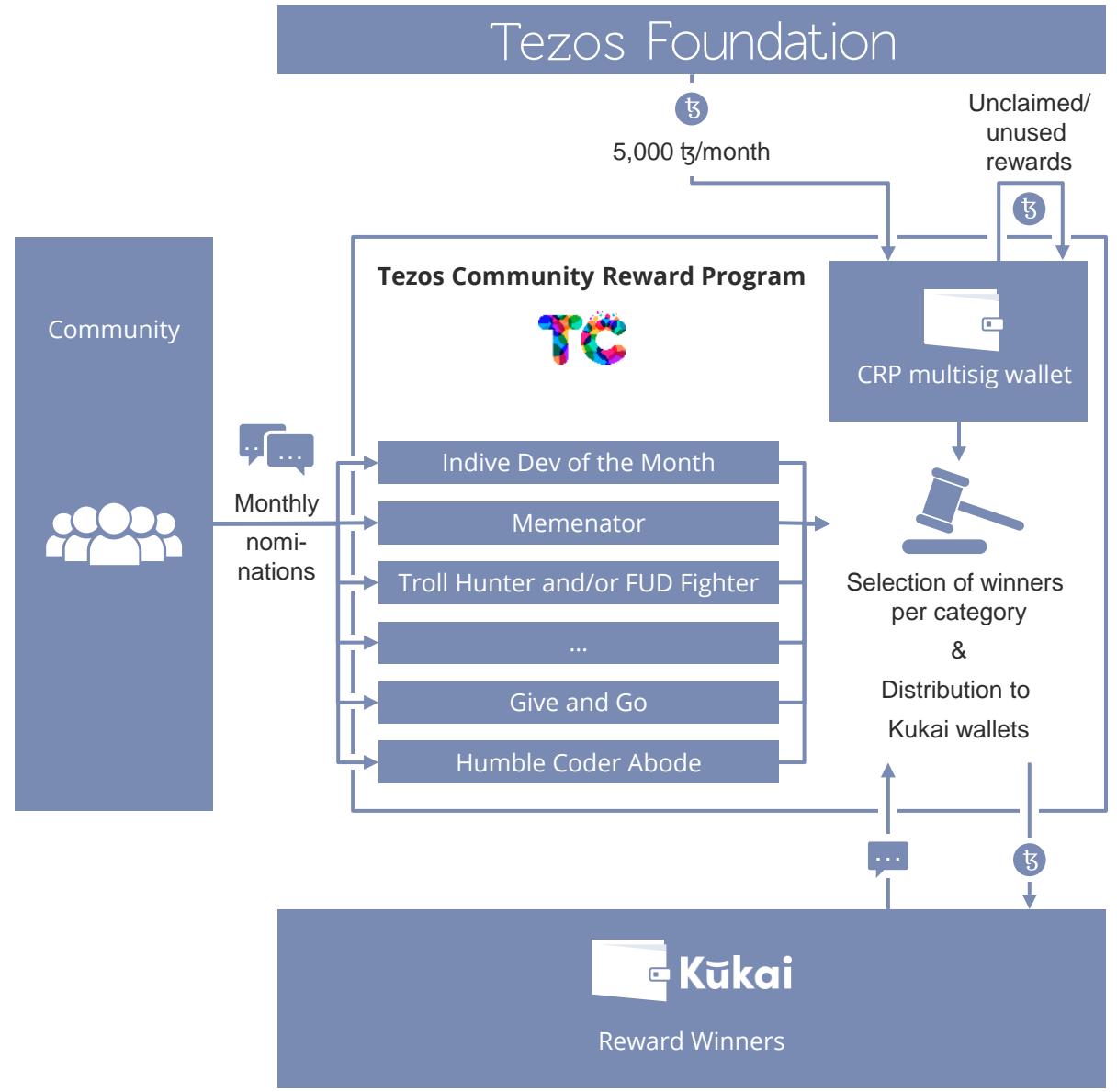
## GRANTMAKING PHILOSOPHY

As the **steward of the funds** gathered during the donation period, we **support** groups in the Tezos ecosystem that actively **work to advance the project** in a variety of ways. **Grants** offer a strategic way to support other stakeholders and community members, such as **educational and research institutions, developers, and enthusiasts** from all over the world as they work to advance the project.

Tezos Foundation

# Tezos Community Rewards

- The **Tezos Community Rewards Program (CRP)** is an evolving rewards program that aims to incentivize active community participation by rewarding exceptional contributions to the Tezos ecosystem along an evolving list of award categories.
- The CRP was announced in September 2020 and first rewards have been distributed to community members for contributions made in October 2020 where there were already 220 submissions of nominees.
- With a funding of **5,000 tʒ per month**, provided to a multisig contract by the **Tezos Foundation**, the program is run by **Tezos Commons** through reviewing nominations, selecting winners and distributing the rewards.
- Community members are **nominated by fellow community members** for their contributions in one or multiple award categories within the month the reward is paid for through using an [online form](#) to provide contact information, category for nomination, and evidence of the nominee's contributions.
- The total reward pool is split among winners along the various categories where most categories can have **up to three winners** (more in selected categories) with some categories having a ranking of winners while others split the rewards evenly between all winners.
- The reward winners selected by the Tezos Commons judges for factors such as quality and quantity of submissions and activity, and verifiable proof of activity done by the nominee, need to **claim their rewards** within **72 hours** and receive the reward via DirectAuth/ **Kukai Wallet** (unclaimed or unused rewards are rolled back into the overall pot that is used to fund the CRP).





# NON-FUNGIBLE TOKENS ON TEZOS

# Of Tokens and Fungibility: What are NFTs?

- A **token** is a **digital representation** of an **asset** or **utility**.
- Depending on its use, a token may be classified as a **currency**, **utility**, **security/equity**, **reward** or **asset** token and require corresponding **properties**.
- The property of **fungibility** is a fundamental characteristic to distinguish token types:
  - ▶ **Fungible tokens** are interchangeable, meaning that there are multiple instances of the same token that are not distinguishable, e.g. crypto currencies, voting tokens, staking tokens, etc.
  - ▶ **Non-fungible tokens (NFTs)** are not interchangeable, meaning that they are unique and they are indivisible, e.g. digital art, etc.
- While a token automatically becomes non-fungible when its **transferability** is restricted, NFTs can also be (and often are) transferable: It makes sense to tie a token's existence to its owner in case of badges, academic certificates, etc. while the value of NFTs representing art, game items, etc. is derived from their tradeability.
- Owning an NFT does not usually go along with owning the **copyright** of the underlying asset in a legal sense, so the creator of a piece of art can still create copies of (or even destroy) it.
- Just like it is the case with crypto currencies, **an NFT does not have an intrinsic value**. The value is created by the people attributing a value to and willing to pay for it.
- NFTs can be held in **wallet** applications in the same way that you hold fungible tokens like crypto currencies.

## Fungible Tokens

(*interchangeable; identical value*)



Typical applications/use cases:

*Crypto currencies, voting tokens, staking tokens*

## Non-Fungible Tokens (NFTs)

(*not interchangeable; unique*)

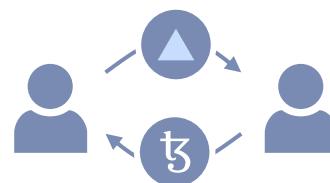


Typical applications/use cases:

*Digital representations of art, music, film, collectibles, items in digital games, certificates in academia, badges*

## Transferable NFTs

(*tradeable*)



## Non-transferable NFTs

(*tied to their owner*)



# NFTs on Tezos: The FA2 token standard

- Basically, a token is nothing more or less than a **smart contract** and theoretically, everyone could use the Tezos blockchain as a platform on which to create arbitrary tokens.
- However, in order for the token to work within the ecosystem, it makes sense to abide by **a common standard** that determines a unified interface, possible token types, and standardizes permissions.
- To that end, the **token standard FA2** ("financial application") has been developed for the Tezos ecosystem and introduced with [TZIP12](#).
- FA2 is agnostic to token type (allows fungible, non-fungible tokens, non-transferable, and multi-asset tokens) and allows both single and multi-token contracts via one standard API. It standardizes:
  - ▶ **Transfer semantics**
  - ▶ **Metadata**
  - ▶ **Accessing balances**
  - ▶ **Total supply**
  - ▶ **Permission rights**
- Permission rights are the rules that determine who can send how many tokens, receive them, and manage tokens for other users. There are three **architecture patterns** how permission rights can be done:
  - ▶ **Monolith**
  - ▶ **Transfer hook to another contract**
  - ▶ **Separate wrapper contract**

## FA2 Standard



Balance between overspecification (surprising expressivity) and underspecification (undermining standardization)



Allows fungible tokens  
(equivalent to ERC-20 on Ethereum)



Allows non-fungible tokens  
(equivalent to ERC-721 on Ethereum)



Allows non-transferable tokens  
(equivalent to ERC-1238 on Ethereum)



Allows multi-asset contracts  
(equivalent to ERC-1151)

### Standardizes:



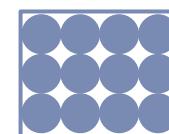
Transfer semantics



Metadata



Accessing balances



Total supply



Permission rights



Transfer Hook



Wrapper



Monolith

# NFTs on Tezos: Why choose Tezos?

## Clean NFTs

Compared to Bitcoin, Ethereum and other PoW-Blockchains, Tezos has a neglectable carbon footprint thanks to its energy efficient LPoS sybil resistance mechanism.

*"What prompted me to look for other platforms and discover Kalamint was first and foremost the huge minting fees on platforms using Ethereum. Using Tezos to tokenise artworks is an undeniable advantage."*

↗ **NFT artist MAIKEUL in a Medium interview with Kalamint**

*"Gas prices from the Ethereum network are not going to stabilize any time soon."*

↗ **NFT artist Cripéra on a Medium interview with Kalamint**

## Fast Transactions

Transactions on Tezos are fast in blockchain dimensions. The update of the consensus algorithm Emmy+ to Emmy\* did speed up finality even further

*"I cannot wait to release my first Juicy Drops collection. [...] However, I want to be mindful of environmental concerns and accessibility to all of my fans before we go live. Happy to now be working with OneOf, who is addressing both of these issues."*

↗ **Doja Cat about Tezos-based OneOf**

## Low Costs

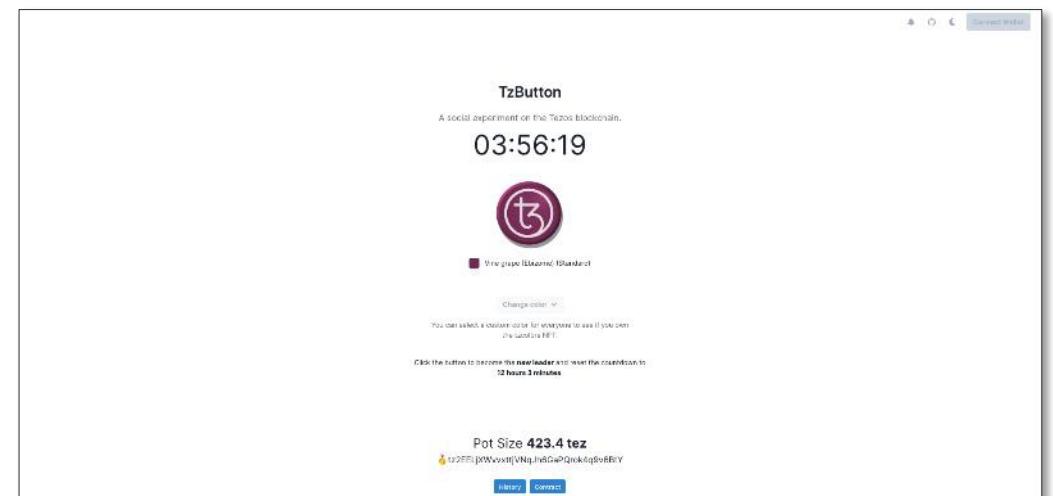
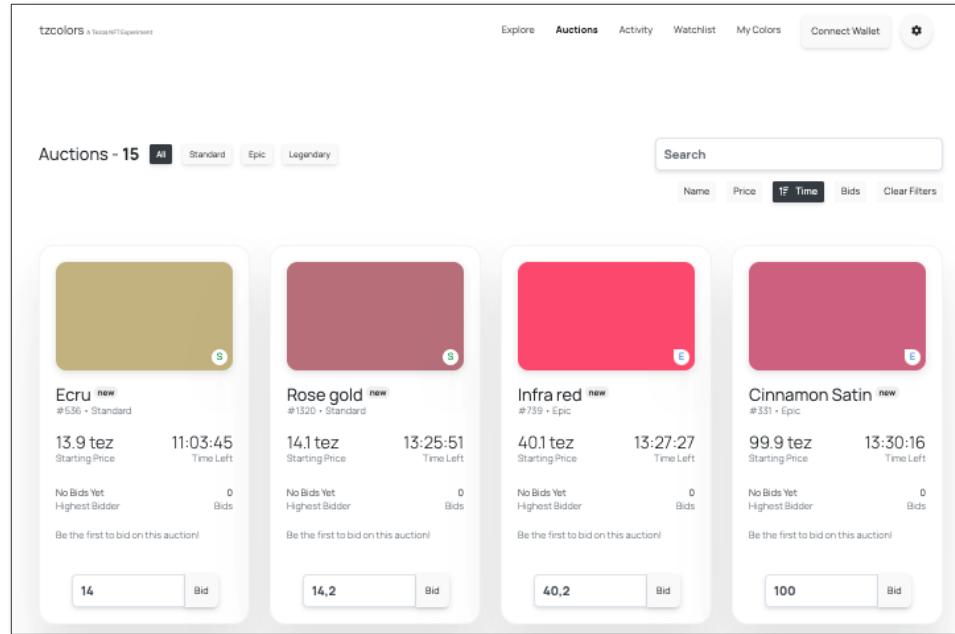
Compared to other Smart Contract platforms like Ethereum, Tezos has an unbeatable cost structure thanks to its scalability and continued efficiency improvements brought about with on-chain governance technology updates.

*"Tezos has important qualities that can be similarly valued by Ethereum's standards. High decentralization and thus safe, secure and trustless. Tezos combines that quality with fast transactions and a high TPS (~121)."*

**Allen Walters on Cryptoslate**

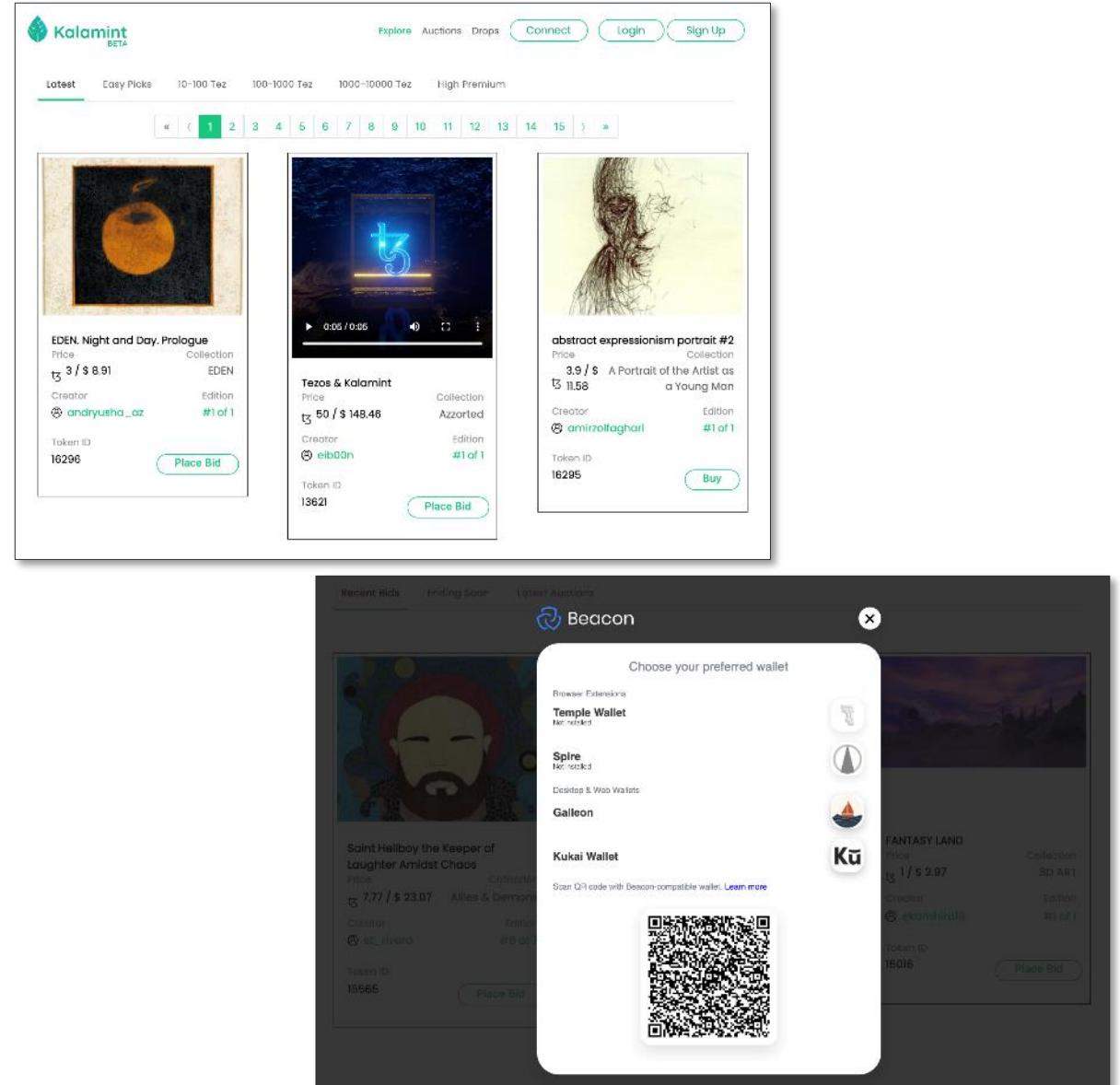
## NFTs on Tezos: tzcolors

- **tzcolors** is an experimental project that was conducted to showcase the latest technology available in the Tezos ecosystem: **FA2-based NFTs**, an **auction house contract**, **Beacon** dApp to Wallet communication, and **Taquito** for contract abstraction in the frontend.
- It is an **NFT marketplace** where a total of **1690 unique colors** that were taken from [Encycolorpedia](#) can be traded in three categories: **Standard** (1530), **Epic** (128) and **Legendary** (32).
- With the launch in **February 2021**, all colors were immediately available for purchase in **initial auctions** where the minimum bid was **1 tz**.
- Auctions last **5 days** and are **extended by 5 minutes**, if a bid is placed during the last five minutes.
- All proceeds from the initial auctions are accumulated in the corresponding contract and it is planned that the color owners shall have a say in their use while at least some of them are planned to be given to the developers of the required tooling.
- Color owners receive **100%** of the proceeds when reselling their color.
- Tzcolors supports Temple, Spire, Galleon and Kukai **wallets** via **Beacon** integration and color NFTs could be used in future **dApps** in the Tezos ecosystem as demonstrated by the social experiment [\*\*TzButton\*\*](#).
- As the **first NFT application on Tezos**, tzcolors has received a lot of attention and close to **10,000 transactions** have taken place on tzcolors as of July 2021.



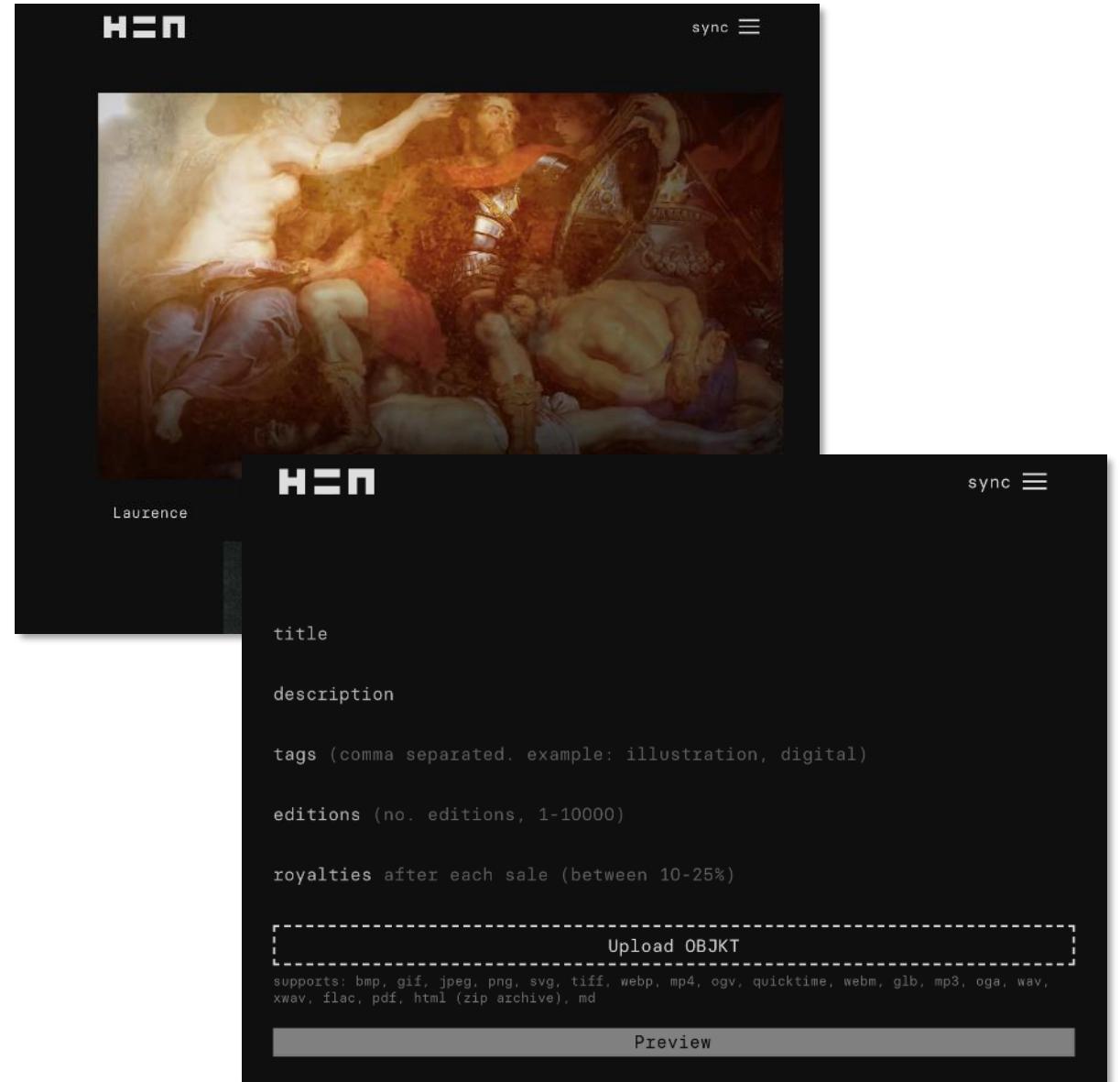
# NFTs on Tezos: Kalamint Kalamint

- Kalamint is a marketplace for **art NFTs** on Tezos and was launched in **February 2021**.
- The platform lets users mint, buy and sell NFTs native to Tezos using the **FA2 token standard**.
- The name **Kalamint** is derived from the words **Kala** (representing art in almost all of the languages native to the Indian subcontinent) and **Calamint** (any aromatic Eurasian plant of the genus Satureja/ Calamintha, having clusters of purple or pink flowers) and meant to represent “art”, “freshness” and “colour”.
- Preceeding the mainnet launch, Kalamint was tested on the Tezos testnet from the end of December 2020.
- The Kalamint team chose to start with a minimum viable feature set in **V1** (mint, buy, sell NFTs based on FA2) and to **roll out new features** like the **creation of collections (limited editions)**, **auctions**, **price discovery curves** and **DAO** in “baby steps”.
- Since then, the team has worked hard and rolled out the promised **auction feature** in **May 2021**.
- Kalamint also issued the **\$KALAM token** (total supply 1,000,000) which has been used as a **reward** on the platform (e.g. for early adopters), can be used for **liquidity mining/farming**, as **payment** on the platform, for **governance** and was **listed on QUIPUSWAP** in **June 2021**.
- Kalamint currently supports the following **wallets**: Temple, Spire, Galleon and Kukai.



# NFTs on Tezos: hic et nunc

- **hic et nunc** (also H=N) is latin for “here and now” and the name of a Tezos-based art NFT platform that was launched (in its alpha phase) on **March 1st, 2021**. NFTs are called **OBJKT** on hic et nunc and next to images, hic et nunc also supports **interactive** and **AR** NFTS. The project is transforming into a [\*\*community movement\*\*](#).
- From its launch in March to mid-April, hic et nunc distributed its **hDAO media governance token** (by matching the amount of t3 passed from buyer to seller in each transaction and splitting the corresponding hDOA tokens equally among buyer and seller), which can only be bought on **Quipuswap** since.
- Like the NFTs, the hDAO token abides to the flexible **FA2 standard**. Its total supply is **651,000** and next to the **token economics**, its use is intended for **upvoting OBJKTs** (curating) and general **governance** on the platform.
- hic et nunc is very **community-driven**, invites **anyone** to contribute and propagates a “**NFT Creators Code of Conduct**” that appeals to the mintors’ honesty and condemns **copyminting** (minting someone else’s work without their knowledge and blessing) and reminting (e.g. across different NFT platforms/blockchains).
- To celebrate **10,000 minted OBJKTs**, on the weekend of **March 26<sup>th</sup>, 2021** with the hashtag **#OBJKT4OBJKT** users were encouraged by Twitter handle **@DiverseNftArt** to give NFTs away for free in order for users to build their collections without a cost.
- As of **July 2021**, hic et nunc has seen more than **1,500,000 total transactions** and **22,000 total users** and supports Temple, Spire, Galleon and Kukai **wallet** via **Beacon** integration.



# NFTs on Tezos: Tezos Domains



Tezos Domains

- **Tezos Domains** is a platform that leverages **FA2-based NFTs** to register meaningful and **user-friendly aliases** to a Tezos address in a globally consistent way.
- Tezos Domains was launched in **April 2021** after a **sunrise period** where **bakers** and **Tezos-related open-source projects** had the opportunity to claim their Tezos Domain.
- After the launch, all domains with **5+ characters** were eligible for purchase via **auctions** and have been available for **first-in-first-served** (FIFS) registration since May 12th, 2021.
- Names with **less than five characters** are available since **Q3 2021**.
- Among the design principles were **price and distribution fairness**, **disincentivation of name squatting/speculation**, **usability** (easy to read, pronounce, communicate), **security** (e.g. spoofing).
- The **top-level-domain** (TLD) controlled by a multisig contract planned to eventually migrate to a DAO is **.tez**.
- The **second-level-domains** are subject to **auctioning/FIFS** registration.
- **Third-and-higher-level-domains** can be **created and managed at the user's leisure** (i.e. the owner of the second-level domain).
- Tezos domains are **censorship resistant** as they do not rely on third parties like Google Domains or Go Daddy.
- Tezos Domains supports **all major wallets** via **Beacon** integration and names are displayed in wallets instead of cryptic addresses.



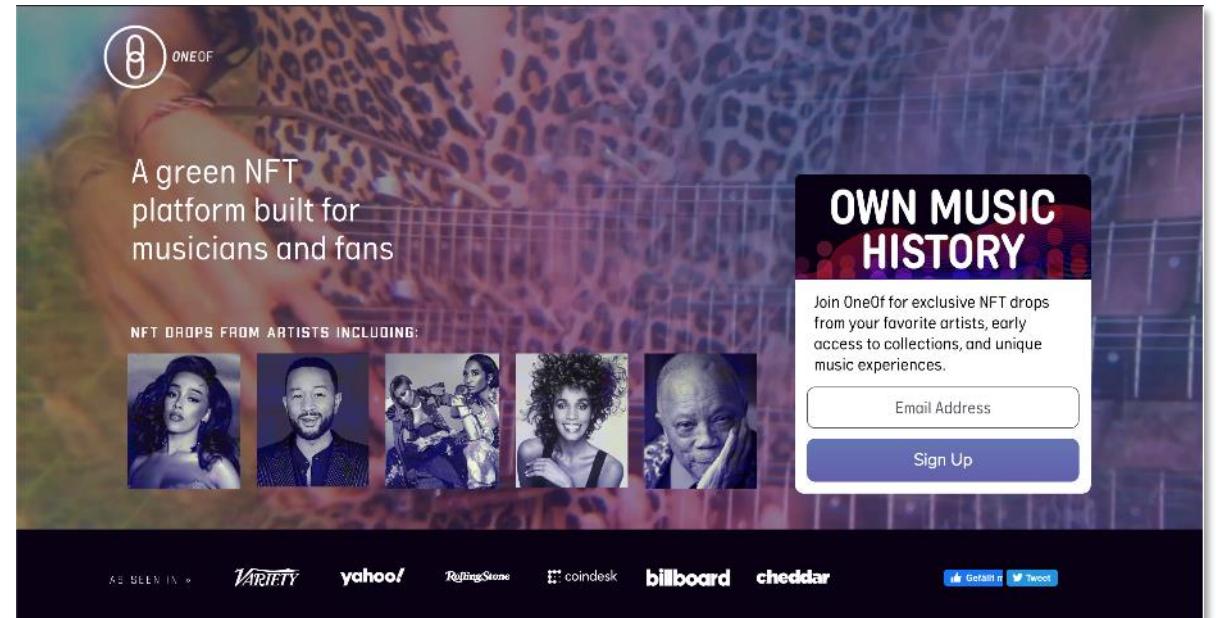
The screenshot shows the Tezos Domains homepage. At the top right are links for "About", "Developers", and "Manage". The main title "Friendly Names Now on Tezos" is prominently displayed. Below it, a subtext encourages users to use names like "alice.tez" instead of addresses like "tz1VBLpuDKMoJuHRLZ4HrCgRuiLpEr7zZx2E". A search bar with a "Search" button is present. The page features several icons with descriptive text:

- Easy to share**: Forget copying and pasting long addresses. Share your .tez name instead!
- Make transacting a breeze**: Just enter the recipients .tez name. No more stress about sending to the wrong address.
- Naming for wallets**: Have other people's wallets display your name when you send them money, and vice versa.
- Decentralized and under your control**: Tezos names are FA2-compliant NFTs which you own and control. Just like cryptocurrency, your names are stored securely in your wallet and only you can manage and move them.
- Open source & cryptographically secure**: Domain names are stored on the Tezos blockchain. Audited, open source smart contracts ensure that sending funds to a Tezos domain name is as secure as sending to a regular address.

## NFTs on Tezos: OneOf



- **OneOf** is a Tezos-based **commercial** platform for **music NFTs** announced to launch in **summer 2021** and has recently raised **\$63M** of funding from a seed round.
- It is – among others - backed by **Quincy Jones** and has already secured **212 big-name NFT drops** for the first 12 months, the estate of **Whitney Houston, TLC, Doja Cat, John Legend** prominent among them.
- While the NFTs will be Tezos-based, OneOf will accept payments both in (other) **crypto** and **135+ fiat currencies** to make the platform accessible to a wide audience.
- Tezos' **eco-friendliness** due to its **low energy consumption** and its comparatively **low transaction costs** were not only the basis for OneOf's decision to build on Tezos, but also serve as the basis for **convincing artists to mint their NFTs on OneOf**.
- OneOf announced to donate 5% of revenue from every sale to a charity of the artist's choice or an environmental cause partner and committed to zero minting costs (while there will be a commission on every transaction made on the marketplace).
- OneOf will provide **onboarding support** for artists willing to bring their NFT vision to life and plans on **supporting influential new voices** through financial commitments and marketing support with their **Emerging Artist Spotlight Program**.
- To empower **artists of every career level**, there will be different tiers from "**one-of-one tokens**" to "**one-of-one-hundred-thousand tokens**".



# NFTs on Tezos: There's more - NFT Applications and Marketplaces in the Making



## Emergents



Digital Collectible Card Game

## RedBull Racing



NFT Fan Experience

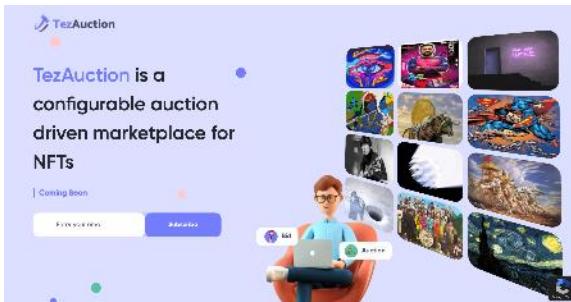
## McLaren Racing



NFT Fan Experience

The NFT space on Tezos is **evolving rapidly** and there are more NFT applications and marketplaces already existing or in the making. Here are **just some of them...**

## TezAuction



Multi auction type NFT marketplace

## D-art



Digital Art NFT Marketplace

## Bazaar



amplify<sup>NFT</sup>



## Truesy

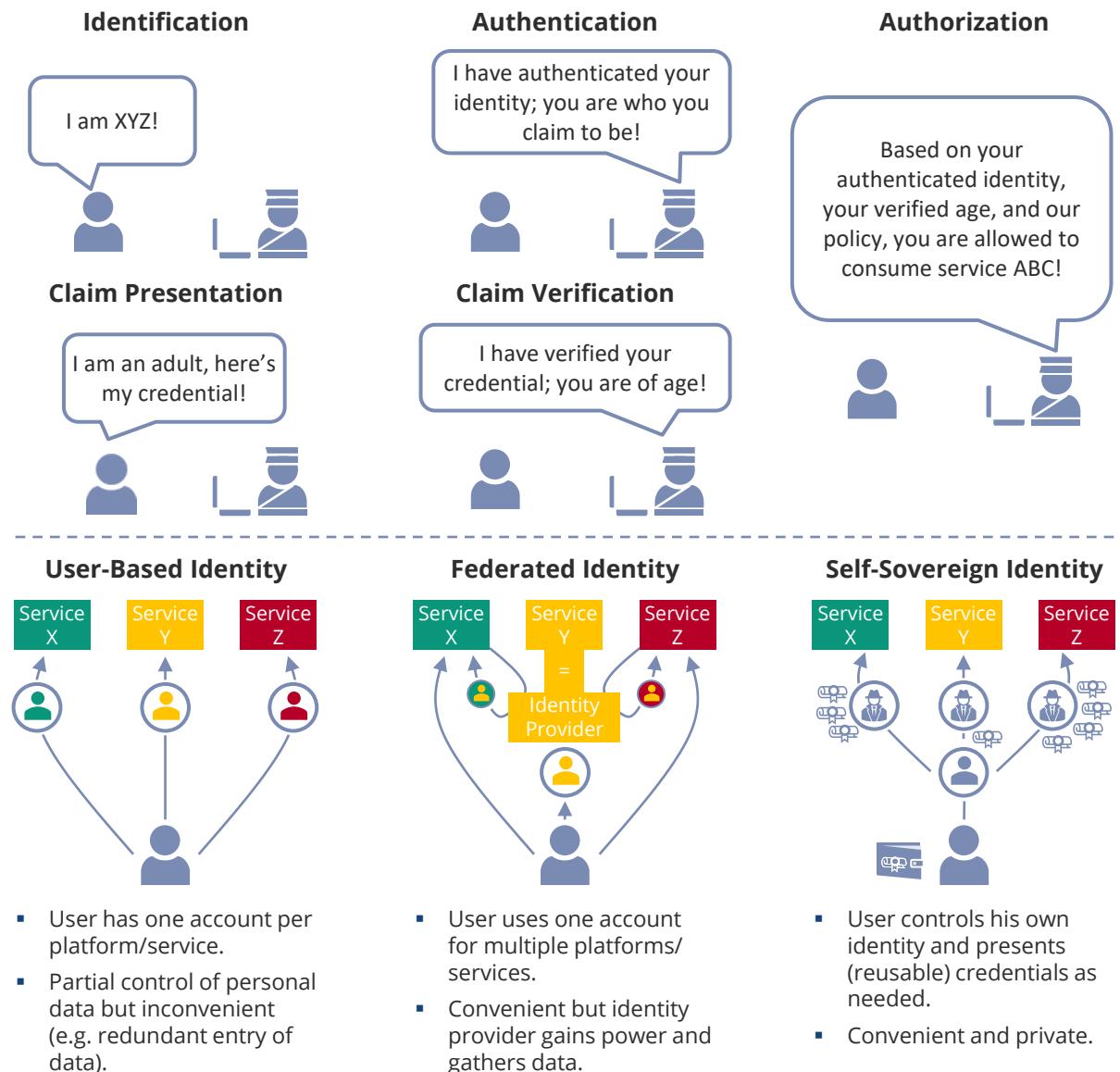




# SELF-SOVEREIGN IDENTITIES ON TEZOS

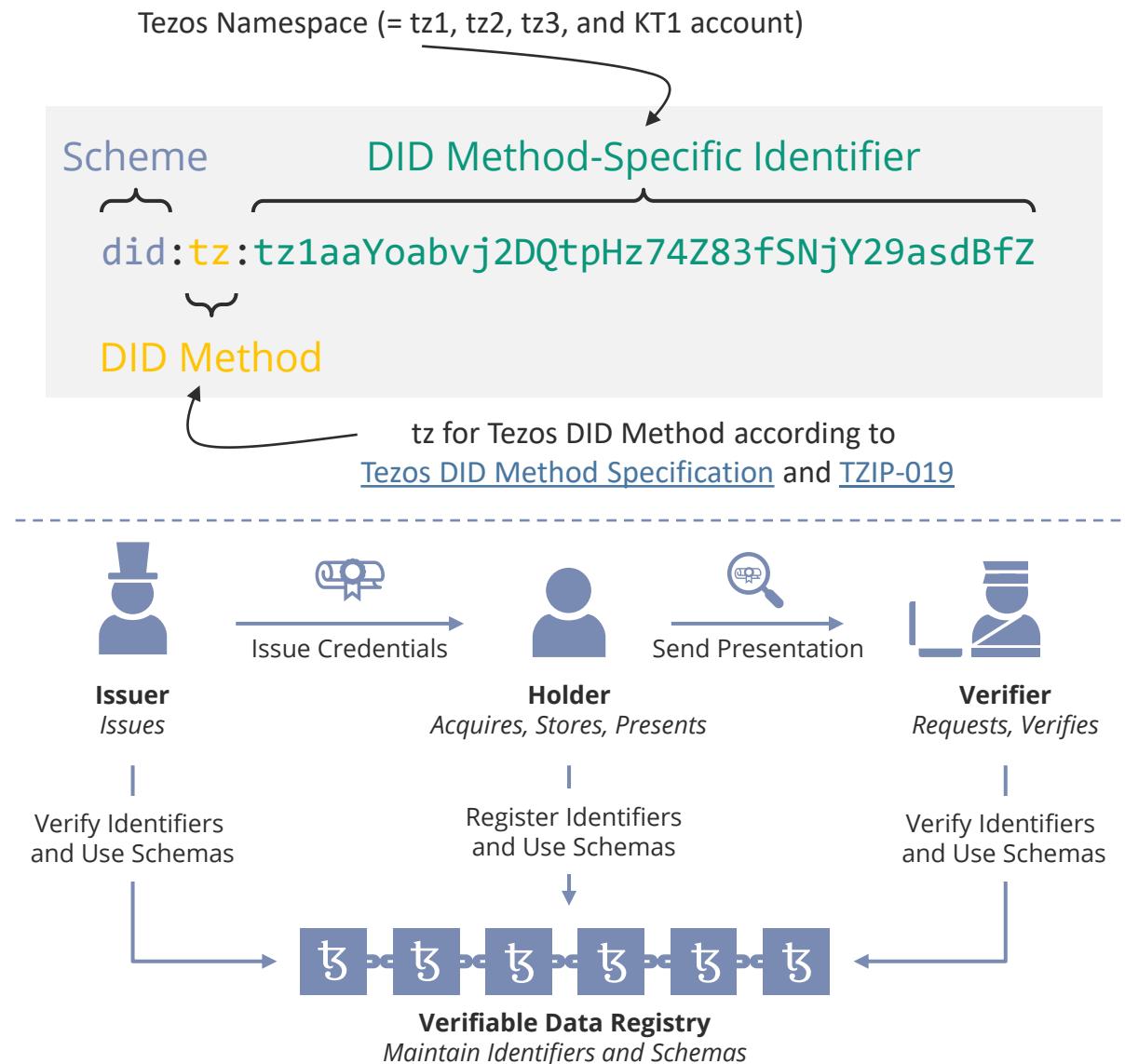
# SSIs on Tezos: What are Self-Sovereign Identities?

- Trusted **digital identities** are a crucial **foundation** for many services in today's digital world, including (but not limited to) blockchain applications.
- They are required to
  - identify** people, things (e.g. IoT devices), private and public/governmental organizations, etc. ("Who are they?").
  - authenticate** these identities ("Are they who they claim to be?").
  - verify claims** about attributes associated with their identities ("Is it true what they claim about themselves?").
  - authorize** access for these identities, e.g. to restricted services, data, etc. based on their identity and/or attributes associated with their identity ("Should they be allowed in?").
- Digital identities have evolved from **centralized** and **user-based** to **federated solutions** where users can use their credentials from well-established identity providers to log in to third-party services.
- However, federated identity solutions give an insane amount of **data** and **power** to the **identity provider** (e.g. which other services does user x use or which services can use the providers identity service?).
- The new paradigm of **self-sovereign identities** (SSIs) aims to give control over their identity and data back to the users.
- Although the concept itself is **technology-agnostic**, blockchains can be used as an important **building block** for SSI solutions due to their decentralized nature and their immutability.



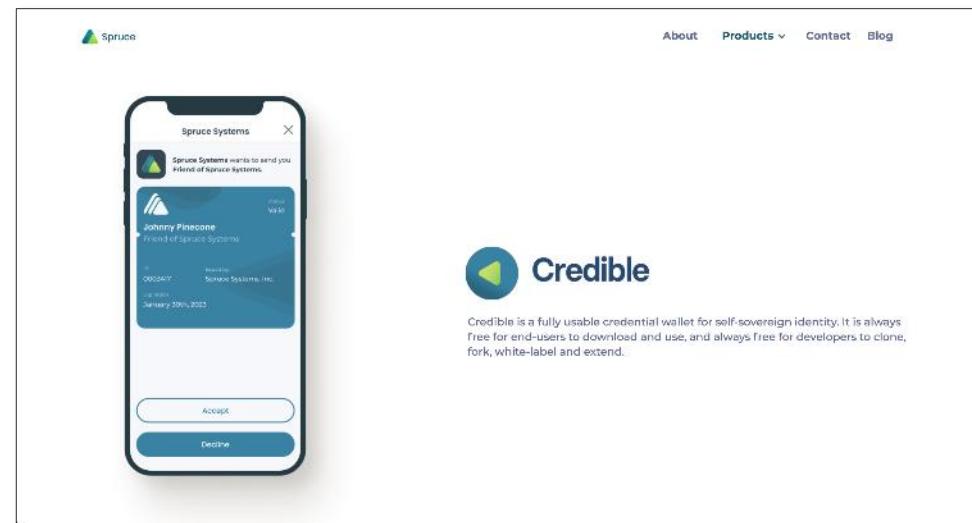
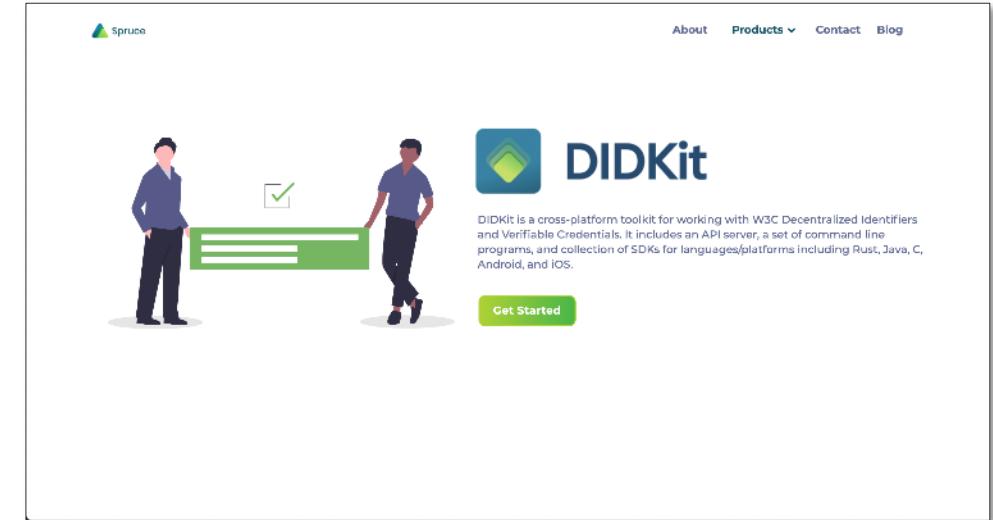
# SSIs on Tezos: Concepts and Standards around SSIs

- There are two emerging **W3C standards** that are shaping the way SSIs are being implemented: [Decentralized Identifiers \(DIDs\)](#) and [Verifiable Credentials \(VCs\)](#).
- DIDs** enable verifiable, decentralized digital identities. They refer to **subjects** (persons, organizations, things, etc.) as determined by the DID's **controller** and have been designed to be **decoupled from centralized registries, identity providers, and certificate authorities**.  
While third parties might be used to help enable the discovery of information related to a DID, the DIDs controller can prove his control independently.
- DIDs** are URIs that associate a **DID subject** with a **DID document** that can be used to prove control over the DID or interact with the DID subject in a trusted way. They consist of three parts: **1) The URI scheme identifier**, **2) the identifier for the DID method** (tz for Tezos) and the **DID method-specific identifier** (a Tezos address for Tezos).
- VCs** are a mechanism to digitally express **(machine-)verifiable assertions** about a (DID) subject in a **cryptographically secure** and **privacy respecting** way.
- An **issuer** (e.g. a government) can **assert** or **revoke** a **claim** about a **subject** (e.g. "is a citizen of country XYZ") using VCs.
- Its **holder** (who may be the subject but could also be a guardian, like a parent) can produce a **verifiable presentation** from his VCs that a **verifier** can verify using the presentation and a **verifiable data registry**, e.g. a distributed ledger like the Tezos blockchain.



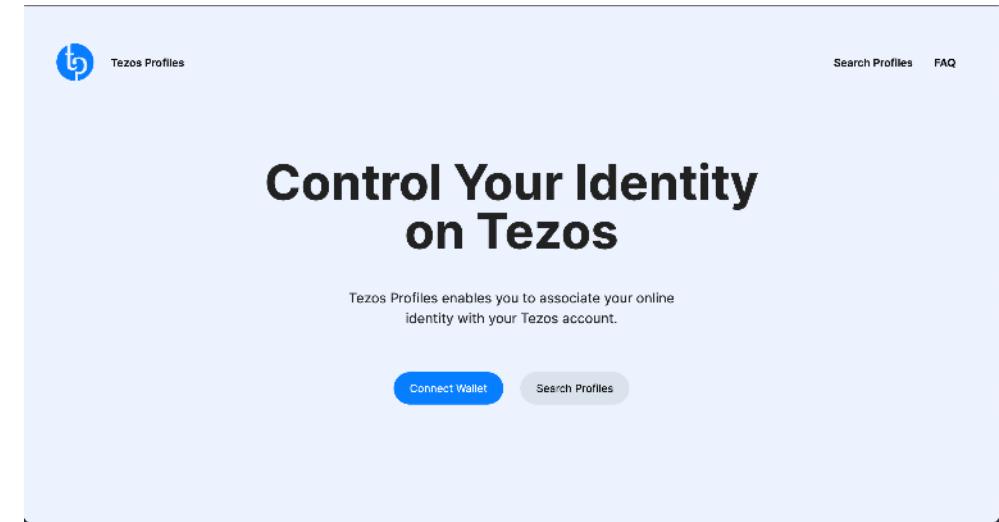
## SSIs on Tezos: Spruce Systems

- **Spruce Systems** is a company that envisions to “go from untrusted data to **verifiable information** that can be **shared privately** and **with consent**” and that is committed to **open source software** (usually published under Apache License, Version 2.0).
- **Spruce** is a member of **W3C** and actively contributing to the development of the **DID** and **VC standards**.
- Based upon these standards, Spruce is building a **suite of tools** and **Tezos-specific specifications** to bring **SSIs to the Tezos ecosystem**:
  - ▶ The **Tezos DID Method** that maps DIDs directly to the Tezos name space (tz1, tz2, tz3, and KT1 account addresses prefixed with did:tz).
  - ▶ The **DIDKit** for working with W3C DIDs and VCs across different platforms.
  - ▶ The wallet **Credible** and its **Kukai integration** to store credentials.
  - ▶ The data takeout **Rebase** allowing users to download their information and prove their verified activity history, reputation, and account data
- While being visionary, Spruce is also **pragmatic** and believes in integrating with existing identity solutions rather than replacing everything at once. Hence, they are also building:
  - ▶ **Keylink** to link existing enterprise accounts to keypairs.
  - ▶ The smart onboarding tool for businesses, **Intake**, for secure document collection and processing.



## SSIs on Tezos: Tezos Profiles

- **Tezos Profiles (TZP)** was built by **Spruce Systems** based on their previously introduced tools.
- It is a **web application** that aims at empowering Tezos users to regain control of their digital identity for use across platforms by allowing users to create portable verified profiles.
- **Verification** is done by **demonstrating control** over their **public social media** and by **self-attesting information**. These verified profiles are then **linked to Tezos accounts**, allowing any platform to resolve and establish trusted information to mitigate identity fraud:
  - ▶ A user connects a Temple/Spire/Galleon/Kukai wallet via Beacon integration and chooses a Tezos address within that wallet.
  - ▶ The user fills in a basic profile with information about himself (an alias, a description, a website URL and a URL to a logo image)
  - ▶ The user verifies his identity by posting a predefined Tweet on Twitter and providing the link to that Tweet, thereby demonstrating control over the given Twitter account.
- A first **use case** has arisen with the accelerated growth of **NFT** adoption, **creator impersonation** and **copyminting**: many buyers have become unsure, if an NFT is being sold by its true creator.
- **TZP** allows creators to attest to their own “reusable” identity and credentials instead of recreating their identity across platforms in a fragmented way.
- Establishing trust in this way can of course be applied to other areas.



The screenshot shows the "My Credentials" section of the Tezos Profiles dashboard. At the top right are links for "My Profile", "Search Profiles", and a copyable Tezos address. The table below lists three types of credentials:

Name	Type	Proof	Status	Action
Basic Profile Information	Basic Profile	Self-Altestation	Incomplete	<a href="#">Verify</a>
Twitter Account Verification	Social Media	Tweet	Incomplete	<a href="#">Verify</a>
Ethereum Address Ownership	Address Ownership	Address Signature	Incomplete	<a href="#">Verify</a>



An exemplary industrial application on Tezos:

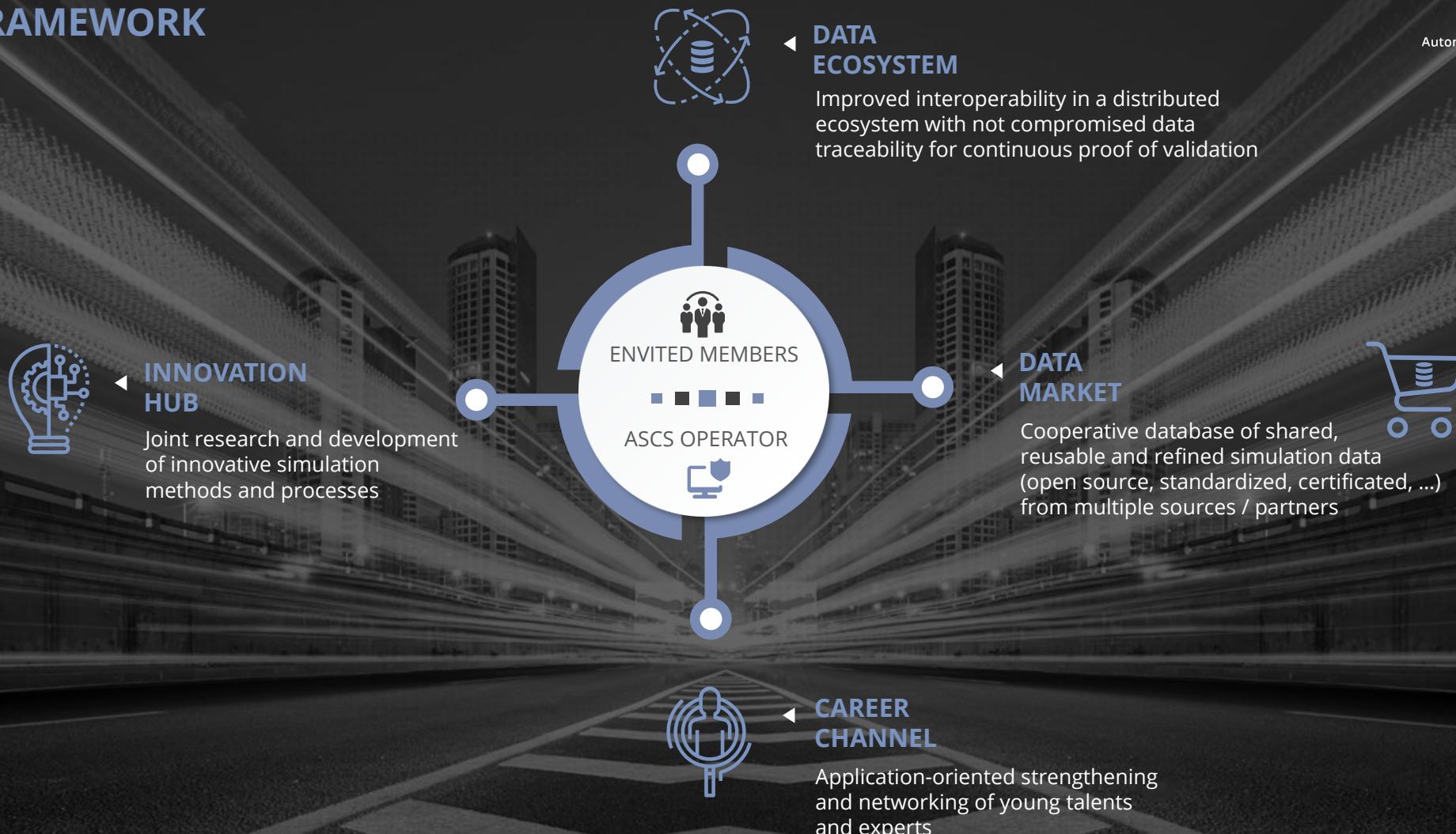
# THE ENVITED ECOSYSTEM



# ENVITED FRAMEWORK

asc(s)

Automotive Solution Center for Simulation



# ECOSYSTEM



traceability of certificated test data along the supply chain



support of virtual proof for homologation (ISO26262)



enables global markets by reducing imbalance of R&D partners (OEMs <-> Start-ups)

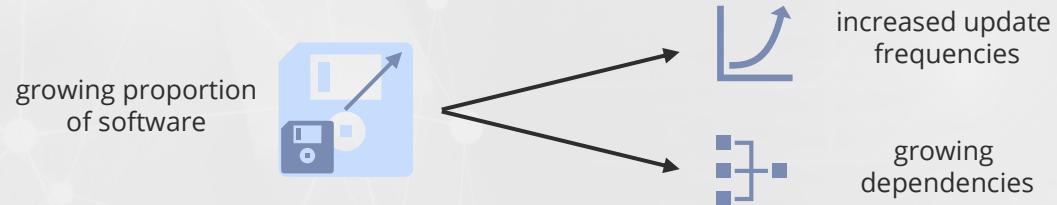


# THE ENVITED ECOSYSTEM: What is ENVITED's Goal?

- With the ultimate goal of **enabling virtual proof for homologation** (the governmental approval process for vehicles), the **ENVITED** working group has set out to create an ecosystem in which:
  - Trusted data marketplaces** provide (fair) **access** to relevant **source data** (like map data, city models, material data, driving scenarios, etc.) and **traceability** of their **provenance**.
  - Test/simulation results** and **certifications** can be **documented** in a **traceable** and **provable** yet **privacy preserving** (i.e. protecting business secrets and intellectual property) way.
  - Authorities** can access and **validate the data** (incl. tracing the entire data supply chain) and formally grant their **approval** in a legally binding way.
- To achieve this ambitious goal, a **powerful cross-company consortium** consisting of automotive OEMs, (data) suppliers, simulation and PLM software vendors, and academic partners has assembled under the ENVITED umbrella and its patron asc(s e.V.).
- While there is **still a long way to go** and many (research) questions to be resolved, ENVITED has **already produced some promising results**.
- Parties interested to join the community and contribute to our common goal should contact the asc(s e.V. office).

## WHY DO WE NEED VIRTUAL PROOF FOR HOMOLOGATION?

- The **growing proportion of software** in modern cars leads to **increased update frequencies** as well as **growing dependencies** and **overall complexity**.



- Simultaneously, **product lifecycles** get **shorter** or even "blur" and **requirements for quality, certification and approval** get ever **stricter**.



- The consequence: **conventional methods of validation** (physical testing) **do not suffice to handle the amount of required testing anymore** and need to be **complemented** with **trusted virtual counterparts**.

# THE ENVITED ECOSYSTEM: Why Blockchain?

- When **analyzing** the **ecosystem** in which our envisioned solution is going to operate and the **requirements** imposed by the regulatory authorities (as well as our own aspirations), **(public) blockchain technology** appears to be a **perfect fit**:
  - ▶ **Diverse multi-agent ecosystem** with **(partly) diverging interests** and a **need for cooperation** in a **competitive environment** (e.g. automotive OEMs are competitors, yet all require the same map data that would be prohibitively expensive to generate for only one player).
  - ▶ Strong need for **(public) immutable documentation**, **transparency** and **complete traceability** of the entire **data supply chain**, incl. data provenance, data ownership, data validation and certification.
  - ▶ Strong need for **efficiency** through **automation of business processes**, **interactions**, and **execution of (smart) contract conditions**.
- While firmly believing in the power of blockchain technology, we also acknowledge its **(current and future) limitations** with respect to storage of large amounts of data, conflicts with protection of personal data (cf. GDPR) as well as business secrets.
- We believe in blockchain as an important **building block** in the **architecture** of our solution that **provides data trust and integrity**.

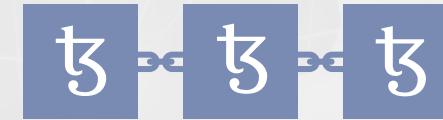


## WHY WE BELIEVE IN PUBLIC BLOCKCHAIN TECHNOLOGY

1. Provide trust in a trustless environment
2. Immutable documentation
3. Transparency
4. Automated contract execution

## HOW WE EMPLOY PUBLIC BLOCKCHAIN TECHNOLOGY

Hybrid System:



Blockchain as settlement layer  
for value transactions and trust



Separate cloud system  
for storage of actual data

# THE ENVITED ECOSYSTEM: Why Tezos?

- As this slide deck should have conveyed already, we believe that Tezos is a **superior** and **future-proof** public blockchain.
- Among the **reasons for building on Tezos**, we consider (non-exhaustive list):
  - ▶ Tezos' low energy **LPoS** mechanism and efficient consensus algorithm **Emmy\*** that enable **fast transactions** in an **environmentally friendly** way.
  - ▶ The **stability** and **future safety** achieved through **on-chain governance** that enables **upgrades** while **avoiding forks**.
  - ▶ **Formally verifiable smart contracts** and the **certified compiler** from higher level programming languages that enable **automated contract execution** while not having to blindly trust that a smart contract does what its developer claims or thinks it does.
  - ▶ Enablement of **privacy-preserving transactions** through **Sapling**.
  - ▶ Emergence of convenient and future proof **identity and access management** and **(revokable) certifications** by **SSI** tooling developed by **Spruce Systems**.
  - ▶ Potential usage of **FA2-based NFTs** (open research question).
  - ▶ Tezos' strong and vibrant **open-source community** that is committed to helping each other out.

## WHY WE CHOSE TEZOS AS THE BLOCKCHAIN FOR ENVITED

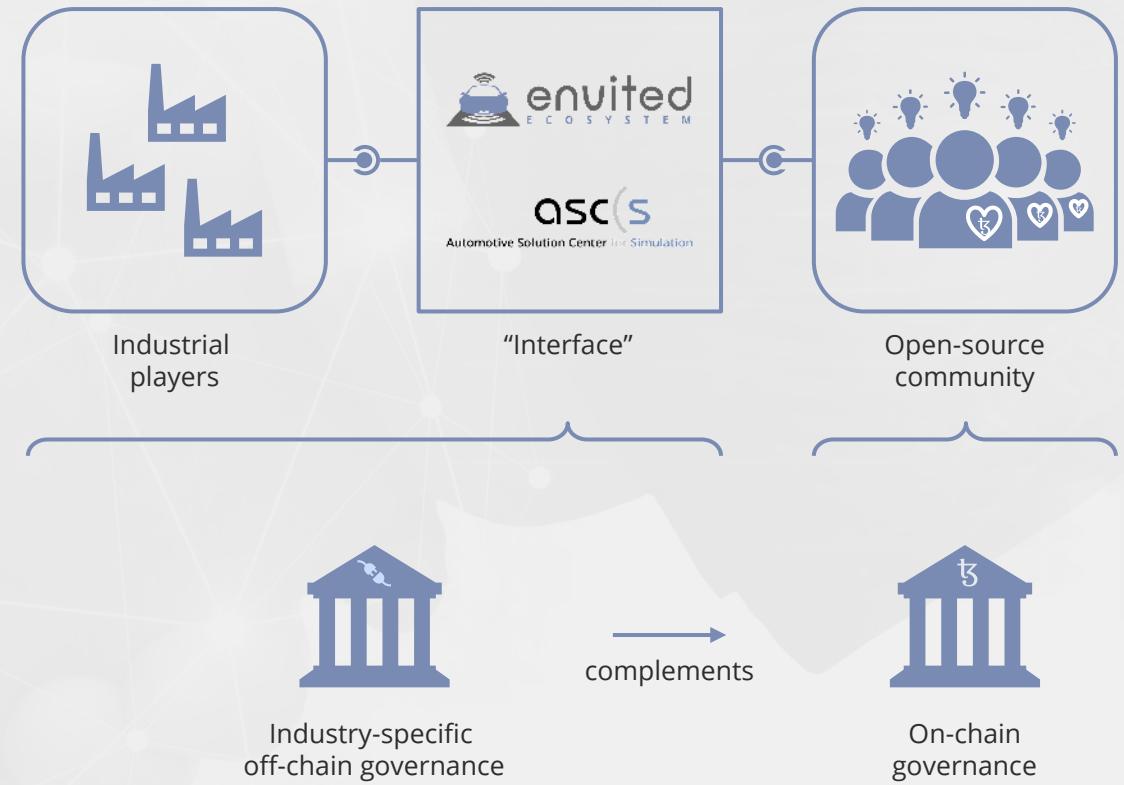


- Low energy consumption
- Fast transactions
- On-chain governance
- Formally verifiable smart contracts
- Privacy-preserving transactions
- SSI
- NFTs
- Strong community

# THE ENVITED ECOSYSTEM: ENVITED as Blueprint for other Projects on Tezos

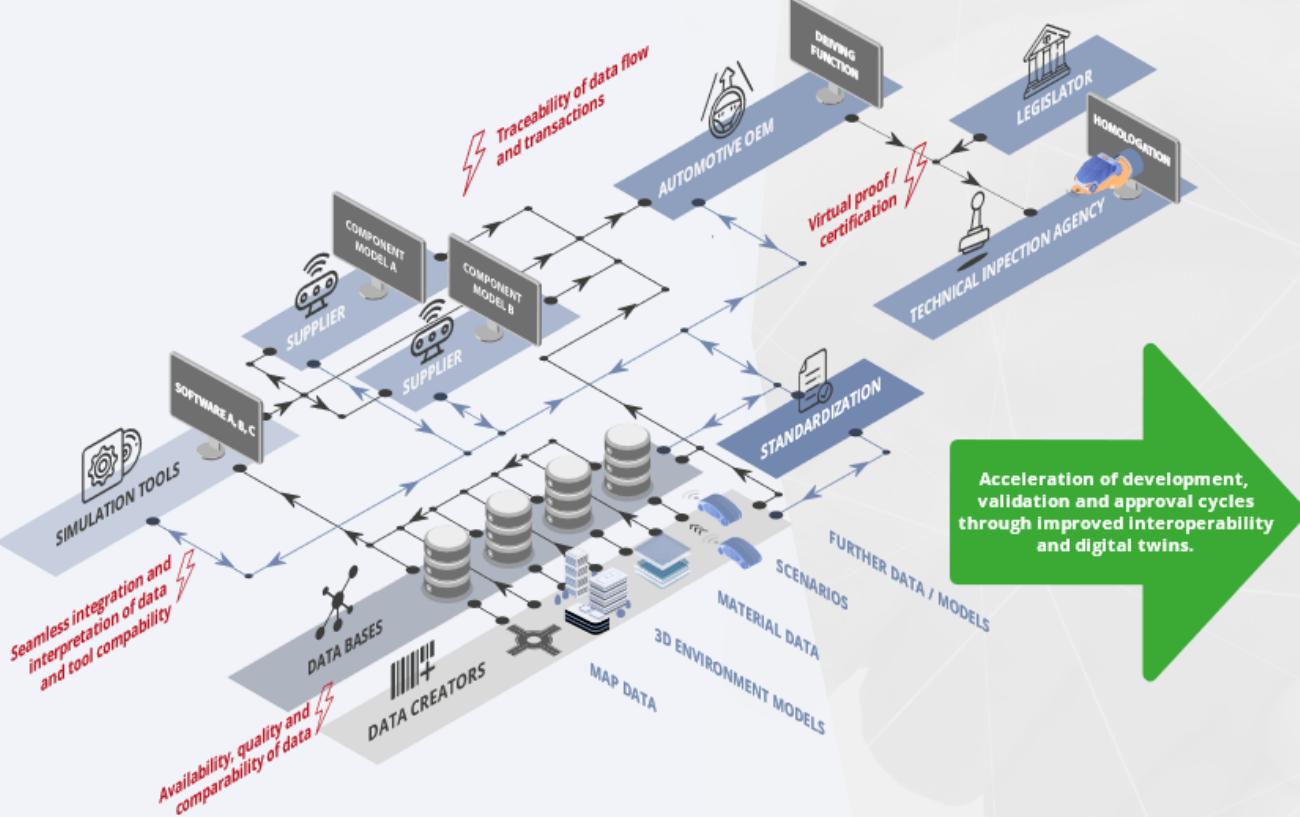
- While we have encountered our fair share of challenges, we believe that we have done a good job so far and our **organizational set-up** as well as the (high-level) **architecture of our solution** can be used as a **template** for other initiatives (even from entirely different industries) of **how to build industrial grade applications based on Tezos**.
  - ENVITED is exemplary when it comes to **reconciling industrial players with an open-source community**.
  - As an “e.V.” (a German legal structure for an association that serves a common cause of its members), ENVITED works as an **interface** for the automotive industry to engage with the community and to **align on requirements** as well as **industry standards** (e.g. industry-specific smart contract templates).
  - The “e.V.” allows to add an **additional governance layer** to complement the on-chain governance with an **off-chain and industry-application-specific governance** that provides a context in which the industry standards and solutions can be deployed (it is basically the pendant of an on-chain DAO).
  - Employing the Tezos blockchain as an (admittedly very important) building block of a larger solutions.
- We are happy to **share our experiences** and give you a leg up, if you want to build an **industrial application on Tezos**.

## WHY ENVITED COULD SERVE AS A BLUEPRINT FOR OTHERS

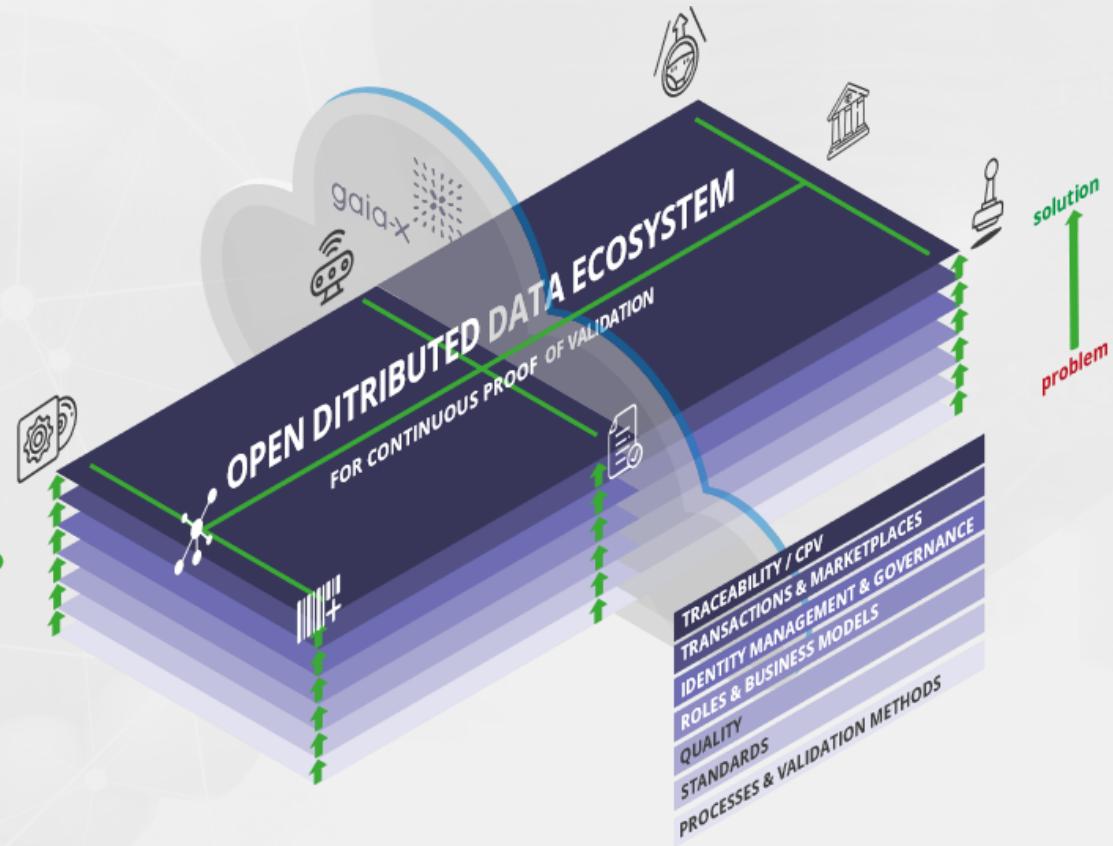


# DATA DRIVEN DEVELOPMENT PROCESS

## Current status



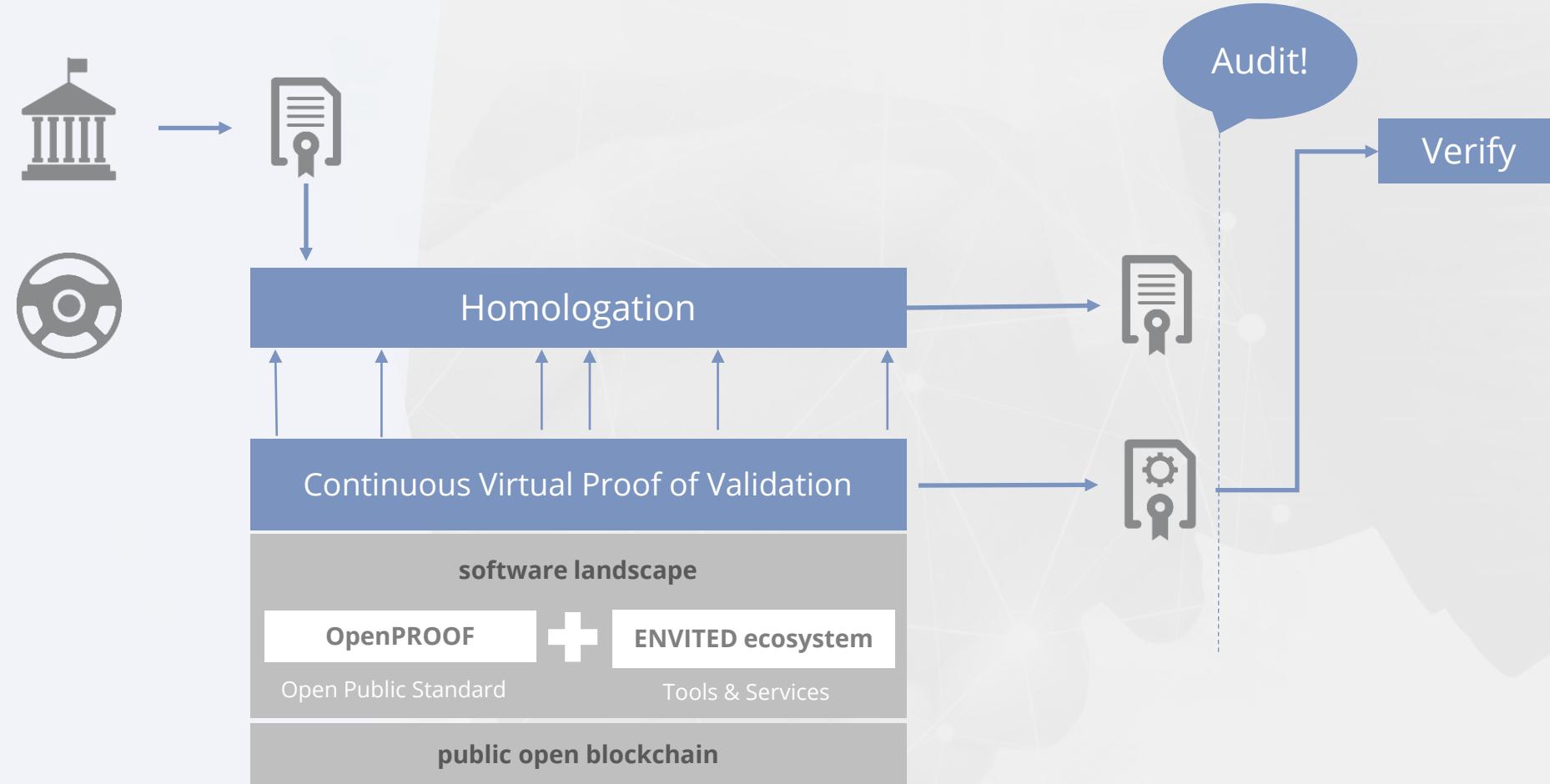
## Target ENVITED ecosystem



- **Immutable Documentation**
- **Transparency**
- **Automated Contract Execution**
- **Licensing**
- **Certification**
- **Convenient Access Management**

→ Most of the ecosystem's challenges can be addressed by the Tezos blockchain and/or solutions evolving around Tezos!

# ECOSYSTEM, VALIDATION ENHANCED



73

# MYTHBUSTERS



# Bitcoin ≠ Blockchain

As Bitcoin was the first blockchain in the world, Bitcoin and blockchain are often confused with one another. However, they are not the same! Blockchain is a technological concept and an umbrella term for any technology following that concept. The relationship between Bitcoin and blockchain is thus better characterized as:  $\text{Bitcoin} \subseteq \text{Blockchain}$ !



# Blockchain ≠ Tremendous Energy Consumption

Bitcoin uses a Proof-of-Work mechanism to prevent Sybil attacks that does consume a lot of energy. With Bitcoin still being the most prominent blockchain and media reporting comparisons of Bitcoin's energy consumption with that of countries, the impression that blockchain requires a lot of energy stuck. However, there are other Sybil control mechanisms such as Proof-of-Stake that do not require a significant amount of energy. The Tezos protocol uses Liquid Proof-of-Stake which is low energy!



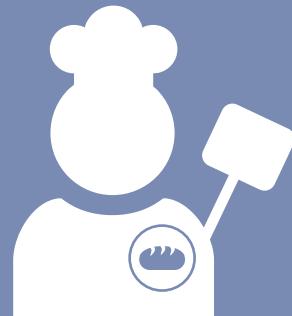
# (Liquid) Proof-of-Stake ≠ Consensus Algorithm

Neither Liquid Proof-of-Stake nor any other Proof-of-Stake mechanism (nor Proof-of-Work for that matter) constitutes a consensus algorithm. The PoX family is a group of mechanisms designed to protect the network and its consensus algorithm against Sybil attacks (i.e. an attacker creating a lot of fake nodes to gain control over the network). They can thus be referred to as Sybil control mechanisms and yes – they are closely entwined with consensus algorithms, but they are not the same thing!



# Liquid Proof-of-Stake ≠ Delegated Proof-of-Stake

As delegation is an integral part of Liquid Proof-of-Stake (LPoS), it is often confused with Delegated Proof-of-Stake (dPoS) as known from EOS and Lisk. However, they are different concepts, with very different grades of decentralization and – respectively – network security. While the number of validators is limited to 21 in EOS and 101 in Lisk and more static, in Tezos' LPoS it is only bounded by the maximum number of rolls depending on the total supply of tez and more dynamic.



# Smart Contracts = $\neg$ Smart $\wedge$ $\neg$ Legal Contracts

Smart contracts are neither legally binding nor are they smart on their own accord. Smart contracts are relatively simple computer programs that are deployed on the blockchain, allow the automated execution of (inter-party) processes and thus the automated execution of contract conditions.





# You Don't Need to Use the Token in Your App

Public blockchains require a cryptocurrency to provide economic incentives for its validators to maintain the network. But just because a blockchain has a token, it does not require you to actively use that token in the application you build on top of the blockchain. You will have to pay for using it by the means of the cryptocurrency but it does not have to play a role in your use case!



# Blockchain has real world applications

As blockchain is a very young yet non-trivial technology, there are a lot of failed or stuck blockchain projects and blockchain has been accused of just being a technology searching for its problem. However, blockchain does have its real world applications it's rather a matter of understanding the technology, its strengths and weaknesses and selecting those applications it is actually well-suited for!



## NOTE ON PUBLICATION

The Tezos Deep Dive Deck 2.0 is licensed under the Creative Commons CC BY 4.0.



This document was created within the activities of the ENVITED research cluster and serves as training and further education material in the ENVITED Career Channel and the ENVITED academy.



Dipl.-Ing. Alexander F. Walser  
Managing Director

**Automotive Solution Center for Simulation e.V.**  
Curiestraße 2 | 70563 Stuttgart | Germany  
Phone: +49 (0) 711 699659-0 | Fax: +49 (0) 711 699659-29  
Email: hello@envited.market  
Web: [www.asc-s.de](http://www.asc-s.de) | [www.envited.market](http://www.envited.market)



Get in touch with us!



# REFERENCES

*NOTE:*

WE HAVE ONLY BEGUN TO LIST REFERENCES TO SOURCES  
CONSULTED TO COMPILE THIS SLIDE DECK WITH THE SEPTEMBER  
2021 UPDATE.

WHILE WE ARE COMMITTED TO MAKE THESE SOURCES  
TRANSPARENT AND INFORMATION CONTAINED IN THIS SLIDE  
DECK VERIFYABLE, REFERENCES TO SLIDES FROM THE INITIAL  
RELEASE OF THE DECK ARE STILL MISSING.

# References for Slide: Why public blockchains are the future...



- [1] <https://www.marigold.dev/project/optimistic-rollups> (A layer 2 solutions for scalability)
- [2] <https://blog.nomadic-labs.com/a-look-ahead-to-tenderbake.html> (New consensus algorithm with deterministic finality)
- [3] <https://research-development.nomadic-labs.com/sapling-integration-in-tezos-tech-preview.html> (Selective privacy integration with Sapling)

# References for Slide: Why public blockchains are the future: Developments in scaling and privacy technologies



- [1] <https://medium.com/boltlabs/introducing-zkchannels-on-tezos-c365830b9efd> (zkChannels eliminates lag time and high transaction fees - while offering strong privacy protections — so you can use Zcash, Bitcoin, Tezos and other digital currencies for everyday payments and purchases)
- [2] <https://news.tezoscommons.org/a-closer-look-into-marigolds-plans-for-tezos-b682b759ffa2> (a closer look into Marigold's Layer 2 solutions)

## References for Slide: Some KPIs: Tezos in numbers...



- [1] <https://tzstats.com/> (tz Stats – information on the creation of the first block, the current block height, number of funded accounts, market capitalization, number of active validators )
- [2] <https://www.tezos.help/#projects> (tezos.help – information on Tezos-based projects)
- [3] <https://www.tezosagora.org/period/50> (Tezos Agora - information on number of successful amendments/protocol updates [replace "50" with respective period to inspect or browse by clicking the linked arrows])
- [4] <https://wiki.tezosagora.org/learn/baking/proofofstake/consensus#scalability> (Tezos Agora Wiki – information on transactions per second)
- [5] <https://www.tezosprojects.com/> (A non-exhaustive list of projects using Tezos)

# References for Slide: Some KPIs: Growth in Smart Contract Calls



- [1] <https://better-call.dev/stats/mainnet/general> (Better Call Dev – Tezos Smart Contract Explorer by Baking Bad )

# References for Slide: How the Tezos on-chain governance/amendment process works



- [1] <https://wiki.tezosagora.org/learn/governance> (Tezos Agora Wiki - Tezos Governance)
- [2] <https://medium.com/tezos/amending-tezos-b77949d97e1e> (Medium - Jacob Arluck on the version of the amendment process valid in 2018)
- [3] <https://www.tezosagora.org/period/12> (Tezos Agora - proposal description for Athens: reduction in roll size)
- [4] <https://www.tezosagora.org/period/18> (Tezos Agora - proposal description for Babylon: introduction of quorum floor and cap and 5% hurdle)
- [5] <https://www.tezosagora.org/period/39> (Tezos Agora - proposal description for Edo: introduction of Adoption period and shortened periods)
- [6] <https://www.tezosagora.org/period/44> (Tezos Agora - proposal description for Florence: discarding of testnet fork and rechristening of Testing period to Cooldown period)
- [7] <https://forum.tezosagora.org/t/envited-why-the-tezos-amendment-process-needs-an-adoption-period-a-proposal-to-improve-the-on-chain-governance-mechanism/1845> (Tezos Agora - Proposition and discussion of Adoption period)
- [8] <https://medium.com/tezos/there-is-no-need-for-hard-forks-86b68165e67d> (Medium - Arthur Breitman on reduced necessity for hard forks due to on-chain governance)

# References for Slide:

## The Tezos consensus algorithm: Emmy / Emmy+ since Babylon / Emmy\* if Granada succeeds

- [1] <https://wiki.tezosagora.org/learn/baking/proofofstake/consensus> (Tezos Agora Wiki - The Tezos Consensus Algorithm)
- [2] <https://www.youtube.com/watch?v=uHViHhOlcz0&t=1010s> (YouTube – Awa Sun Yin on Consensus Algorithms and PoX mechanisms)
- [3] <https://blog.nomadic-labs.com/faster-finality-with-emmy.html> (Nomadic Labs Blog - Faster finality with Emmy\*)
- [4] [https://gitlab.com/tezos/tzip/-/blob/master/drafts/current/draft\\_emmy-star.md](https://gitlab.com/tezos/tzip/-/blob/master/drafts/current/draft_emmy-star.md) (TZIP Gitlab - Emmy\* specification)

# References for Slide: Is there a development roadmap for Tezos?



- [1] <https://blog.nomadic-labs.com/introducing-mi-cho-coq-v10.html> (Nomadic Labs Blog - Introducing Mi-Cho-Coq v1.0)
- [2] <https://blog.nomadic-labs.com/simulating-tenderbake.html> (Nomadic Labs Blog - Simulating Tenderbake)
- [3] <https://blog.nomadic-labs.com/announcing-the-report-possible-evolutions-of-the-voting-system-in-tezos.html> (Nomadic Labs Blog - Announcing the report "Possible evolutions of the voting system in Tezos")
- [4] [https://gitlab.com/tezos/tzip/-/merge requests/133](https://gitlab.com/tezos/tzip/-/merge_requests/133) (TZIP - Draft: baking accounts proposal)
- [5] [https://gitlab.com/tezos/tzip/-/blob/5addee1ca26925d2e65e363b900689da090557497/drafts/current/draft-baking\\_accounts.md](https://gitlab.com/tezos/tzip/-/blob/5addee1ca26925d2e65e363b900689da090557497/drafts/current/draft-baking_accounts.md) (TZIP - Baking Accounts)

# References for Slides:

## The self-amendment process works: 6 successful amendments and counting... (1/2) & (2/2)



- [1] <https://www.tezosagora.org/period/12> (Tezos Agora - proposal description for Athens)
- [2] <https://www.tezosagora.org/period/18> (Tezos Agora - proposal description for Babylon)
- [3] <https://www.tezosagora.org/period/24> (Tezos Agora - proposal description for Carthage)
- [4] <https://www.tezosagora.org/period/35> (Tezos Agora - proposal description for Delphi)
- [5] <https://www.tezosagora.org/period/39> (Tezos Agora - proposal description for Edo)
- [6] <https://www.tezosagora.org/period/44> (Tezos Agora - proposal description for Florence)

## References for Slides:

### An overview of Tezos' self-amendment history so far... (1/2) & (2/2)



- [1] <https://www.tezosagora.org/period/50> (Tezos Agora - replace "50" with respective period to inspect or browse by clicking the linked arrows)

# References for Slides: Delphi – the fourth amendment to the Tezos protocol



- [1] <https://www.tezosagora.org/period/35> (Tezos Agora - proposal description for Delphi)
- [2] <https://blog.nomadic-labs.com/delphi-official-release.html> (Nomadic Labs Blog – Delphi: official release notes)
- [3] <https://blog.nomadic-labs.com/delphi-changelog.html> (Nomadic Labs Blog – Delphi: changelog)
- [4] <https://nomadic-labs.com/> (Nomadic Labs Website)
- [5] <https://metastate.dev/> (Metastate Website [retired website] )
- [6] <https://twitter.com/AlfourG> (Twitter Profile of Gabriel Alfour)

# References for Slide: Edo - the fifth amendment to the Tezos protocol



- [1] <https://www.tezosagora.org/period/39> (Tezos Agora - proposal description for Edo)
- [2] [https://tezos.gitlab.io/protocols/008\\_edo.html](https://tezos.gitlab.io/protocols/008_edo.html) (Tezos Gitlab – Edo: official release notes & changelog)
- [3] <https://medium.com/@MetastateTeam/governance-improvements-725fba622615> (Medium – Metastate on Governance Improvements)
- [4] <https://blog.nomadic-labs.com/sapling-integration-in-tezos-tech-preview.html> (Nomadic Labs Blog - Tech Preview on Sapling integration in Tezos )
- [5] <https://tezos.gitlab.io/active/sapling.html> (Tezos Gitlab – Sapling integration)
- [6] <http://zerocoin.org/media/pdf/ZerocoinOakland.pdf> (Further reading on Sapling's origin (paper) – Zerocoin: Anonymous Distributed E-Cash from Bitcoin)
- [7] <https://github.com/zcash/zips/blob/master/protocol/sapling.pdf> (Further reading - Zcash Protocol Specification)
- [8] <https://tezos.gitlab.io/active/michelson.html#michelsontickets> (Tezos Gitlab – Operations on tickets)
- [9] <https://medium.com/tezos-israel/tickets-on-edo-simply-explained-c5a411cc27f9> (Medium – Adam Shinder explains Tickets on Edo)
- [10] <https://medium.com/tqtezos/tickets-on-tezos-part-1-a7cad8cc71cd> (Medium – Eli Guenzburger explains Tickets on Edo)
- [11] <https://nomadic-labs.com/> (Nomadic Labs Website)
- [12] <https://metastate.dev/> (Metastate Website [retired website] )

# References for Slide: Florence - the sixth amendment to the Tezos protocol



- [1] <https://www.tezosagora.org/period/44> (Tezos Agora - proposal description for Florence)
- [2] <https://blog.nomadic-labs.com/florence-our-next-protocol-upgrade-proposal.html> (Nomadic Labs Blog – Florence: official release notes)
- [3] [http://doc.tzalpha.net/protocols/009\\_florence.html](http://doc.tzalpha.net/protocols/009_florence.html) (Tezos Gitlab – Florence: changelog)
- [4] <https://blog.nomadic-labs.com/baking-accounts-proposal-contains-unexpected-breaking-changes.html> (Nomadic Labs Blog - Reasoning for postponement of baking accounts)
- [5] <https://nomadic-labs.com/> (Nomadic Labs Website)
- [6] <https://tarides.com/> (Company website of Tarides)
- [7] <https://twitter.com/dailambda> (Twitter Profile of DaiLambda)
- [8] <https://gitlab.com/keefertaylor> (Gitlab Profile of Keefer Taylor)

# References for Slide: Granada - the seventh amendment to the Tezos protocol (?)



- [1] <https://www.tezosagora.org/period/50> (Tezos Agora - proposal description for Granada)
- [2] <https://blog.nomadic-labs.com/announcing-granada.html> (Nomadic Labs Blog – Announcing Granada)
- [3] [https://tezos.gitlab.io/protocols/010\\_granada.html](https://tezos.gitlab.io/protocols/010_granada.html) (Tezos Gitlab – Granada: changelog)
- [4] <https://blog.nomadic-labs.com/faster-finality-with-emmy.html> (Nomadic Labs Blog - Faster finality with Emmy\*)
- [5] [https://gitlab.com/tezos/tzip/-/blob/master/drafts/current/draft-liquidity\\_baking.md](https://gitlab.com/tezos/tzip/-/blob/master/drafts/current/draft-liquidity_baking.md) (Gitlab - Liquidity Baking)
- [6] <https://nomadic-labs.com/> (Nomadic Labs Website)
- [7] <https://tarides.com/> (Company website of Tarides)
- [8] <https://twitter.com/dailambda> (Twitter Profile of DaiLambda)
- [9] <https://tqtezos.com/> (Website of TQ Tezos)

# References for Slides:

## A brief history of Tezos and the Tezos foundation (1/2) & (2/2)



- [1] <https://tezos.foundation/history> (Tezos Foundation - History [Site does not exist anymore])
- [2] <https://www.tezosagora.org/period/50> (Tezos Agora - replace "50" with respective period to inspect or browse by clicking the linked arrows)
- [3] <https://en.wikipedia.org/wiki/Tezos> (Wikipedia – Article on Tezos)
- [4] <https://www.redbull.com/int-en/redbullracing/tezos-joins-as-official-blockchain-partner> (Redbull Racing - partnership press release)
- [5] <https://www.mclaren.com/racing/partners/tezos/> (McLaren Racing – partnership press release)
- [6] <https://cdn.uc.assets.prezly.com/c35dc0ac-7d41-436a-8389-779fc91cdc67/-/inline/no/20210420ubisoftxtezoseng.pdf> (Ubisoft – corporate baker press release)
- [7] <https://www.societegenerale.com/en/news/press-release/first-structured-product-public-blockchain> (Société Générale – STO press release)
- [8] <https://www.lefigaro.fr/societes/lugh-le-pari-crypto-de-groupe-casino-20210325> (Le Figaro - Article on Groupe Casino's stable coin Lugh)
- [9] <https://exaion.edf.fr/en/exaion/our-news/exaion-edf-group-subsidiary-becomes-a-tezos-baker> (Bloomberg - Article on EDF group plans as corporate baker)
- [10] <https://www.bloomberg.com/press-releases/2019-07-03/btg-pactual-and-dalma-capital-to-utilize-tezos-blockchain-for-security-token-offerings-stos> (Bloomberg - Article on BTG Pactual and Dalma Capital's plans for STOs)
- [11] <https://www.bloomberg.com/news/articles/2019-02-11/on-the-menu-from-chefs-club-owner-selling-property-for-crypto> (Bloomberg - Article on Elevated Returns' plans for tokenized real-estate offerings)
- [12] <https://www.artnews.com/list/art-in-america/features/gans-and-nfts-1234594335/> (Art in America - Article on Hit et Nunc & Art NFTs)

# References for Slide (1/2): Tezos Community Rewards



- [1] <https://tezoscommons.org/rewards/> (Tezos Commons Website with links to latest reward winners and nomination form)
- [2] <https://tezos.foundation/an-update-on-community-engagement/> (Article on Tezos Foundation website from 09/22/2020 announcing the CRP)
- [3] <https://medium.com/tezoscommons/community-rewards-for-tezos-contributors-d6e2813a83d8> (Medium article introducing and explaining the CRP)
- [4] <https://medium.com/tezoscommons/tezos-community-rewards-winners-october-2020-7d1b8f520033> (Announcement of October 2020 winners)
- [5] <https://medium.com/tezoscommons/tezos-community-rewards-winners-november-2020-b228fe054ae2> (Announcement of November 2020 winners)
- [6] <https://medium.com/tezoscommons/tezos-community-rewards-winners-december-2020-eb46ee7af519> (Announcement of December 2020 winners)
- [7] <https://medium.com/tezoscommons/tezos-community-reward-winners-january-2021-66a1e8e22d43> (Announcement of January 2021 winners)
- [8] <https://medium.com/tezoscommons/tezos-community-reward-winners-february-2021-6fc3dd75e250> (Announcement of February 2021 winners)
- [9] <https://medium.com/tezoscommons/tezos-community-reward-winners-march-2021-76f51cdc333f> (Announcement of March 2021 winners)

## References for Slide (2/2): Tezos Community Rewards



- [10] <https://medium.com/tezoscommons/tezos-community-reward-winners-april-2e6c2a066048> (Announcement of April 2021 winners)
- [11] <https://medium.com/tezoscommons/tezos-community-reward-winners-may-2021-a1f60900816a> (Announcement of May 2021 winners)

# References for Slide: Of Tokens and Fungibility: What are NFTs?



- [1] [https://en.wikipedia.org/wiki/Non-fungible\\_token](https://en.wikipedia.org/wiki/Non-fungible_token) (Wikipedia - article on non-fungible tokens)
- [2] <https://tezos.b9lab.com/fa2> (B9 Lab / Tezos Developer Portal - FA2: A unified token contract interface)
- [3] <https://assets.tqtezos.com/docs/token-contracts/fa2/2-fa2-nft-tutorial/> (TQ Tezos - Tutorials)
- [4] <https://medium.com/@medipedia/the-various-types-of-crypto-tokens-26bab8f6622c> (Medium article naming different token applications/token classes)
- [5] <https://finematics.com/what-are-nfts-and-how-can-they-be-used-in-defi/> (Finematics – What are NFTs and how can they be used in DeFi)

# References for Slide: NFTs on Tezos: The FA2 token standard



- [1] <https://tezos.b9lab.com/fa2> (B9 Lab / Tezos Developer Portal - FA2: A unified token contract interface)
- [2] <https://assets.tqtezos.com/docs/token-contracts/fa2/2-fa2-nft-tutorial/> (TQ Tezos - Tutorials)
- [3] <https://gitlab.com/tezos/tzip/-/blob/master/proposals/tzip-12/tzip-12.md> (TZIP Gitlab - TZIP 12)
- [4] <https://medium.com/tqtezos/introducing-fa2-a-multi-asset-interface-for-tezos-55173d505e5f> (Medium - article by TQ Tezos introducing the FA2 standard on Tezos)
- [5] <https://opentezos.com/defi/token-standards/> (Open Tezos – Token standards)

# References for Slide: NFTs on Tezos: tzcolors



- [1] <https://www.tzcolors.io/> (tzcolors NFT platform)
- [2] <https://xtz.news/latest-tezos-news/first-nft-auctions-on-tezos-take-off-tzcolors/> (XTZ.news – Allen Walters on tzcolors)
- [3] <https://blog.tezoscommons.org/the-growing-nft-momentum-3c32a4bf8c46> (Medium - The Growing NFT Momentum by William McKenzie)
- [4] <https://tzkt.io/KT1CpeSQKdkhWi4pinYcseCFKmDhs5M74BkU/operations/> (tzcolors Auction House Contract in TzKT blockchain explorer)
- [5] <https://tzkt.io/KT1FyaDqiMQWg7Exo7VUiXAgZbd2kCzo3d4s/operations/> (tzcolors NFTs Contract in TzKT blockchain explorer)
- [6] <https://github.com/tzcolors> (Gitlab - tzcolors source code)
- [7] <https://twitter.com/tzcolors> (Twitter account of tzcolors)
- [8] <https://www.youtube.com/watch?v=dvA4fET1ujw> (YouTube – Yoeshi Roberts demonstrates and comments on bidding on tzcolors)
- [9] [https://www.reddit.com/r/tezos/comments/lkfqrp/tzcolors\\_has\\_321\\_open\\_auctions\\_for\\_unique\\_color/](https://www.reddit.com/r/tezos/comments/lkfqrp/tzcolors_has_321_open_auctions_for_unique_color/) (Reddit – discussion on reception of tzcolors within the community/the users)
- [10] <https://tzbutton.io/> (TzButton social experiment utilizing tzcolors)

## References for Slide: NFTs on Tezos: Kalamint



- [1] <https://kalamint.medium.com/kalamint-bringing-nfts-to-tezos-a51daa0c38cd> (Medium - Kalamint: Bringing NFTs to Tezos)
- [2] <https://kalamint.medium.com/kalamint-launch-important-dates-b70613f2d4c4> (Medium - Kalamint Launch: Important Dates)
- [3] <https://kalamint.medium.com/auctions-now-live-on-the-kalamint-platform-d77b142e6279> (Medium - Auctions now live on the Kalamint platform)
- [4] <https://kalamint.medium.com/kalam-token-listing-on-quipuswap-on-jun-3-thu-8458d67fcc3> (Medium - \$KALAM token listing on Quipuswap on Jun3, Thu.)
- [5] <https://kalamint.medium.com/kalam-tokenomics-and-distribution-c1e0ccb0800b> (Medium - \$KALAM: Tokenomics and Distribution)
- [6] <https://kalamint.medium.com/kalamint-update-4-e970fc10d914> (Medium - Kalamint Update #4)
- [7] <https://kalamint.io/> (Kalamint NFT platform)

## References for Slide: NFTs on Tezos: hic et nunc



- [1] <https://www.hicetnunc.xyz/> (hic et nunc NFT platform)
- [2] <https://github.com/hicetnunc2000/hicetnunc/wiki> (GitHub - hic et nunc wiki)
- [3] <https://www.youtube.com/watch?v=KJSjapuG3o> (YouTube – tutorial video on NFTs on Tezos by Noealz)
- [4] <https://www.youtube.com/watch?v=Apyd-l2DMVk> (YouTube – tutorial video on minting NFTs on hic et nunc by Kris G)
- [5] <https://gorillasun.de/blog/Hicetnunc.xyz-and-NFTs-on-the-Tezos-Blockchain-~-What's-new-~-April-2021-Update> (Hicetnunc.xyz and NFTs on the Tezos Blockchain ~ What's new ~April 2021 Mega Update)
- [6] <https://www.plummerfernandez.com/works/not-another-jpeg/> (M Plummer-Fernández – Not another JPEG)

# References for Slide (1/2): NFTs on Tezos: Tezos Domains



- [1] <https://tezos.domains/> (Tezos Domains platform)
- [2] <https://blog.tezos.domains/introducing-tezos-domains-78cfadc08c75> (Medium - Introducing Tezos Domains)
- [3] <https://developers.tezos.domains/design-document/smart-contract-overview> (Tezos Domains Developer Documentation)
- [4] <https://blog.tezos.domains/tezos-domains-for-developers-1-resolving-domains-2a037e4b9a72> (Medium - Tezos Domains for Developers #1: Resolving Domains)
- [5] <https://blog.tezos.domains/tezos-domains-for-developers-2-buying-updating-domains-470497736ce1> (Medium - Tezos Domains for Developers #2: Buying & Updating Domains)
- [6] <https://blog.tezoscommons.org/a-closer-look-into-tezos-domains-c1ee325752df> (Medium - A Closer Look into Tezos Domains)
- [7] <https://blog.tezos.domains/designing-a-tezos-name-service-part-1-introduction-4b94b2a5ac6b> (Medium - Designing a Tezos Name Service - Part 1: Introduction)
- [8] <https://blog.tezos.domains/designing-a-tezos-name-service-part-2-namespace-and-structure-2131bd99853b> (Medium - Designing a Tezos Name Service - Part 2: Namespace and Structure)
- [9] <https://blog.tezos.domains/designing-a-name-service-part-3-name-distribution-and-pricing-96429352279> (Medium - Designing a Name Service - Part 3: Name Distribution and Pricing)
- [10] <https://blog.tezos.domains/designing-a-tezos-name-service-part-4-validation-normalization-encoding-73e01a5e09c9> (Medium - Designing a Tezos Name Service - Part 4: Validation, Normalization, Encoding)

## References for Slide (2/2): NFTs on Tezos: Tezos Domains



- [11] <https://blog.tezos.domains/designing-a-name-service-part-5-retaining-trademarks-e43a89fee762> (Medium - Designing a Name Service – Part 5: Retaining Trademarks)
- [12] <https://blog.tezos.domains/tezos-domains-developer-preview-550cf56b8174> (Medium - Tezos Domains Developer Preview)
- [13] <https://gitlab.com/tezos-domains/contracts> (Gitlab - Tezos Domains)
- [14] <https://blog.tezos.domains/tezos-domains-alpha-release-1a992d15b4f8> (Medium - Tezos Domains Alpha Release)
- [15] <https://twitter.com/tezosdomains?lang=de> (Twitter Account of Tezos Domains)

# References for Slide (1/2): NFTs on Tezos: OneOf



- [1] <https://oneof.com/> (OneOf landing page / future platform)
- [2] <https://twitter.com/oneofnft> (Twitter account of OneOf)
- [3] <https://www.rollingstone.com/pro/news/oneof-nft-marketplace-quincy-jones-whitney-houston-tlc-doja-cat-crypto-1173557/> (RollongStone – Quincy Jones Is Backing a New NFT Marketplace for the Average Music Fan)
- [4] <https://cointelegraph.com/news/oneof-raises-63m-for-new-green-nft-platform-for-musicians> (Cointelegraph - OneOf raises \$63M for new Green NFT platform for musicians)
- [5] <https://www.forbes.com/sites/eamonnforde/2021/05/25/green-light-musicians-back-eco-friendly-nfts/?sh=7373c02c573d> (Forbes – Green Light: Musicians Back Eco-Friendlier NFTs)
- [6] <https://www.coindesk.com/oneof-raises-63m-for-music-nft-platform-with-green-credentials> (Coindesk - OneOf Raises \$63M in Seed Funding to Build Music NFT Platform on Tezos)
- [7] <https://www.billboard.com/articles/business/9577834/nft-marketplace-oneof-doja-cat-john-legend> (billboard - Doja Cat, John Legend Join Eco-Friendly Music NFT Marketplace OneOf)
- [8] <https://www.engadget.com/oneof-nft-marketplace-music-industry-140018743.html?guccounter=1> (engadget – OneOf wants to sell you a John Legend NFT)
- [9] <https://labusinessjournal.com/news/2021/may/28/nft-platform-oneof-launches-63-million-funding/> (Los Angeles Business Journal – NFT Platform one of Launches With \$63 Million in Funding)

## References for Slide (2/2): NFTs on Tezos: OneOf



- [10] <https://xtz.news/nft-news/quincy-jones-john-legend-doja-cat-tld-the-estate-of-whitney-houston-tezos-oneof/> (XTZ.news – Allen Walters on OneOf)
- [11] <https://oneofnft.medium.com/bringing-green-nfts-to-the-music-industry-with-tezos-902a7167f3b> (Medium - Bringing Green NFTs to the Music Industry with Tezos)

## References for Slide:

### NFTs on Tezos: There's more - NFT Applications and Marketplaces in the Making



- [1] <https://www.emergents.gg/> (Landing page of future digital collectible card game Emergents)
- [2] <https://www.redbull.com/int-en/redbullracing/tezos-joins-as-official-blockchain-partner> (RedBull Racing - Press release on Tezos partnership and NFT fan experience plans)
- [3] <https://www.mclaren.com/racing/partners/tezos/> (McLaren Racing – Press release on Tezos partnership and NFT fan experience plans)
- [4] <https://tez.auction/#/> (Landing page of future multiple auction type NFT marketplace TezAuction)
- [5] <https://d-art.tech/> (Landing page of future curated digital art NFT marketplace D-art)
- [6] <https://bazaarnft.xyz/> (Bazaar NFT marketplace)
- [7] <https://nft.amplifyx.com/xl/> (amplify<sup>NFT</sup> commercial art NFT marketplace)
- [8] <https://www.truesy.com/> (Truesy commercial art NFT marketplace)

# References for Slide: SSIs on Tezos: What are Self-Sovereign Identities?



- [1] <https://www.emergents.gg/> (Landing page of future digital collectible card game Emergents)
- [2] <https://www.redbull.com/int-en/redbullracing/tezos-joins-as-official-blockchain-partner> (RedBull Racing - Press release on Tezos partnership and NFT fan experience plans)
- [3] <https://www.mclaren.com/racing/partners/tezos/> (McLaren Racing – Press release on Tezos partnership and NFT fan experience plans)
- [4] <https://tez.auction/#/> (Landing page of future multiple auction type NFT marketplace TezAuction)
- [5] <https://d-art.tech/> (Landing page of future curated digital art NFT marketplace D-art)
- [6] <https://bazaarnft.xyz/> (Bazaar NFT marketplace)
- [7] <https://nft.amplifyx.com/xl/> (amplify<sup>NFT</sup> commercial art NFT marketplace)

# References for Slide: SSIs on Tezos: Concepts and Standards around SSIs



- [1] <https://www.w3.org/TR/did-core/> (W3C – DID standard)
- [2] <https://www.w3.org/TR/vc-data-model/> (W3C – VC standard)
- [3] <https://did-tezos.spruceid.com/#why-a-tezos-did-method> (Tezos DID Method Specification)
- [4] <https://gitlab.com/tezos/tzip/-/blob/master/proposals/tzip-19/tzip-19.md> (TZIP-019)
- [5] <https://spruceid.dev/docs/primer/> (Spruce Systems Developer Portal – What is Decentralized Identity?)
- [6] <https://identity.foundation/peer-did-method-spec/> (W3C – Peer DID Method Specification)
- [7] <https://did-tezos.spruceid.com/#why-a-tezos-did-method> (Tezos DID Method Specification)

# References for Slide (1/3): SSIs on Tezos: Spruce Systems



- [1] <https://sprucesystems.medium.com/introducing-spruce-8e3116b581a6> (Spruce Systems Blog on Medium – Introducing Spruce)
- [2] <https://sprucesystems.medium.com/announcing-decentralized-identity-on-tezos-4bf266a7af3f> (Spruce Systems Blog on Medium – Announcing Decentralized Identity on Tezos)
- [3] <https://sprucesystems.medium.com/spruce-developer-update-1-3efef055ab9d> (Spruce Systems Blog on Medium – Spruce Developer Update #1)
- [4] <https://sprucesystems.medium.com/reimagining-the-social-security-number-bdb17559ddb> (Spruce Systems Blog on Medium – Reimagining the Social Security Number)
- [5] <https://sprucesystems.medium.com/spruce-joins-the-w3c-4cae3a9357c4> (Spruce Systems Blog on Medium – Spruce Joins the W3C)
- [6] <https://sprucesystems.medium.com/spruces-origins-decentralized-markets-and-identity-4fda40c6db49> (Spruce Systems Blog on Medium – Spruce's Origins, Decentralized Markets, and Identity)
- [7] <https://sprucesystems.medium.com/spruce-developer-update-2-484368f87ee9> (Spruce Systems Blog on Medium – Spruce Developer Update #2)
- [8] <https://sprucesystems.medium.com/spruce-joins-the-decentralized-identity-foundation-200bd2948ad0> (Spruce Systems Blog on Medium – Spruce Joins the Decentralized Identity Foundation)
- [9] <https://sprucesystems.medium.com/spruce-developer-update-3-8565d9a1cf23> (Spruce Systems Blog on Medium – Spruce Developer Update #3)

## References for Slide (2/3): SSIs on Tezos: Spruce Systems



- [10] <https://did-tezos-draft.spruceid.com/> (W3C – Tezos DID Method Specification)
- [11] <https://sprucesystems.medium.com/introducing-didkit-an-identity-toolkit-e0dfa292f53d> (Spruce Systems Blog on Medium – Introducing DIDKit)
- [12] <https://sprucesystems.medium.com/spruce-developer-update-4-cd6472c58fe1> (Spruce Systems Blog on Medium – Spruce Developer Update #4)
- [13] <https://sprucesystems.medium.com/spruce-developer-update-5-86d6f517a220> (Spruce Systems Blog on Medium – Spruce Developer Update #5)
- [14] <https://sprucesystems.medium.com/spruce-developer-update-6-d9e692a13668> (Spruce Systems Blog on Medium – Spruce Developer Update #6)
- [15] <https://sprucesystems.medium.com/credible-v0-1-is-live-6d81a50b7967> (Spruce Systems Blog on Medium – Credible v1.0 is Live)
- [16] <https://sprucesystems.medium.com/decentralized-identity-with-the-tezos-did-method-d9cf6676dd64> (Spruce Systems Blog on Medium – Decentralized Identity with the Tezos DID Method)
- [17] <https://sprucesystems.medium.com/spruce-developer-update-7-5fe6776f25bb> (Spruce Systems Blog on Medium – Spruce Developer Update #7)
- [18] <https://sprucesystems.medium.com/spruce-developer-update-8-70f04e95a5d4> (Spruce Systems Blog on Medium – Spruce Developer Update #8)

## References for Slide (3/3): SSIs on Tezos: Spruce Systems



- [19] <https://sprucesystems.medium.com/announcing-tezos-profiles-own-and-control-your-creator-identity-ec0eddf9706d> (Spruce Systems Blog on Medium – Announcing Tezos Profiles)
- [20] <https://sprucesystems.medium.com/spruce-developer-update-9-7211c666efce> (Spruce Systems Blog on Medium – Spruce Developer Update #9)
- [21] <https://sprucesystems.medium.com/spruce-developer-update-10-9babe565efe9> (Spruce Systems Blog on Medium – Spruce Developer Update #10)

## References for Slide: SSIs on Tezos: Tezos Profiles



- [1] <https://sprucesystems.medium.com/announcing-tezos-profiles-own-and-control-your-creator-identity-ec0eddf9706d> (Spruce Systems Blog on Medium – Announcing Tezos Profiles)
- [2] <https://sprucesystems.medium.com/announcing-the-tezos-profiles-alpha-launch-7e889de2f6c3> (Spruce Systems Blog on Medium – Announcing the Tezos Profiles Alpha Launch)
- [3] <https://tzprofiles.com/> (Tezos Profiles)
- [4] <https://github.com/spruceid/tzprofiles> (Github Spruce - Tezos Profiles Source Code)

## References for Slide:

### THE ENVITED ECOSYSTEM: What is ENVITED's Goal?



- [1] <https://envited.market/> (ENVITED website)
- [2] <https://www.asc-s.de/en/> (asc(s website))