

# TEZOS in LUXEMBOURG



## Blockchain 3.0

Program:

30 ' – presentation and short questions

Few hours – free drinks, free finger-food

Networking. Free pictures ...!

Detailed questions

**BAKING ! BAKERS ! BAKERY !**

The last person that leaves the venue, receive a special gift from Grant Thornton Technology HUB : a VR Glasses set!

The third generation of Blockchain

Three new technical features

The third chance for us.



Iulian Nita

**Blockchain Expert,**  
Grant Thornton Technology HUB,  
Luxembourg

**Blockchain Architect,**  
European Commission,  
Luxembourg

**Baker**  
[www.tezos.lu](http://www.tezos.lu), Baking service.



Jonas Lamis

**Member Board of Directors,**  
Tezos Commons Foundation,  
Palo Alto

**Baker,**  
Tezos.community,  
Baking service



Sorin Cristescu

**Blockchain Competence Centre Leader,**  
European Commission,  
Luxembourg



Iulian – organizer

Jonas – Speaker – about TEZOS

Sorin – Speaker – about European regulation on Blockchain and Cryptocurrencies



The organizer of this event: Grant Thornton Technology HUB Luxembourg with a clear focus of developing and supporting projects in Blockchain, Cybersecurity and Start-ups market

# TEZOS COMMONS FOUNDATION

The mission of Tezos Commons Foundation is to foster the growth of the global Tezos ecosystem through the identification, funding and execution of projects that drive community growth, awareness and success.

[FIND OUT MORE ↓](#)

The sponsor of the event: The mission of Tezos Commons Foundation is to foster the growth of the global Tezos ecosystem through the identification, funding and execution of projects that drive community growth, awareness and success.

# TEZOS



[www.tezos.lu](http://www.tezos.lu)

Tezos.lu – is the Tezos community in Luxembourg. Our goal is to increase the awareness about TEZOS technology and to support Blockchain related projects.

# What is TEZOS ?



Tezos is a new decentralized Blockchain that governs itself by establishing a true digital commonwealth.

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

A [commonwealth](#) is a group that chooses to be linked together because of their shared goals and interests. Tezos aims to have their token holders make decisions together to govern the platform and improve it over time.

# The Evolution



**First Gen.**

**Blockchain  
Distributed  
Decentralized  
Immutable  
Resilient  
Open source  
Secure**



**Second Gen.**

**1<sup>st</sup> generation  
+  
Smart Contract  
Programmable  
New dApp model  
Multiple Tokens**



**Third Gen.**

**1<sup>st</sup> generation  
+  
2<sup>nd</sup> generation  
+  
Governance  
Formal Verification  
DPOS**

A new Blockchain technology to beat them all.  
A unique combination of new features.

# What is different ?



**First Gen.**



**Second Gen.**



**Third Gen.**

**TX=5 tx/s  
POW=70 TWh  
74 active forks**

**TX=15 tx/s  
POW=20 TWh  
5 active forks**

**TX=30 tx/s ?  
DPOS=few MWh  
0 active forks**

**C and C++  
2009  
Version 0.16**

**GoLang/Rust  
2015  
Version 1.8/2.0**

**OCaml  
2018  
Version 0.1**

70 TWh is the average consumption in a country like AUSTRIA.

The upgrades in client-server application are easy. The upgrades in decentralized and distributed systems need on chain governance!

The choice of OCaml was made, from the very beginning, to benefit from the safety and security of a statically-typed language, while still being able to execute code pretty fast. It also provides a well-designed module system, that helps encapsulate the economic protocol (the part of the crypto-ledger that needs to be updated) and abstract it from the other parts of the implementation.

# On-chain governance

## Problem

**Software!!!**

**Errors, bugs,  
improvements,  
new features**

**Upgrade!!!**

**Who? When?  
How? Why?**



## Solution

**Decentralized innovation  
and maintenance:  
reworded!**

**On-Chain governance:  
voting for amendments.**

**Self-amendment:  
upgrades without forks**



**Decentralized Innovation:** Proposed amendments to the protocol will include payments to groups or individuals to improve the protocol, furthering innovation and decentralizing the maintenance of the network.

**On-Chain governance:** stakeholders reach agreement (by voting) on proposed protocol amendments (upgrades).

**Self-amendment:** Allowing the network to upgrade itself over time without having to hardfork.

Tezos incorporates a process for upgrading the protocol over time through on-chain governance. This governance system is designed to allow for a smooth evolution of the blockchain rather than having to hard fork, which is a split of the blockchain into two separate versions. Hard forks, which both the Bitcoin and Ethereum blockchains have been subject to in the past, shouldn't be the standard way to upgrade over time.

In Tezos, developers are able to independently submit proposals for protocol upgrades wherein they include a request for compensation for their work. Tezos token holders can then vote on whether the proposal should be approved. Adding this compensation structure provides incentives for developers to continue improving upon Tezos rather than having to work for free, relying on donations, or being sponsored by a centralized entity. This innovative structure is intended to enable Tezos to support independent developers that contribute to the protocol over time.

# Formal Verification

**ETHEREUM Smart Contracts**

**Solidity / Assembly**

**Errors, Bugs, Hacks**

**Learning curve**

**Limitations?**



**TEZOS Smart Contracts**

**Liquidity / Michelson**

**Mathematically proof the correctness**

**Learning curve**

**Limitations?**



Programming is hard. Not because our hardware is complex, but simply because we're all humans. Our attention span is limited, our memory is volatile—in other words, we tend to make mistakes. There is a huge difference between “program correctness was *checked* by tests” and “program correctness was logically *proven*”. Unfortunately, even if we have a test for every single line of our code, we still cannot be sure that it's correct. However, having a formal system that would prove our code is correct (at least in some aspects) is another story. Smart contracts are both the strongest features and the weakest point of modern crypto- ledgers. Tezos also differs from Ethereum in that its smart contract programming language, named [Michelson](#), is a functional language which facilitates formal verification. Formal verification essentially allows developers to mathematically prove the correctness of their smart contract code. Formal verification proves that some properties of the contract will be maintained, but does not necessarily mean that the code is 100% correct. Formal verification is used in industries where there is little room for error (e.g. nuclear reactors, aircraft, medical devices). There have been [instances](#) of bugs within poorly implemented Ethereum smart contracts that could have been avoided had formal verification been applied. This does not mean that Ethereum itself had bugs, but it does provide a strong argument for creating formal verification tools that developers may use to facilitate ensuring smart contracts will behave as expected.

# Delegated Proof of Stake

**Proof of Work  
MINER / MINING**



**Delegated Proof of Stake  
BAKER/BAKING**

**High Power Consume**



**Low Power Consume**

**Hardware needed**



**Tokens/Delegation needed**

**High Maintenance cost**



**Low Maintenance cost**

**Risk to be centralized?**

**Economic penalties**



Ethereum is currently working towards [switching](#) from Proof of Work (PoW) to Proof of Stake (PoS) while Tezos lunched with delegated PoS from the start. PoW is an effective but resource intensive method of maintaining consensus across a peer to peer network, in fact, currently Ethereum miners are already using [more electricity than a small country like Cyprus](#). With PoS, validations are conducted through virtual mining rather than physical mining. In order to participate you only need to own the tokens rather than spend money purchasing mining hardware and electricity. An added benefit of PoS is that it enables [economic penalties](#) if someone tries to attack the network. Delegated PoS means that Tezos token holders can delegate someone else to validate on their behalf if they do not wish to participate in staking directly (e.g. lack of time, knowledge, or resources).

Bitcoin has mining, Tezos has baking. Bakers obtain the right to create a block when a Tezos token (a roll) they own (or that is delegated to them) is randomly selected to create a block. Since not everyone holding tokens is interested in being a baker, tokens can be “delegated” to another party. The delegate does not own or control the tokens in any way. In particular, it cannot spend them.

[www.tezos.lu](http://www.tezos.lu)



**The self-amending cryptographic ledger**