TzLibre

A blockchain virus to reboot Tezos*

Juan Dadores Huber Benitez

July 31, 2019 – v0.2 (DRAFT)

Abstract

In this paper we outline how to reboot Tezos by replacing the KYC-Tezos (XTZ) instantiation with the TzLibre (TZL) one and by democratically electing the Tezos Foundation board. To achieve these two goals we introduce the TzLibre Blockchain Virus. Inspired by the concept of dark DAO, a Blockchain Virus is designed to shutdown a Proof-of-Stake blockchain network by distorting stakeholders financial incentives and implemented as a collection of smart contracts deployed on the target blockchain. The TzLibre Blockchain Virus has been assigned a TZL genesis allocation, to be sold by a smart contract deployed on KYC-Tezos. Raised XTZ will fund the virus, which is made of three procedures: *Blockchain Slowdown* (blockchain slowdown by rewarding empty blocks), *Dump&Burn* (XTZ dump, TZL buyback, TZL burn), *Zimbabwe Inflation* (upgrading the protocol to increase bakers rewards). TzLibre, a new Tezos instantiation, is the first ungoverned Proof-of-Stake blockchain and it aims to address issues in KYC-Tezos such as: KYC, lack of hard-cap, token premine, low baking rewards, insecure consensus, low throughput, baking centralization, unbounded on-chain governance ("tyranny of the majority"). TzLibre is supported by the TzLibre Decentralized Foundation (TDF), a DAO with a TZL genesis allocation where funds are directly controlled by stakeholders to guarantee decentralized governance. The TzLibre blockchain has been deployed and an open-source client is available.

1 Introduction

> "Tezos is a Ferrari driven by my grandpa."
>
> —/u/bycherea

Tezos [1] is a great, disruptive idea: a truly decentralized commonwealth governed by its stakeholders and built upon provably safe code. Tezos has the technological and financial potential to overcome Ethereum: it raised more than 100,000 BTC in ICO contributions, and has a functioning, state-of-the-art PoS codebase. If properly managed it would capitalize as much as Cardano [2, 3] or EOS [4], its direct competitors. Unfortunately KYC-Tezos, the first Tezos instantiation, capitalizes a fraction of EOS, which launched around the same time and has inferior technology. Despite its great technological and financial potential, KYC-Tezos is currently the worst performer among the top-30 cryptocurrencies. We ascribe this to an incompetent management team responsible

* This document is targeted at specialists and not at the general public. It has been created, edited and will be constantly updated by the TzLibre community. It is not binding in any way, shape or form.

for fatal strategic mistakes and lost opportunities. As we predicted over a year ago, Tezos Stiftung (Tezos Swiss-based foundation, henceforth TS) has failed its mission and is now stalling Tezos. In a permissionless environment social consensus is vital and TS has lost it: a majority of XTZ stakeholders is now against its current management and wants decentralized decision making to steer the Tezos project. The current TS board must be removed and a new one shall be democratically elected by Tezos stakeholders. The purpose of this document is to describe a decentralized, incentive-driven Blockchain Virus to reboot Tezos, replace the current TS board and offer stakeholders direct governance over the project itself. The results of the reboot will be: 1) democratic election of a new board (or democratic confirmation of the current one); 2) decentralization of TS by handing decision making over to a DAO; 3) deployment of the TzLibre blockchain, a better instantiation of the Tezos idea; 4) slowdown and halt of the KYC-Tezos instantiation; 5) replacing KYC-Tezos with TzLibre; 6) anonymous activation of inactive XTZ accounts. The main components of the Blockchain Virus are: *Blockchain Slowdown*, an incentive scheme for baking empty blocks, *Dump&Burn*, the process of raising XTZ and selling them on the open market in exchange for TZL to burn, *Zimbabwe Inflation*, the process of upgrading the KYC-Tezos protocol to increase baking rewards.

The remainder of this paper is organized as follows. Section 2 provides an analysis of Tezos fatal management mistakes and estimates their financial impact on Tezos stakeholders. Section 3 offers an overview of the TzLibre blockchain and its token allocation. Section 4 introduces the blockchain virus and describes how it works, how it spreads and the effects it causes. Section 5 outlines the project's roadmap and major milestones. Finally, Section 6 reports some conclusive remarks.

2 Background

We estimate the damage caused by TS to amount between $700M and $3bn: this value must therefore be added to Tezos stakeholders in order to recover lost returns and express Tezos true potential. We ascribe this loss to TS management incompetence.

2.1 Tezos Stiftung Mistakes

We identified nine major mistakes by TS. They are outlined in what follows.

Locked Genesis and Mandatory KYC. TS deployed a locked genesis, forcing all ICO contributors to undergo a mandatory KYC under threat of spoliation and with no refund option. KYC was not agreed upon at ICO and is in clear violation of contributor's privacy rights. To date (Jul 2019) more than one third of ICO contributors was unable to unlock their own funds via forced KYC.

Low XTZ Value. No hard-cap has been set for XTZ, nor any bound to yearly inflation of money supply, which can be increased via on-chain upgrades. Additionally, more than 152M free XTZ have been premined and assigned to TS. TS has been using premined XTZ to pay contributors, who are forced to liquidate

them to cover their running costs. All of the above has contributed to XTZ price decrease and loss of confidence.

Abnormally Low XTZ Liquidity. TS deliberately chose not to work to list XTZ on exchanges (*e.g.*, Binance) nor hasn't it engaged in market making. The result is an abnormally low liquidity for a top-30 cryptocurrency. To date (Jul 2019) ZEC has similar market cap and 100x more liquidity than XTZ, while direct competitor EOS has 400x more liquidity. Our analysis shows that selling 2M XTZ will trigger a 70% price drop on average. We sampled XTZ liquidity over time, our analysis was carried out by aggregating data from the orderbooks of five exchanges (Bitfinex, Kraken, gate.io, HitBTC, KuCoin). For each exchange we fetched orderbook data of the following pairs: XTZ/BTC, XTZ/ETH, XTZ/USD, XTZ/USDT. We then normalized data by reducing fetched pairs to the reference XTZ/USD one, and ended up with a single aggregated orderbook. Finally, we simulated SELL take orders of 10K XTZ, 100K XTZ, 1M XTZ, 2M XTZ, and looked at price variations over time. Figure 1 shows the result of our analysis for a 5-days time window (from Jul 04 2019 12:00 UTC to Jul 09 2019 12:00 UTC). Data was sampled every 10 seconds and averaged each 1 hour.

Centralized Foundation. The current TS board is unelected, and its actions are not publicly audited. TS expenses are kept secret and not publicly audited, and decision making is fully centralized in the hands of a President with no qualifications. This has led to mismanagement, lost opportunities, misuse of funds and loss of confidence.

Low Baking Rewards. TS has unethically used its premined vested stake (more than 152M XTZ) to become the biggest baker in the KYC-Tezos network. TS has continuously earned liquid XTZ rewards from vested XTZ, taking rewards away from legitimate small bakers. As a result, baking is now extremely centralized in the hands of TS, and financial incentives for small, independent network validators ("solo bakers") have been and still are extremely low.

Centralized On-Chain Governance. TS premined XTZ can be used to take part in on-chain governance thus distorting quorum and votes. This violates the principle of decentralized governance.

No Developers. Two years after ICO, TS has failed at building a thriving developers community around the Tezos technology. Not only did it fail to attract new developers, it also alienated OcamlPro, the company that developed the Tezos technology itself. This resulted in OcamlPro's involvement in Dune [5], a competing blockchain project based on the same programming language and know-how.

No Traction. TS chose to not engage in any marketing and has failed at developing business through other means, such as strategic relationships with companies and nation states. This is the opposite of what was promised during ICO [6]. The end result is lack of any business traction or real usage of the

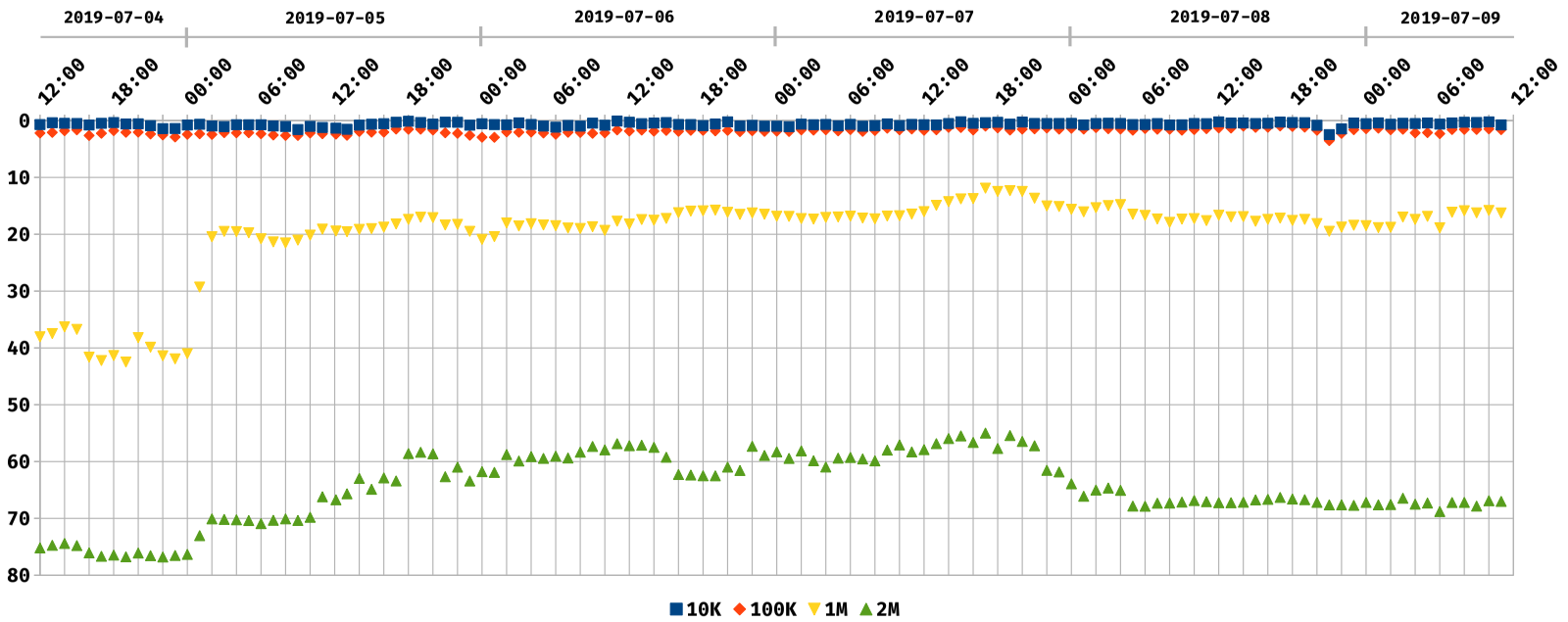


Figure 1: Decrease in XTZ price over 5-days time window (2019-07-04 12:00 UTC → 2019-07-09 12:00 UTC) for SELL orders of 10K, 100K, 1M, 2M XTZ, on aggregated orderbook of multiple exchanges (Bitfinex, Kraken, gate.io, HitBTC, KuCoin) and pairs (XTZ/BTC, XTZ/ETH, XTZ/USD, XTZ/USDT)).

KYC-Tezos blockchain: two years after ICO, at block 500,000 there were only 26,515 accounts with more than 1 XTZ, less than the 30,317 ICO contributors.

Poor ICO Wallet and Lost Passwords. Due to a poor ICO wallet design many contributors lost their ICO password. No option was offered them to unlock funds via proof of ownership of their BTC/ETH contribution wallet.

2.2 Estimating the Damage

We hereafter estimate the financial loss caused by TS to Tezos ICO contributors. Table 1 reports a comparison among ICOs of EOS, Cardano and Tezos.

	Volume	Mkt cap	ICO ROI
EOS	∼68,000 BTC	∼372K BTC	+6%
Cardano	∼4,700 BTC	∼146K BTC	+153%
Tezos	∼159 BTC	∼69K BTC	-50%

Table 1: EOS, Cardano and KYC-Tezos ICO comparison on July 23 2019.

KYC-Tezos has better features than Cardano and EOS, as shown in Table 2.

	EOS	Cardano	KYC-Tezos
Smart contracts	Yes	No	Yes
Validators	21	n/a	400+
On-chain governance	No	No	Yes
Formal verification	No	No	Yes

Table 2: EOS, Cardano, KYC-Tezos features comparison.

To estimate KYC-Tezos potential value we therefore assume the Cardano market cap as lower bound and the EOS market cap as upper bound. If properly managed, KYC-Tezos would now trade within ranges reported in Table 3.

	Potential value (low)	Potential value (high)	Actual value
Market cap	146K BTC	372K BTC	69K BTC
Price	0.00021 BTC	0.00053 BTC	0.00010 BTC

Table 3: KYC-Tezos potential and actual value, July 23 2019.

We therefore estimate the damage caused by TS between 77K and 303K BTC (equivalent to $700M and $3bn at current BTC value, Jul 2019).

3 Blockchain

TzLibre is a new, improved instantiation of Tezos. Designed for bakers by bakers, it's based on a fork of KYC-Tezos and it's the first ungoverned Proof-of-Stake blockchain network. An open-source client is available[1] and a test network is currently up and running.

[1] `https://github.com/tzlibre/tzlibre`

3.1 Distinctive features

Compared to KYC-Tezos, the TzLibre blockchain features improvements on several aspects, namely: tokenomics, decentralization, privacy, performance and governance.

3.1.1 Tokenomics

Unlike KYC-Tezos, TzLibre has a hard-cap, no premine, different rewards for bakers, a token allocation to TzLibre Decentralized Foundation (henceforth TDF, a DAO managed by stakeholders, see Section 3.4.4). TzLibre has a hard-capped supply of 763,306,929.69 coins. No premine means that no coins are created out of thin air and assigned for free to special groups. Stakeholders interests are more protected because TZL are more evenly distributed. TZL are more valuable because, unlike KYC-Tezos, TzLibre founders don't get any free coin.

3.1.2 Decentralization

TzLibre is more decentralized than KYC-Tezos thanks to a different baking model. Solo bakers are strongly incentivized and there's no centralized entity baking with premined tokens.

3.1.3 Privacy

TzLibre is fully permissionless and unlike KYC-Tezos no identification (KYC) is required. TzLibre founders and developers are pseudonymous. Tezos ICO contributors who refused to KYC ("inactive" contributors) have the same rights as other contributors ("active" contributors).

3.1.4 Performance

We successfully tested a 5x increase in block gas limit and a 50% blocktime reduction compared to KYC-Tezos. We achieved 100+ transactions per second (tps), a 1,000% increase in max throughput.

3.1.5 Governance

TzLibre addresses flaws in the KYC-Tezos governance model.

Decentralized Foundation. Stakeholders directly control TDF funds: they can therefore directly vote to choose Foundation expenses (*e.g.*, Binance listing, marketing, OcamlPro funding, etc.).

Trustlessness. Unlike KYC-Tezos, no one holds special powers or premined voting stake in TzLibre. There are no premined coins in TzLibre: founders can't influence decisions with their own stake (see Section 3.4). TzLibre founders are pseudonymous to stay protected from undue pressure, coercion and special interests. TzLibre development team is open, with no single developer in charge.

Direct Democracy. Given increased deposits, network participants are incentivised to take direct part in on-chain governance rather than delegating voting power to other bakers (delegation).

Off-Chain Schelling Fences. Any true blockchain network needs strong Schelling fences: an unbreakable social consensus on non-negotiable rules. TzLibre's Schelling fences are: 1) hard-cap: there will never be more than 763,306,929.69 TZL in circulation; 2) no non-technical forks: to protect the network from social attacks, TzLibre mainnet shall never fork for non-technical reasons. The TzLibre mainnet will mostly upgrade via on-chain governance. Hard forks will only be accepted for fixing serious and urgent issues that can't be fixed via on-chain governance in a timely fashion. These Schelling fences will be expressed and agreed upon in a "wet code" (natural language) Constitution, cryptographically signed by network stakeholders.

3.2 Network releases

Each stage is associated with release of a new network version.

Devnet. Test network.

Betanet. Transaction are final, frequent hard forks, presale, XTZ snapshot free airdrops.

Gammanet. Only trustless TZL allocations (no presale, no XTZ snapshot, TDF allocation locked in escrow contract), Blockchain Virus deployed, performance improvements.

Mainnet. TDF deployed, Liquid Avalanche consensus protocol, constitutional on-chain governance.

3.3 TZL Token

TZL is the ticker for both the native TzLibre coin and the ERC20 prelaunch token[2]. TZL ERC-20 prelaunch tokens have been issued on Ethereum since July 2018. All ERC-20 prelaunch tokens shall be migrated into TZL native coins before Jul 31 2020: tokens that haven't been migrated will effectively be lost (for a detailed description of the ERC-20 token migration procedure refer to Appendix A.2). TZL has a non-negotiable hard-cap of 763,306,929.69 TZL. The genesis block carries 47.34% of the hard-cap, while up to 52.66% will be baked over time.

Genesis	→	361,374,769.69 TZL
Baking	→	401,932,160.00 TZL
Hard-cap	→	763,306,929.69 TZL

[2] `https://etherscan.io/token/0x6b91bc206eed0a8474f071339d1fd7ed7156f856`

3.4 Genesis

TzLibre genesis block includes six different allocations. Table 4 provides details on these allocations and their attributes. See Section 5 to learn more about TzLibre four development stages mentioned in the "Notes" column of Table 4.

	Amount	Bakes	Votes	Notes
Protocol injection	100.00	No	No	—
Presale	107,917,258.00	No	No	Sold OTC in stages 1,2
Bootstrap bakers	2,082,742.00	Yes	Yes	—
XTZ Snapshot	50,487,114.00	No	No	Distributed in stage 2
TDF	100,887,555.69	No	No	Active in stage 4
Blockchain virus	100,000,000.00	No	No	Sold by smart contract in stages 3,4
Total in genesis	361,374,769.69			
Total staked	2,082,742.00			

Table 4: Genesis allocation.

3.4.1 Presale

This allocation will be sold in exchange for XTZ: raised funds will be used to fund development of gammanet. The presale will end when 2M XTZ have been raised. Unlike KYC-Tezos premined XTZ, unsold tokens won't be used for baking or on-chain voting, and any remaining token will be assigned to TDF when presale ends.

Over The Counter. OTC presale will begin Oct 1 2019, at increasingly higher prices. Current presale price and total raised amount will be available on our website.

TZL Minting: Delegations and deposits. Delegating XTZ to LibreDelegate (see Section 4.5.1) and depositing XTZ into LibreBank (see Section 4.5.2) allows to "mint" TZL: an indirect way to buy TZL with XTZ baking rewards. Between Jul 1 2018 and Jul 15 2019, 8,309,197 TZL have minted, at an average cost of 0.01 XTZ. TZL airdrops have been based on the amount of XTZ delegated to LibreDelegate and the amount of XTZ deposited into LibreBank: their fair distribution can be publicly audited downloading cryptographic proofs from our website[3]. A total of 2,082,742.00 TZL ERC-20 have been migrated before genesis (see Section 3.4.2). From Oct 1 2019 onward, TZL minting cost will be a function of current OTC price (deposit = 3x OTC price, delegation = 9x OTC price).

3.4.2 Bootstrap Bakers

ERC-20 prelaunch tokens migrated before Jul 16 04.00 UTC (min 8,000 TZL) are assigned the genesis allocation named "Bootstrap Bakers". Unlike KYC-Tezos, there is no premine in TzLibre and therefore no premined allocation can

[3] `https://tzlibre.io/audit.csv`

bake. See Section 3.4.1) for more information on ERC-20 prelaunch tokens, and Section A.2 for more information on token migration.

3.4.3 XTZ Snapshot

A snapshot of the KYC-Tezos blockchain has been taken at block 500,000. A total of 37,509 accounts (26,497 "active" and 11,012 "inactive") are eligible to receive **1,346 free TZL** each, regardless of their XTZ balance, as incentive to join the TzLibre network as bakers and thus foster decentralization. Such democratic allocation is designed to foster network decentralization and Sybil-resistance. Accounts with less than 1 XTZ and those owned by Tezos Foundation are not eligible. We will introduce a Constitution for XTZ holders to cryptographically sign and support TzLibre. Snapshot tokens can be claimed with the LibreBox wallet (see Appendix A.5) from Jan 13 2020 until Jun 13 2020. Unlike KYC-Tezos premined XTZ, unclaimed coins won't be used for baking or on-chain voting, and any remaining coin will be assigned to TDF before gammanet launch.

3.4.4 TDF

At mainnet launch the TzLibre Decentralized Foundation, a DAO managed by TZL owners, will be deployed as a smart contract with its own TZL allocation. Funds will be directly controlled by TZL stakeholders, with no centralized entity in charge. TZL stakeholders will be able to directly fund ongoing development of the project via grants, bounties, salaries, etc. Unlike KYC-Tezos premined XTZ, TDF tokens won't be used for baking or on-chain voting. At gammanet launch the final TDF allocation will be locked in an escrow contract until mainnet launch, when it will be assigned to the DAO contract.

3.4.5 Blockchain Virus

Allocation for raising XTZ to fund the Blockchain Virus (see Section 4) and mainnet development. TZL tokens will be sold by an ICO-like smart contract at increasingly higher price starting from 0.10 XTZ / TZL up to 10 XTZ / TZL. The sale will begin on gammanet launch and end when 110M XTZ have been raised. Unlike KYC-Tezos premined XTZ, unsold TZL can't be used for baking or on-chain voting.

3.5 Baking

Baking in TzLibre is significantly different than KYC-Tezos. The main differences are: larger baking coinbase (52.66% allocated to baking), no premine baking (no genesis allocation used for baking except bootstrap bakers), lower roll size, higher deposits, rewards halving. This results in significantly higher rewards for bakers and increased network decentralization. Unlike KYC-Tezos, bakers are heavily incentivized to support network growth. As in Bitcoin, TzLibre rewards halve regularly: TzLibre halving period is set to 256 cycles (estimated 2 years). Figure 2 shows how TZL supply grows over time.

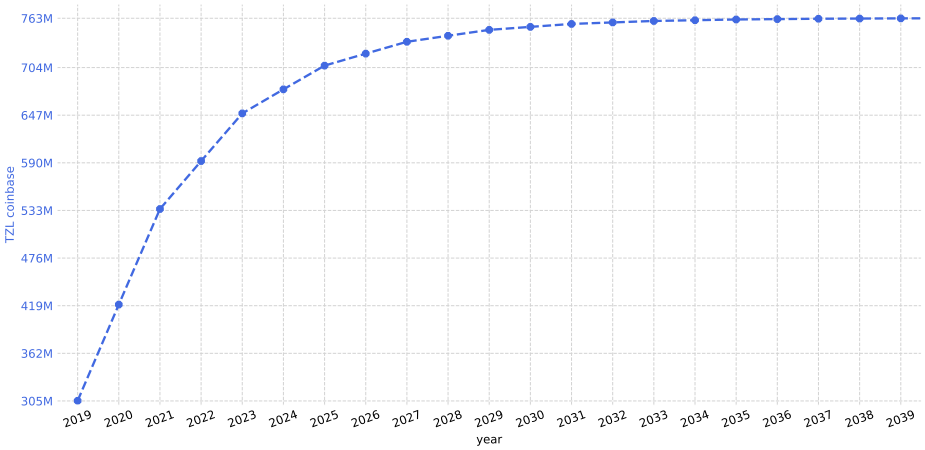


Figure 2: Expansion of TZL supply.

	Month 1	**Month 12**	**Month 24**	**Month 36**
Secure deposit (max)	44.28%	48.19%	25.85%	20.05%
Monthly reward (max)	253.03%	9.59%	4.57%	1.76%

Table 5: Estimate baking secure deposits and rewards (best case).

Table 5 estimates secure deposits and rewards for a TzLibre baker staking 20,000 TZL from the beginning (best case scenario): thanks to rewards compounding, at the end of the first halving period this baker owns more than 1M TZL.
Table 6 reports the most relevant baking parameters and constants.

hard-cap	763,306,929.69	TZL
total rewards for first halving period	200,572,800.00	TZL
total reward for first year	100,679,680.00	TZL
upper bound coinbase from rewards	460,537,728.00	TZL
`tokens_per_roll` (roll size)	1,000.00	
`cycles_per_halving_period`	256	
`blocks_per_cycle`	4,096	
`preserved_cycles`	3	
`no_reward_cycles`	1	
`block_reward`	64.00	TZL
`endorsement_reward`	4.00	TZL
`seed_nonce_revelation_tip`	1.00	TZL
`security_deposit_ramp_up_cycles`	128	
`block_security_deposit`	1,344.00	TZL
`endorsement_security_deposit`	84	TZL
`time_between_blocks`	60/75	sec
`blocks_per_roll_snapshot`	256	
`blocks_per_commitment`	32	

Table 6: A selection of the most relevant baking parameters and constants.

3.6 Upcoming Features

The following improvements are part of the TzLibre development roadmap toward mainnet.

3.6.1 Performance and Scalability

In order to gain real traction a Tezos instantiation shall reach a performance comparable to or greater than EOS. TzLibre mainnet will reach a maximum throughput greater than **1,000 tps**, greater than EOS and two orders of magnitude greater than KYC-Tezos (∼13 tps). Such performance will be achieved with six key innovations.

Transactions caching. Instead of sending a block with raw transactions, mempool txs are indexed and only an index is sent. This allows to propagate 100x larger blocks at the same speed. This is how Graphene [7], the technology powering EOS transactions caching, works.

Multithreading. Rather than running on a single thread, the TzLibre node will scale horizontally implementing native multithreading.

Cut-Through Routing. Rather than transmitting blocks to its peers only when the block is fully received and validated, nodes don't wait until the entire block is received before sending it to a peer node. Each packet of data is immediately streamed as it is received. This technique allows data to broadcast 10–100x quicker.

Increased Gas Limit and Shorter Blocktime. Improving on KYC-Tezos, we already successfully tested a 5x increase in block gas limit and a 2x shorter blocktime, already enabling 10x more transactions per second. We plan to gradually increase it even more, up to 100x current KYC-Tezos levels.

Optimized Network Topology. KYC-Tezos seed nodes provide joining nodes with their initial peer list to connect to, and from there new nodes can crawl through the network. The result is a web of random connections where data is not propagated throughout the network in the most optimal route. Instead of random connections, TzLibre nodes will connect to other nodes with lower latency, resulting in an optimized network topology [8].

Ad-Hoc Relay Network. KYC-Tezos p2p network is badly designed: bakers are mixed with non-bakers in the same p2p network. In TzLibre a UDP-based network is deployed, dedicated to TzLibre bakers. Inspired by Bitcoin's FIBRE[4] it also eliminates latency spikes by sending extra data to compensate for packet loss.

[4] `http://bitcoinfibre.org`

3.6.2 Liquid Avalanche: a New Consensus Protocol

The LPoS consensus protocol has never been formally proven safe: not surprisingly it already had catastrophic failures, *e.g.*, Nov 23rd, 2018. The new Avalanche protocol [9, 10], a breakthrough in distributed systems, can achieve greater performance than EOS DPoS in a fully decentralized network with a wide and dynamic validator set. Avalanche has been formally defined and unlike LPoS already has correctness proofs. After optimizing performance (see Section 3.1.4) TzLibre will then switch to a new model implementing "Liquid Avalanche", a variant of the Avalanche consensus protocol adapted for Tezos and inspired by LPoS. Liquid Avalanche can reach better performance compared to the upcoming AVA blockchain by allowing stakeholders to delegate other nodes shall they find that more profitable. The free market of delegations then discovers the most optimal equilibrium in the performance / decentralization tradeoff. Liquid Avalanche can compete with EOS DPoS performance (1,000+ tps) while at the same time being orders of magnitude more decentralized (21 static validators).

3.6.3 Constitutional On-Chain Governance.

A major TzLibre tech milestone is to protect ledger immutability from on-chain governance, to avoid a "tyranny of the majority". Unlike KYC-Tezos, TzLibre's will implement a "bounded governance" with a dry code Constitution: a set of immutable norms encoded in the protocol. These norms are hardcoded and non-negotiable, they can't be changed with on-chain governance. These rules are: 763,306,929.69 coins hard-cap, smart contracts immutability, transactions irreversibility, addresses uncensorability. Transactions, balances and smart contracts can't be changed with on-chain governance.

4 Blockchain Virus

> "With two [blockchain] players, and the underdog incentivized to launch a bribery attack to destroy their competitors, such equilibria can be disrupted, changed, and destroyed."
>
> —[11]

We define Blockchain Virus as a collection of procedures designed to shutdown a Proof-of-Stake blockchain network (*target* blockchain) and transition to a new instantiation (*replacement* blockchain). It does so by distorting stakeholders financial incentives, and can be implemented as a set of smart contracts deployed on the target and/or replacement blockchain. A Blockchain Virus works to shutdown throughput and dump price of the target blockchain coin. It does so by distorting collective incentives with individual ones so that rational actors will profit at the expense of the target blockchain. Effectiveness of this model is based on Proof-of-Stake inherent weaknesses and the understanding that blockchain networks safety is ultimately based upon social consensus among stakeholders, the lack of which may prelude to an attack. If an attack does indeed take place and reaches a tipping point, a critical run to liquidate

target blockchain coins will take place (a “blockchain run”) in favor of replacement blockchain coins. A Blockchain Virus is a specific instance of the class of incentive-driven attacks on public blockchain networks introduced in [11] by Daian, Kell, Miers and Juels.

4.1 TzLibre Blockchain Virus

TzLibre Blockchain Virus is the first implementation of a Blockchain Virus specifically designed to target KYC-Tezos, as Daian, Kell, Miers and Juels shown in [11], is vulnerable to such attack. The TzLibre Blockchain Virus aims to reboot Tezos by replacing the KYC-Tezos blockchain with the TzLibre blockchain and by resetting the TS board. The expected outcome is a gradual shutdown of the KYC-Tezos blockchain and transition to the TzLibre blockchain. The virus can be stopped by a supermajority of TZL holders. A Schelling point exists in that the virus shall be stopped if and when the current TS board stands for democratic election: should that happen, former board members will be rewarded for stepping down. It is deployed as a collection of smart contracts on the KYC-Tezos and TzLibre blockchains. It leverages generic Proof-of-Stake weaknesses as well as KYC-Tezos specific design mistakes (LPoS, unbounded on-chain governance, XTZ premine, no hard cap) and the result of TS management mistakes (abnormally low XTZ liquidity, low social consensus among stakeholders).

4.2 Mechanics

The TzLibre Blockchain Virus attacks KYC-Tezos on three sides: **throughput** (*Blockchain Slowdown* procedure), **price** (*Dump&Burn* procedure) and **supply** (*Zimbabwe Inflation* procedure). While any blockchain could be targeted by a bribery attack [12, 13, 14], XTZ abnormally low liquidity is a unique weakness that allows for significant price suppression with relatively limited means. These attacks are funded with XTZ raised by selling TZL from the Blockchain Virus allocation in genesis as depicted in Figure 3.

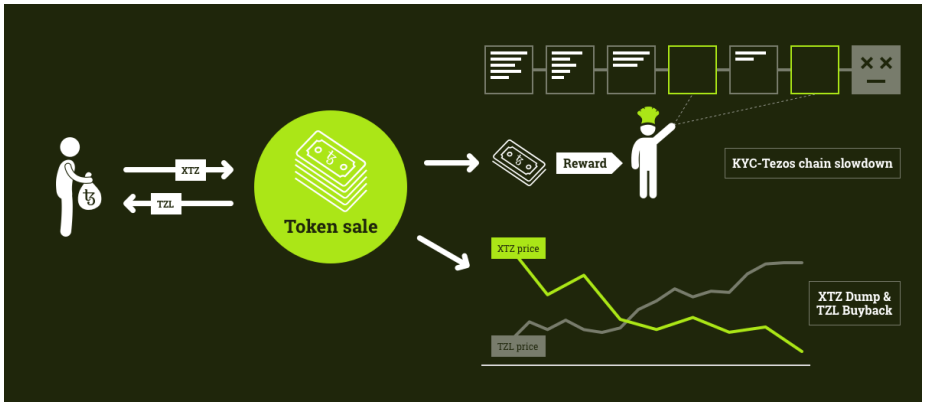


Figure 3: Mechanics of *Blockchain Slowdown* and *Dump&Burn*.

4.2.1 *Blockchain Slowdown*

KYC-Tezos bakers closing empty blocks (blocks with no transactions) receive XTZ rewards from an ad-hoc smart contract. Essentially, block producers are rewarded to slow down the KYC-Tezos blockchain. As more empty blocks are closed, the KYC-Tezos blockchain throughput decreases. To close empty blocks, a KYC-Tezos baker only needs to significantly increase the minimum transaction fee. Additional rewards will range from 32 XTZ to 64 XTZ (standard KYC-Tezos block reward is 16 XTZ). *Blockchain Slowdown*is a core procedure and the first to be activated.

4.2.2 *Dump&Burn*

XTZ are sold on the open market (dump) and TZL are bought in exchange (buyback). Bought TZL are then burned to decrease money supply (burn). This process increases TZL price in XTZ terms, and given XTZ abnormally low liquidity it can quickly lead to a blockchain run and/or a flippening event (TZL price > XTZ price). As TZL price grows, confidence in TzLibre and likelihood of success increase as well: more XTZ are then raised and dumped to buy TZL, in a virtuous cycle. As XTZ price begins to drop significantly, panic sell dynamics will amplify the effect of *Dump&Burn* in a downward spiral. *Dump&Burn*is a core procedure and the second to be activated.

4.2.3 *Zimbabwe Inflation*

Following the example of bankers management of fiat currencies, XTZ inflation rate will be gradually increased to better reward KYC-Tezos bakers. As shown in Figure 4, new protocol upgrades will provide additional coinbase to bakers supporting them: this manipulates on-chain governance creating a financial incentive to vote for such upgrades.

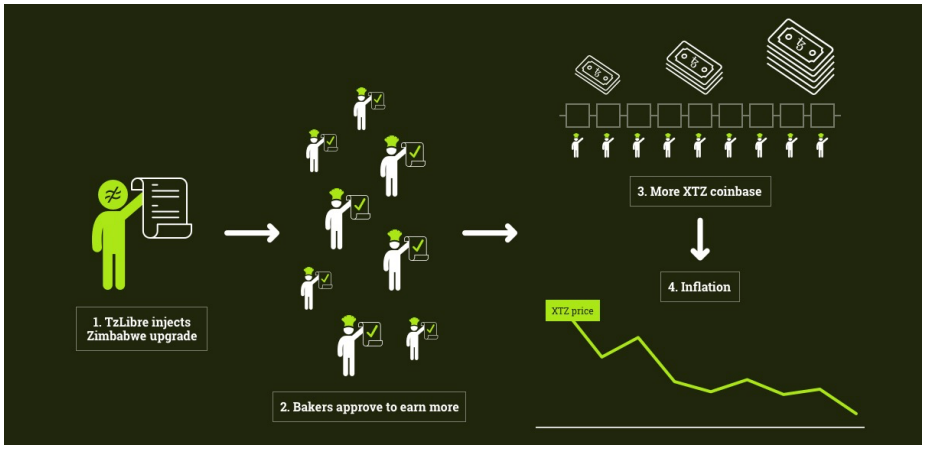


Figure 4: Mechanics of *Zimbabwe Inflation*.

Zimbabwe Inflation exploits the fatal mistake of combining on-chain protocol upgrades with the absence of a money supply hard-cap. While profitable on the

short term and at an individual level, unbounded increase in money supply will inevitably result in decreased confidence in XTZ as hard currency [15], and will contribute to its capitulation (*i.e.*, "tragedy of the commons" [16]). Inflation will be increased via protocol upgrade proposals injected by LibreDelegate (see Section 4.5.1). *Zimbabwe Inflation* is an optional procedure and the last to be activated, only after a majority of blocks are already empty thanks to *Blockchain Slowdown*.

4.3 Dynamics

Here are three steps for rational XTZ holders to take after the Blockchain Virus is deployed.

I. Get Rewarded. Rational XTZ delegators should delegate bakers offering increased rewards earned by baking empty blocks. Any rational XTZ baker should begin to bake empty blocks in order to receive additional rewards.

II. Early Conversion. As confidence in XTZ decreases, rational XTZ holders should hedge their Tezos exposure by early converting a minor chunk of their stake into TZL at a convenient price.

III. Full Conversion. As flippening approaches it becomes rational for XTZ holders to convert their full stake.

IV. Blockchain Run. A blockchain token can only survive as long as most of its holders have confidence in its future value. As soon as confidence is lost, holders try to liquidate their stake. XTZ abnormally low liquidity makes it a perfect target for a "blockchain run", a blockchain version of a bank run (for a theoretic explanation see "sunspot equilibrium" [17, 18]). As TzLibre slowly grows, confidence in XTZ will decrease and eventually trigger a critical run to liquidate XTZ. After beginning the attack we therefore expect an initially unnoticeable yet exponential decrease in XTZ price. This process will be driven by *Dump&Burn* until a tipping point is reached: at that point a critical run to liquidate tokens takes place (a "blockchain run").

4.4 Implementation

Four main procedures will be implemented as a set of trustless KYC-Tezos smart contracts. These procedures will be supported by a TZL representation on the KYC-Tezos blockchain, a token akin to the TZL ERC-20 deployed on Ethereum. The process can be stopped by a supermajority of TZL holders.

Sell TZL. An ICO-like smart contract is deployed on KYC-Tezos: it raises XTZ selling TZL allocated to the Blockchain Virus in genesis. These XTZ are then transferred to the following two contracts.

Reward empty blocks. A smart contract deployed on KYC-Tezos allows bakers to redeem additional XTZ rewards for each empty block baked (RPC data provided by an external oracle).

Buyback TZL. An ad-hoc decentralized exchange (DEX) is deployed on KYC-Tezos and funded with XTZ. TZL holders can sell their tokens to the DEX, which buys them with XTZ.

Burn TZL. Bought TZL are locked in a smart contract and thus become effectively burned.

4.5 Supporting tools

Three additional tools will support the TzLibre Blockchain Virus.

4.5.1 LibreDelegate

LibreDelegate[5] is a major baker and public delegate on KYC-Tezos. LibreDelegate has been successfully baking on XTZ since cycle 8, with a bake success greater than 99%[6]. A secure and redundant infrastructure has been developed to allow for massive scaling of its baking operations. LibreDelegate rewards delegators with TZL from presale allocation (see Section 3.4.1, "Delegations and Deposits"). LibreDelegate is the first baker to produce empty blocks as part of *Blockchain Slowdown*, and it will be used to inject *Zimbabwe Inflation* protocol upgrades on KYC-Tezos.

4.5.2 LibreBank

LibreBank is the first bond pooling contract ever deployed on KYC-Tezos[7]. It accepts XTZ deposits and rewards depositors with TZL from presale allocation (see Section 3.4.1, "Delegations and Deposits"). LibreBank v2 was deployed on Sep 06 2018[8] and has been successfully working ever since. It currently holds 200K+ XTZ in deposits, and it's fully collateralized. LibreBank provides the required XTZ to cover LibreDelegate's security deposit.

4.5.3 LibreActivate

A significant amount of XTZ owned by Tezos ICO contributors is still seized by TS. TS is asking contributors ("inactive" contributors) to provide an ID in exchange for returning their funds, while contributors are refusing to give up their privacy rights. LibreActive allows "inactive" accounts to join TzLibre. LibreActivate is a pseudonymous, trustless XTZ activation: it allows XTZ ICO contributors whose XTZ have been seized by TS to liberate their account without sharing any personal data. A smart contract allows inactive accounts to pre-sign a transaction and place a bid for the activation of their own account. Activators then

[5] LibreDelegate address `tz1iDu3tHhf7H4jyXk6rGV4FNUsMqQmRkwLp`
[6] Check Bakendorse stats.
[7] LibreBank v1 deployed on Aug 17 2018, address `KT1Ag29Dotu8iEigVrCARu7jmW5gkF1RyHUB`
[8] LibreBank v2 address `KT1V7VoyjbvqSmnRtv9pHkRuBCPT7UubCrCX`

compete to activate those accounts and thus earn a fee. LibreActivate allows contributors to unlock their XTZ and use them to join TzLibre.

4.6 Potential outcomes

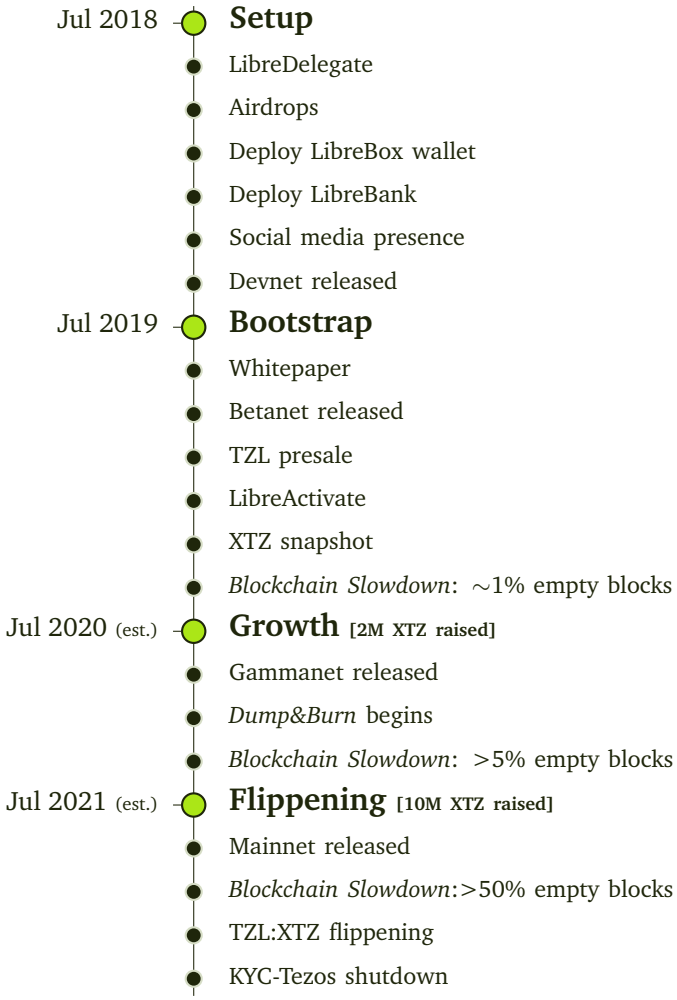
Presale pace will determine timing of TzLibre Blockchain Virus injection. In stage 3 TzLibre Blockchain Virus will be deployed and an irreversible process will begin. There are two potential outcomes of such process:

Replacement (default). If the current TS board does not stand for election, the attack on XTZ price and throughput will not stop. After reaching a majority of rewarded bakers, a protocol upgrade will be injected to permanently halt the KYC-Tezos blockchain ("Terminator upgrade"). This final upgrade will trigger full capitulation of KYC-Tezos, rendering the blockchain unusable and/or XTZ worthless, and its voters will be rewarded with TZL coins.

Coexistance. If the current TS board stands for election or resigns and is replaced by a democratically elected one, the attack on throughput (*Blockchain Slowdown*) and XTZ price (*Dump&Burn*) will stop. Board memebers will be rewarded with TZL by TzLibre Decentralized Foundation and with unused XTZ raised. Now officially supported by TS, KYC-Tezos and TzLibre will cooperate as two official Tezos instantiations.

5 Roadmap

In its first year TzLibre already accomplished all goals set. We now show a tentative roadmap of activities the TzLibre community should accomplish in the coming years. The beginning of each stage is triggered by specific fundraising milestones as described in Table 7. While it's hard to predict how long will stage 2 last, in stage 3 an irreversible process is initiated by deploying the Blockchain Virus.



In Table7 we outline a summary TzLibre's four stages. Each stage is triggered by a predefined fundraising milestone, and during each stage TZL are sold at increasing prices. During the first two phases only presale allocation TZL is sold, while in the last two phases only TzLibre Blockchain Virus allocation TZL is sold. Due to *Dump&Burn* our estimates assume falling XTZ prices (see also Figure 1 and Section 4.2.2).

Stage	**1.Setup**	**2.Bootstrap**	**3.Growth**	**4.Flippening**
Start	07/18	07/19	07/20**	07/21**
TzLibre network	Devnet	Betanet	Gammanet	Mainnet
Amount raised (start)	—	100K XTZ	2M XTZ	10M XTZ
Amount raised (end)	100K XTZ	1M XTZ	10M XTZ	100M XTZ
Raised by	Presale	Presale	Blockchain Virus	Blockchain Virus
Sold (max)	10M TZL	100M TZL	50M TZL	50M TZL
XTZ				
Total dumped	100K XTZ	2M XTZ	8M XTZ	75M XTZ
Price (avg)	0.00015 BTC	0.00010 BTC	0.00005 BTC**	0.00002 BTC**
Expenses				
Development	100K XTZ	1M XTZ	4M XTZ	(tbd)
Dump&Burn	—	—	4M XTZ	75M XTZ
Burned	—	—	21M TZL	37M TZL
Reward per block	—	—	32 XTZ	64 XTZ
Empty blocks	—	—	10%	75%
Blockchain Slowdown	—	—	1.7M XTZ	25M XTZ
TZL				
Supply**	10M TZL	260M TZL	410M TZL	510M TZL
Stock/flow	—	0.04	1.74	4.10
Reception				
Censorship	Yes	Yes	Yes	No
Attitude	Ignore	Ridicule	Lessen	Panic

Table 7: Roadmap summary. (**: estimate)

5.1 Governance Roadmap

Here's a preliminary list of potential TDF expenses.

Developers. Bounties, grants, development.

Binance. List TZL, market making.

OcamlPro. Liquidity development, full open-sourcing of TzScan.

Major PR firm. Massive marketing campaign for TzLibre.

Current TS board. Reward board members to resign and be replaced by democratically elected ones.

Swiss legal firm. Hold TS accountable for mismanagement, democratic election of the board, transparent and democratic fund allocation.

Future TS board. Reward future board members for executing stakeholders decisions.

XTZ bakers. Reward XTZ bakers with TZL to upgrade the KYC-Tezos protocol and terminate the blockchain ("Terminator upgrade") or significantly inflate XTZ ("Zimbabwe upgrade").

5.2 Development Roadmap

In addition to implementing useful and secure KYC-Tezos protocol upgrades, TzLibre plans to focus on blockchain scalability and immutability as described in Section 3.6.

5.3 Important dates

Who	What	How	Start (est.)
Active XTZ	Get TZL airdrops	Delegate/deposit[9]	Jul 1 2018
TZL ERC-20	Migrate ERC-20 tokens	Link and burn[10]	Jul 1 2019
Active XTZ	Buy TZL OTC	LibreBox	Oct 1 2019
Inactive XTZ	Activate without KYC	LibreBox	Oct 1 2019
Active XTZ	Get ∼1.3K free TZL	LibreBox	Jan 1 2020
Inactive XTZ	Get ∼1.3K free TZL	LibreBox	Jan 1 2020

6 Conclusion

TzLibre, a new Tezos instantiation, is the first ungoverned Proof-of-Stake blockchain and it addresses major flaws in KYC-Tezos. Some of the TzLibre innovations are: token hard-cap, no token premine, majority of tokens assigned as baking rewards, DAO-based Foundation, Liquid Avalanche consensus protocol and high throughput, baking decentralization (strong incentives for solo bakers), constitutional on-chain governance to protect from "tyranny of the majority".

A potential outcome is for the current TS board to be removed and for TzLibre to establish itself as other forks (Bitcoin Cash, Ethereum Classic, ZClassic, and others). An alternative outcome is for TzLibre to completely replace KYC-Tezos. To achieve its goals a Blockchain Virus has been designed: a set of smart contracts to distort KYC-Tezos incentives so that rational actors can profit at the expense of the KYC-Tezos commonwealth. This is allowed by KYC-Tezos fatal design mistakes (LPoS, unbounded on-chain governance, XTZ premine, no hard cap) combined with its specific management errors (abnormally low XTZ liquidity, low social consensus among stakeholders). To our knowledge this is the first real-world implementation of a dark DAO [11], and the first time the concepts of "blockchain virus" (a collection of smart contracts aimed at shutting down a Proof-of-Stake network) and "blockchain run" (a critical run to liquidate blockchain tokens) were introduced. A Blockchain Virus could be used to test blockchain networks resilience in adversarial environments, and to shut down those networks that are not decentralized enough. We leave up to future work to explore and formalize the concepts introduced in this paper, to investigate KYC-Tezos governance flaws (resulting from the wrong combination of Proof-of-Stake, token premine, on-chain upgrades and delegation) and to formally prove the insecurity of the LPoS consensus protocol.

Acknowledgements. We acknowledge for contributing to this work: Memur01, QuuxFoo, RoaringElder, as well as other contributors who prefer to preserve

[9] Check our website `https://tzlibre.io` for more information.
[10] Check Appendix A.2 for more information.

complete anonymity. We also acknowledge OCamlPro for developing KYC-Tezos, a significant engineering achievement we used to build upon. We finally acknowledge Arthur Robert Meunier Breitman (a/k/a LM Goodman), who first described the idea we believe in: a truly self-governing, decentralized commonwealth.

References

[1] L. Goodman. (2014). Tezos — a self-amending crypto-ledger white paper, [Online]. Available: https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf (visited on 07/20/2019) (*cited on p. 1*).

[2] S. Buchko. (Oct. 22, 2018). What is cardano (ada)? | the all-inclusive guide, [Online]. Available: https://coincentral.com/cardano-beginner-guide/ (visited on 06/17/2019) (*cited on p. 1*).

[3] CRYPTOSYNDACATE. (Oct. 2, 2017). In-depth analysis for cardano. business intelligence report., [Online]. Available: https://thecryptosyndicate.com/wp-content/uploads/2017/10/The-CryptoSyndicate-ADA-Intelligence-Report.pdf (visited on 06/17/2019) (*cited on p. 1*).

[4] ICODROPS. (2019). Eos analysis page, [Online]. Available: https://icodrops.com/eos/ (*cited on p. 1*).

[5] A. Lucian. (Jun. 2019). Tezos developers walk away, plan "dune" hard fork. beincrypto.com, Ed., [Online]. Available: https://beincrypto.com/tezos-developers-walk-away-plan-dune-hard-fork/ (visited on 07/20/2019) (*cited on p. 3*).

[6] T. Stiftung. (2017). Fundraiser overview, [Online]. Available: http://www.xn--928a.cc/static/papers/Tezos_Overview.pdf (visited on 07/20/2019) (*cited on p. 3*).

[7] D. Larimer. (2018). Graphene documentation, [Online]. Available: http://docs.bitshares.org/en/master/technology/graphene.html (visited on 07/20/2019) (*cited on p. 11*).

[8] bloXroute Labs. (2019). The scalability problem, [Online]. Available: https://bloxroute.com/documents/ (visited on 07/20/2019) (*cited on p. 11*).

[9] Team Rocket, *Snowflake to avalanche: A novel metastable consensus protocol family for cryptocurrencies*, 2018 (*cited on p. 12*).

[10] Team Rocket, M. Yin, K. Sekniqi, R. van Renesse, and E. G. Sirer, "Scalable and probabilistic leaderless bft consensus through metastability," *arXiv preprint arXiv:1906.08936*, 2019. [Online]. Available: https://arxiv.org/pdf/1906.08936.pdf (*cited on p. 12*).

[11] P. Daian, T. Kell, I. Miers, and A. Juels. (Jul. 2, 2018). On-chain vote buying and the rise of dark daos. D. Hacking, Ed., [Online]. Available: http://hackingdistributed.com/2018/07/02/on-chain-vote-buying/ (visited on 07/20/2019) (*cited pp. 12, 13, 20*).

[12] V. Buterin. (Mar. 28, 2018). Governance, part 2: Plutocracy is still bad, [Online]. Available: https://vitalik.ca/general/2018/03/28/plutocracy.html (visited on 07/20/2019) (*cited on p. 13*).

[13] T. Blummer. (May 8, 2019). How to bribe miners to re-org? medium.com, Ed., [Online]. Available: https://medium.com/@tamas.blummer/how-to-bribe-miners-to-re-org-d48025cb3788 (visited on 07/20/2019) (*cited on p. 13*).

[14] P. McCorry, A. Hicks, and S. Meiklejohn, "Smart contracts for bribing miners," in *International Conference on Financial Cryptography and Data Security*, Springer, 2018, pp. 3–18 (*cited on p. 13*).

[15] L. von Mises, *The theory of money and credit*. 1912 (*cited on p. 15*).

[16] G. Hardin, "The tragedy of the commons," *science*, vol. 162, no. 3859, pp. 1243–1248, 1968 (*cited on p. 15*).

[17] K. Shell, "Sunspot equilibrium," in *General Equilibrium*, Springer, 1989, pp. 274–280 (*cited on p. 15*).

[18] ——, "Sunspot equilibrium," *The New Palgrave Dictionary of Economics: Volume 1–8*, pp. 6439–6447, 2008 (*cited on p. 15*).

A Procedures

Here are some relevant TZL token/coin management procedures. The LibreBox wallet is available on our official website[11] ("Wallet" link in the header).

A.1 ERC-20 Token Minting

Use the LibreBox wallet to mint TZL ERC-20 tokens.

A.2 ERC-20 Token Migration

To migrate TZL ERC-20 tokens from Ethereum to TzLibre native coins, follow these instructions.

1. Create a brand new KYC-Tezos address with LibreBox without Ledger (keep your seed data safe or you'll lose funds) and a brand new Ethereum address.
2. Link the two addresses with LibreBox (green button).
3. Transfer TZL ERC20 tokens to your new Ethereum address.
4. Transfer these tokens to `0x0000000000000000000000000000000000000001` (burn address).

Your TZL ERC-20 tokens are now burned: you will receive the same amount of native TZL coins in the TzLibre network. To bake TZL check the TzLibre GitHub[12].

A.3 Buy presale TZL

Use the LibreBox wallet to buy native TZL presale coins OTC.

A.4 KYC-Free Activation

Use the LibreBox wallet to activate your inactive XTZ account.

A.5 Free TZL claim

Open LibreBox, select TzLibre network, follow instructions.

[11] `https://tzlibre.io`
[12] `https://github.com/tzlibre/tzlibre`