ALETHEO

Aletheo(from Greek - God of Truth) is a marketing platform, which allows to monetize human and AI activity on the internet, with secondary utilities. It allows to transform money into the purest form of power. As it was said in the Bible: "In the beginning was The Word". The ticker "LET" attempts to highlight the significance of first Bible verse as primary utility.

Decentralized word-of-mouth marketing service

What ad trailers and internet personalities attempt to do is not just to sell, but to start a *discussion* to increase awareness, to pump up the popularity of the product. Word-of-mouth marketing, proof-of-discussion, is what promotes the product today. Celebrities and ads are just a third-party and it is certainly possible to eliminate this third-party and pay directly for discussion and mentions instead.

The primary utility of the token is being a sovereign currency for exchange between employers and posters. Employers either setup and fund campaigns. Posters commit to these campaigns by discussing certain posts or anything eligible(matching keyword) for paid discussion. By default, posters are allowed to express any opinion on every topic, and, depending on the resource, posters by default have the right to completely derail the discussion and talk about anything. Posters will get paid for unrelated discussion as long as it for example bumps the thread, or adds another comment to discussion making it look more heated and popular. LET default marketing paradigm(employers can choose their own specific terms though) promotes critical thinking. It might however depend on the resource and a forum could simply ban/remove unrelated posts. Posts need to be witnessed by oracles, so a poster has to ensure that his post satisfies the rules of a website, chat, resource.

There are two types of campaigns, funded and stake campaigns. Funded campaigns can be funded with LET tokens or any approved tokens. Stake campaigns are campaigns created by stakers as a part of Aletheo default campaign and are funded by a corresponding share of treasury emission for default campaign. Basically if a staker creates a campaign that is not related to Aletheo, this staker takes away a share of default campaign emission for his own needs. Funded campaigns are only required as a familiar, simple way of ordering services, rather than studying Aletheo in-depth.

Campaign settings available to employers are very flexible to meet every need:

1.Ppp – pay-per-post. Defines how much posters get paid for a post, and in which token it is denominated.

2.Array of key strings. A key string can be a word or a phrase, a sentence, a text of any length. If employer sets more than one key string, then these key strings become options to make the posting more natural.

3.Mandatory key string can be left blank. Requires to use mandatory key string in every post regardless whether the post is related to key string discussion or not.

4.Array of target urls. The campaign works only on the websites with these urls or platforms(like online videogames). If none set – it means everywhere Aletheo can reach.

5.minStaked. Minimum requirement of locked LET tokens for a poster to have to join the campaign.

6.nonEditable, a boolean. If a campaign is non-editable, it can attract funding from other employers, since keywords will stay the same until the funds run out, basically allows to make it last longer potentially and decentralize it.

7.noFiring, a boolean. If set to true, posters can't be fired at all, so that posters will more likely join the campaign.

8.onlyManualApproval, a boolean. If set to true, posters can't join the campaign without employer' approval.

9.keyStringPerWords. As an example, in a job which requires 1 key string per 1000 words, if a poster writes 4 posts 250 words each, he has to mention the key string in those 4 posts at least once, and he will get paid for those 4 posts. If this is at 0(default), then the poster is being paid for every post.

10.minPostLength. Minimum amount of symbols in the post to be eligible for a reward.

11.modsPay. Needed if the employer does not feel confident and wants to moderate the campaign, but has no time for that. In purely decentralized setup, LET mods are not obliged to follow the rules he wants to enforce, however they are assumed to follow the rules he wants to enforce, since mods profits depend on Aletheo profits and success as a whole and because the governance can fire them prematurely.

12.rulesLink. A link to a post explaining the rules for posting in detail and ban rules. In the spirit of default LET campaign can be left blank.

13.expirationDate. If the budget of the expired campaign is not exhausted, the remaining budget is being refunded to the employer.

14.minShillPower. Minimum poster' shill power.

15.postRate. Determines how often a poster can post eligible for payout posts in this particular campaign. Example: 60 seconds. If a poster posts more often he is not getting paid for more.

16.maxPosters. A limit to make small budgets viable. If not set, might be computed automatically, considering that posters have to have sufficient profit.

17.startTime-endTime. Time of day in UTC. By default 0 to 0, which means 24 hours per day. Specifies time when the campaign is active and posters are paid.

18.An array of campaign languages. Left blank if any language. If not left blank, then only posters who can join are those who stated their language.

General philosophy and technical principles

-Politicians are as naive in the face of innovation as we are. All their experience means very little when an innovative technology turns upside down everything what they knew about.

-Everything is inefficient. The world' scientific progress while advancing everyday is actually close to stagnation in comparison to how fast it could be.

-The probability of a new innovative technology appearing increases exponentially with each passing year. The probability of a new existential threat appearing increases exponentially with each passing year. Humanity either evolves or goes extinct.

-Richest governments spend billions on medical research paying full salaries in their inefficient bloated jurisdictions.

-The world has so much more brain power than ever, and the most of this brain power is unable to innovate.

-Historically most smart people were failing to achieve power, because they were always busy with concepts nobody understands.

-The internet is the watch. The internet saves more lives than all governments' laws combined. As long as we keep open borders for the internet, devastating conventional warfare or even World War 3 won't happen regardless of Power Vacuum. Or, if it will happen, there will be significantly less victims.

-Modern humans are potentially immortal. We don't need a spit in the face in a form of elders' care. We can use our retirement money for cryopreservation.

-Humanity will always remain an existential threat to itself. In the future many absolutely unimaginable technologies will be researched to prevent extinction.

-Dying people just stop wanting to live, because their systems are failing, that's it. That's how we die.

-Eternally healthy humans will strive for new experience and knowledge for eternity.

-LET doesn't care what's your gender, ethnicity or skin color.

-Today, cryptocurrency is potentially mutable as is. There are ways to change this. Aletheo technology can shape public opinion of cryptocurrency to ensure free cryptocurrency agenda survival in post-cbdc world.

-Some of the most expensive commercials ever made cost around $30 millions. This amount of money in LET could produce an absolute overkill Aletheo campaign. A campaign of this scale could be used to promote brand commercials on Youtube, build community around official accounts and set given keywords trending for a prolonged period of time on different social networks and potentially create unprecedented so far public interest.

Architecture

The core of Aletheo – oracles and DAO. Oracles are supposed to be an anonymous decentralized network.

Pseudo-anonymous oracle network

Pseudo-, because it relies on some facts of identity. Oracles witness posters' activity on different platforms like Twitter, Discord, Telegram, etc, by fetching data from these resources. This data is being processed entirely on the oracle side and the results are being pushed to the aggregator smart contract as rewards numbers and to Aletheo website as posters' posts and statistics.

It is possible to make anonymous and pseudo-anonymous oracles to deliver true results. Oracles shouldn't know what role they are performing in a given iteration of publishing results. There have to be two roles: witnesses and supervisors. Chosen supervisors have to be a small uneven amount of all oracles. Supervisors' results are considered to be true, and witnesses results have to match it. If supervisors' results don't match, another attempt of choosing supervisors occurs, until supervisors results match, while published results stay, no republishing occurs during that. In case of lies, a part of oracle' stake is being slashed. To decrease the probability of Sybil attack to practically 0, Aletheo can rely on:

1.Language. Language communities could be required to elect oracles out of subjectively and programmatically proven unique posters.

2.Balance. Allow anonymous oracles only with considerably high balance.

3.Transaction history. Some projects are currently building tech which attempts to measure unique humanness by transaction history.

4.Many other proofs of unique human exist to date, which could easily match our purposes.

The governance must always review and approve oracle results or reject those results, so a case of fake rewards is less likely but still possible. An independent observer software is required for this. Both posters and oracles have emissions for rewards, so rewards are not available in full as approved, so even if results are fake and approved, malicious actors will require a significant amount of time to claim those fake rewards, so such act will lead to most investors exiting before these rewards are claimed, so it can't possibly be profitable unless the aim is to damage Aletheo DAO reputation. This system most probably eliminates "big" lies, but "small" lies can still work. This is still a pending issue *(the issue is that in current proposed design, anonymous oracles have some probability of profiting in collective small lies)* to resolve elegantly. Autistic roll-ups could be required for this – a form of an even lighter optimistic roll-up, mostly event based.

Of other possible malicious threats, anonymous oracles can censor some addresses collectively. If a poster is censored, then he moves to a different oracle cluster, so that censoring oracles lose money. Since Aletheo does not require high-frequency oracles, and publishing of results occurs not more often than twice a month, proper architecture of the process and game theory should elimite all risks. However, using anonymous oracles in this design could still be an utopistic idea, so an easy more conservative solution is still on the table: kyced oracles or revision of results by trusted observer from the team.

Smart contracts overview

1. LET token contract is a modified ERC-20 with small changes like allowances made booleans to reduce gas cost of transfer and imposes 10% tax on every transaction to all registered in the contract pools, whether it's a sell or liquidity addition. The tax is required for sustainability of Aletheo treasury.

2.Trust-minimized proxy or simply trustless proxy. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-3561.md

All Aletheo contracts will be behind this proxy. It's an altered upgradeability proxy EIP-1967 with some features that allow to remove trust to developers and/or governance. New logic implementation is not being set as soon as transaction with new logic was mined, instead it is being stored in NEXT_LOGIC_SLOT up to NEXT_LOGIC_BLOCK_SLOT, or for a month or so. The period allows participants to identify if the deployer or the governance is malicious and therefore to exit safely. Next logic can be canceled in case of a bug discovered or upgraded to after month passes. For convenience, it is impossible to cancel next logic and immediately propose another next logic. Proxy admin can also prolong lock(), if for example a situation arises in which there are no plans to upgrade a particular contract for a time being, so that it keeps participants peace of mind for that period.

3. Liquidity Manager contract. Aletheo liquidity will be managed in order to avoid loss of LET token value in market downtrends, in other words all liquidity from for example ETH pool will be moved to USDC pool. The contract is supposed to be managed by the DAO or a trader.

4. Treasury contract. Treasury contract balance will be distributed to LET token(not liquidity tokens) stakers, oracles, posters, airdrop recipients and the team in a trust-minimized way.

5. Job Market contract. A contract in which marketing campaigns will be registered by employers and non-default campaign rewards will be held.

6. Governance contract. This contract will be in charge of Aletheo after all contracts will be locked forever, or, there is a chance that it might manage upgradeable proxies as long as at that stage Aletheo will be "too big to fail", or only with the team proposing upgrades. Managing treasury requires absolutely next level DAO' purity of intentions, *fundamentally pure governance*. A governance that is incapable to act maliciously towards the project as a whole. Of all proposed by Szabo options, we should choose "ruthlessly minimized".

Multistage governance can allow this, first stage of voting is voting by shill power of posters(see:

decentralized moderation), if it passes then it goes to voting by stake. For some proposals there could be third stage: again by stake, but voters' stake will be locked for a year. This way the DAO will be long term thinking regardless of most issues and almost entirely incapable of being malicious towards itself. For example, a grant must not be transferred in one big transaction, it should be vested slowly, and the DAO should be able to revoke it. The problem of participation will be solved by incentivizing voting, a vote must have a small reward.

7. Staking contract. Staking contract for posters and voters to lock their tokens as commitment stake for a period shorter than 1 month(shorter than trust-minimized proxy upgrade period). Staking produces some LET yield as of now and is supposed to eventually entirely depend on fees from campaigns.

8. Oracle Aggregator contract. The aggregator must use Chainlink verifiable random numbers or an alternative to determine supervisor oracles and slash lies.

9. Trust-minimized cross-chain bridge. Very efficient economically, since works with only one centralized oracle in a trust minimized way, in case of a hack of bridge oracle, only stopping the bridge is possible, because commit-reveal scheme disallows the oracle to alter transactions. First what a user(or an oracle network, an oracle, or a some sort of a bot automating the process for a user) needs to do is to announceHash(), Hash has to be generated by the off-chain by the user maybe through a web ui and has to correspond with:

keccak256(abi.encodePacked(userAddress,arg1,arg2,arg3,arg4,anyDisposableKey))

The user keeps all arguments and disposable key to himself, until bridge oracle relays the hash to the other chain, he then must verify if the hash is indeed his, and if it is, then he sends the actual transaction with all arguments and used disposable key. The contract on the other chain will only accept address, arguments and a key that matches previously posted hash. This bridge allows not just to cross() or simply relay tokens value, but it also allows to callAcross() - to relay data which enables trustless cross-chain contracts communication and therefore cross-chain governance.

LET wallet

LET wallet is a browser extension. The wallet' sole purpose is to send posters data to the oracle from the resources which do not have usernames, for example 4chan. Posters, which would like to post on imageboards or any other resource which does not have usernames, will be required to use this browser extension to allow oracles track their activity and send the data either to oracles or send it to some optimistic roll-up as transactions.

Commit-reveal scheme with a delay could almost entirely eliminate front-running. Another, probably better way or an addition could be: if two identical datas where posted from two posters, and that data is confirmed to exist on the imageboard, then a poster with higher stake will get the reward, since front-running will be predominantly attempted by 0 stake posters. Posters with locked stake can be banned from the system, so they are unlikely to go through such a small risk.

Currently the wallet sends the data directly to the oracle, as an option for future development, it can send a transaction to an optimistic roll-up with every post automatically.

Mirrors

Mirrors are smart contract instances of Aletheo deployed on different chains and layers, mainly required to have a legitimate reason to monetize more communities centered around different chains.

LET chain

Let chain might be a fork of Oxen. Oxen by default is an XMR POS fork, therefore LET chain will have privacy of data by default, with some differences, like an option to make some blocks public, these blocks will postpone all private transactions to the next first following private block.

It's smart contracts will be written in HolyC. HolyC for a logical continuation of Bitcoin and Ethereum, so next-generation God Protocol' Holy Chain with Holy Contracts.

Secondary utilities

Secondary utility is an utility that might not be able to generate enough value on it's own for a functioning protocol.

An example could be charity or/and grants from treasury. Charity protocol on it's own would likely fail to attract/generate value on it's own, but charity as a secondary utility might create a positive feedback loop.

Another one could be valuable enough on it's own, but still is a logical addition to post-to-earn: meme market. Meme contests of any budget, for any given topic, including Aletheo itself.

And another one that expands post-to-earn, and can pretty much be sufficient on it's own, but makes absolute sense to be a part of Aletheo: monetizing observable activity everywhere, even in online games.

Decentralized moderation

There is a very specific need in online word-of-mouth marketing: the need to determine whether a poster is a bot or not, 'humanness'. Several solutions to identify a unique human behind an address do not really work so well here, since a human can solve whatever puzzles or equations once to prove he is a human, and then most of the time run some gpt-3 bot. A different, subjective metric is required, determined in decentralized way. Since 'humanness' is a limiting toxic term, Aletheo must stop using it and replace with a broader one: creativity or *shill power*. It's very useful for any employer to look at posters' ratings in creativity, sense of humor, persuasiveness, and overall likelihood of how often a given poster posts as a human and not an AI.

Shill power metric is supposed to include all of that, and will be a part of posters' rewards formula: the more shill power, the higher is the pay.

Voting by stake will discover shill power of different posters over time.

Tokenomics

Note: numbers shown below will be valid for every major Aletheo mirror(ETH, BSC for example). Currently live are AVAX and FTM mirrors, which are exceptions: have much less supply(50k and 30k respectively).

Starting supply: 100000 LET tokens.

Total supply: 300000 LET tokens. Total supply was loosely defined and most likely the treasury will afford to burn at least a half of the tokens.

Emission: maximum emission is approximately 10000-20000 LET tokens each year. It depends on if all treasury emissions are being used, Aletheo team however wants to keep it never higher than at 15k LET yearly even if higher emission is possible.

On launch of every mirror, at least 200000 tokens are locked in treasury. **Treasury will support:**

1. Default Aletheo promotion campaigns. Posters will receive rewards for participation in default campaigns from treasury.

2. Airdrops. Everything that can be claimed from treasury is vested. Aletheo airdrops will be vested, except for first airdrops of AVAX and FTM mirrors. These airdrops have passive emission of 0% and unlock gradually only on top of posters' rewards, effectively making poster with an airdrop earn twice more as long as there are still tokens for his address to airdrop. Current airdrops include locked balances of AVAX snowflake to Aletheo migration, "Founders" of previous Ethereum and Fantom launches.

3. Oracles.

5. Team, bug bounty and audits.

7. Anything else that governance will be interested in supporting, as long as functionality for grants and financial support for a particular idea is possible to fulfill in trust minimized way.

Commitment stake. Posters, to increase their rewards, lock LET tokens in staking contact for at least 25 days(a period, shorter than trust-minimized proxy fastest upgrade). Posters can increase their pay to as much as 50x more(this modifier is subject to change as protocol userbase matures), by locking a maximum of 1000 LET tokens. The more skin in the game, the more Aletheo gives back.

Sell tax. Fixed 10% tax from every transaction to any of registered LET token pools goes back to treasury to ensure Aletheo is sustainable.

Liquidity management. Aletheo liquidity is locked in the contract, but this contract can swap that liquidity to a pair with a different token. In a downtrend it can swap to a stable coin, and in an uptrend to a potentially one of the best performing projects on a given chain. The list of tokens must be trusted by the community(no new ponzi rugs) and shouldn't be easily edited. There are two options to provide liquidity to Aletheo, both of which do not require any timelocking at all:

1. The usual constant pairing with a given pool through uniswap or a fork. Allows to sometimes greatly decrease impermanent loss, because the pool of liquidity manager is not a permanent variable.
2. Staking liquidity, so it will be swapped by liquidity manager together with liquidity it owns, to preserve value while still collecting trading fees.

Beta-test

Beta-test is Aletheo in a much different state from the design proposed in this draft:
1. it uses centralized black-box oracle in trust-minimized way, in a way that even if the oracle gets hacked, it won't be able to steal any funds, and even if the deployer of smart contracts is malicious, emission limits won't allow the deployer to steal any sufficient amount before community notices something is wrong.

2. no decentralized moderation and no shill power, only stake. Posters which do nothing but spam or clearly malicious otherwise(shock content posting) are being banned in a centralized way.

3.Aletheo browser extension only automatically signs a message with post data and sends to the centralized oracle, it does not send any transactions to any layers 0 or 1.

4.At the time of writing trust-minimized proxies are still not locked(still act as EIP-1967 proxies).

5.Governance, job market and meme market are not yet live.

Legal

Some countries forbid paid endorsement without disclosure. Depending on the language and platform, sometimes posters will have to include a disclaimer in their bio. Otherwise FUD is certainly legal everywhere.

Another possible problem is that massive platforms enjoy having ads profits for themselves, attempting for peaceful co-existence, without testing it's unbannable nature, Aletheo should endorse posters who use paid services of different platforms, 4chan pass buyers must earn more, Discord nitro buyers

must earn more, so are Telegram premium users and so on.

Risks

You acknowledge and agree that there are numerous risks associated with purchasing LET Token, holding LET Token, and using LET Token for participation in the LET Network. In the worst scenario, this could lead to the loss of all or part of the LET Token which had been purchased. IF YOU DECIDE TO PURCHASE LET Token, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND ASSUME THE FOLLOWING RISKS:

Uncertain Regulations and Enforcement Actions : The regulatory status of LET Token and distributed ledger technology is unclear or unsettled in many jurisdictions. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including LET Token and/or the LET Network. Regulatory actions could negatively impact LET Token and/or the LET Network in various ways.

Inadequate disclosure of information : As at the date hereof, the LET Network is still under development and its design concepts, consensus mechanisms, algorithms, codes, and other technical details and parameters may be constantly and frequently updated and changed. Although this white paper contains the most current information relating to the LET Network, it is not absolutely complete and may still be adjusted and updated by the LET Network Development team from time to time. The LET Development team has no ability and obligation to keep holders of LET Token informed of every detail (including development progress and expected milestones) regarding the project to develop the LET Network, hence insufficient information disclosure is inevitable and reasonable.

Competitors : Various types of decentralised applications are emerging at a rapid rate, and the industry is increasingly competitive. It is possible that alternative networks could be established that utilise the same or similar code and protocol underlying LET Token and/or the LET Network and attempt to re-create similar facilities. The LET Network may be required to compete with these alternative networks, which could negatively impact LET Token and/or the LET Network.

Failure to develop : There is the risk that the development of the LET Network will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or LET Token, unforeseen technical difficulties, and shortage of development funds for activities.

Security weaknesses : Hackers or other malicious groups or organisations may attempt to interfere with LET Token and/or the LET Network in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of LET development team may intentionally or unintentionally introduce weaknesses into the core infrastructure of LET Token and/or the LET Network, which could negatively affect LET Token and/or the LET Network. Further, the future of cryptography and security innovations are highly unpredictable and advances in cryptography, or technical advances (including without limitation development of quantum computing), could present unknown risks to LET Token and/or the LET Network by rendering ineffective the cryptographic consensus mechanism that underpins that blockchain protocol.

Other risks : In addition, the potential risks briefly mentioned above are not exhaustive and there are many other risks associated with your purchase, holding and use of LET Token, including those that the risks that LET development team cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on Aletheo, as well as understand the overall framework, mission and vision for the LET Network prior to purchasing LET Token.