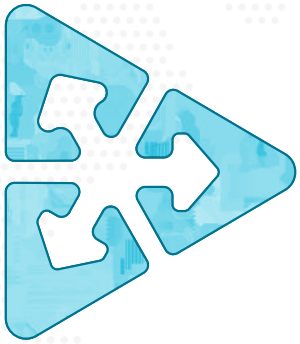


Callisto Network

Blockchain as seen by security experts.

Whitepaper

Revision 2.1.1 | 15 June 2022, Callisto Network Team

This document is intended to formally describe the features and concepts of the Callisto Network. The project features a blockchain platform with its own native cryptocurrency (CLO) and an ecosystem of applications based on smart contracts.

Callisto Network was founded as a public blockchain protocol with the original goal of researching and developing experimental features. These features aim to enhance and strengthen the long-term sustainability of the network and its components, including third-party decentralized applications (DAPPs).

Callisto Network is an EVM-based chain, implying that it supports the execution of smart contracts written in Solidity, making it fully compatible with **Ethereum**, the leading smart contract platform. Hence, it also compatible with any EVM-based chain, with the most-known being **Binance Smart Chain, Polygon, and Avalanche**. Therefore, all smart contracts and DAPPs developed for these chains can easily migrate to Callisto Network – without code changes – to take advantage of the significantly lower transaction fees and the higher security standards.

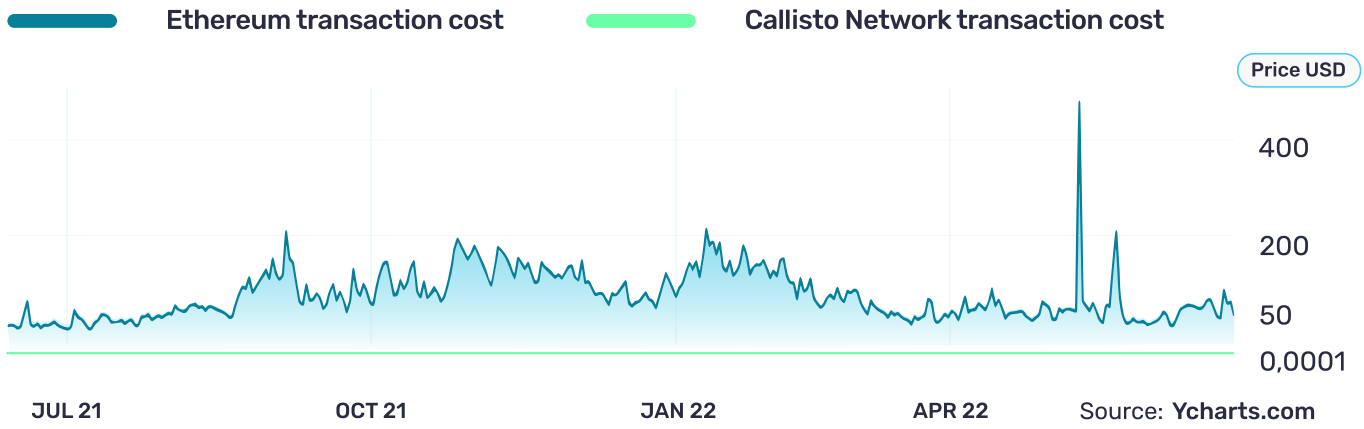


Figure 1: Ethereum VS Callisto Network transaction cost over 2021-2022.

Callisto Network relies on the Proof of Work (PoW) consensus mechanism, widely considered the most secure solution. Although many alternatives have been proposed during the last decade, such as the Proof of Stake (PoS) consensus, PoW remains the most reliable solution thanks to proven technology.

With this in mind, we are dedicated to improving the PoW consensus mechanism by designing and implementing unique features, including the Nakamoto Consensus Amendment and the Dynamic Gas Price. In addition, a dynamic monetary policy approach means the Callisto Network platform will offer the industry's lowest transaction cost and coupled with the Cold Staking will enable the Callisto Network coin (CLO) to be a store of value.

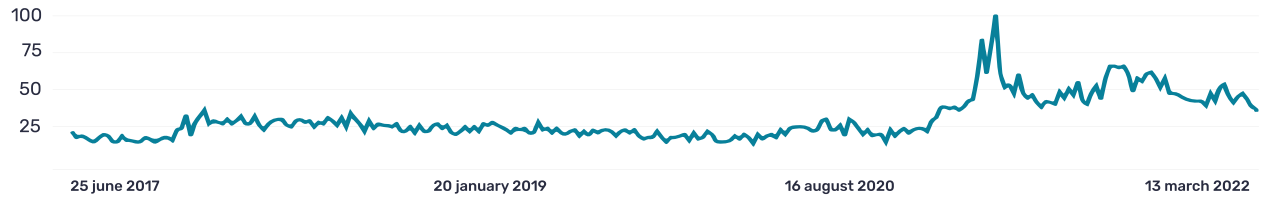
In this direction, we are conducting extensive research to reduce the protocol's energy consumption further, while also increasing network speed without any security compromises.

Introduction

A cryptocurrency is a digital currency in a decentralized system using cryptography rather than a centralized authority to verify and record the transactions. In such a system, the creation of additional units is controlled at protocol level. In contrast to fiat money, cryptocurrency is monitored and controlled by a peer-to-peer network, with all transactions recorded in a secure transactions ledger known as the Blockchain.

The first decentralized cryptocurrency created was Bitcoin in 2009. Since then, the crypto world has grown exponentially. A few years later, in July 2015, **Ethereum** was launched as a decentralized application execution environment capable of storing programs on the blockchain and executing them whenever the predetermined criteria are met. This innovation made Ethereum one of the most-used crypto projects, and it has grown into the second-largest cryptocurrency in market capitalization. Smart-contracts have become the industry standard, and almost all blockchain projects developed after 2018 support smart contracts in one way or another.

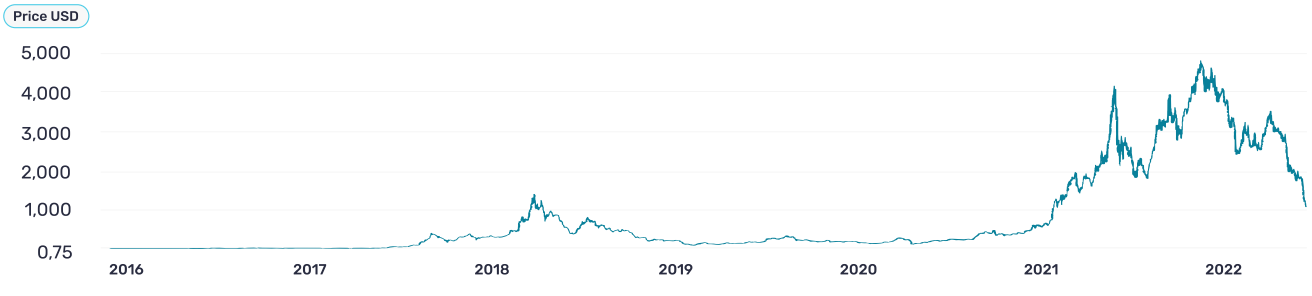
Ethereum adoption has surged and has been accompanied by a significant increase in the number of DAPPs, or decentralized apps. Since their introduction, interest in DAPPs has been growing steadily, showing the interest of developers and users. From **less than 100** DAPPs in 2015 to nearly 3000 today, while another 4,000 Dapps are in development at the time of writing. The demand for Dapps, regardless of market cycles, tends to reach new heights during periods of market growth and remain stable thereafter.



Source: **Google Trends**

Figure 2: Evolution of interest in Dapps keyword searches.

This growth led to Ethereum's vast price increase from **$2** in **2015** to **$2000,** an increase in **99900%.**



Source: **Coinmarketcap.com**

Figure 3: Ethereum to USD Chart.

Callisto Network follows the same **fundamental** approach by increasing the number of "use cases". It also relies on a deflationary monetary policy designed to decrease the number of CLO coins in circulation during periods of high network utilization, which is the essential prerequisite for achieving a significant increase in value. Hence, similar to Bitcoin, Callisto Coin (CLO) can also be seen as a "store-of-value" currency.

From the start of the project, the developed DAPPs received the community's attention, with the Cold Staking smart contract being the most known and successful among them.

Currently, the Cold Staking contract collects 40% of all mining rewards and distributes it to the cold stakers in direct proportion to their holdings. In other words, cold stakers earn a passive income by freezing their coins; therefore, it's a much more secure and eco-friendly way to earn passive income with cryptocurrencies.

At the time of writing, **1,297,748,933 CLO**, representing **40% of the coins in circulation**, are stored in the Cold Staking smart contract.

Callisto Network first introduced the Cold Staking principle, which rewards long-term coin holders. Cold Staking is not tied to Proof of Work or a consensus mecanism.

The main limiting factor to the widespread adoption of DAPPs is evident: **Security**.
As programs, smart contracts are just as prone to bugs and flaws as any other software. And with their increasing popularity, the potential risk for users increases as fast as the number of hacks.

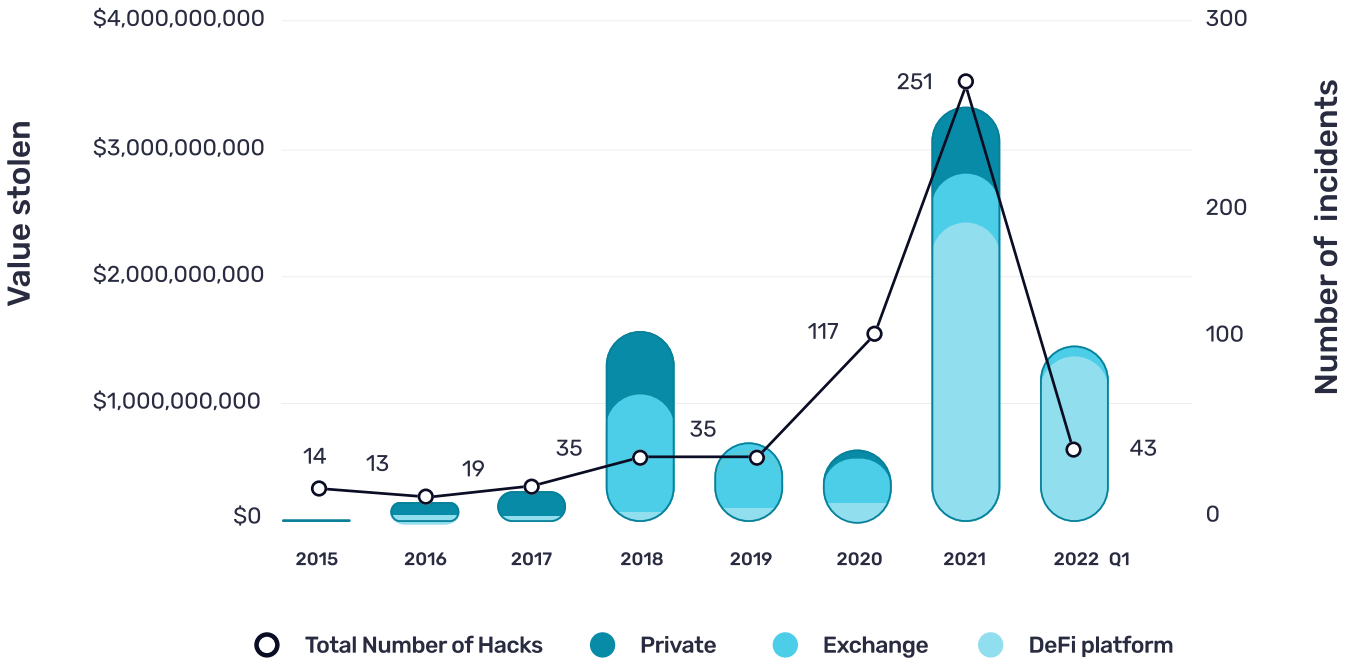
The most notorious example of a DAPP security failure is **TheDAO hack**. In June 2016, users exploited a vulnerability in TheDAO and transferred 33% of TheDAO's funds to a subsidiary account. The community controversially decided to hard-fork the Ethereum blockchain to restore the funds to the original contract. This decision split the Ethereum blockchain into two branches – Ethereum and Ethereum Classic.

As institutions increasingly embrace smart contracts, the amount of funds stored in these contracts will continue to grow exponentially. The risk means potentially dramatic financial losses for the participating parties and the users of any particular crypto platform.

In recent months, the rapid proliferation of DeFi platforms has gone hand in hand with the number of hacks, resulting in a sharp increase in the amount of funds stolen.

Here is a series of figures showing the extent of the phenomenon and its acceleration.

According to [Chainalysis](), 97% of the cryptocurrency stolen in Q1 2022 was from DeFi protocols, compared to 72% in 2021 and only 30% in 2020.



Source: **Chainalysis.com**

Figure 4: Total number of thefts and value stolen by type of victim, between 2015 and 2022 Q1.

Callisto Network Security Department was founded in 2018 with the goal of improving the security of the programmable blockchain.

The figures below illustrate how DeFi platforms are those most affected by the hacks.

The recent hacks of **Poly Network** and **Axie Infinity** account for losses of $612 million and $625 million, respectively, making them the largest hacks to date. It is important to note that the vast majority of these platforms appeal primarily to ordinary users, with institutions preferring centralized platforms.

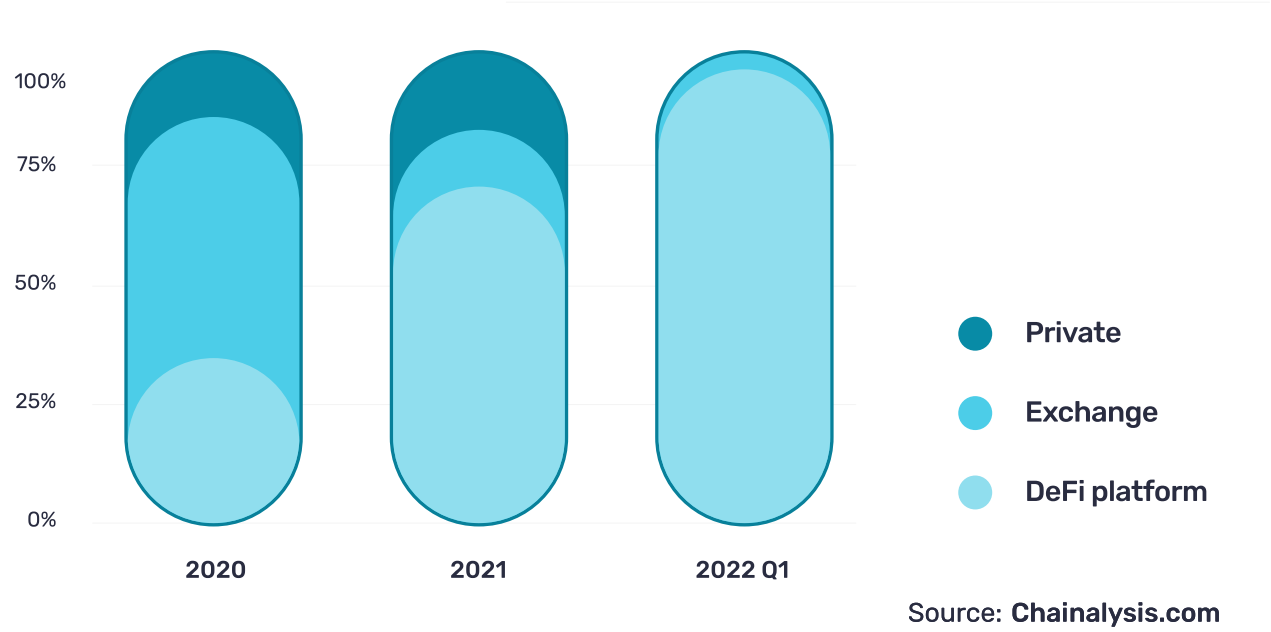


Figure 5: Percentage of value stolen by type of victim, 2020-2020 Q1.

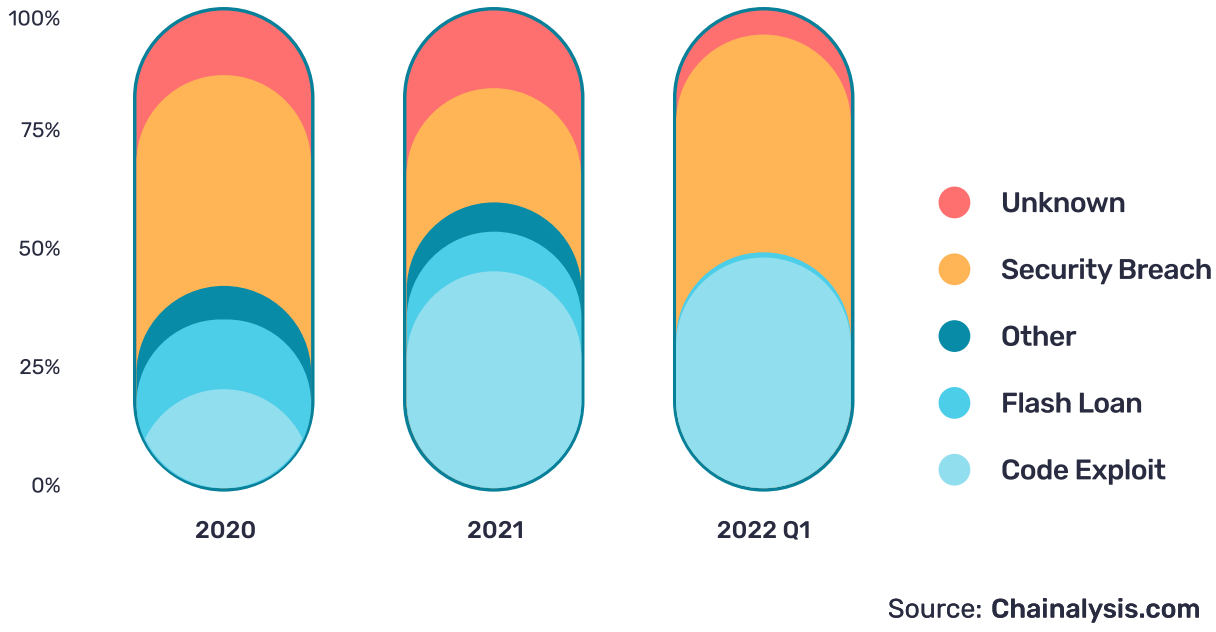


Figure 6: Percentage of value stolen by attack type, 2020-2022 Q1.

Looking at the data more closely, it becomes clear that most thefts related to DeFi protocols are due to faulty code. A security audit would have prevented the hacking in most cases.

Callisto Network has quickly made a name for itself in the cybersecurity world, having audited over 400 smart contracts, including many well-known projects such as Tether, Basic Attention Token, Enjin, Idex, Binance BNB, Maker, Shiba INU, Fantom, and many others. To date, none of the smart contracts audited by Callisto Network has been hacked.

In addition to security audits, Callisto Network contributed directly to several major projects, such as Ethereum Classic and EOS, making the expertise of Callisto Network's Security Department team unmatched.

Based on this experience gained over the years, we also pay special attention to Level 2 issues, i.e. current token and NFT standards.

Source: **Coin98 Analytics September 2020.**

Figure 7: Common smart contract audits companies comparison.

Security

While innovation is important, **security is the most important factor in the adoption of any blockchain.** As we have seen in numerous projects, and most recently in the case of the Poly Network Hack where $612 million were stolen, without security a blockchain dies and innovation becomes irrelevant.

With this in mind, we approach all aspects of our products starting with a "security-first" mindset, and that begins with the Callisto Network PoW consensus.

The PoW consensus, or Proof-of-Work, is the most secure decentralized consensus mechanism, though as with all technology it has benefits and downsides.

In a context where projects are increasingly adopting the PoS (Proof-of-Stake) consensus, the number of flaws involving PoS-based projects is booming. Therefore, we believe the current implementation is not secure enough, and it will take some time for the technology to mature.

This is why we've worked diligently to address the shortcomings that are generally associated with the PoW architecture:

- It's too expensive (solved)
- It consumes too much electricity (solved)
- Its per-second transaction speed is too slow. (Work in progress)

Our Proof of Work vision is not limited to these three areas. Moreover, we have described our plans for improving the blockchain base layer in our publication "Callisto Network Vision".

In 2016 alone, more than $10 million was lost on Ethereum due to a well-known flaw. Since then, the number of tokens lost due to the flaw in the ERC20 tokens standard has increased continuously. Every day, we see users sending their tokens directly to the smart contract by mistake, therefore losing them permanently.

In this context, and to address these issues, we designed our own token standards – ERC-223 and Callisto NFT standard.

The widely used ERC721 NFT standard is based on the ERC223 communication model, but we have further enhanced the approach and extended its functionality with the CallistoNFT standard. Adding a number of built-in features eliminates the need for third parties and empowers users, as financial freedom is the essence of blockchain.

Key Advantages of the CallistoNFT and ERC-223 Standards:

- **Built-in Trades:** Buy, sell, or Bid on NFTs without relying on a third-party marketplace.
- **Built-in Data:** NFT specifications are standardized and stored on-chain without relying on third-party websites.
- **User-generated Data:** User-generated content is attached via built-in data without IPFS links.
- **Built-in Monetization:** Creators can retain control of their intellectual property and continually earn fees from trades.
- **Upgradability:** Unlike the ERC721 standard, which mainly stores data on IPFS, CallistoNFT allows data updates (when this option is enabled at the moment of the NFT deployment.
- **Communication Model:** Prevents accidental token losses for higher security.

PirlGuard - 51% Attacks Protection

Among the consensus mechanisms, Proof of Work is undeniably the safest. The networks with the largest capitalization, Bitcoin and Ethereum, are also the safest thanks to the Proof of Work consensus. However, despite the Proof of Work consensus being the safest, a flaw can arise: 51% attacks.

PirlGuard is a modified Proof of Work consensus algorithm inspired by the Horizen penalty system intended to defend the blockchain from virtually all 51% attacks.

To safeguard the blockchain, PirlGuard penalizes any un-peered node that attempts to pair with the network nodes. It does this by sentencing the un-peered to mine a determined amount of penalty blocks. This security measure drastically reduces the chances of a successful attack to approximately 0.03%.

On 28 March 2019, PirlGuard protection was successfully activated on Callisto Network on block number 2,135,000. To ensure a successful implementation, several tests were conducted with our partners, **Stex, HitBTC, Epool, MaxhashPool, and CLOPool** during the implementation process.

Thanks to PirlGuard, Callisto Network is protected against 51% attacks, with no successful attack being reported since implementation. Meanwhile, several Proof of Work blockchains have been hit by 51% attacks, inlcuding Bitcoin Gold, Bitcoin SV, and Ethereum Classic, which has suffered multiple attacks, **causing $9 million in losses in 2020 alone.**

Ecosystem

As a blockchain offers a use case, it will become successful over time. With this in mind, Callisto Network has focused on introducing multiple projects that drive the ecosystem growth and showcase the security standards we've developed.

Launched on 1 October 2021, SOY Finance is a decentralized exchange providing trading, yield farming, and **blockchain-based financial services** on the [Callisto Network blockchain.](#) SOY Finance is **the world's safest and the first fully-insured** decentralized exchange, adhering to industry best practices and adopting the highest level of security and standards:

- Whitelisting of audited tokens.
- Hybrid ERC20 and ERC223 token standard.
- Decentralized insurance.

To date, SOY Finance has processed over two million transactions valued at more than $75 million.

Gems & Goblins is a **play-to-earn game** developed by [We Make Games](#). It combines strategy, construction, epic battles, and cryptocurrencies.

Through a captivating storyline, players are taken on daring expeditions, confront ugly villains, and explore a diverse and colorful universe to collect **Non Fungible Tokens (NFTs) and GNG tokens**, the game's native cryptocurrency.

The game is structured around a classification system consisting of legions and leagues, with players receiving points based on their in-game performance. But there is more! Gems and Goblins takes advantage of cutting-edge tokenomics to feature passive income and burning mechanisms for an ultimate GameFi experience!

Launched in 2019, Absolute Wallet has quickly become the most used Telegram crypto wallet. As of writing, Absolute Wallet has more than 130,000 active users trusting it to hold their cryptocurrencies, and is being used in nearly 260 telegram groups.

Although Absolute Wallet is popular among the crypto-community and community managers for its community-oriented features, several major technical achievements have allowed Absolute Wallet to appeal to a growing number of users. Indeed, Absolute Wallet has constantly evolved to integrate an increasing number of blockchains. It was also the first crypto wallet to implement the storage and display of NFTs in an advanced manner.

Our vision does not end with Absolute Wallet, and we want to develop a decentralized ecosystem driven by FUN, where the community, investors, and community managers can generate profits. Just imagine:

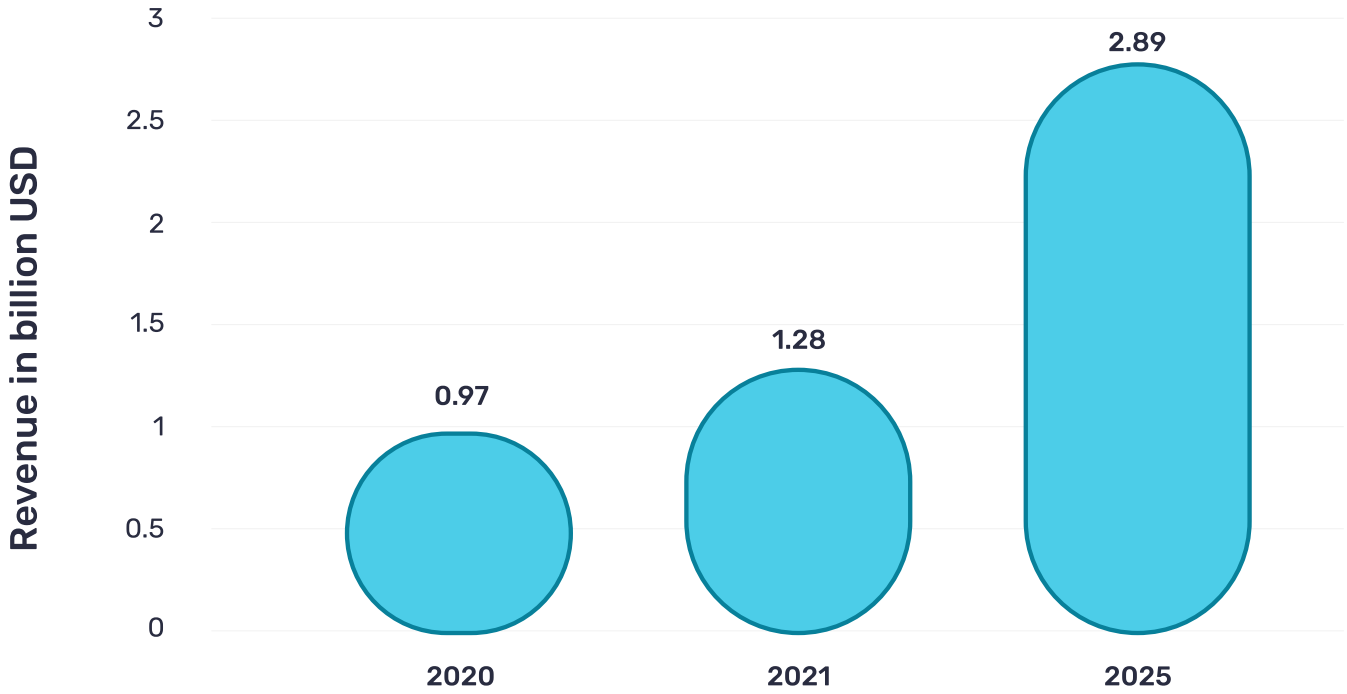
- **Absolute Fun:** The core of our ecosystem offers all of the tools of crypto-marketing, along with innovative additions, with one significant advantage: decentralization.
- **Absolute Wallet:** The successor of Cryptobot, the well-known Telegram wallet. Simple, intuitive and powerful. CryptoBot has established itself as a leader in crypto-wallet architecture.
- **Absolute Bridge:** The crypto community is moving fast so it must be Absolute! For that reason, Absolute Wallet developed its bridge, which will include a series of innovative features.
- **Fun Token:** The FUN token is the underlying asset of the Absolute ecosystem and offers multiple benefits to the holder. Whether you're a user, crypto money maker, or community manager, the FUN token will provide numerous benefits and innovations.
- **AbsoluteDEX:** An exchange platform geared for FUN, efficiency, and security.

[Esport Innovation Group] is a Venture Corporation funded by Micheal Broda (founder of ESPL - Esport Players League) and Nik Adams (founder of Twitch).

EIG is committed to empowering companies to drive the esport's future through innovation and access to advanced technology that benefits gamers worldwide.

With headquarters in Basel, Switzerland, and having offices in Los Angeles and New York, EIG has partnered with some of the most prominent esport and gaming brands internationally. Esport Innovation Group is also an incubator for esport companies that aim to bring game- and sports-related metaverses to the global mass of sports consumers.

The esports industry is set to become one of the hottest, largest, and most profitable trends in the crypto space and across broader society with a market projected to hit $3 billion in annual sales by 2025, a 23% yearly growth rate.



Source: **Statista.com**

Figure 8: eSports market size worldwide from 2020 to 2025.

Monetary Policy

In contrast to the static, block reward emission that is followed by the majority of cryptocurrencies, Callisto Network has designed a dynamic monetary policy with fixed rewards per block that decrease with time.

These rewards will be shared among:

- Miners
- Cold Stakers
- Treasury Fund

Miners receive the highest proportion (60%) of each block reward.

Cold Staking, a core smart contract within the Callisto Network, will receive 30% of the block reward, and at an APR expected to exceed 5%. We believe that offers incentives to users to trust this passive income mechanism in the long term.

Finally, the remaining 10% from the block reward is allocated to Treasury Funds, with a twofold purpose:

- Ensuring the continuous growth of the project.
- Providing insurance to the audited tokens.

Additionally, a burning mechanism will be implemented to burn coins based on the current network utilization. Therefore, the more the blockchain is utilized, the higher the burning rate and the lower the coins in circulation, effectively rewarding users and holders. To do so, the burning mechanism will introduce a minimum, fixed fee that will burn CLO coins with every transaction made while ensuring a very low transaction cost.

Consequently, the more transactions on the network, the more coins will be burnt. This can result in a high deflation rate (burned tokens outnumbering newly minted tokens) in high utilization periods, which should further increase the value of the coins in circulation.

Governance

Another challenge we aim to address is Callisto Network's governance system, which takes advantage of the Treasury fund that's built-in at the protocol level. Governance refers to how the collective decisions are made, how conflicts are resolved, and how protocol changes are implemented.

The Callisto Network team believes that governance is essential to every project, especially in the wake of the Terra Luna collapse **(see analysis)**, as it offers a fully transparent and distributed way to make decisions for the further improvement of the ecosystem collectively.

By providing voting rights on certain governance decisions, the ultimate goal is to base our Governance system on a fully **Decentralized Autonomous Organization** (DAO), where the community collectively makes all the decisions according to a specific set of rules implemented into smart contracts.

In this direction, we will implement the governance model into the Callisto Network using a three-phase approach, as follows:

Phase 1

A. The team is fully in control of the project.

B. The community is voting on additional features and priorities, etc.

Phase 2

A. The team is partially in control (veto power).

B. The community is voting on Treasury spending and all critical decisions.

The vote are structured in "levels":

1. Minor feature.
2. Medium feature.
3. Major change or feature.

Phase 3

A. The team concedes control of the project, and allows the community to assume full control.

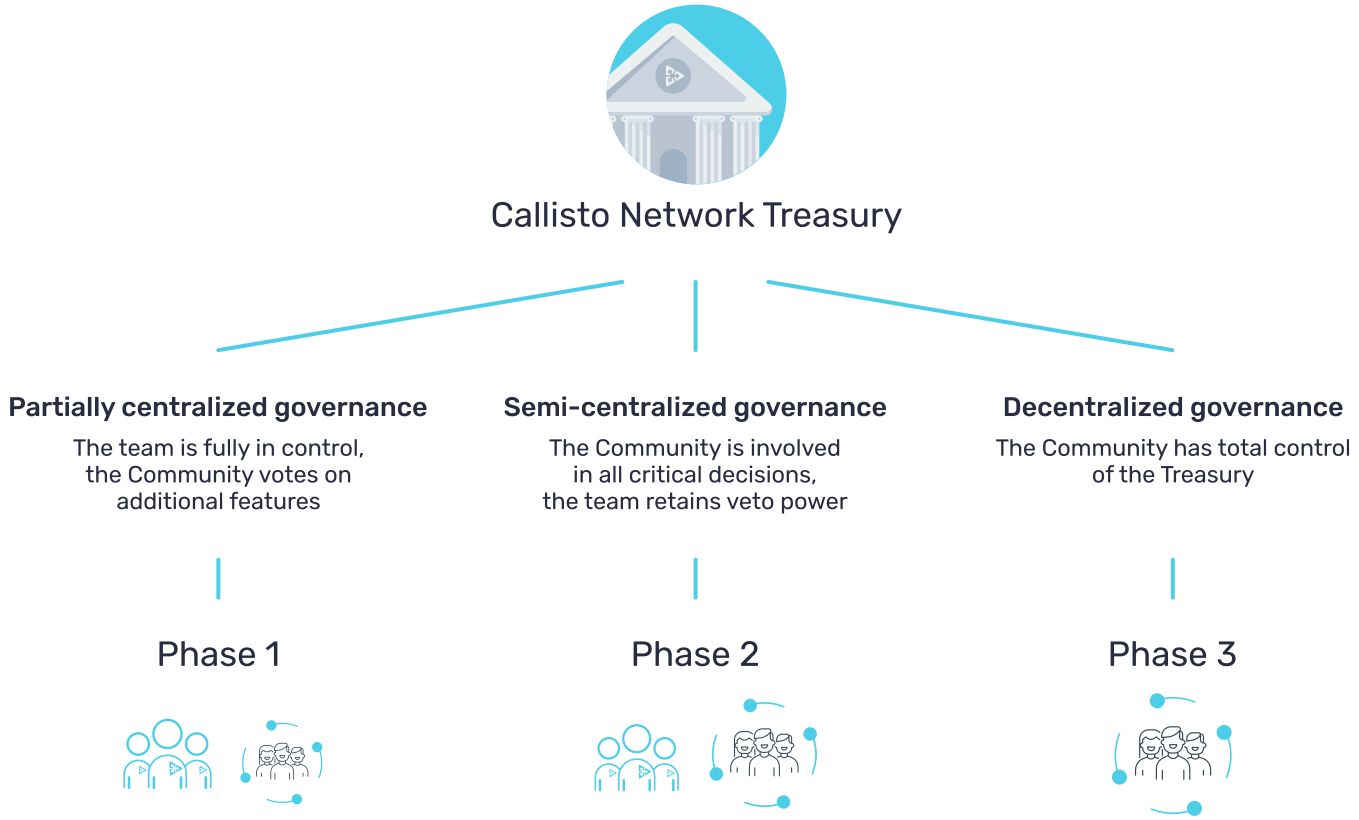


Figure 9: Decentralized governances phases.

Callisto Network will also provide the tools to easily implement the decentralized governance system into every application built on top of Callisto Network, making DAO creation a simple procedure requiring just a few clicks.