July 9, 2021

BitOoda

Sarcophagus

Decentralized Dead Man's Switch

Advisory

Sam Doctor[ac]
sam@bitooda.io
@CryptoSamDoctor

Mark Chin | mchin@bitooda.io

The Sarcophagus platform is an automated, decentralized dead man's switch built around blockchain technology to allow users to guarantee the proper, untampered, and permanent transfer of information or assets without a trusted intermediary, based on the absence of activity.

The core "dead man's switch" functionality of Sarcophagus allows a user to upload information or assets to be encrypted by a third party, who releases only to a specified recipient after a specified amount of time has passed. If the user does not want to transfer the data, they must extend the file release date. Only when the user fails an attestation is the file – which can include wills and trusts, passwords, accounts, data backups, and other data – passed to a recipient. **We assess this functionality creates value by mitigating trust issues – especially for anonymous bearer assets where intermediaries pose risks.**

The immutability of the file storage on Arweave eliminates fraud and doubt when transferring files. One such use case is mitigating disputes regarding wills. A lost or damaged document could allow malicious claims, with the execution failing to meet the original intent. Sarcophagus guarantees the original unaltered file will be transferred to the intended recipient.

Sarcophagus has three main stages: a data-wrapping phase, a validation phase, and a decryption phase. Each stage is carried out independently to ensure that the payload is never visible to the "middle-man" or Archaeologist, who is a third-party, utility provider on the network who receives revenue for encrypting user data and for following instructions appropriately. The user encrypts data with the public key of the intended recipient; the Archaeologist then encrypts this file further before uploading to Arweave. Before expiration of the contract, the user can extend the contract; if s/he fails to do so, the Archaeologist unwraps the outer encryption layer, now allowing the recipient to access the inner layer and decrypt it to receive the payload.

Archaeologists earn revenue when data is encrypted, the encryption time is extended, and ultimately decrypted. They stake SARCO tokens, the native tokens on the platform, and are paid in SARCO tokens. In addition, the Archaeologist posts a SARCO bond that may be slashed or taken from them in response to malicious or negligent behavior – such as premature or delayed unwrapping of the file. Fees earned by the Archaeologist against staked SARCO are the key value accrual mechanism for the tokens.

Sarcophagus allows users to replicate actions that would normally require paid, trusted middle-men, and offers improved security at a lower price point. The trust level required in the traditional attorney or advisor relationship to transfer anonymous bearer assets is especially high, and is mitigated in the Sarcophagus ecosystem.

Sarcophagus has successfully combined functionality from multiple blockchains. The platform relies on Ethereum for code execution guarantees and Arweave for a permanent, immutable file system. As data is stored permanently, Sarcophagus can certify that sensitive documents, when unwrapped, are unaltered from the original.

Sarcophagus v2, expected in 2022, permits multiple Archaeologists and variable bonds to reduce collusion risks, and allows for trading between Archaeologists.

Platform adoption is the key challenge – always a chicken and egg problem between users and service providers, to achieve a critical mass. The platform currently offers token grants to help seed the ecosystem and drive adoption.

In summary:

- Sarcophagus functions as a dead man's switch to ensure passage of a payload to a recipient.
- Traditional will and trusts introduce the issue of human error and malicious action – especially with bearer assets.
- Dual encryption provides Sarcophagus users guaranteed delivery of reliable data, with encryption protecting the data from the middle-man.
- Fees earned by the middle-man, who stakes SARCO tokens as a guarantee of appropriate actions, are the key value driver in the token ecosystem.
- Token grants help mitigate adoption challenges.

Key Takeaways

- Sarcophagus functions as a dead man's switch to ensure passage of a payload to a recipient.
- Traditional will and trusts introduce the issue of human error and malicious action – especially with bearer assets.
- Dual encryption provides Sarcophagus users guaranteed delivery of reliable data, with encryption protecting the data from the middle-man.
- Fees earned by the middle-man, who stakes SARCO tokens as a guarantee of appropriate actions, are the key value driver in the token ecosystem.
- Token grants help mitigate adoption challenges.

BitOoda has been retained by The Sarcophagus Builders to produce this report. Please see slide 25 for important disclosures.

CONTENTS

Introduction and Use Cases

Understanding the Dead Man's Switch

Traditional and Potential Applications

A dead man's switch is a mechanism that is designed to trigger a specific action in the instance the user is no longer able to attest to their continued activity. Conceptually, these capabilities are beneficial because they are triggered through inaction, and as such, enable an action to occur even if one party is either absent, or unable to perform.

In a traditional sense, dead man's switches are commonplace with vehicles such as locomotives, airplanes, etc. In a locomotive, the engineer is constantly pressing a pedal or a switch, and if released, the train's emergency brakes are activated, and the train is stopped. This serves as a fail-safe if the engineer becomes incapacitated or falls asleep.

Dead man's switches are commonly used with software as well. There are many applications: if a user does not log in for a set period, they may receive a notification on their phone. Computers may also be put in sleep mode after a set period of inactivity.

Currently, however, there is no dead man's switch that transfers data if a user is unable to attest and facilitates the storage of this data over a long period of time. **Sarcophagus not only creates this functionality, but also utilizes blockchain technology to effectively eliminate the need for a *trusted* intermediary.**

Who can benefit from Sarcophagus?

Sarcophagus can be used to transfer access – into the distant future – to information or financial assets to a beneficiary in a trustless, fail-safe manner upon:

1. The owner's death, incapacity or other event-based trigger or
2. The owner's failure to extend a time-based automatic unlocking.

People seeking to conditionally transfer assets or access to assets, especially digital and/or bearer assets, can especially benefit from not needing to trust an intermediary.

Sarcophagus Overview
Decentralized Dead Man’s Switch

Sarcophagus is a decentralized dead man’s switch application built on top of the Arweave and Ethereum networks. The platform uses blockchain technology to eliminate the need for a trusted third party when transferring data. Through Sarcophagus, anyone with access to a Web3 account can sign up to be an “Embalmer” or user, and upload any type of file to be later transferred to a recipient. When uploaded through Sarcophagus, the data is stored for as long as the user desires, even into the distant future. The third party involved, known as an ”Archaeologist”, stakes SARCO tokens and double-encrypts the uploaded file.

By staking their own tokens, network participants can choose to take on the role of “Archaeologists” and earn profit through double-encrypting Embalmers' data. Archaeologists define their terms and stake tokens for each sarcophagus contract as a locked bond. The bond is based on a reserve requirement, multiplied by the sum of the digging fees and bounty of the curse contract. The network automatically matches Embalmers’ filters with appropriate Archaeologists, who can then generate revenue as compensation for their role in encryption, as well as for the illiquidity of their bond.

Archaeologists are never given access to the data itself, as it is already encrypted by the originator before the Archaeologist adds a second layer of encryption. When it is time to decrypt the file, the Archaeologist’s role is automated by Sarcophagus, meaning that no manual action is necessary by the Archaeologist at the time of decryption.

The ecosystem is powered by the SARCO token, an ERC-20 token used in multiple ways throughout the Sarcophagus process. Independent ”Archaeologists” are paid using the SARCO token to double-encrypt data using Arweave. These Archaeologists expend their own capital to encrypt Embalmer data and generate revenue through SARCO as an incentive.

The app, which is functional though not yet incorporating all planned features, has already launched on mainnet, with the full version to be released within a year.

Use Cases

The Electronic Alternative

Will or Trust

A basic use case of Sarcophagus would be to store a will. In the United States, it is estimated that up to 3% of wills are contested, meaning that up to 100,000 wills are contested annually. Fraud and undue influence are common legal bases to challenge the legitimacy of wills, which Sarcophagus effectively eliminates.

Using Sarcophagus, the originator of the will can store relevant data in advance, to become accessible only after their passing. Because this data is hosted on Arweave, the underlying content will be stored in its original form forever. Loss of access to a will is a common issue, but now preventable by a platform like Sarcophagus, as information is completely encrypted and guaranteed to be delivered at the desired time.

Confidential Information Exchange

Sarcophagus can also be used to transfer information. For example, if a person or an entity is looking to keep information encrypted until after the end of its confidentiality, they could wrap it in a sarcophagus until its release date. This would guarantee the recipient will receive the original confidential information, while allowing the embalmer to extend the encryption as necessary.

Password Recovery

A dead man's switch can also be used to recover lost passwords. A user may upload a file containing credentials to a password manager and continuously extend the resurrection until needed, or set the release to a recipient who will take control of the account in the event of passing.

Emergency Contact

Another potential use of the dead man's switch is to store emergency contact information. Suppose a traveler plans a dangerous excursion: the resurrection time would mirror the timeline of the trip, and the daily attestation allows others to confirm the traveler's liveliness. Sarcophagus could also be used to keep certain information confidential unless it is otherwise required.

Political Activism

An activist holding sensitive information may use a dead man's switch to release data in the event of failure to attest. This ensures proper transfer in the event of detainment, imprisonment, or assassination.

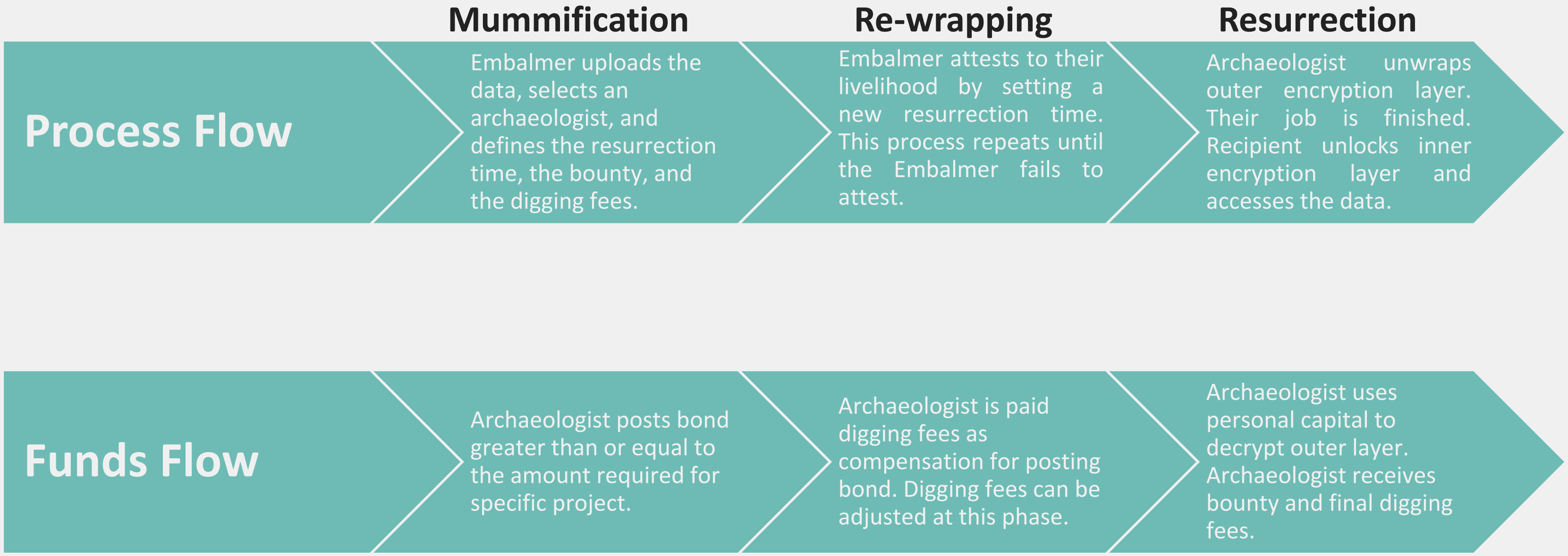
Source: Sarcophagus

BitOoda Advisory

Application Process

Overview

Three Stages



	Mummification	Re-wrapping	Resurrection
Process Flow	Embalmer uploads the data, selects an archaeologist, and defines the resurrection time, the bounty, and the digging fees.	Embalmer attests to their livelihood by setting a new resurrection time. This process repeats until the Embalmer fails to attest.	Archaeologist unwraps outer encryption layer. Their job is finished. Recipient unlocks inner encryption layer and accesses the data.
Funds Flow	Archaeologist posts bond greater than or equal to the amount required for specific project.	Archaeologist is paid digging fees as compensation for posting bond. Digging fees can be adjusted at this phase.	Archaeologist uses personal capital to decrypt outer layer. Archaeologist receives bounty and final digging fees.

Figure: Sarcophagus usage and funds flow

Source: BitOoda, Sarcophagus

Phase 1: Mummification

Sarcophagus Creation

- To create a sarcophagus, the Embalmer first uploads a file, enters a recipient public key, and enters a resurrection time. This creates a layer of encryption around the file.
- The Embalmer then establishes a ”curse contract” with an Archaeologist who meets defined bounty and digging fees.
- The Archaeologist, using their own Arweave public key, wraps the data with an outer encryption layer, and uploads it to Arweave for permanent storage.

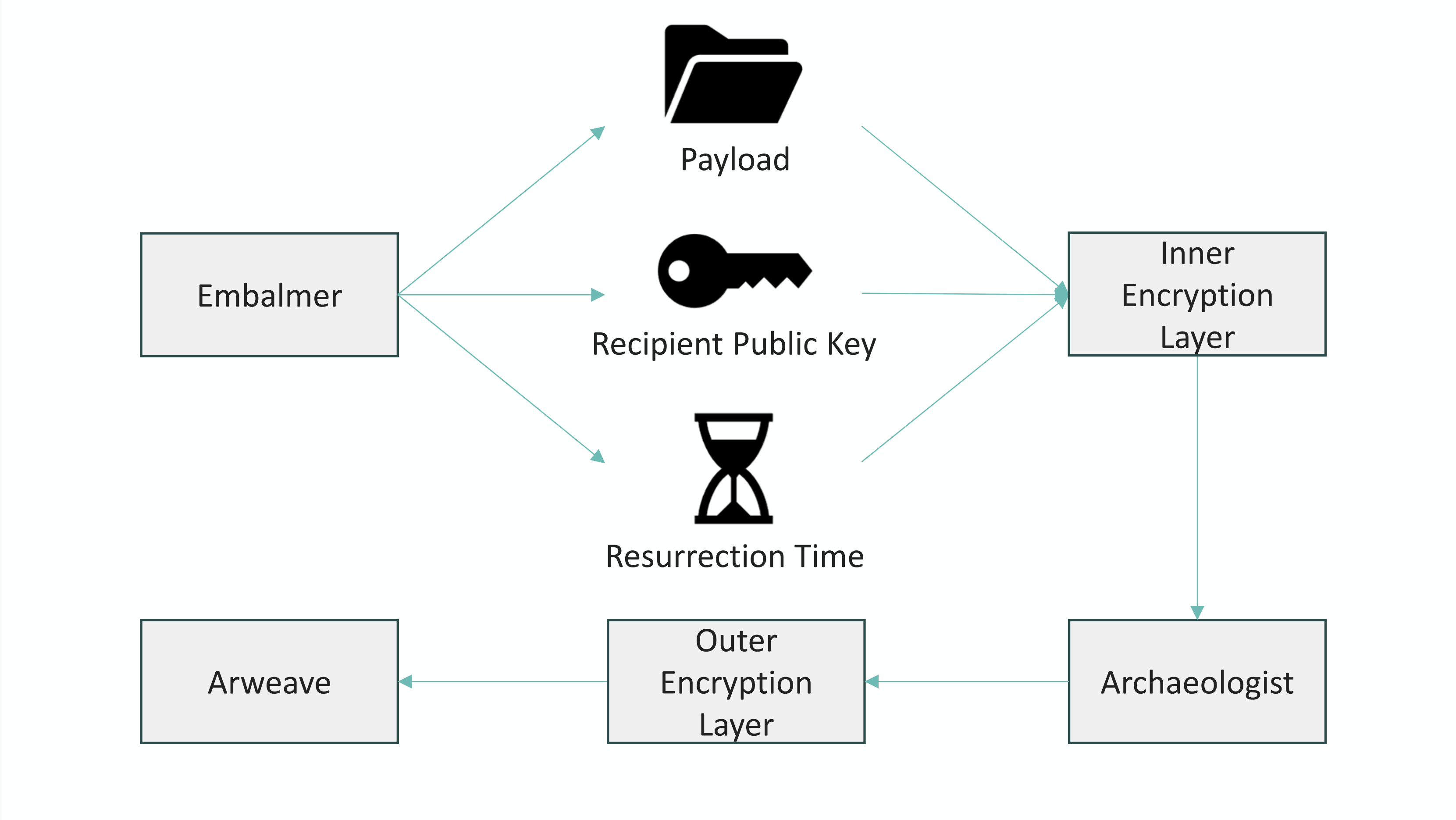


Figure: Sarcophagus creation

Source: BitOoda, Sarcophagus

Phase 2: Re-wrapping

Embalmer Attests to Liveliness

- The second phase of the process is called the re-wrapping phase, in which the Embalmer (and only the Embalmer) attests to their liveliness.
- The data is re-wrapped with a new resurrection time, along with new digging fees.
- At this point, the Embalmer can increase or decrease the bounty if they choose
- Previous digging fees are released from the curse contract to the Archaeologist, while the Embalmer's new digging fee payment compensates for the illiquidity of the bond.

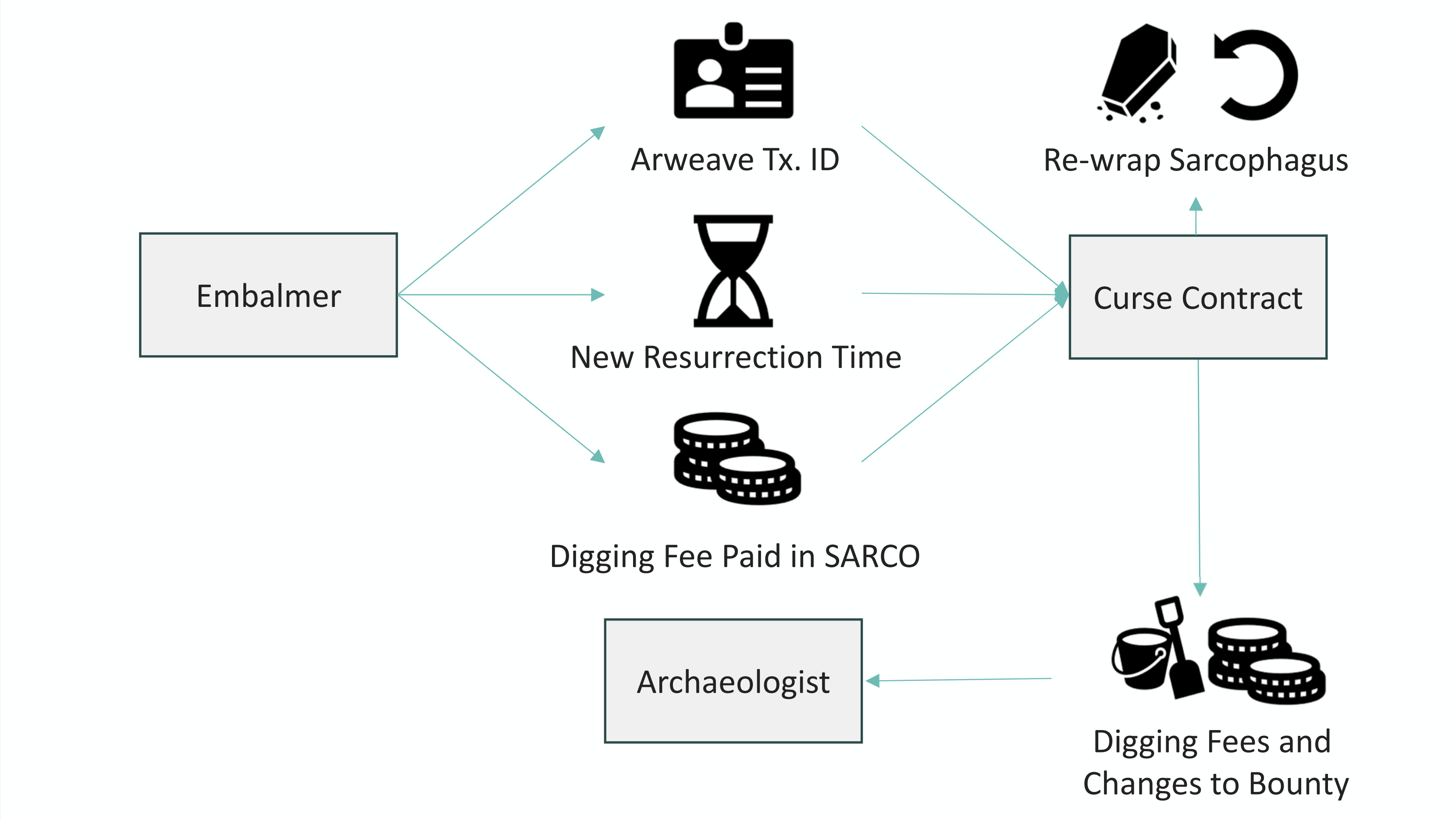


Figure: Re-wrapping mechanics

Source: BitOoda, Sarcophagus

Phase 3: Resurrection

Un-wrapping and Release of Bounty

- The third phase of the process is called Resurrection, which is triggered if the Embalmer does not specify a new resurrection time by the expiration of the current resurrection time.
- At this point, the Archaeologist decrypts the outer layer of the sarcophagus, and is paid the bounty and digging fees if completed on time.
- The recipient can then decrypt the inner layer of the data and access the payload.

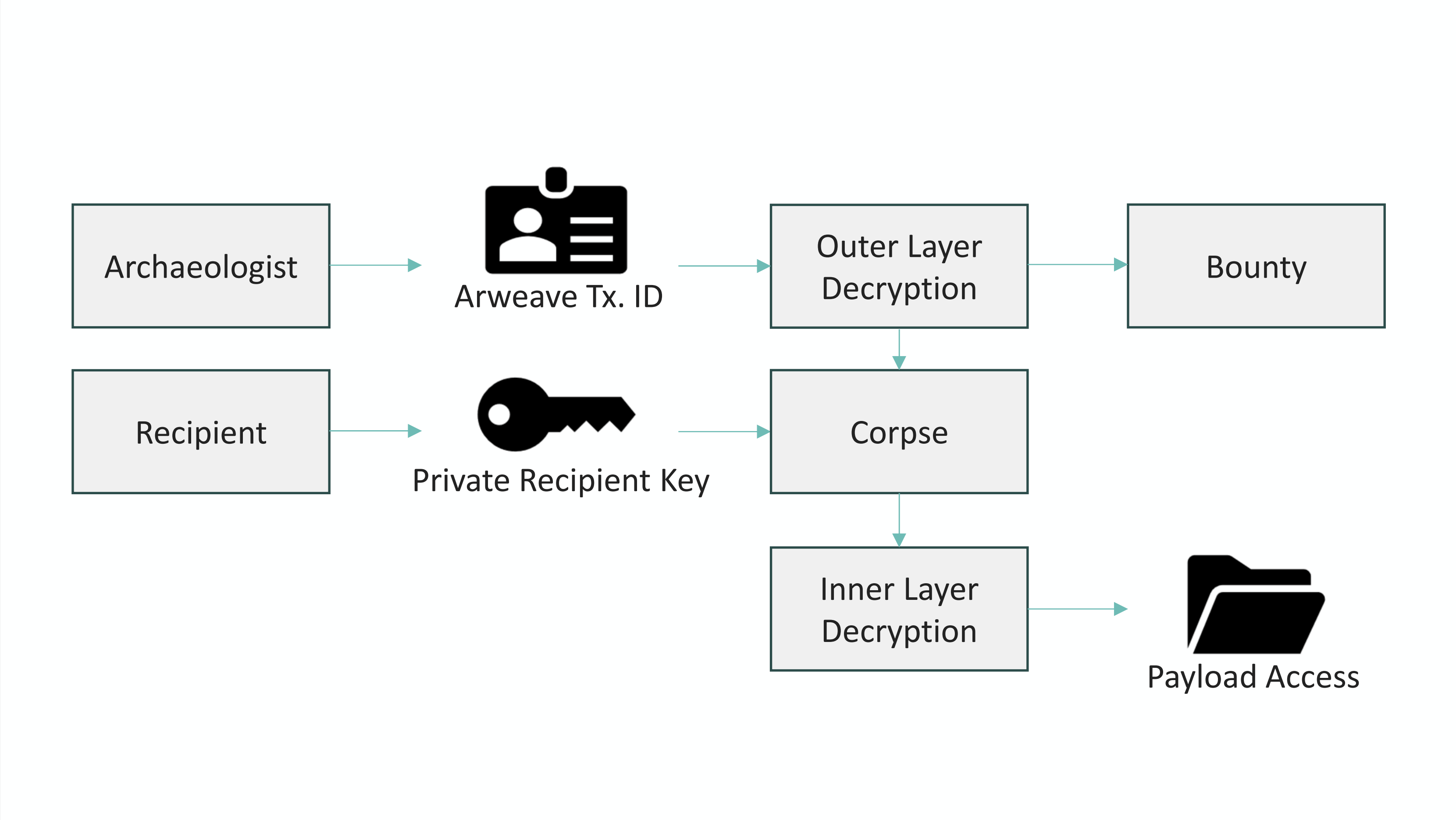


Figure: Un-wrapping of a sarcophagus

Source: BitOoda, Sarcophagus

Security Measures

Built-in Data Safety Features

Archaeologists, when chosen by an embalmer, are NOT given access to the contents of the data file. The payload has been encrypted client side, preventing any breach of privacy.

Upon resurrection, the Archaeologist's job is complete, and the recipient may decrypt the inner layer of the payload.

Sarcophagus incentivizes proper behavior as the combination of bonds, digging fees, and bounties will only be rewarded if the sarcophagus is resurrected within the designated time frame.

The platform has also put in place a slashing penalty, where in the instance that an Archaeologist unwraps a sarcophagus too early, too late, or not at all (beyond the grace period), the Archaeologist will not be rewarded. Bonded funds and digging fees are burned, while the bounty is returned to the Embalmer.

Dishonest behavior should be rare, as all actions are carried out by the software. For an Archaeologist to unwrap a sarcophagus early, the server code would need to be directly modified.

Reputation matters. Establishing a good behavior score requires proven consistency, and while it would be unfortunate for an heir to receive their payload late or not at all, good behavior is expected and enforced by the fact that as the network matures, Archaeologists will have established their reputation with a history of properly carrying out their role.

Most slashing-based networks see very little malicious activity due to early operators being long term holders and insiders, and as such, there is very little incentive to act maliciously.

All Archaeologists are required to post bonds of SARCO tokens. The amount required to post is the sum of the digging fees and the bounty for a given Sarcophagus (which must be approved by the Embalmer) multiplied by a set reserve rate. This reserve rate by default is 100%.

Attack Vectors

The most damaging method of attack is through Archaeologist and Recipient collusion; while this is possible, it can be avoided by using multiple sarcophagi and Archaeologists. Sarcophagus V2 plans to introduce a multi-archaeologist structure which will mitigate this danger.

Source: Sarcophagus

BitOoda Advisory

SARCO Token Economics

The SARCO Token

At a Glance

SARCO is an ERC-20 token with a built-in fixed supply of 100 million tokens.

The token is used in three ways:

1. By Archaeologists to pay for their services via digging fees and bounty,
2. By the Archaeologist to post their bond, and
3. By stakeholders in the DAO to control the future of SARCO

While digging fees and bounty are quoted in SARCO, the fees the Archaeologist pays to Arweave and Ethereum can be paid using any currency or token the Archaeologist chooses.

The Archaeologist bonds SARCO tokens, as well as spends ETH and AR tokens to store contracts and files on Ethereum and Arweave, respectively. Digging fees and Bounty, paid by the user / Embalmer in SARCO, cover the costs as well as a reasonable return on the Archaeologist's time, computing equipment, and the ETH / AR expenses. This relationship is the mechanism by which the SARCO ecosystem accrues value – and the limited token supply of 100 million, as well as the relationship between SARCO revenue and AR / ETH expenses, drive individual token value.

Archaeologists are incentivized to optimize their operations to reduce fees and to maximize the value they provide.

In order to promote usage of the token, SARCO has allocated 1% (1 million) of the fixed token supply to liquidity mining. This is the process of locking stablecoins into a contract and receiving SARCO in exchange, calculated proportionally to the deposited amount. Specific to this project, the allocation emission has been ongoing since January 13th 2021, 00:00 UTC and spans one year before the supply runs out.

SARCO is fully decentralized under a DAO; thus, no single entity is in control and decisions are driven by user votes. A single user's influence is determined by the volume of their stake.

To incentivize uniswap liquidity, the builders have created a farming contract, that distributes 2.5m tokens of the course of one year to any User that locks their UNI v2 sarco/ETH LP tokens. This contract started on 5/12/21 00:00 UTC and will run for exactly one year. This contract was funded by the DAO via vote

Source: Sarcophagus

Token Distribution
Grants to Seed Network Adoption

- All actions by the DAO are controlled via vote, the DAO will vote in the future to fund both embalmer incentive programs as well as archaeologist bonding bonuses
- Of the 100m fixed total token supply, 76.5m are held by the DAO

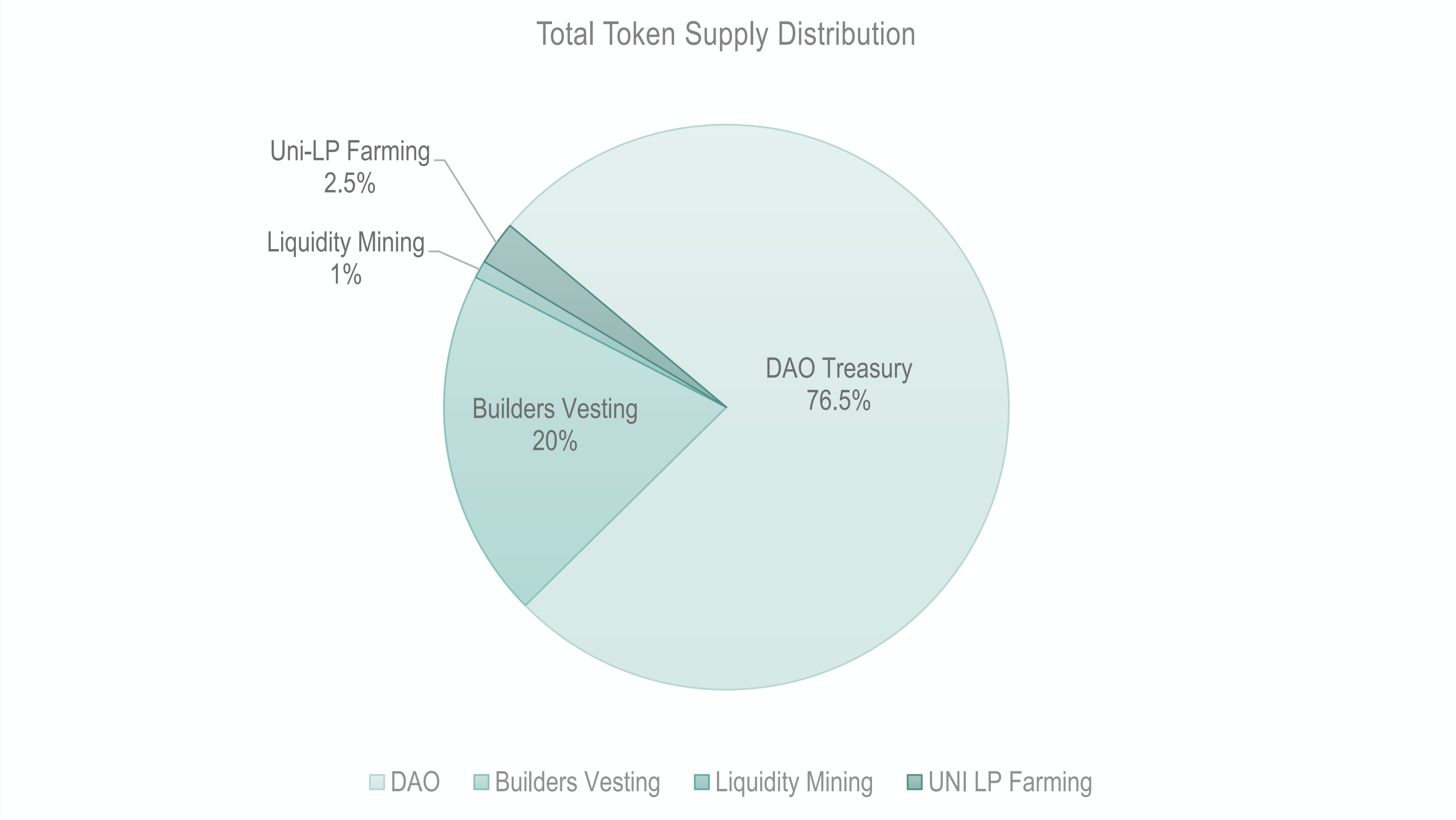


Figure: Token supply distribution by year end 2022

Source: BitOoda, Sarcophagus

Releasing SARCO

Mining Pool & Early Distribution

- 1% of SARCO tokens exist in a liquidity mining pool, which is expected to be fully mined by January 13, 2022.
- 2.5% of SARCO tokens allocated to UNI-LP farming
- SARCO tokens for early investors/developers will be distributed over two years.
- The remainder of the SARCO tokens are allocated to the DAO.

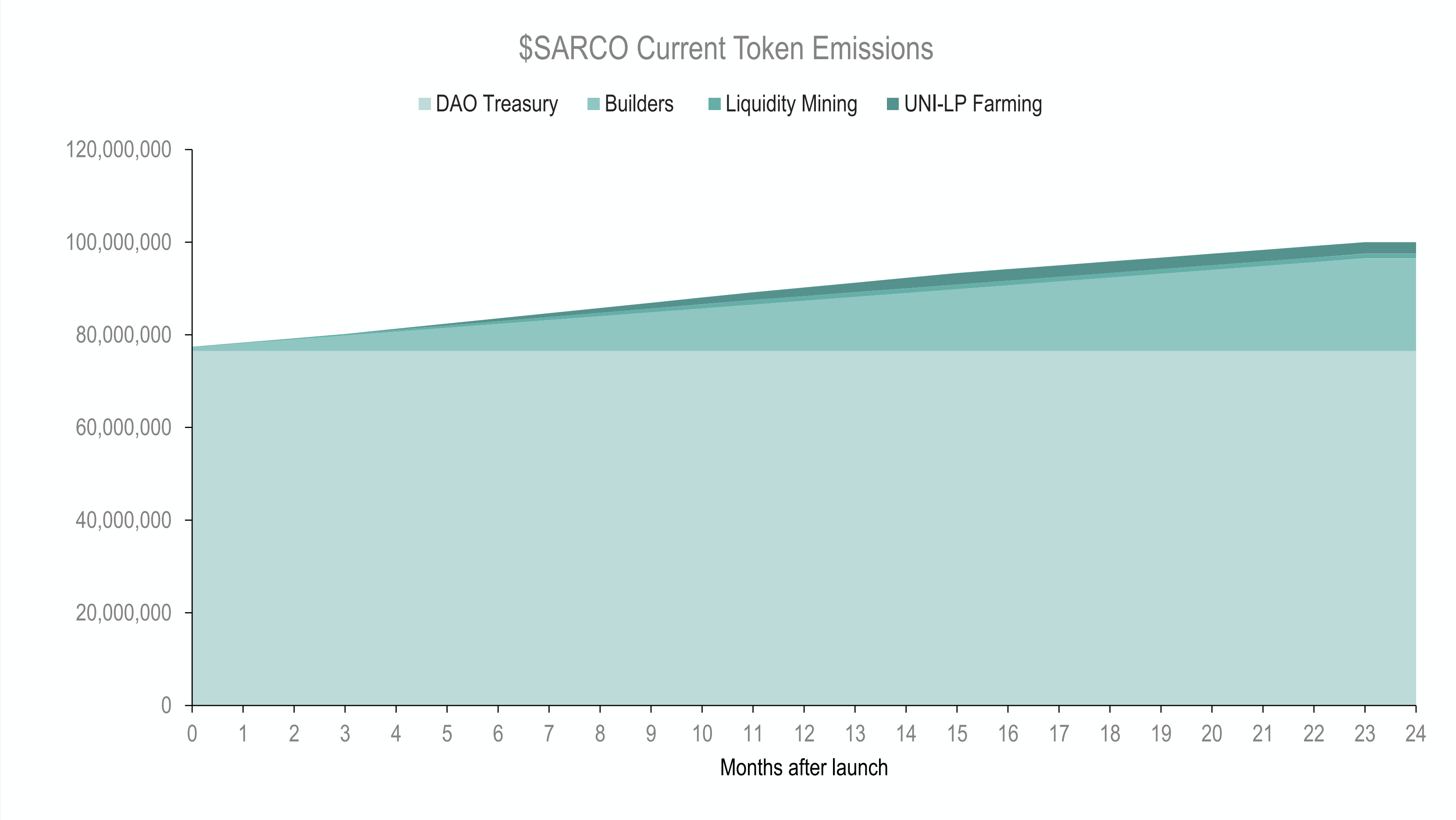


Figure: SARCO token emission schedule

Source: BitOoda, Sarcophagus

Decentralized Decision Making
Through a Decentralized Autonomous Organization (DAO)

Sarcophagus utilizes the Aragon DAO for governance. A DAO is a decentralized autonomous organization with no central management. DAOs utilize smart contracts which are programmed and enforced on blockchain networks. The result is a faster, cheaper, and scalable solution for governance.

Aragon itself is an online client that creates a user-friendly interface for DAO smart contracts. Apps on Aragon include voting, where holders of SARCO tokens can vote on decisions. This creates a system of checks and balances and prevents any malicious activity as Sarcophagus continues developing. Any holder of SARCO tokens can create a vote through the Aragon DAO client. Through Aragon, users have access to the DAOs finances and can manage their token balances.

In Q3 2021, Sarcophagus is launching funding through the DAO.

Sarcophagus also has an internal governance protocol which allows users to stake SARCO tokens in exchange for voting power. As of July 1st 2021, 1,096,504 SARCO have been staked. Sarcophagus plans to use this governance protocol in addition to the DAO as development proceeds.

Source: Sarcophagus, Aragon DAO

BitOoda Advisory

Outlook

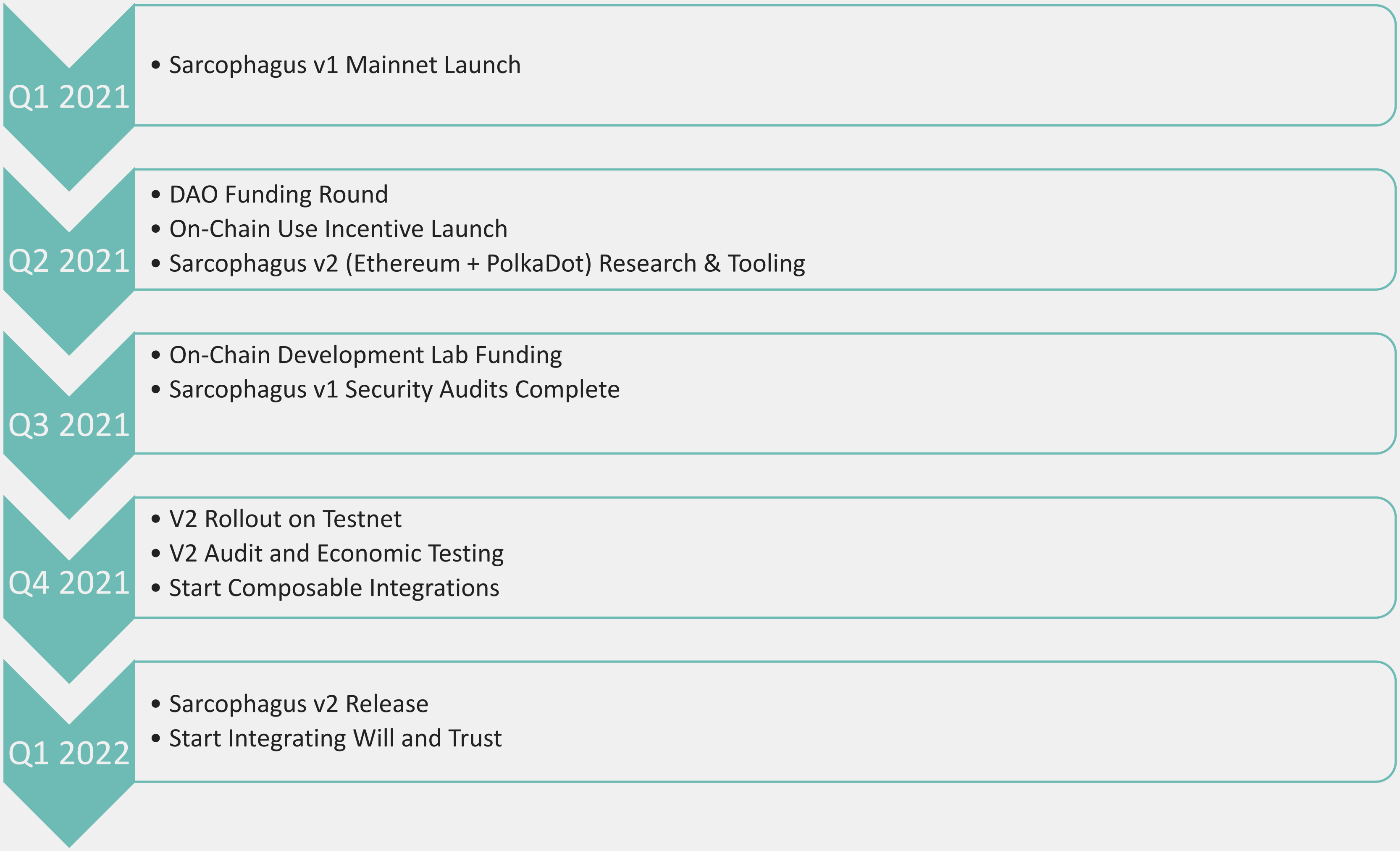
Network Upgrades
Sarcophagus v2

- Sarcophagus v2 is expected to be launched within a year to improve many of the features included in the initial Sarcophagus release.

- Allowing multiple Archaeologists to be cursed by a single Embalmer.
  - We expect this will reduce the risk of any type of collusion between parties.
  - Currently, if Embalmers are looking to rewrap a sarcophagus with a different Archaeologist, their only option is to ”bury” the sarcophagus and create a new sarcophagus with the same data. This will be prevented by a multi-Archaeologist curse structure.
  - A multi-Archaeologist curse structure also acts to reduce the risk of Archaeologist and Recipient collusion.
- Implementing Quadratic Digging Fee Settings.
- Creating variable bond requirements will allow Archaeologists bonds to vary based off malicious intent on the server.
  - If the network detects less malicious activity, the bond will be reduced as low as 10% to reduce illiquidity for Archaeologists.
  - We assess that there will be low server maliciousness, as there is little incentive for Archaeologists to act poorly.
  - Similar slashing-based projects have had very low volumes of malicious activity, but this may reflect selection bias, as many early users are long-term holders and insiders.
- Enabling trading between Archaeologists that meet minimum Embalmer requirements.

Upgrade Timeline

Roadmap Overview



Q1 2021

- Sarcophagus v1 Mainnet Launch

Q2 2021

- DAO Funding Round
- On-Chain Use Incentive Launch
- Sarcophagus v2 (Ethereum + PolkaDot) Research & Tooling

Q3 2021

- On-Chain Development Lab Funding
- Sarcophagus v1 Security Audits Complete

Q4 2021

- V2 Rollout on Testnet
- V2 Audit and Economic Testing
- Start Composable Integrations

Q1 2022

- Sarcophagus v2 Release
- Start Integrating Will and Trust

Source: Sarcophagus, BitOoda

Risks and Mitigants

Sarcophagus faces multiple risks to adoption:

- Competing technologies – either specialized dead man's switches or generalized functionality on evolving platforms including, but not limited to, Ethereum or Arweave – could offer superior functionality, lower costs, or both.
- Ethereum transaction fees have been extremely high because its adoption is outpacing its throughput advances. This situation is not expected to materially ease until the full deployment of layer-2 scaling for Ethereum. Until then, high transaction fees could slow adoption.
- Any malicious collusion between Archaeologists and recipients to provide early access to the payload could pose a reputational risk to the overall platform.

Mitigants:

- Ongoing upgrades and new Sarcophagus functionality are designed to stay ahead of the competition and offer increasingly robust solutions to the problem of asset and data transfer.
- Sarcophagus v2 is seeking to add PolkaDot support, among other upgrades. This diversification of protocols should help mitigate the transaction fee risk. V2 has the additional ability to run on any EVM compatible network.
- Allowing multiple Archaeologists to be cursed by a single Embalmer significantly mitigates the collusion risk.

Appendix

Arweave

Permanent Storage

Arweave (AR) was created because of the need for permanent storage of information posted on the internet. Today, using the internet relies on the ability to access centralized stores of data. Access to this data can be revoked by the owners. As it stands, using Ethereum as a storage method can be very costly due to gas fees. Arweave looks to improve upon this by making permanent, immutable storage a reality.

The Permaweb is built on top of the Arweave network. The idea is that this new web allows any uploaded content to be permanent and globally accessible, with guarantees on the integrity of the information.

Arweave allows the monetization and decentralization of storage space, where any user can provide storage for data on the network regardless the size. With this new approach to data storage, one entity no longer controls the data stored, and archiving is now significantly improved with information replicated on thousands of machines, making a network wipe nearly impossible.

Blockweave is a new form of involved blockchain created by Arweave which allows nodes in the network to store just a portion of the blocks.

Source: Arweave Litepaper

Glossary

Sarcophagus: The double-encrypted container that lives on Arweave forever.

Corpse: The un-wrapped sarcophagus that is available to download if the resurrection time has passed. This can be accessed if the user holds both the Arweave location and the Recipient key.

Embalmer: The creator of the sarcophagus and the party that chooses the corpse and resurrection time. The Embalmer pays for digging fees and determines how to handle the re-wrapping processes.

Archaeologist: Third-party, disinterested, incentivized utility providers. Archaeologists are looking to generate income through fees and bounties, which are offset by costs to operate the infrastructure.

Curse: The agreement between the Embalmer and Archaeologist. The Embalmer unilaterally chooses a specific Archaeologist to be responsible for resurrecting their file at the specified time. At this time, a portion of the Archaeologist's posted bond is locked. Bond must be posted in SARCO tokens to be available for new curses.

Resurrection Date: A time period set by the Embalmer. If the sarcophagus is not attested to within this time period, then the outer layer of the data will be decrypted.

Bounty: The fee paid upfront by the Embalmer. The bounty must meet the minimum set by the Archaeologist and is only transferred upon proper resurrection.

Digging Fees: The additional fee paid upfront by the Embalmer. This fee must meet the minimum set by the Archaeologist and is released to the Archaeologist upon subsequent re-wrapping or resurrection. These fees allow recurring cash-flow to the archaeologist.

Source: Sarcophagus

Disclosures

Purpose

This commissioned research is only for the clients of BitOoda and is intended for providers on the Sarcophagus network. This research is not intended to constitute an offer, solicitation, or invitation for any securities and may not be distributed into jurisdictions where it is unlawful to do so. For additional disclosures and information, please contact a BitOoda representative at info@bitooda.io.

Analyst Certification

Sam Doctor, the research analyst denoted by an "AC" on the cover of this report, hereby certifies that all of the views expressed in this report accurately reflect his personal views, which have not been influenced by considerations of the firm's business or client relationships.

Conflicts of Interest

This research has been commissioned by Sarcophagus for informational and educational purposes, and may be made available by the client to all interested parties who wish to learn more about the subject of this report.

The report contains the views, opinions, and recommendations of BitOoda. While BitOoda has been compensated to produce this report, such compensation is not in any way based upon any specific view or recommendation.

General Disclosures

Any information ("Information") provided by BitOoda Holdings, Inc., BitOoda Digital, LLC, BitOoda Technologies, LLC or Ooda Commodities, LLC and its affiliated or related companies (collectively, "BitOoda"), either in this publication or document, in any other communication, or on or through http://www.bitooda.io/, including any information regarding proposed transactions or trading strategies, is for informational purposes only and is provided without charge. BitOoda is not and does not act as a fiduciary or adviser, or in any similar capacity, in providing the Information, and the Information may not be relied upon as investment, financial, legal, tax, regulatory, or any other type of advice. The Information is being distributed as part of BitOoda's sales and marketing efforts as an introducing broker and is incidental to its business as such. BitOoda seeks to earn execution fees when its clients execute transactions using its brokerage services. BitOoda makes no representations or warranties (express or implied) regarding, nor shall it have any responsibility or liability for the accuracy, adequacy, timeliness or completeness of, the Information, and no representation is made or is to be implied that the Information will remain unchanged. BitOoda undertakes no duty to amend, correct, update, or otherwise supplement the Information.

The Information has not been prepared or tailored to address, and may not be suitable or appropriate for the particular financial needs, circumstances or requirements of any person, and it should not be the basis for making any investment or transaction decision. The Information is not a recommendation to engage in any transaction. The digital asset industry is subject to a range of inherent risks, including but not limited to: price volatility, limited liquidity, limited and incomplete information regarding certain instruments, products, or digital assets, and a still emerging and evolving regulatory environment. The past performance of any instruments, products or digital assets addressed in the Information is not a guide to future performance, nor is it a reliable indicator of future results or performance.

SARCO is only listed on cryptocurrency exchanges that list cryptocurrencies that are not deemed to be securities.

Ooda Commodities, LLC is a member of NFA and is subject to NFA's regulatory oversight and examinations. However, you should be aware that NFA does not have regulatory oversight authority over underlying or spot virtual currency products or transactions or virtual currency exchanges, custodians or markets.

BitOoda Technologies, LLC is a member of FINRA.

"BitOoda", "BitOoda Difficulty", "BitOoda Hash", "BitOoda Compute", and the BitOoda logo are trademarks of BitOoda Holdings, LLC.