
SARC
OPHAG
US

A Decentralized Dead Man’s Switch

Sarcophagus is an autonomous, incentivized application built on Ethereum and Arweave.

Sarcophagus Litepaper v0.2

August 2020

What Is It?

Sarcophagus is a blockchain-enabled, general-purpose digital dead man's switch. It is autonomous, censorship resistant and immutable. We rely on modern smart contracting networks like Ethereum or Tezos as well as Arweave's permanent file storage network; files you place in a sarcophagus are only unlocked in the event of you failing to attest to the contract.

Historically, dead man's switches have been used in heavy machinery to ensure the operator is paying attention and is present at their post. However, there are many other examples of physical-use cases such as suicide bomber vests and even Russia's Strangelovian Dead Hand nuclear program.

A dead man's switch is a mechanism (digital or physical) that triggers when the user fails to perform an action.

Bitcoin gave us the base of blockchain tech, it proved to us that making computers do physical things to supplant human trust (or violence) is not only sustainable, but approaches antifragility. Ethereum gave us the ability to execute code on a 100% uptime, decentralized and immutable computer. Arweave gives us the ability to economically store and retrieve files from a separate, immutable and permanent file system. Only the combination of multiple groundbreaking innovations in the past 10 years has made sarcophagus possible.

Leaving Secrets to The Future

Our goal with this is to make secret recovery easier and more intuitive. However, we know that we can't simply start offering password recovery with a centralized server (ZK or otherwise); that would be going backwards. We have to conceptualize the idea of *secrets*, how they affect us as humans, the value they hold, and the nature of timeline concerning their storage and recovery.

Centralized Demo

We built a version with a centralized server as an 'Archaeologist' to show how sarcophagus will work in the future. (It works today, but you probably shouldn't trust it with anything important.)

Available at demo.sarcophagus.io , this version requires Metamask to operate. The Recipient account will require private key exposure, but does not need to have any value, so feel free to spin up a new keypair to play with. There is also no concept of 'digging fees' or 'bounties' in this demo version.

Screenshare walk through link: https://vimeo.com/376933654

If you would like to create a link to a demo s7arcophagus for public disclosure, you can use this URL format:

https://demo.sarcophagus.io/resurrect?ar_id=YOUR_ARWEAVE_TRANSACTION_ID&eth_pk=RECIPIENT_ETH_PRIVATE_KEY

Replace ARWEAVE_TRANSACTION_ID and RECIPIENT_ETH_PRIVATE_KEY with your data and post wherever.

Public Disclosure Example

Here is an example link with sarco_demo_text.md as a payload. Metamask is required to login but no signatures are needed:

https://demo.sarcophagus.io/resurrect?ar_id=peDUL3yRRZnuQWJv2UE7Eu5yyHlyWUuM6sPaDX0eu8g&eth_pk=6A1F9801C570AAACE31A560EF35233B7477636A08AF4ABAB2CDBD7747DE912BB

Built Using Arweave

Arweave is a new decentralized protocol that makes permanent data possible for the first time.

From arweave.org:

"The traditional web that you know is full of broken links, ever-evolving information, and monolithic data warehouses. Have you ever clicked on a broken link or been served a 404 page? Well, that's evidence of the problem, and exactly what Arweave solves. We're making a new, permanent web called the 'permaweb.' "

We currently rely on the Arweave network exclusively for storage. When compared with the other decentralized file storage options. Arweave's endowment-based payment mechanism is a direct fit for the mission and scope of sarcophagus.

SARCO Token

The ERC20 SARCO token is the primary unit of exchange in the network and is used in two ways:

- By the Embalmer to curse an Archaeologist (pay for resurrection services)

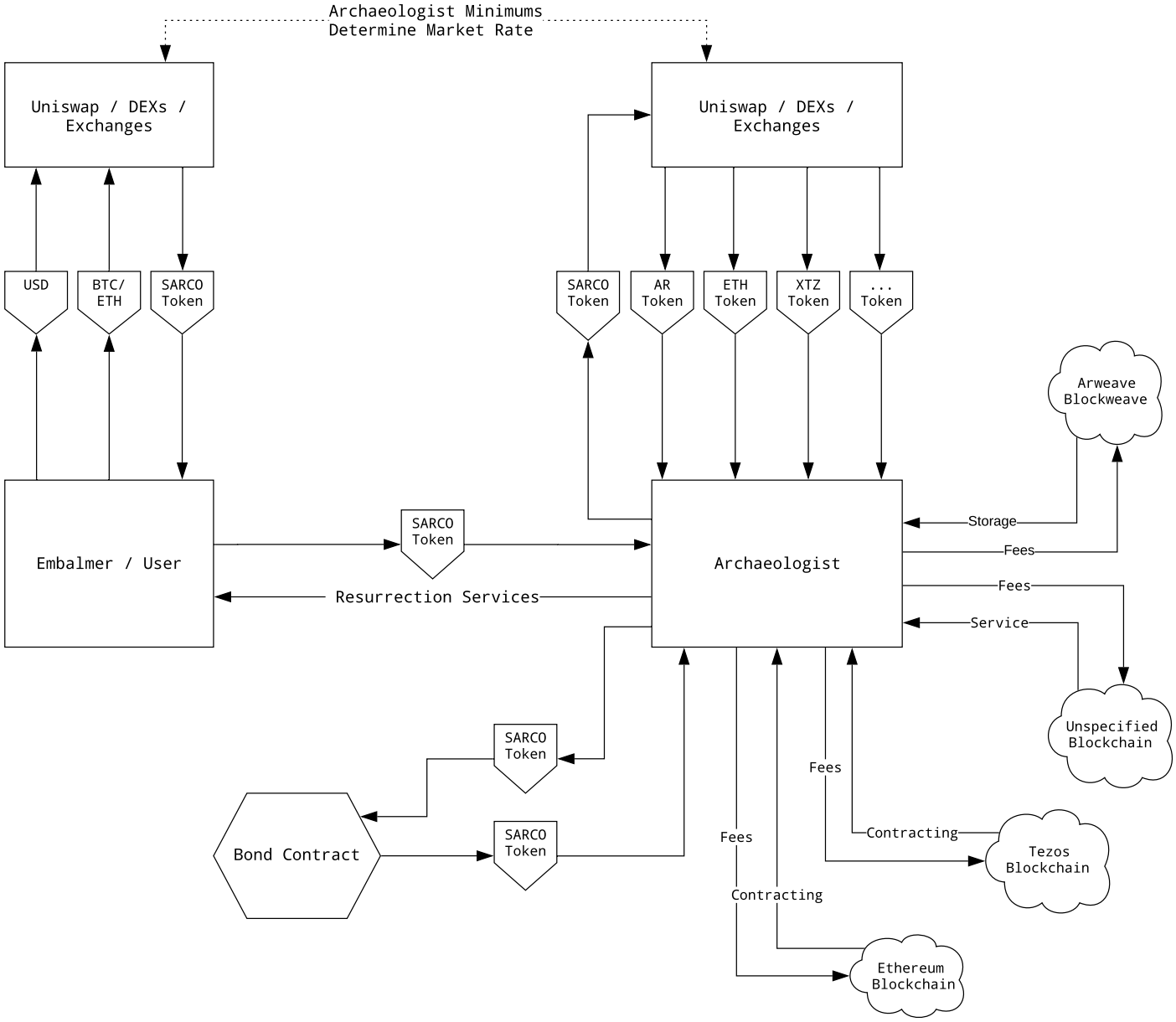
- By the Archaeologist to post their bond

The token represents the price that an Archaeologist will charge in servicing a given sarcophagus. The Archaeologist will list their minimum digging fees and bounty in terms of SARCO.

The archaeologist must pay fees to the contracting and storage networks to service a given sarcophagus (currently Arweave and Ethereum). Thus the value of a SARCO token will hit an equilibrium point when the network matures that is equal to all costs expended by all Archaeologists on the application plus the human value of the services received by the embalmer.

Any changes in the underlying value of the tokens consumed during the Archaeologists' operations will also affect the relative price of SARCO.

This basis of value accretion in the SARCO token allows Archaeologists to further optimize their operations not just by avoiding slashing penalties, but additionally by employing creative strategies in their treasury management of SARCO, as well as their management of required fee token wallets.



1 of 3 - Mummification Phase

In the mummification phase, the Embalmer will upload the 'corpse' (payload data), which is encrypted client-side with the public key of the Recipient. The Embalmer will also include several other parameters in the mummification process:

- The Resurrection Time (when the sarcophagus should be decrypted if the Embalmer fails to re-wrap)

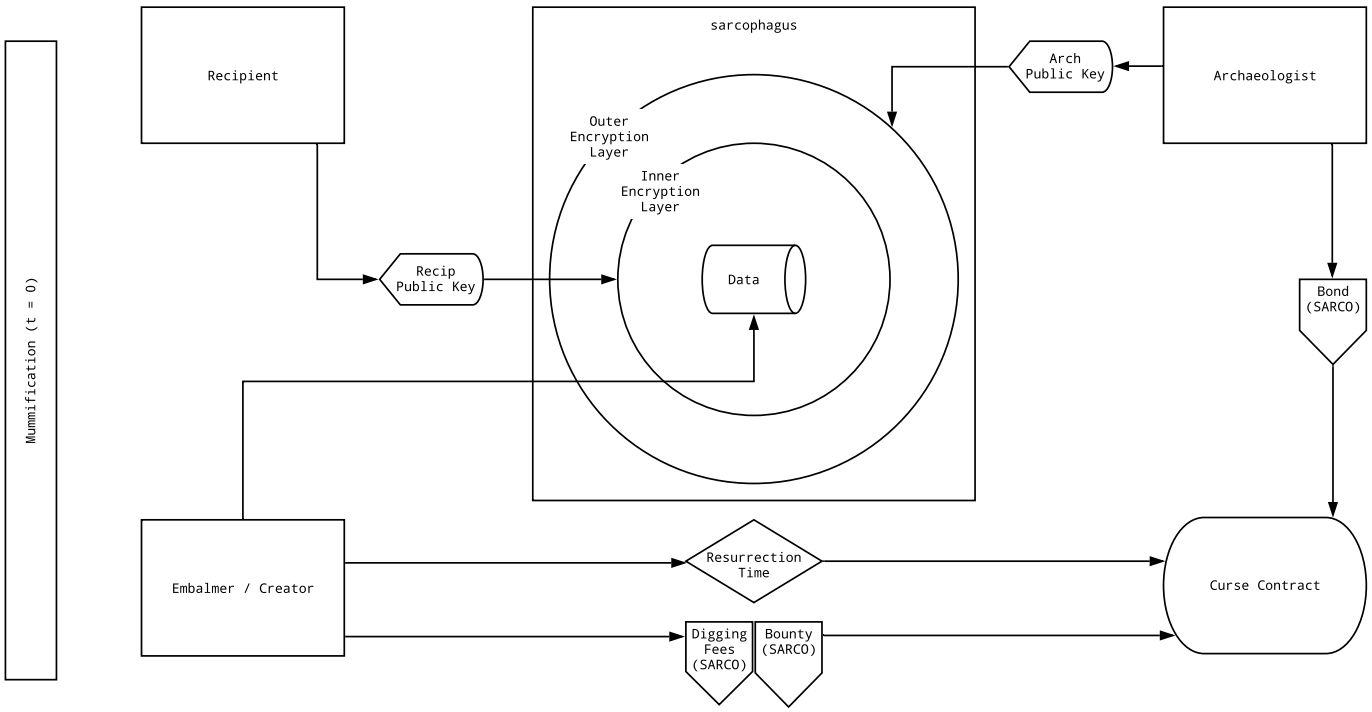
- The Bounty (the primary motivation payment to the Archaeologist, paid only upon resurrection)

- Digging Fees (payments to the Archaeologists that are guaranteed and paid upon re-wrapping or resurrection)

During the process of mummification, the Embalmer must select one or more Archaeologists to curse. A curse is a willfully entered contract with an Embalmer by an Archaeologist that locks away a portion of the Archaeologist's posted bond. This portion that is locked until re-wrapping or resurrection and is the sum of the digging fee and the bounty multiplied by the reserve requirement.

In order to become an Archaeologist, an operator must spin up the server as well as post a bond in SARCO tokens that is available for curses. Once an Embalmer chooses to curse an Archaeologist, and all of the public minimum parameters of the Archaeologist are exceeded, there is no way for an Archaeologist to recover the cursed portion of their bond other than to perform their duties as specified in the curse contract.

In the final step of this phase, the Embalmer will use the public key of the Archaeologist to encrypt the outer layer of the sarcophagus.



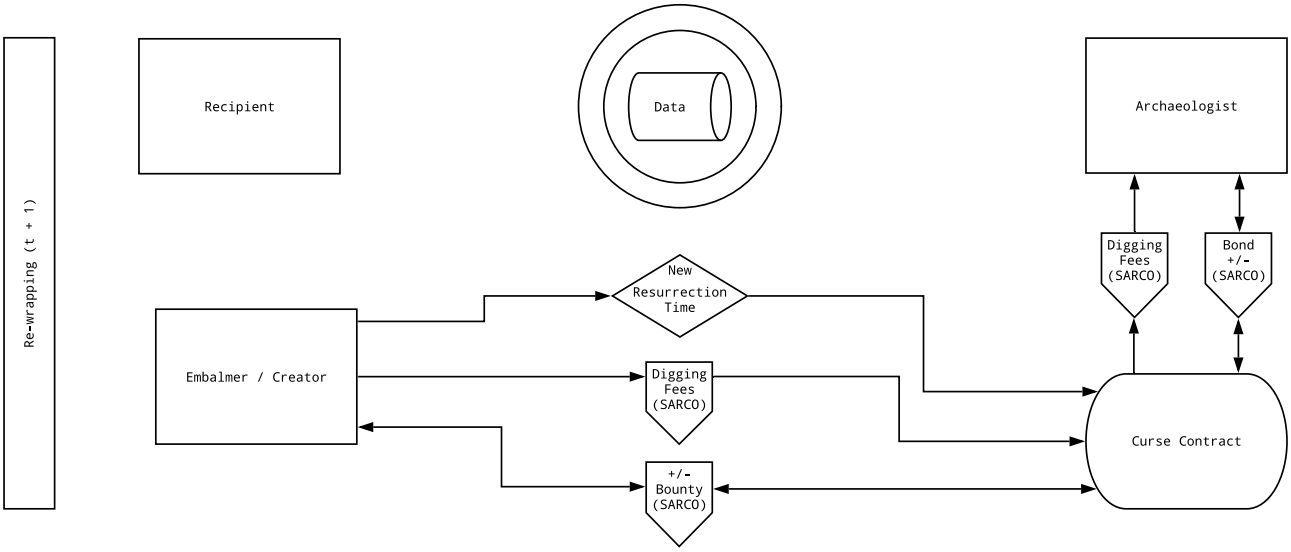
2 of 3 Re-wrapping Phase

When the Embalmer wants to attest to their liveliness, they re-wrap the sarcophagus by sending a transaction through the contract with a new resurrection time.

Resurrection times can be set to anything in the future, and can be decreased or increased from the previous value; only the Embalmer is able to re-wrap a sarcophagus.

The Embalmer is also able to increase or decrease the bounty at this time as long as the resurrection time has not passed.

During each re-wrapping, digging fees for the previous period are also released from the curse contract and paid to the Archaeologist. At this point the Embalmer now must pay more digging fees to the Archaeologist in order to compensate for the illiquidity of the bond that was cursed and locked on their behalf.

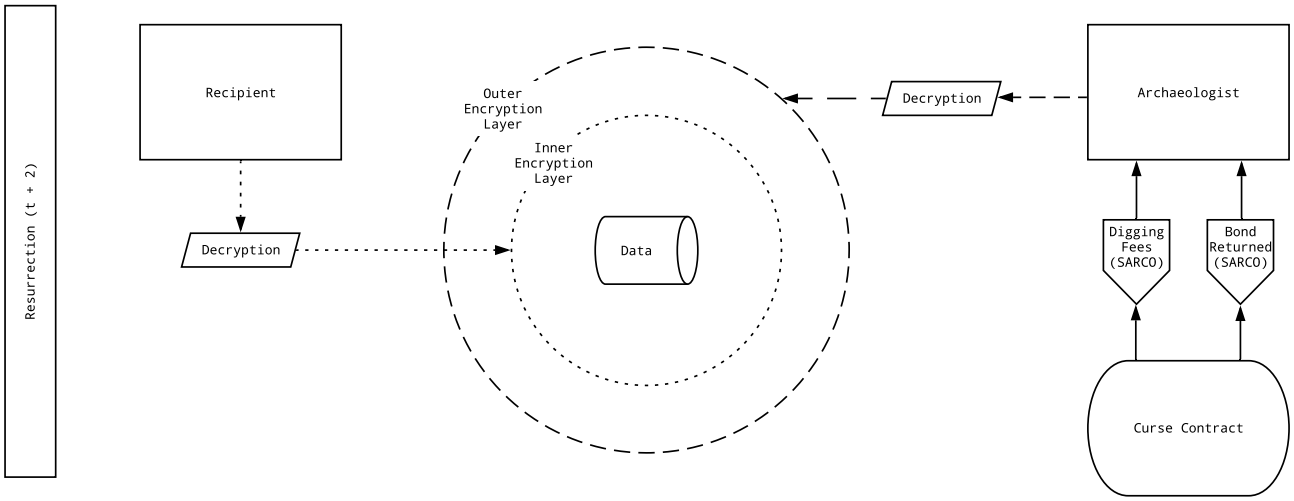


3 of 3 Resurrection Phase

If the Embalmer fails to re-wrap the sarcophagus, the Archaeologist is now able to decrypt the outer layer and retrieve the bounty.

Since the inner layer is still fully encrypted with the Recipient's public key, the Archaeologist (or anyone other than the recipient) is not able to decrypt the corpse.

Once the Archaeologist has unwrapped the outer layer and the bounty has been claimed, their work is done. (Digging fees are also paid to the Archaeologist at this time.)



Entity Definitions and Attributes:

The following sections will describe all of the entities involved within the sarcophagus application. The order in which they appear may not strictly follow the order of operations in use.

Sarcophagi

The sarcophagus is the file that sits on the Arweave network and is wrapped, re-wrapped and resurrected by the Embalmer and Archaeologist. It consists of two layers of encryption, with the outermost layer of encryption controlled by Archaeologist game theory, and the inner one being controlled by the Recipient's private key.

Inside the sarcophagus is what we call the "corpse" - this is the payload and can be any file type. This file is what will be available for download as long as the resurrection time has passed, and the user holds both the Arweave location and Recipient key. It is important to remember that any file placed on the Arweave network never changes, we just use contracts as lenses through the layers of encryption.

Embalmer

The Embalmer is the creator of the sarcophagus. They are the party that chooses the payload, and the resurrection time, pays for digging fees, attaches the bounty and determines how to handle the re-wrapping process.

In order to rely on the Archaeologist network to unwrap the outer layer of the sarcophagus, the Embalmer must attach a bounty in excess of the Archaeologist's minimum, as well as digging fees as compensation for the portion of the Archaeologist bond that they have locked up (cursed).

The Embalmer can choose digging fees and bounties that are just above minimums, or they can choose to use higher fees and bounties to further incentivize Archaeologist honesty in resurrection.

Corpse

The corpse is the payload contained within the sarcophagus. The corpse can be made of any file type as long as it is within network limits, and can even be an encrypted container itself.

Mummification

Mummification is the process of wrapping the corpse (data payload) - this process is completed by the Embalmer (creator). Once a corpse has been mummified by the Embalmer and the contract, it is then stored on Arweave forever as a sarcophagus.

Re-wrapping

Re-wrapping is the process by which the Embalmer attests to their liveness; it is the equivalent of a train operator holding down the dead man's switch safety pedal. In order to re-wrap the sarcophagus, the Embalmer must use the key that was used in the mummification process. It is only possible to re-wrap a sarcophagus prior to the resurrection time.

During the re-wrapping, the Embalmer must:

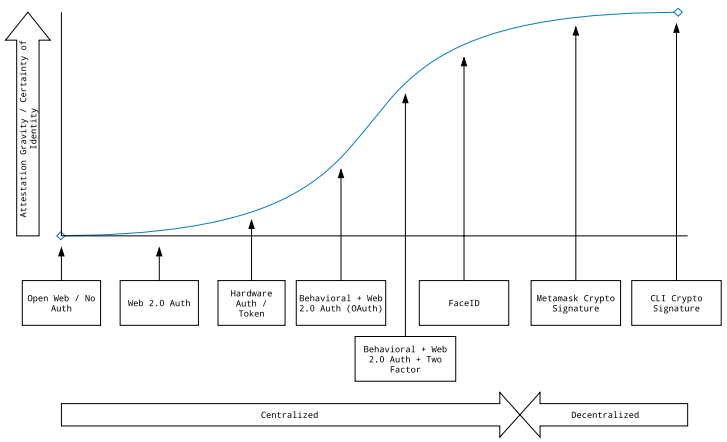
1. Specify the new resurrection time (must be in the future).

2. Specify and pay the new digging fees for the updated resurrection time.

3. Specify the new bounty amount and add or subtract from the current bounty.

Most re-wrapping events will entail re-wrapping the sarcophagus for the same amount of time as the previous period. This is possible in a purely decentralized manner with just a few clicks in Metamask.

It is also possible to introduce some web 2.0 authentication methods like FaceID and OAuth for less mission-critical sarcophagus operations. The gravity of the attestation method should match the value of the contents of the sarcophagus.



Resurrection

Every sarcophagus has a resurrection time, the Archaeologist will receive the bounty payment if they unwrap it after the resurrection period, (but only within resurrection the grace period0.

The Archaeologist has a powerful incentive to monitor the resurrection times of all sarcophagi that have cursed them, and to unwrap them as soon as possible after the resurrection time has passed.

Once the Archaeologist has unwrapped the outer layer of the sarcophagus, it is now accessible on-chain forever.

Now, all that is needed will be the Recipient key for the inner layer of encryption. If the Embalmer has chosen to make this key public, the files are now available for anyone to download on the web. Forever.

Deleting a Sarcophagus

Once created, a sarcophagus can never be destroyed, it can only be locked away forever. It is the nature of the Arweave network that all files live on in their original form, on-chain, forever. The only way to ensure that a sarcophagus will never be opened is to use the built-in Archaeologist incentive mechanisms.

The application will allow the Embalmer to re-wrap a sarcophagus with no bounty or digging fees, as long as the resurrection date is further in the future than the Archaeologist's published maximum resurrection time. This will release the Archaeologist of any financial obligation of resurrection.

Any sarcophagi that are unwrapped prior to the resurrection time will still be logged in the public statistics of the Archaeologist. However, while resurrecting a "buried" sarcophagus will not carry a financial penalty for the Archaeologist, it will cause a major negative hit to their performance and trust metrics.

Curses

An Embalmer must curse an Archaeologist in order to have their sarcophagus monitored and resurrected in the case of a failed attestation. A curse is initiated by the Embalmer selecting an Archaeologist that has posted a bond that is in excess of their requirements. A curse can be thought of as a contract that is unilaterally entered by the Embalmer, but one which also affects the Archaeologist.

An Archaeologist is required to post a bond as well as the requirements in order for curses to be placed upon them. The posting of this bond can be seen as consent for curses.

During the mummification phase, the Embalmer must select an Archaeologist that has made itself available for curses. The sarcophagus that they are attempting to create must fall within the parameters set by the Archaeologist operator in order to be created. These parameters are:

- Max resurrection time (the furthest point in the future for which the Archaeologist is willing to lock up their bond)

- Min digging fees (the lowest amount of compensation the Archaeologist will accept for locking the bond)

- Min bounty (the lowest reward accepted in the case of a successful resurrection).

Recipients

The Recipient is the ETH keypair that is able to download the corpse after it has been resurrected. This keypair can be retained like any other private key (i.e. stored privately) or it can be posted publicly.

It is important to remember that the Recipient key is able to unwrap only the inner layer of the sarcophagus. This means the sarcophagus is useless (or less than useless) prior to the unwrapping of the outer layer by the Archaeologist.

The Recipient account does not need to have any ETH to download a file, thus it can be shared widely in the case of public disclosure.

Archaeologists

Archaeologists are third-party, disinterested, incentivized utility providers. Their goal is to make more money in bounties and digging fees than it costs them to operate their infrastructure. They operate servers and post their own capital as bonds. If a resurrection time has elapsed (i.e., the Embalmer fails an attestation) the Archaeologist will spend their own funds to affect the unwrapping of the outer layer of the sarcophagus (a resurrection).

The only attributes of a sarcophagus that an Archaeologist (or any other party) can see on-chain are:

1. Sarcophagus total file size
2. Resurrection time
3. Bounty
4. Digging Fees

It is our goal to make the Archaeologist server so lightweight that it will be able to run on a raspberry pi. There is no heavy storage or computation needed, just some initial SARCO to fund the bond, ETH for gas, and AR tokens for storage payments.

We think of Archaeologists as disinterested utility providers because they are providing a service to an Embalmer and Recipient that they have absolutely no control over or visibility into. The Archaeologist is only able to decrypt the outer layer, and is not able to know prior to the resurrection if a given sarcophagus is public or private. These servers are operated for a profit motive at an arm's length from the use cases of individual sarcophagi.

The combination of bonds, digging fees, and bounties come together to incentivize the Archaeologist to only resurrect the sarcophagus after there has been a failed attestation. The Archaeologist can technically unwrap the outer layer of the sarcophagus at any time, but they will be slashed the full cursed amount of their bond. A slashing event occurs when an Archaeologist unwraps the sarcophagus too early, late or not at all.

Minimums to Curse

An Archaeologist has several publicly available and adjustable parameters that will affect their economics, and the Embalmers who will wish to curse them. These parameters are:

- Minimum digging fee (SARCO/block)

- Minimum bounty (SARCO)

- Max resurrection time

By allowing Archaeologists to set their own parameters, they can ensure revenue as well as limit how long their bonds can be locked up for.

Reserve Requirement

All Archaeologists are required to post a bond of SARCO tokens. The amount that they are required to post is equal to the sum of the digging fees and bounty for a given sarcophagus, multiplied by the reserve requirement. The reserve requirement is calculated by looking at the amount of malicious volume as a portion of the total network volume in SARCO.

We take the malicious volume (early/late/missed resurrections) for the previous 175,000 blocks (~1 month) over the total volume for that same period of time. Each basis point of malicious activity over this period increases the reserve requirement by 10% with a maximum of 100%.

- If there is no malicious activity over this period, the reserve requirement will equal 10%.

- If there is rampant malicious activity (more than 1% by value) the reserve requirement will ratchet to its maximum of 100%.

By adding this ratcheting mechanism we can further incentivize Archaeologists to resurrect files only during the proper period. The reserve requirement has a direct relationship to the Archaeologists rate of return for their work and the illiquidity of their bond.

Slashing

A slashing event will occur if:

- The Archaeologist unwraps the sarcophagus prior to the resurrection time set by the Embalmer.

- The Archaeologist unwraps the sarcophagus after the resurrection time + resurrection grace period (network variable).

- The Archaeologist does nothing and the resurrection time + resurrection grace period has elapsed.

The slashing event will cause the Archaeologist to lose the amount of the bond cursed by the sarcophagus that was resurrected too early, late or was missed. This cursed amount is the sum of the bounty and digging fees multiplied by the network reserve requirement.

During a slashing event:

- Bonded funds from the Archaeologist will be burned.

- Digging fees will be burned.

- Bounties will be returned to the embalmer.

History / Statistics

In addition to the amounts involved, all re-wrapping, unwrapping and slashing events are public, as well as the amounts involved, so it is easy for an Embalmer to see which Archaeologists have performed well in the past and make choices based on historical operations as well as current pricing / minimums.

Reputation matters, and it would require a total failure and loss of bond to shut down one Archaeologist server in order to spin up another.

Resurrection Grace Period

This is the amount of time that is given to the Archaeologist after the resurrection time to decrypt the outer layer of the sarcophagus. If they fail to perform the resurrection within this time frame for any reason, they will be slashed.

The resurrection grace period must be wide enough to account for network downtime, long confirmation times, and other uncontrollable issues. Currently the resurrection grace period is 240 blocks (~1 hour)

Digging Fees

Since a bounty can be changed at any time prior to the resurrection time and may never be paid to the Archaeologist, we must introduce an incentive mechanism for nominal infrastructure payments to the Archaeologist.

An Archaeologist will set minimum digging fees that they will accept during a curse; these fees are expressed as a function of the time-value of liquidity of the cursed amount of the bond. The best way to think about pricing digging fees would be to reference a fiat certificate of deposit yield curve.

Digging fees are calculated and paid up front by the Embalmer to the curse contract for the full length of time between the mummification and the resurrection. They are then distributed to the Archaeologist at the next re-wrapping or in the event of a resurrection.

By requiring Embalmers to pay digging fees up front for the full duration between the present and the resurrection time, we can guide Embalmers to think about re-wrapping time frames in human terms, and incentivize them to be more accurate. By paying the digging fees out to the Archaeologist after each re-wrapping or after the resurrection, we can allow Archaeologists to predict future income and plan accordingly.

An Archaeologist who has been cursed by an Embalmer for a given period of time knows that the digging fees will be paid to them at some point on or before the resurrection time (assuming good behavior).

Digging fees are meant to serve as nominal infrastructure payments to Archaeologists, not to be the primary motivation for operating an Archaeologist server. We expect digging fees to fall in line with the decentralized lending yield curve and we also expect Archaeologists to compete by using lower minimums when it comes to digging fees.

Considering this will be an open and permissionless application, digging fees do not have to stay minimal, an Archaeologist can choose to make their minimums as high as they want, and Embalmers can choose to pay in excess of minimums if they wish.

Bounties

A bounty is the treasure inside of the sarcophagus. It is only paid to the Archaeologist in the event of a successful resurrection, and only if that resurrection takes place after the resurrection time, but before the resurrection time + the resurrection grace period.

When an Embalmer chooses a(n) Archaeologist(s) they will be required to include a bounty that is greater than the minimum bounty set by the Archaeologist. This bounty can be increased or decreased at each re-wrapping, but must always stay higher than the minimum of the Archaeologist in order to retain financial slashing-based protections.

Bounties are meant to be the primary motivator of the Archaeologist. They are not guaranteed to be paid like digging fees, but are included in the calculation for bond cursing. A relatively high bounty is the best way for an Embalmer to incentivize an Archaeologist to behave rationally, and to unwrap the sarcophagus within the specified time frame.

Future Work

A few concepts need further exploration:

Intrinsic value of SARCO tokens

As the application matures and the sum of the network fees paid by the Archaeologists start to normalize into a curve, we should be able to calculate a ratio that is the multiple of the value the application and the floating values of the tokens being used within the application.

Additional Networks

Since the user is paying for services in SARCO ERC20 tokens, there is no reason that the Archaeologist cannot offer services running on entirely different networks.

As long as the networks have a capacity for proper smart contracting and data storage, it is possible to make sarcophagus work. Currently, the application is being built on Ethereum and Arweave, but future implementations could include the addition of Tezos and Filecoin.

App Explorer / Statistics

Statistics for Archaeologists are going to be incredibly important. Historical stats will help the embalmer choose which Archaeologist is the best for them. However, there are more influencing factors that could be more important than how they look on the surface. For example, historical change in digging fees. If an Archaeologist is changing (specifically raising) digging fees all the time, the Embalmer will be less likely to choose them over an archaeologist with more stable fees, everything else being equal.

Further research is needed concerning which Archaeologist statistics will be the most important to the Embalmer. This will further help inform the consumer facing UI.

Contact

https://sarcophagus.io

nospam@sarcophagus.io

70d1 c643 bb60 8217 6ec9 2b75 1cb6 5ad6 f69e 4fb8

https://t.me/sarcophagusio