erasureprotocol / **erasure-protocol** Public

<> Code ⊙ Issues 45 **Pull requests 39** ▷ Actions Projects Wiki Security Ins

<> Code ▾ Jump to bottom

v1.2.0 Escrows #253

Merged **thegostep** merged 59 commits into `master` from `steph/bay` on Nov 23, 2019

Conversation 33 Commits 59 Checks 0 Files changed 149

thegostep commented on Nov 5, 2019 • edited ▾ Contributor

Done

- ☑ get rid of agreement metadata
- ☑ events to distinguish each function
- ☑ check if better way to pass in agreementFactory
- ☑ check if possible to avoid agreementParams
- ☑ check if possible to have roles module
- ☑ create new deposit module to remove paymentAmount and stakeAmount (may need to be coupled with role)
- ☑ rename status functions at lower level to clarify etherscan ABI and inheritance
- ☑ check for current stake breaks if seller == buyer
- ☑ should agreement inherit operator from escrow?
- ☑ add state machine
- ☑ gas benchmarks
- ☑ use explicit return statements
- ☑ Spawner as Library ✓ **MultiHashWrapper and Spawner are more appropriate to be libraries** #281
- ☑ getPunishment ✓ 💣 **The function getPunishment is inaccurate** #276
- ☑ solc 0.5.13 ✓ **The latest version of Solidity should be used** #270

WIP

- ☑ add distinction between new and deprecated to releases
- ☑ complete natspec module commenting
- ☑ documentation on use of registries, factories and templates
- ☑ Contract descriptions ⊙ **Contract-level introductions are missing** #263
- ☑ Save state machines to github (https://github.com/erasureprotocol/erasure-protocol/blob/v1.2.0/docs/state-machines/CountdownGriefing.png)

Abandoned

- □ generalize escrow execution and move functionality to a module

erasureprotocol deleted a comment from **harsh103** on Nov 6, 2019

erasureprotocol deleted a comment from **harsh103** on Nov 6, 2019

thegostep added 6 commits 4 years ago

`Escrow WIP`	57e1c75
`add events`	2d061bb
`optimizations and natspec`	93c92e9
`fix tests`	7534005
`fix tests`	182a1ea
`fix typo`	cf9348c

thegostep force-pushed the `steph/bay` branch from **`785a4b7`** to **`cf9348c`** 4 years ago Compare

thegostep added 4 commits 4 years ago

`deploy rinkeby test`	98d6bc3
`initial tests and optimizations`	ede263e
`tests WIP`	c39a6c4
`tests WIP`	f4ebcc1

jparyani reviewed on Nov 9, 2019

View reviewed changes

`contracts/escrows/CountdownGriefingEscrow.sol` Outdated Show resolved

`contracts/escrows/CountdownGriefingEscrow.sol` Outdated Show resolved

`contracts/escrows/CountdownGriefingEscrow.sol` Show resolved

`contracts/escrows/CountdownGriefingEscrow.sol` Show resolved

`contracts/escrows/CountdownGriefingEscrow.sol` Show resolved contracts/escrows/CountdownGriefingEscrow.sol Outdated Show resolved

contracts/escrows/CountdownGriefingEscrow.sol Outdated Show resolved

contracts/escrows/CountdownGriefingEscrow.sol Outdated Show resolved

contracts/escrows/CountdownGriefingEscrow.sol Outdated Show resolved

contracts/escrows/CountdownGriefingEscrow.sol Show resolved

thegostep added 7 commits 4 years ago

complete happy tests	628855a
fix state machine bugs	50df9d5
add state machine diagram	b7027aa
refactor staking module	0d01fc5
fix typos	769d36c
fix countdown status visibility	d27d13a
add contract titles	bc8845c

thegostep requested a review from **jparyani** 4 years ago

jparyani reviewed on Nov 12, 2019

View reviewed changes

contracts/escrows/CountdownGriefingEscrow.sol Outdated Show resolved

jparyani reviewed on Nov 12, 2019

View reviewed changes

contracts/escrows/CountdownGriefingEscrow.sol Show resolved

thegostep added 6 commits 4 years ago

update rinkeby deployment	7856c56
fix finalize require	de34e9c
update metadata access control	77d1fd3

`remove unused imports`	`9297f74`
`update countdown griefing state machine`	`fd580fb`
`add state machines`	`2db2b51`

7 hidden items
Load more...

fulldecent suggested changes on Nov 19, 2019

View reviewed changes

fulldecent left a comment • edited

Contributor

2019-11-18 Erasure Bay Contract Review

Erasure Bay Contract Review
William Entriken
Delivered 2019-11-18

Review scope

This is a review of Erasure Protocol, pre-release version 1.2.0. Code as published at https://github.com/erasureprotocol/erasure-protocol, commit `4a3d98c` .

The scope of review included code-level review (human reading source code), automated code review, (compute reading source code), unit testing (computer running small-scope tests), and a limited amount of functional testing (human using compiled program).

The review was performed for the purpose of comparing Erasure Protocol to the advertised specifications (documentation) and understood use cases (product README, product introduction, architecture explanation, private application specification, private conversations with team). Any deviation from this standard, or deficiency against relevant best programming practices would be an in-scope review finding.

Review exclusions

The following code was excluded from review:

- `/contracts-wip` folder

Additionally, certain items were excluded from review:

- Suitability and security of cryptographic primitives (ECDSA, Fernet.js, etc.)
- Other library dependencies
- Downstream SDK modules

Findings

Each finding is listed as a bullet item and is organized by topic. Critical findings that are not resolved are marked with the bomb symbol (💣) and other unresolved material findings are marked with the warning symbol (⚠️). Resolved and less-than-material findings have no emoji marking.

Design

All findings are Just from reading the user documentation.

- Use of multihash adds complexity and the decision is not explicitly justified ✓ **Use of multihash adds complexity and the decision is not explicitly justified** #258

- Posts and feeds are not differentiated ✓ **Posts and feeds are not differentiated** #259

- 💣 Files should be encrypted offline and uploaded online https://docs.google.com/document/d/1XN4gXOA9VgkX7f80qwmlJDSm-iKWzAq-e5E4VeqCaFg/edit?disco=AAAADgDoZXA

- Documentation shows posts as “unlisted” which is not appropriate https://docs.google.com/document/d/1XN4gXOA9VgkX7f80qwmlJDSm-iKWzAq-e5E4VeqCaFg/edit?disco=AAAADgDoZXU

- Design specifications should use prescriptive language https://docs.google.com/document/d/1XN4gXOA9VgkX7f80qwmlJDSm-iKWzAq-e5E4VeqCaFg/edit?disco=AAAADgDoZXc

Documentation

- Griefing specification is unclear and/or incorrect ✓ **Griefing specification is unclear and/or incorrect** #260
- Erasure is not able to directly transact ETH or other ERC-20 tokens ✓ **Erasure is not able to directly transact ETH or other ERC-20 tokens** #261
- Is there one “protocol” or many? ✓ **Is there one “protocol” or many?** #262
- Contract-level introductions are missing ⊙ **Contract-level introductions are missing** #263
- 💣 Documentation identifies the wrong party as paying money ✓ 💣 **Documentation identifies the wrong party as paying money** #264
- A state diagram could be helpful https://docs.google.com/document/d/1XN4gXOA9VgkX7f80qwmlJDSm-iKWzAq-e5E4VeqCaFg/edit?disco=AAAADgDoZXs
- Documentation shows that information is available to only certain parties, but actually it is public https://docs.google.com/document/d/1XN4gXOA9VgkX7f80qwmlJDSm-iKWzAq-e5E4VeqCaFg/edit?disco=AAAADgDoZX8

Specifications

These are from reading just the developer documentation.

- proofHash is underspecified, in regards to prepending ⊙ **proofHash is underspecified** #265

- Some of the API surface is unnecessary and/or duplicative ✓ **Some of the API surface is unnecessary and/or duplicative** #266

Word choice

The choice of words is scrutinized here.

- Use of “counterparty” is confusing ⊙ **Use of “counterparty” is confusing** #267

Testing / assurance

These relate to included test cases.

- CountdownGriefingEscrow.js test fails ✓ **CountdownGriefingEscrow.js test fails** #268
- Build artifacts from testenv should be excluded from the repository ✓ **Build artifacts from testenv should be excluded from the repository** #269

Build

These relate to the build system, not necessarily code.

- The latest version of Solidity should be used ✓ **The latest version of Solidity should be used** #270
- Test scripts exit with success code when build fails ⊙ **Test scripts exit with success code when build fails** #271
- Solidity linter is missing from test suite ⊙ **Solidity linter is missing from test suite** #272
- Third-party code is not attributed ⊙ **Third-party code is not attributed** #273

Implementation

These are from reviewing the actual code and program output.

- Implementation of multihash is not future proof ✓ **Implementation of multihash is not future proof** #274
- Implementation of multihash does not adhere to its documentation ✓ **Implementation of multihash does not adhere to its documentation** #275
- 💣 The function getPunishment is inaccurate ✓ 💣 **The function getPunishment is inaccurate** #276
- onlyPayloadSize should not be necessary with Solidity 0.5 ⊙ **onlyPayloadSize should not be necessary with Solidity 0.5** #277
- Factory uses bytes4 to track instanceTypes, this is unjustifiably restrictive ⊙ **Factory uses bytes4 to track instanceTypes, this is unjustifiably restrictive** #278
- ⚠️ Inconsistent type usage: countdownLength, ratio ✓ ⚠️ **Inconsistent type usage: countdownLength, ratio** #279

Implementation — leaking storage

These are situations where the terminal state of a contract uses more storage than necessary.

- Enumeration status do not use zero for final state ✓ **Enumeration status do not use zero for final state** #280

Code style and quality

These are sniffs not directly related to implementation functionality.

- MultiHashWrapper and Spawner are more appropriate to be libraries **MultiHashWrapper and Spawner are more appropriate to be libraries** #281
- 💣 Griefing RatioType is not type safe, improper decoding 💣 **Griefing RatioType is not type safe, improper decoding** #282
- Purpose of Operated. _status is unclear **Purpose of Operated. _status is unclear** #283
- Operator module functions are WET **Operator module functions are WET** #284
- isCreator can be removed from API surface **isCreator can be removed from API surface** #285
- All test contracts should have Test in their name **All test contracts should have Test in their name** #286
- Functions with similar arguments should have similar argument order **Functions with similar arguments should have similar argument order** #287
- Same-contract variable is accessed using internal scoping **Same-contract variable is accessed using internal scoping** #288
- Separate all test code **Separate all test code** #289
- Uses of address types can be more specific **Uses of address types can be more specific** #290
- TODO is present in code **TODO is present in code** #291
- Variety of approaches is used for restricting actor for permission checking **Variety of approaches is used for restricting actor for permission checking** #292

Code documentation

These relate to communicating to other developers on the project.

- ⚠️ Mint / burn should be explained clearly ⚠️ **Mint / burn should be explained clearly** #293
- ⚠️ submitHash does NOT accept multihashes ⚠️ **submitHash does NOT accept multihashes** #294

Unused code

These are implementation details which have no effect on the product.

- contracts-wip should be deleted **contracts-wip should be deleted** #295
- Unused libraries are checked into the repository **Unused libraries are checked into the repository** #296

Quick fixes

These are all pull requests against the steph/bay branch.

- fix-remove-wip-contracts **Fix remove wip contracts** #297
- fix-whitespace **Fix doubled whitespace** #298
- fix-prescriptive-hashing **Be prescriptive in hashing introduction** #299

- fix-countdown-griefing-build Fix test for countdown griefing #300
- fix-erc-20-approve Clarify the meaning of "approve" for staking #301
- fix-wording Fix wording #302

Other notes

- I love the bracket blocks to scope out variable assignments (in `finalize()`). This is very c-like, very readable!

2 hidden items

Load more...

fulldecent and others added 23 commits 4 years ago

Be prescriptive in hashing introduction	3674009
Fix test for countdown griefing	98c6d2a
Clarify the meaning of "approve" for staking	bfc30f2
Spelling and wording updates	8062a46
clarify griefing docs fixes #260	1923453
clarify use of NMR in escrow fixes #261	ee33618
clarify single protocol fixes #262	889172b
update approval documentation fixes #264	491d057
remove unused contracts fixes #296	77504c1
remove TODO fixes #291	a99ff0f
deprecate Post fixes #259	8d2fbb7
use SHA-256 for proofhash fixes #258	0d59cb4
remove build artifacts fixes #269	1866d77
remove deployment from CI	1905758
fix testenv	d47e4f0
clarify burn behavior fixes #293	22f3d11
move MockNMR fixes #289	aa248c1
clean func reference fix #288 fix #285 fix #266	ef607af

`make consistent argument order fix #287`	8e72eac
`remove unused contract fix #286`	c9f4110
`simplify operated module fix #283`	63d3d68
`explicit ratioType fix #282`	3b4f97c
`fix travis build`	a62d801

jgeary reviewed on Nov 22, 2019

View reviewed changes

`contracts/modules/Countdown.sol` Show resolved

thegostep added 5 commits 4 years ago

`update solc to 0.5.13`	8ecfe27
`clarify getPunishment fix #276`	0f963d8
`update deployment script`	5326057
`host state machines on github`	929eeff
`update contract headers WIP`	7323709

thegostep merged commit **6a28933** into `master` on Nov 23, 2019

Revert

Reviewers

jparyani

jgeary

fulldecent

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants