

Dissecting Ponzi Schemes on Ethereum

Identification, Analysis, and Impact[1]

Liu Yihao

November 10, 2020

Outline

- 1 Introduction
- 2 Ponzi Schemes on Ethereum
 - Identification
 - Analysis
 - Impact
- 3 Conclusion

Definition

Ethereum[2] is a decentralized open source blockchain featuring [smart contract](#) functionality.

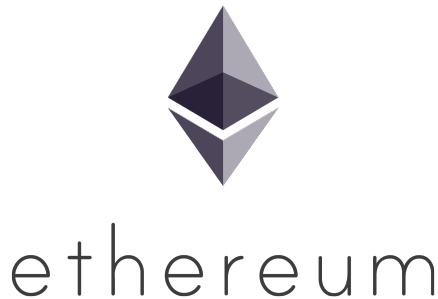


Figure 1: The logo of Ethereum.

Smart Contracts

Smart Contracts are often programmed in the language [Solidity](#)[3].

Smart Contracts

Smart Contracts are often programmed in the language [Solidity](#)[3].

```
1  contract AWallet {
2      address owner;
3      mapping (address => uint) public outflow;
4      mapping (address => uint) public inflow;
5
6      function AWallet() { owner = msg.sender; }
7
8      function pay(uint amount, address recipient) returns (bool) {
9          if (msg.sender != owner || msg.value != 0) throw;
10         if (amount > this.balance) return false;
11         outflow[recipient] += amount;
12         if (!recipient.send(amount)) throw;
13         return true;
14     }
15
16     function () { inflow[msg.sender] += msg.value; }
17 }
```

Ponzi Scheme

Definition ¹

A Ponzi scheme is an investment fraud that returns money to existing investors from funds contributed by new investors.

Ponzi scheme organizers often attract new investors by promising high returns with little or no risk.

Ponzi schemes require a constant flow of money from new investors to continue. Ponzi schemes inevitably collapse, most often when it becomes difficult to find new investors or when a large number of investors ask for their funds to be returned.

¹www.sec.gov/spotlight/enf-actions-ponzi

Smart Ponzi Scheme

Implementing Ponzi schemes as smart contracts would have several attractive features:

- The initiator of a Ponzi scheme could stay anonymous.
- Smart contracts are “unmodifiable” and “unstoppable”, no central authority can revert its effects in order to refund the victims.
- Investors may gain a false sense of trustworthiness from the fact that the code of smart contracts is public and immutable, and their execution is automatically enforced.

Outline

- 1 Introduction
- 2 Ponzi Schemes on Ethereum
 - Identification
 - Analysis
 - Impact
- 3 Conclusion

Identification of Ponzi Schemes

Contracts likely to be Ponzi Schemes:



Figure 2: Gambling games and lotteries.



Figure 3: Insurances and bonds.

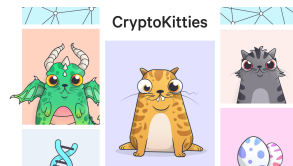


Figure 4: Blockchain games.

Criteria for Classifying a Contract as a Ponzi Scheme

Requirement 1

The contract distributes money to [investors](#).

- Most contracts studied satisfy this requirement
- Rules out some contracts such as cryptocurrency exchanges

Criteria for Classifying a Contract as a Ponzi Scheme

Requirement 1

The contract distributes money to **investors**.

Requirement 2

The money gathered by the contract comes from investors, **only**.

Rules out the cases where the money comes from external sources (eg. a bookmaker)

Criteria for Classifying a Contract as a Ponzi Scheme

Requirement 1

The contract distributes money to **investors**.

Requirement 2

The money gathered by the contract comes from investors, **only**.

Requirement 3

Each investor makes a profit, if **new investors** continue to send money to the contract.

Rules out the cases where an unlucky investor is not guaranteed to make any profit:

- Gambling games
- Betting
- Lotteries

Criteria for Classifying a Contract as a Ponzi Scheme

Requirement 1

The contract distributes money to **investors**.

Requirement 2

The money gathered by the contract comes from investors, **only**.

Requirement 3

Each investor makes a profit, if **new investors** continue to send money to the contract.

Requirement 4

The **risk of losing** ones investment grows with the time one joins the scheme.

Criteria for Classifying a Contract as a Ponzi Scheme

Requirement 4

The [risk of losing](#) ones investment grows with the time one joins the scheme.

Many Blockchain games are blamed to be [Ponzi schemes](#), but actually they only meet the requirements 1, 2, 3, and they can be called [pseudo-Ponzi schemes](#):

- CryptoKitties
- Fomo3D
- PoWH3D (Proof of Weak Hands 3D)

Outline

- 1 Introduction
- 2 Ponzi Schemes on Ethereum
 - Identification
 - Analysis
 - Impact
- 3 Conclusion

Category of Ponzi schemes

Ponzi schemes can be further classified by anatomy into several categories:

- Tree-shaped schemes
- Chain-shaped schemes
- Waterfall schemes
- Handover schemes

Category of Ponzi schemes

Tree-shaped schemes

Characteristic:

- Use a tree data structure to induce an ordering among users.
- Whenever a user joins the scheme, she must indicate another user as **inviter**, who becomes her parent node.
- If no inviter is indicated, the parent will be the root node (the owner)
- The money of the new user is split among her ancestors with the logic that the nearest ancestor is, the greater her share.

Some examples:

- Etheramid
- DynamicPyramid

Category of Ponzi schemes

Chain-shaped schemes

Characteristic:

- A special case of tree-shaped schemes, where each node of the tree has exactly one child.
- The ordering induced among users is linear.
- The scheme starts paying back users when its balance reaches a predefined value, one at a time, in order of arrival.
- Usually, the contract owner retains a fee from each investment.

Some examples:

- Doubler
- DianaEthereum
- ZeroPonzi

Category of Ponzi schemes

Waterfall schemes

Characteristic:

- Similar to chain shaped-schemes for the user ordering
- Each new investment is poured along the chain of investors, so that each can take their share.
- To ensure that all users receive payouts (requirement 3), the investments of new users must grow proportionally to the number of users.
- Usually, the contract owner retains a fee from each investment.

Some examples:

- TreasureChest
- PiggyBank2

Category of Ponzi schemes

Handover schemes

Characteristic:

- An instance of chain-shaped scheme.
- The entry toll is increased each time a new investor joins the scheme.
- The toll of a new investor is given in full to the previous one, the previous investor makes an instant profit.
- Usually, the contract owner retains a fee from each investment.

Some examples:

- KingOfTheEtherThrone

Outline

- 1 Introduction
- 2 Ponzi Schemes on Ethereum
 - Identification
 - Analysis
 - Impact
- 3 Conclusion

General Statistics of the Ponzi Schemes

Contract name	Transactions		ETH		Users	
	in	out	in	out	paying	paid
DynamicPyramid	444	143	7474	7437	175	51
DianaEthereum-x1.8	288	168	5307	5303	129	84
Doubler2	395	161	4858	4825	211	68
ZeroPonzi	627	499	4490	4489	47	28
Doubler	156	57	3073	3073	92	17
Government	723	846	2939	2939	40	27
Rubixi	686	66	1367	1363	104	28
ProtectTheCastle2	890	1257	1332	1332	101	68
EthereumPyramid	978	339	986	917	327	125
Total (184 schemes)	18925	9100	43881	43332	2378	1232

Table 1: Top-10 Ponzi schemes by amount of invested ether.

Statistics by Category of Ponzi Schemes

Category	Number	ETH		Users		%
		in	out	paying	paid	
Tree-shaped	4	410	400	161	83	51%
Chain-shaped	151	41514	40170	1967	968	48%
Waterfall	4	452	444	111	82	73%
Handover	4	486	483	97	63	64%
Other	21	1017	933	42	36	85%
Total	21	43881	43332	2378	1232	51%

Table 2: Statistics by category of scheme.

Lifetime of Ponzi Schemes

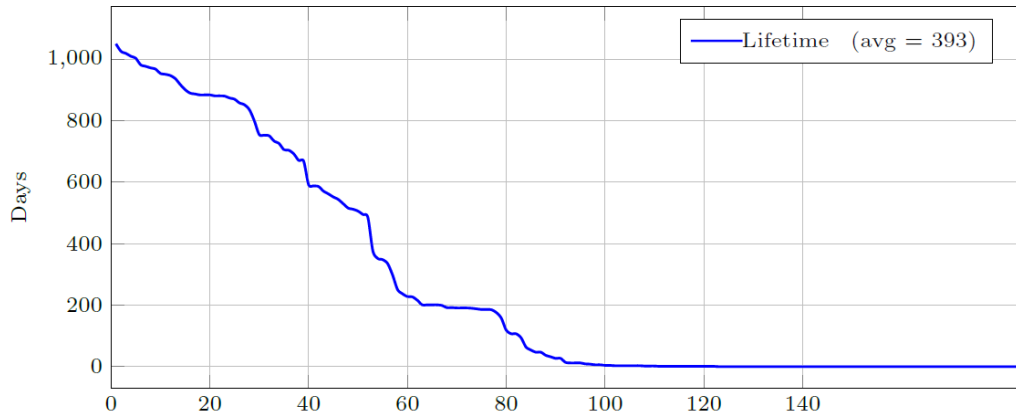


Figure 5: Lifetime of Ponzi schemes

Outline

- 1 Introduction
- 2 Ponzi Schemes on Ethereum
 - Identification
 - Analysis
 - Impact
- 3 Conclusion

Detect Ponzi Schemes

- Check the advertisements
- Analyze the contract code
- Analyze the transaction logs

Critical Thinking of Methodology Used

Similarities with other works in analyzing the Bitcoin network:

- Data Collection and Management
- Analyze based on categories
- Analyze based on evolution (time)
- Measure of the gains and losses of the users

Critical Thinking of Methodology Used




Similarities with other works in analyzing the Bitcoin network:

- Data Collection and Management
- Analyze based on categories
- Analyze based on evolution (time)
- Measure of the gains and losses of the users

Differences:

- Focus on source code of contrasts
- Measure of the economic impact of Ponzi schemes
- Measure of inequality of payments to and from the schemes

References

-  M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, “Dissecting ponzi schemes on ethereum: identification, analysis, and impact,” *Future Generation Computer Systems*, vol. 102, pp. 259–277, 2020.
-  G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
-  C. Dannen, *Introducing Ethereum and solidity*. Springer, 2017, vol. 1.

Thank you!