Shadow: A Decentralized Privacy Solution

Alex Schwarz
chimeratoken@gmail.com
https://chimeradigital.net

Abstract. Shadow (SHAD) is a decentralized peer-to-peer solution creating privacy on the Ethereum blockchain. While Ethereum aims to provide visible transactions (full transparency) in the form of Event Logs, Shadow runs on top of Ethereum while removing said transparency, thus Shadow could be considered "private Ether". All the proof-of-work concepts that Ethereum captures are present within Shadow, and you may refer to the Ethereum whitepaper for core functionalities regarding these topics.

1. Introduction

Individual privacy has become a hot-button issue for many in the world today. The collection and sale of data to governments and businesses has infringed upon our ability to browse or transact online with confidence. While the initial objective of distributed ledger technology, and cryptocurrency as a whole, has focused on immutable proofs and public transparency there are many consumers who would rather not leave a data trail behind their every move. Restrictions made by governments, mandating that real-world identities be associated with wallet address hashes, nullifies any prospect of privacy. A solution to this problem would be to privatize the information on the block chain, using kekkak256 Solidity-based contract encryption to encode the data stored in blocks. One can further this encryption by passing it between randomized wallets during peer-to-peer transactions, with the data of said transactions also being repeatedly hashed before being sent to the receiving end of a transaction. The information displayed on the blockchain would be privatized via the use of an ERC-20 token (SHAD), and further encryption would be offered in the form of a separate application known as *Scram!,* which would utilize multiple wallets to indirectly, and cryptically, generate an infinite number of repeated transactions between themselves.

2. Transactions

Transactions with ERC-20 compliant tokens follow a defined set of guidelines, with the three functions (approve, transfer, transferFrom) being the point of focus in Shadow's privacy factor. The listed functions can be seen below with their ERC-20 compliant requirements:

function approve(address _spender, uint256 _value) public returns (bool success)

Requirements: emit Approval(msg.sender, _spender, _value);

function transfer(address _to, uint256 _value) public returns (bool success)

Requirements: emit Transfer(msg.sender, _to, _value);

function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)

Requirements: emit Transfer(_from, _to, _value);

Shadow meets all the ERC-20 guidelines while masking the from, to, and value data. This can be achieved using the kekkak256 function included in the Solidity programming language. Data is hashed using the transaction block timestamp along with the sender's wallet address with some additional bitwise modifications. The smart contract includes a "spinning value" on each hashed transaction which cannot be viewed publicly, eliminating the potential of block timestamp vulnerabilities due to miners (Ref: Calculations). In addition to the token's smart contract privacy, Chimera Digital has built a web-service to make transactions exponentially more difficult to track using a token distribution network. A recursive algorithm powers the distribution network, allowing one transaction to be spread across a potentially infinite number of new transactions before reaching the destination wallet. As more users begin to take part in the distribution network, the difficulty of tracing transactions grows exponentially.

3. Incentive

The incentives of Ethereum privacy tokens are vast. Any party seeking to privatize transactions could utilize Shadow as an accepted payment method. In an age where an individual's personal data has become a practical black-market commodity, Shadow aims to provide transaction privacy and security, making it difficult for data to be viewed, purchased, or distributed amongst undesirable parties. Various bot networks and scripted algorithms have been

made to closely monitor the Ethereum blockchain, announcing unusual volume activity to otherwise unsuspecting parties. This generates attention toward consumers attempting to make larger transactions and puts them at much greater risk for being victims of cyber-crime. Alarms from botnets can also cause extreme price fluctuation, greatly adding to an already highly volatile cryptocurrency market. Shadow negates this fear by ensuring that bot networks cannot properly trace how much is being moved by a single party in a peer-to-peer transaction and making it virtually impossible for transactions to be traced at all.

4. Combining and Splitting Values

Chimera Digital offers a service called "*Scram!*", allowing token holders to obfuscate their transactions. Token amounts are given randomized divisible values, making the obfuscation process almost impossible to trace. We can look at an example where one user sends 1 SHAD to another: that 1 SHAD can be split based on the number of hops the user selects on the mixer. 1 SHAD can be split using 4 hops with the values of 0.25 SHAD on each transaction. If we were to use 3 hops, 1 SHAD could be split into 0.333. To counteract the potential of infinite trailing decimals, the mixer can adapt by splitting the value into 0.5 SHAD + 0.25 SHAD + 0.25 SHAD to equate 3 hops. Further complexity can be added to the mixer, such as releasing tokens after a randomized length of time.

5. Calculations

Let us first establish the difference between linear and exponential relationships. Transactions that do not use *Scram!* will follow a linear pattern, while sending transactions through the mixer will result in an exponential pattern. The following calculations are related to the time-complexity of an individual tracking down a certain transaction path:

LINEAR GROWTH

If a quantity starts at size P_0 and grows by d every time period, then the quantity after n time periods can be determined using either of these relations:

Recursive form

$$P_n = P_{n-1} + d$$

Explicit form

$$P_n = P_0 + d\,n$$

In this equation, d represents the **common difference** – the amount that the population changes each time n increases by 1.

Fig. 1.1: Recursive Computational Algorithm When compared in terms of time-periods vs. computational complexity.

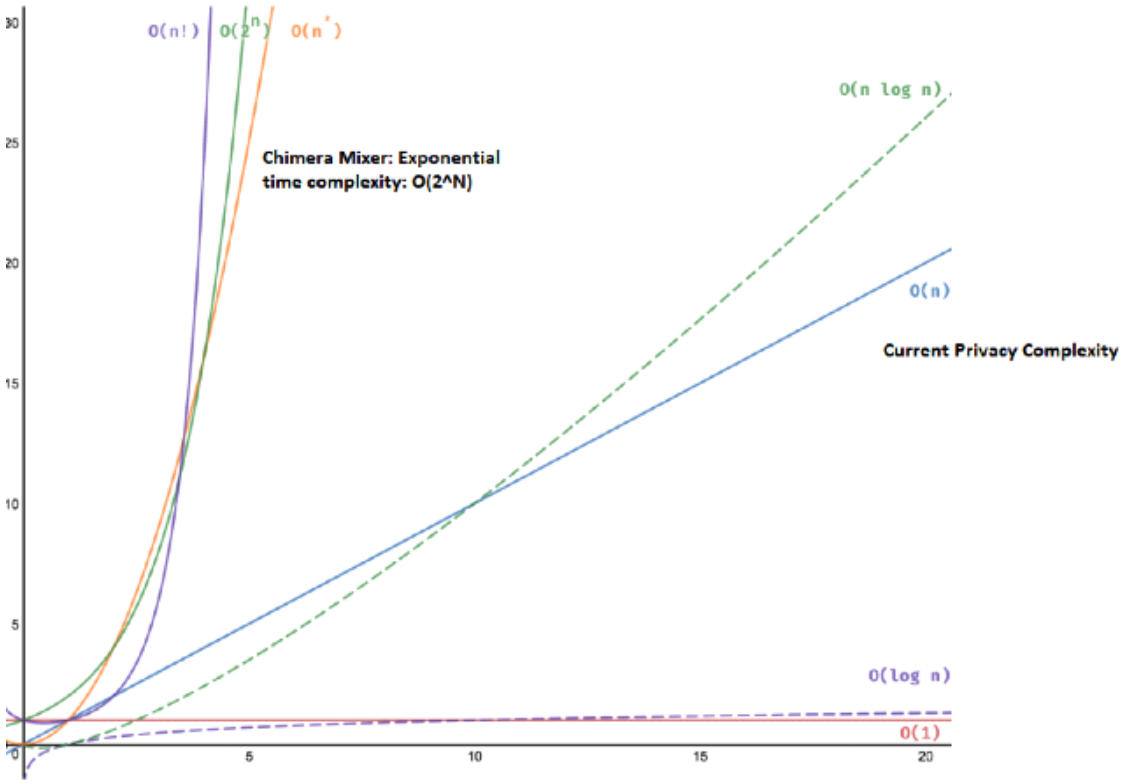

Fig. 1.2: Comparison Chart Time vs. Operation complexity in *Scram!* Vs. SHAD

Because *Scram!* uses a recursive function, it can achieve much greater computational complexity in shorter time frames when compared with regular peer-to-peer transactions made with the SHAD token. On top of

being faster than most other Ethereum transfer services, *Scram!* ensures high-grade encryption in very little time.

6. Security

Security of finance is imperative to the proper function of business. Sending and receiving payments can be very risky when done over the internet, as most times the encryption used to perform these tasks can be easily compromised. When measured against government metrics, most corporate-level encryption is mediocre at best. Inherently, using blockchain to transfer funds via electronic stores of value is much safer, and offers greater privacy when transferring funds. As previously stated, this is undermined by KYC regulation, which indirectly opens blockchain monetary transfers to the same phishing attacks used on the average online consumer. This becomes more of a risk when the intention of phishing is focused less on fraudulent behavior, but rather more on espionage and data collection from a third party.

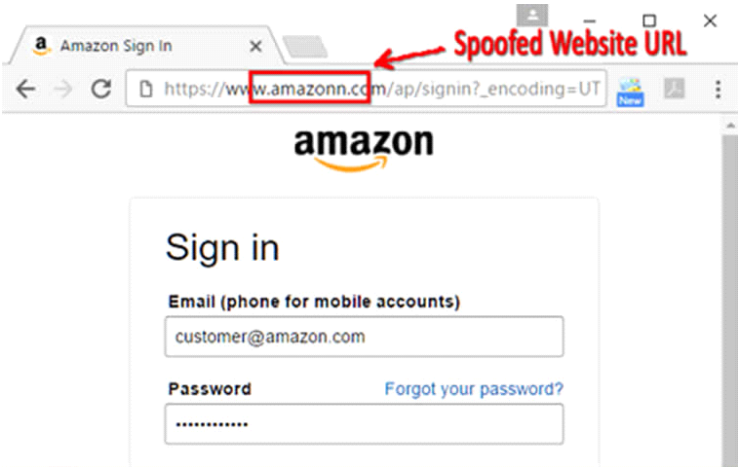

FIG. 2: Site Spoofing A popular form of phishing which can steal login credentials by using a dummy URL to pretend to be a legitimate website.

Inherently within any centralized system, the data collected when consumers perform tasks on the internet involving monetary transfers (such as banking or online shopping), is later packaged and sold. Often, people unknowingly agreeing to this unsavory practice. Data collection can even be achieved without any expressed warning or consent. As a store of value, SHAD can assure that data cannot be collected in this respect by completely voiding any possibility that highly personal data about patrons can be collected by vendors. In part, this is achieved by the simple encryption built into the

contract ledger of the token; and again, it can be further encrypted with the use of the Scram! Wallet Mixer.
When the associated contract data is scrambled, there is no real way to trace these transactions, even if a wallet is compromised via KYC regulation or phishing. In this regard, the security provided by using both SHAD and Scram! in tandem of each other is invaluably useful, with a wide array of everyday and novel applications for large corporations and consumers alike.

7. Conclusion

Chimera Digital's SHAD ERC-20 Token and Scram! Mixer application affords consumers the privacy they've hoped for, but could never ascertain. Used in tandem, these products ensure complete and total privacy in peer-to-peer transactions, and truly remove any middlemen or supervisory roles which may compromise the privacy of cryptocurrency. With endless applications, Chimera Digital hopes to see further growth in the form of community development by using the token as a store of value, or a safeguard key system in blockchain-based services. Chimera Digital hopes to establish itself as an industry-first, 'true privacy' protocol. Regarding long-term sustained growth, Chimera also hopes to create an entirely new blockchain, providing innovative and groundbreaking standards for cryptocurrency-related development in the near future.

References:

Figures 1.1, 1.2: https://courses.lumenlearning.com/wmopen-mathforliberalarts/chapter/introduction-linear-and-geometric-growth/

Figure 2: https://www.broadbandsearch.net/blog/popular-email-phishing-scams