Forsage: Anatomy of a Smart-Contract Pyramid Scheme

Tyler Kell[1,3] Haaroon Yousaf[2,3] Sarah Allen[1,3] Sarah Meiklejohn[1,3] Ari Juels[2,3]

[1]Cornell Tech [2] University College London [3] IC3

Abstract. Pyramid schemes are investment scams in which top-level participants in a hierarchical network recruit and profit from an expanding base of defrauded newer participants. They have existed for over a century, but their historical opacity has prevented in-depth studies.
This paper presents an empirical study of Forsage, a smart-contract-based pyramid scheme with unprecedented transparency. Our study focuses on the period around 2020, when Forsage was one of the largest contracts (by gas usage) in Ethereum. In 2022, some months after initial release of this work, the U.S. SEC dubbed Forsage a “fraudulent crypto pyramid and Ponzi scheme” and filed charges against its creators and promoters.
We quantify the (multi-million-dollar) gains of top-level participants as well as the losses of the vast majority (around 88%) of users. We analyze Forsage code both manually and using a purpose-built transaction simulator that we release as open source software to uncover the complex mechanics of the scheme. Through complementary study of promotional videos and social media, we show how Forsage promoters leveraged the unique features of smart contracts to lure users with false claims of trustworthiness and profitability, and how Forsage activity is concentrated within a small number of national communities.
Our analysis is the most complete study of a pyramid scheme to date.

1 Introduction

Cryptocurrencies and smart contracts are new and powerful technologies that promise a range of benefits, including faster monetary transactions, innovative financial instruments, and global financial inclusion for the world’s unbanked. Conversely, though, these same technologies have fueled new forms of fraud and theft [46,36] and new ways of perpetrating existing types of crime [23,31].

Pyramid schemes, for example, are a prevalent type of scam in which top-tier participants in a hierarchical network recruit and profit at the expense of an expanding base of new participants. They have existed for more than a century, but have recently emerged in a new form: as smart contracts on blockchains such as Ethereum.

Smart contracts are in some ways an ideal medium for pyramid schemes and other scams. Because they run in decentralized systems, they cannot easily be dismantled by law enforcement agencies. They can instantaneously ingest payments from victims across the globe. They provide privacy protection for their creators in the form of pseudonymous addresses. Finally, as so-called "trustless" applications—with world-readable (byte)code—they present a veneer of trustworthiness to unsuspecting users.

The flip side of such transparency is that smart contracts offer researchers a degree of visibility into the mechanics of online (and offline) scams that is without historical precedent. Not only is the (byte)code specifying the scam's mechanics visible on chain, but so is every transaction performed by every participant.

In this paper, we take advantage of this newfound visibility to conduct an in-depth measurement study of the largest smart contract-based pyramid scheme to date, called *Forsage Smartway* or *Forsage* for short.

Forsage came into existence in late January 2020. It was at one point the second most active contract in Ethereum by daily transaction count and spent almost 1/3 of the year—100 days—as one of the top five contracts by number of transactions per day. As we show throughout this paper, it is a classic pyramid scheme, defined by the SEC as "a type of fraud in which participants profit almost exclusively through recruiting other people to participate in the program" [2]. Indeed, in 2022, the SEC declared Forsage a "fraudulent crypto pyramid and Ponzi scheme" and filed charges against eleven individuals involved in the creation and promotion of the scheme [37].

The Forsage contract requires players to send currency (Ether) in order to participate. Funds sent by newly recruited users immediately pass through the contract to existing players, with those at the top of the (smart contract-defined) pyramid obtaining the largest returns.

Understanding the success of Forsage requires study of not just the contract itself, but also its community of hundreds of thousands of users, many of whom have actively discussed and marketed the scam. Consequently, to paint a detailed picture of how Forsage lures and defrauds users, our study combines measurement and analysis of a range of complementary forms of data, including source code, on-chain transaction data, and social media interactions.

Forsage was not just a blip: it was a major consumer of resources on Ethereum at its height, producing more transaction fees than even the most popular smart-contract-based cryptocurrency exchanges for 67 days. While the largest smart contract pyramid scheme identified to date, Forsage was not the only active pyramid scheme we identified on Ethereum and will not be the last. As a focused measurement study (see, e.g., [4,30] for important examples of such work), our work can act as a template for further, in-depth understanding of blockchain pyramid schemes more generally. New such schemes, as we explain, often closely resemble Forsage.

1.1 Main study results

We believe that our study's findings are not just relevant to Forsage, but provide durable insights into the conception, mechanics, and evolution of smart-contract scams and financial scams more generally. They also point to effective strategies that government authorities and the cryptocurrency community can use to combat pyramid schemes and other scams, as we discuss in Appendix C.

Our focus is on the peak period of activity for the contract, over the year 2020. (After that time, the contract saw little use, giving way to later, similar schemes.)

1.2 Summary of contributions

In summary, the main contributions of our study of Forsage in this paper are:

– *Contract measurement study:* In a measurement study of Forsage contract activity on Ethereum, we document the flow of 721k ETH (226M USD) and show monetary losses by the vast majority of users. One of our most striking findings is characteristic of pyramid schemes: The vast majority of Forsage players have lost money, with net losses for over 88% of players. A small few at the top of the pyramid have profited handsomely, e.g., the contract owner, who has received over 5000 ETH (1.2M USD). To the best of our knowledge, our study offers the first precise quantification of payouts and losses in any large pyramid scheme, internet-based or historical. We also quantify the cost of Forsage's complexity in terms of on-chain transaction fees, showing that Forsage transactions are more expensive for its users than normal transactions.

– *Community-dynamics study:* By tagging claims in promotional videos and studying social media interactions, we shed light on the evolution of the community, documenting tactics used to attract users and combine location data from various social networks to identify the user geographical distribution. We show that Forsage activity is internationally broad, but highly concentrated within a few geographies (e.g., western Africa).

– *Contract deconstruction:* Using a tool for transaction simulation that is of possible independent interest, we detail the operating rules of Forsage and show the concentration of power and wealth at the top of its defined pyramid(s).

We emphasize that our results, which reveal a combination of classic and smart contract-specific scam characteristics, offer insights not just into Forsage, but into both blockchain and non-blockchain scams more generally.

Section 3 provides an overview of the inner workings of Forsage. Section 4 analyzes measurement data and provides statistics of the usage and profitability of the Forsage smart contract. Section 5 uses social media analysis to find out the geographical distribution of Forsage victims. Further information can be found in the appendices: Appendix A provides detailed evaluation of the Forsage smart contract, including a custom-build simulator to visualize Forsage smart contract state. Appendix B analyzes Forsage promotional and social media content.

2 Background

Smart contracts: The most popular public (permissionless) blockchain for smart contracts today is *Ethereum* [9]. Ethereum smart contracts are launched in the form of bytecode that runs in a Turing-complete environment known as the Ethereum Virtual Machine (EVM). *Transactions* sent to smart contracts by users are processed by contract code and are publicly visible on chain.

Transactions may send money to a contract from user accounts or other contracts and must specify payment of execution fees to block creators in the form of *gas*, a parallel currency converted into ETH upon transaction execution. This conversion is calculated by multiplying the amount of work performed by a transaction (its "gas consumed") by the price of gas in ETH set by user when submitting the transaction [40].

Correctness of contract execution is enforced by the consensus mechanism underlying the Ethereum blockchain, so a miner's execution of contract code in the EVM must be agreed upon by all network participants to be included in a confirmed block.

Other permissionless blockchains with similarly constructed smart contract functionality are growing in popularity, e.g., Tron [12], to which Forsage has also been ported. Ethereum, however, remains the dominant smart contract platform.

Scams: Scams, i.e., fraudulent schemes involving financial deception, have been documented for centuries. Many scams involving large populations of victims assume the form of *pyramid schemes*. The U.S. Securities and Exchange Commission (SEC) defines a pyramid scheme as "a type of fraud in which participants profit almost exclusively through recruiting other people to participate in the program" [2]. Pyramid schemes, which are illegal in most jurisdictions, have many variants. One variant is a *Ponzi scheme*, which specifically involves investment in financial instruments. *Multi-level marketing* (MLM) schemes, which involve the sale of a product or service, are related to pyramid schemes. They are legal in the U.S., but outlawed in some jurisdictions (e.g., China) [1].

Blockchain scams: A multitude of scams have arisen within the blockchain ecosystem. Some scams have solicited investments from victims in new blockchain technologies. Examples include Onecoin, a Ponzi scheme that involved a fake (centralized) blockchain in which victims invested $19+ billion [19], Bitconnect, a token that promised returns of 1% per day and saw investment of $3.5 billion from victims, as well as other, related $1+ billion schemes such as Plustoken and WoToken.pro [28,7].

Other scams instead use blockchain technology to realize variants of scams, such as pyramid schemes, that were seen well before the advent of blockchains. Prominent examples are Million.Money[1] and Doubleway.io[2], which are both currently active, and the defunct Bullrun.live.[3] All three have similarities with Forsage: they use similar promotional materials, have a similar structure for the user dashboard, and use similar language and terminology (e.g., a referrer to the program is called an "upline"). We explore Forsage user interactions with multiple scam contracts in section 4.2.

[1] https://million.money

[2] https://doubleway.io/

[3] http://bullrun.live

3 Forsage Overview

The creators and promoters of Forsage advertise it as a *matrix* MLM scheme, despite the lack of a service or product. It operates primarily on Ethereum, where its initial Matrix contract has been active since January 31st, 2020. Since then, Forsage creators have also launched a Forsage contract on Tron (TRX), an additional, followup smart contracts called Forsage xGold on both Tron and Ethereum, and a Forsage Binance Smart Chain (BSC) contract.

The Forsage website: Users interact with Forsage using the forsage.io website, which shows how much they have paid into and earned from the contract. The website encourages the use of user-friendly cryptocurrency tools. It shows users how to purchase cryptocurrency using Trust Wallet, a user-friendly tool to exchange fiat for cryptocurrency, and how to use MetaMask, a browser extension that allows users to easily transact with cryptocurrency. The combination of these tools makes Forsage accessible to novice users who may not previously have used cryptocurrencies or smart contracts. Screenshots of the Forsage website prior to SEC takedown show the different matrices and their structure, can be found in Appendix D.

Forsage use and structure: A new Forsage user must pay a minimum of 0.05 ETH, which opens up the *slot* at the first *level* in the two matrix systems, called X3 and X4. Each matrix consists of 12 slots. To unlock the ability to use the next slot (at level $i + 1$), a user must pay twice as much ETH as for their currently highest slot (at level i). In both X3 and X4, the first slot costs 0.025 ETH, while the twelfth and final slot costs 51.2 ETH. This means that the total cost to open all slots in either matrix is 102.375 ETH. Figure 1 shows the correlation between profitability of participants and how many slots they unlocked.

Each Forsage user has a *referral code*, created at the time they register. The referral code links a recruited user's account to the account that recruited them, called their *upline*. These referral codes thus organize Forsage users into pyramids, with the oldest accounts at the top. Payments flow upwards within a pyramid as additional users join it. The pyramids of users linked by chains of referral code are referred to as Forsage *teams*. It is possible to join Forsage without entering a referral code; users who do so are assigned the referral code of the creator of Forsage.

Appendix A contains detailed description and simulation of the logic for payment flow of user funds sent through the Forsage contract. Briefly, users earn money in the X3 and X4 matrices as follows:

X3: In X3, users earn income by recruiting others into the system. A user must recruit three additional users to recoup their initial investment within each slot. Any recruits beyond the first three per slot will generate income for the recruiting user and those further up in their pyramid. Each subsequent slot costs more to open, but its resulting payout if filled with recruits will be higher because the expected payout for each three recruits is equal to the

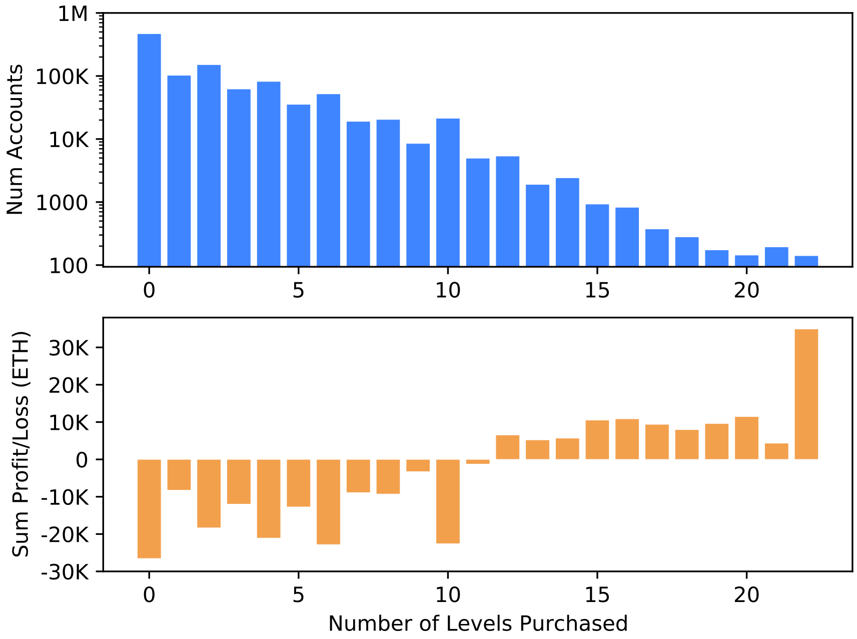


Fig. 1. The distribution of how many users had unlocked a given number of levels in the contract (on top, and at log scale), and the collective amount of money gained or lost by the users who had unlocked this number of levels (on bottom, and at linear scale). Users that bought the most levels were on average the most profitable.

initial cost to open the slot for the recruiter. After a user fills a slot (i.e. recruits 3 users into that slot), Forsage *blocks* the filled slot, causing the user to forfeit future earnings from it until it is unblocked. Unblocking means paying to open the slot at the next level up in the system, at which point this lower-level slot cannot become blocked again.

X4: In X4, users can earn both by recruiting other users and by being on an active team. When a user recruits the six additional users necessary to recoup their initial investment in an X4 slot (twice as many as are required in X3), that slot becomes blocked and the user will have received the same amount of money paid to open the slot, with others in their team getting paid as well. X4 also has an element of competition: If a newer user on a team is more active than the user whose referral code they used to join Forsage, that user can switch spots on the team, giving the more active, newer user the profits that would otherwise flow to the older, referring account [26].

4 Measurement Study

In this section, we present the results of our measurement study of Forsage contract transactions, which encompasses all monetary transactions in the scheme. A description of our data collection process is in Appendix A. We first present

Contract	Total TXs	Unique sending addresses	Total coins	Total USD	Launch date	Address
ETH Matrix	3M	1M	721k	225M	Jan 31, 2020	0x5a...
TRX Clone	217k	78k	537M	14M	July 25, 2020	TJRv...
TRX Matrix	1M	342k	1B	31M	Sept 6, 2020	TREb...
TRX xGold	307k	105k	90M	2M	Nov 7, 2020	TA6p...
ETH xGold	37k	17k	8k	9M	Jan 4, 2021	0x48...

Table 1. Summary statistics of the four official Forsage smart contracts and one clone. The USD value was calculated by taking a sum of the payments per day and multiplying it by the average of the 24-hour high and low on the respective day.

statistics capturing the degree of user interaction with the various Forsage contracts on Ethereum and Tron (Section 4.1). We then present an analysis of the account behaviour and profits over the Forsage user population (Section 4.2), in particular analyzing where funds are obtained and how funds flow through the five most profitable accounts.

4.1 Scheme statistics

Table 1 shows summary statistics for the four official Forsage contracts and an additional contract, TRX Clone, a clone of the Ethereum Matrix contract operating on Tron. This clone launched before the official TRX Matrix contract, and has a different domain[4] but with graphics and style akin to the official website. The official Forsage website added a warning after the clone's appearance, asking users to "beware of fake resources" and stating that the "forsage.io" website is the only official domain.

In total, the table shows that the official Forsage contracts amassed over 267M USD within the first year of operation. Among all of these contracts, the ETH Matrix contract brought in the most money and raised the highest amount on a single day: 3.7 million USD on August 1, 2020. The more recent xGold contracts (deployed on both Ethereum and Tron) were sent a combined 11.53 million USD in ETH and TRX in less than two months.

Figure 2 shows the number of transactions received by each contract over time. For each contract introduced after the original ETH Matrix one, we observe a large number of initial transactions followed by a substantial drop. We also see a decline in the number of transactions sent to the original ETH Matrix contract after other contracts become available. Given the particular longevity and popularity of the ETH Matrix contract, it is our main focus in the rest of this section.

To illustrate the popularity of Forsage, Figure 3 shows the number of daily transactions associated with the six most popular contracts across a six-month period in 2020. Of these contracts, Tether and USDC are stablecoins; Uniswap is a decentralized exchange; and Easy Club, MMBSC Global, and Forsage are

[4] forsagetron.io

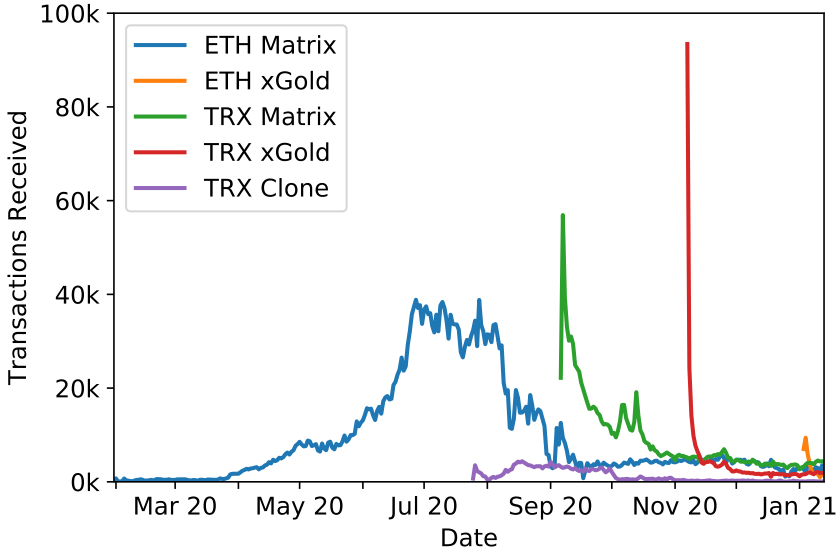


Fig. 2. Number of transactions sent from users to the four Forsage contracts across Ethereum and Tron and to an unofficial Tron-based clone.

believed to be scams/pyramid schemes. We can see that Tether is consistently the most popular contract and that for most of its peak from June to August, Forsage (as represented by ETH Matrix) had the second highest transaction rate among Ethereum smart contracts. This data is supported by Google Trends results for 2020: From April to August of 2020, Forsage had the highest search traffic globally of any of the smart contracts we studied, including both Tether and Uniswap, the two most heavily used smart contracts on the network as of the time of writing.

4.2 Account behavior and profitability

To understand how Forsage users obtained the funds needed to interact with the contract, we looked at the transactions that sent ETH to their accounts, and at when their accounts first became active. Figure 4 shows the ETH received by Forsage users over time and the cumulative count of active Forsage-related accounts (i.e., the first time an account was used that later interacted with the Forsage contract), with a vertical line indicating when Forsage was deployed. It is clear that these accounts became active and began to receive substantially more ether after the deployment of Forsage; in fact, 98.89% of Forsage users had accounts that did not exist (or at least did not transact) before Forsage. We found a similar increase when looking at the number of transactions conducted by these users as well: prior to the deployment of Forsage, 11k accounts were involved in 278k transactions, but after Forsage's release this increased to 1.04M users engaging in 16M transactions. While the curve in Figure 4 looks steep given the timescale, it in fact reflects a steady growth in the first appearance of accounts

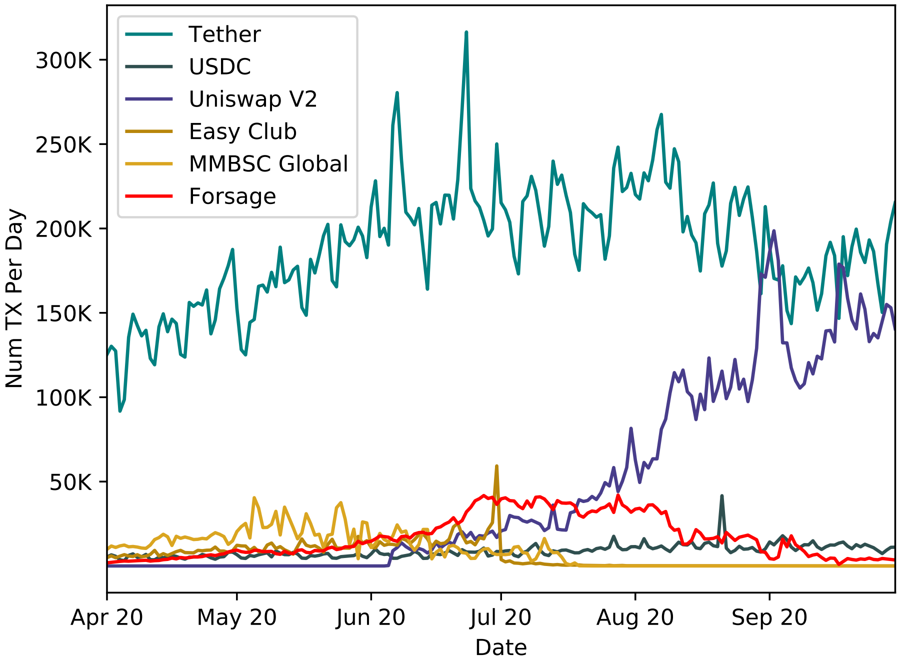


Fig. 3. The daily transaction count associated with the six most transacted contracts between April 1 and September 30, 2020. Here Forsage refers to the ETH Matrix contract.

between April and August 2020, which aligns with the peak of Forsage we saw in Figure 3. Each of these months saw thousands of new accounts appearing per day, on average: 1659 in April, 3653 in May, 8272 in June, 10,798 in July, and 4987 in August. In contrast there were at most 20 new accounts appearing per day for each month in 2019 (except December, when there were 68).

To identify which types of services were the source of this money, we used tags from Etherscan. Of the ETH sent to Forsage users, over 56% (1.5M) came from untagged sources, and only 15% came from known exchanges, with 5% of this coming from the decentralized exchange Uniswap. As mentioned in Section 3, Forsage promotional material recommends that users obtain ETH from TrustWallet. This is a non-custodial service, which means accounts are associated with individual users rather than with the exchange. Thus, if most users followed this advice, we would expect to see that most of the ETH came from untagged sources.

Figures 6 and 7 show a histogram of all of the accounts that interacted with the ETH Matrix contract organized by the amount of money either gained or lost by each account (including the amount spent on transaction fees) as of January 14, 2021. In total, of the 1.04 million Ethereum addresses that took part in the ETH Matrix scheme, only 11.8% (123,979) earned a profit. These profitable accounts made 265,618.52 ETH collectively, and the loss-making accounts (919,194 in total) lost 305,785.44 ETH collectively (0.33 ETH on average). We

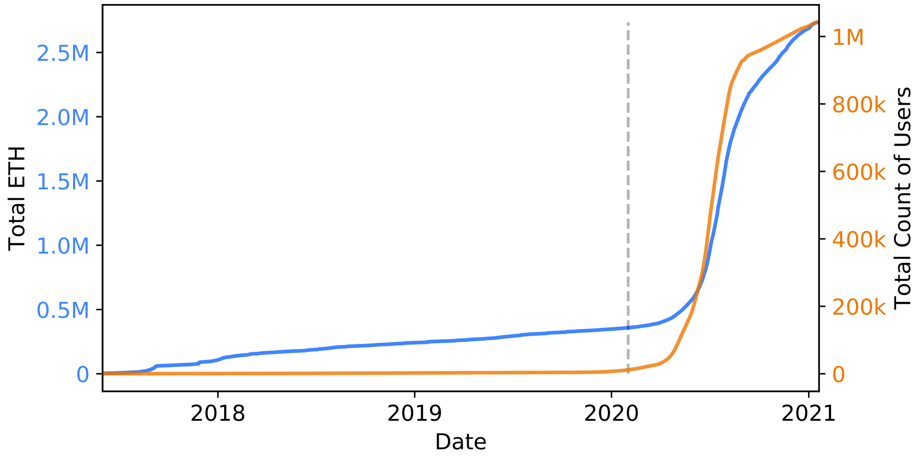


Fig. 4. Total ether received by Forsage users over time and total number of Forsage users according to when their accounts were first used, with a dashed line indicating the Forsage creation date.

revisit these profit-making accounts below. Users incur additional losses from the high transaction fees paid for transacting with the contract. This is demonstrated by the right-shifted peak in the Forsage curve relative to that of all ETH transactions in figure 5. The reasons for this are further explained in Appendix A.

Address	Profit (in ETH)	Notes/First Seen
0x81...	5409.6	Owner of the contract
0x44...	3445.0	March 22, 2020
0xde...	1954.9	March 22, 2020
0x4a...	1943.2	January 31, 2020
0x59...	1573.0	June 4, 2020

Table 2. Top five profitable accounts interacting with Forsage.

Profit-making accounts: The five addresses with the highest profits in Forsage can be found in Table 2. Perhaps unsurprisingly given our discussion in Section A, the most profitable Forsage user is the owner of the contract, who earned 5409.6 ETH, or 2.04% of the total profits. Collectively, the five most profitable users made 14,325.7 ETH, or 5.4% of profits, despite representing only 0.0004% of users. The top 1000 users made 50% of the total profits.

Examination of the five most profitable addresses shows that the most profitable address is another Ethereum contract created by the owner of the ETH Matrix contract. Of the money received by this contract, 99% came from ETH Matrix. The fourth highest earner sent 9% of received ETH directly back to Forsage. In fact, if we follow all the addresses to which this user sent money, we see over 1321 ETH sent back to Forsage eventually. Similarly, the fifth highest earner sent 204 ETH directly back to Forsage.

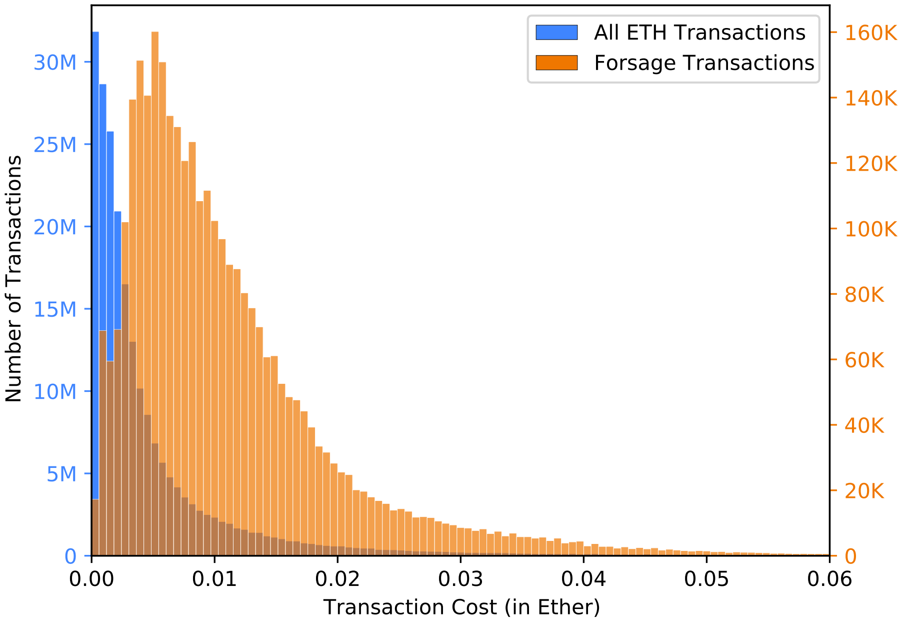


Fig. 5. Histogram of transaction costs on the Ethereum blockchain—from January 31, 2020 to January 14, 2021—that involve successful smart contract function calls. Blue bars indicate the number of all transactions that paid fees within the given bucket. Orange bars indicate the same data, but only for transactions sent to the Forsage smart contract. The data excludes outlier transactions with fees above 0.06 ETH, which is above the 99th percentile of all transactions from this time period.

Some of the top addresses interact directly with other known scams, such as Beurax.com and TorqueBot.net, meaning they sent or received coins directly from addresses associated with these scams. The top five profit-making accounts received 6.987 ETH from these scams.

Interestingly, the first transaction sent to the address that deployed Forsage was from 0xb1..., which is the Ethereum address that deployed Million.money. This suggests interaction between smart contract-based scam operators.

Finally, we consider the extent to which users who profited by interacting with the Forsage ETH Matrix contract also interacted with other Forsage contracts. The ETH xGold contract has 17,560 users, of which 17,129 (97.5%) also interacted with ETH Matrix. Furthermore, the highest earner in xGold was the third highest earner in Matrix, the fourth highest xGold earner was the seventh highest earner in Matrix, and the eighth highest earner in xGold was the second highest earner in Matrix. These three earners (all of which are within the ten wealthiest Matrix users) hold 21.85% of net profits in xGold. This suggests that at least some prominent users of Matrix did indeed migrate over to xGold.

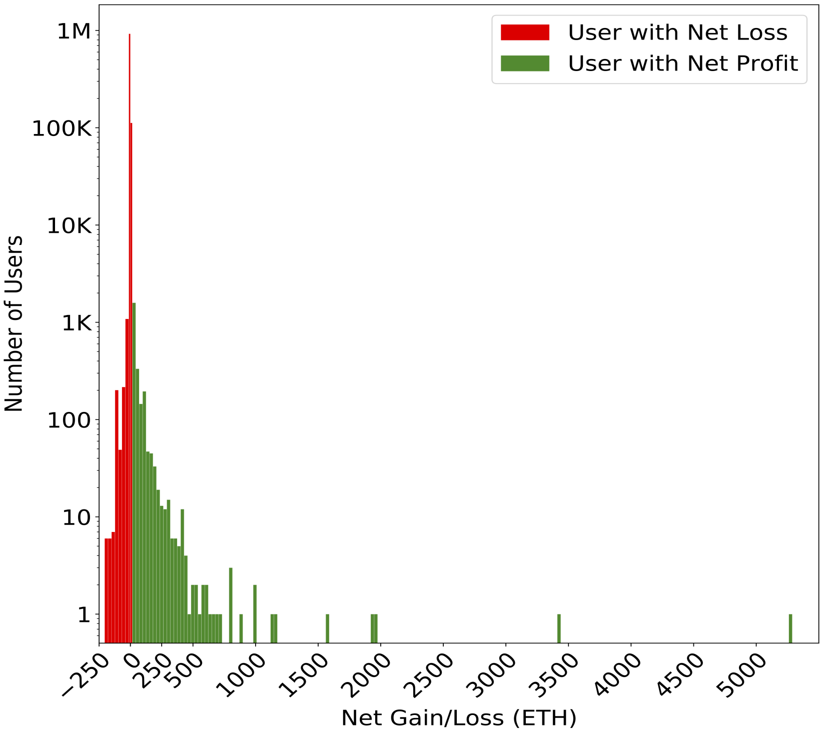


Fig. 6. Profit/loss histogram of Ethereum accounts that interacted with the Forsage smart contract, on a log scale. This graph shows the number of accounts that made a profit or loss for each range of ETH. The majority of accounts incurred a small net loss, less than 1 ETH.

5 Study of Forsage Community

Methodology: We studied the Forsage community by examining the presence of Forsage on social media. The Forsage website promotes official social media presences on Facebook, Instagram, Telegram, Twitter, and YouTube. All of these services have official APIs to collect data, but some of the research we conducted required manual interaction with the various social websites via a web browser, or more sophisticated data collection techniques like web scraping.

In summary we identified over 403,029 distinct Facebook members in various Forsage Facebook groups, 285,788 people signed across 49 telegram channels and over 57,551 Youtube promotional videos. This is explained in more detail in Appendix B.

5.1 Forsage user geography

Since transactions on the Ethereum network do not carry any inherent geographic metadata, we turned to social media analysis in order to gain a sense of the geographic placement of people interested in Forsage. In the data we collected

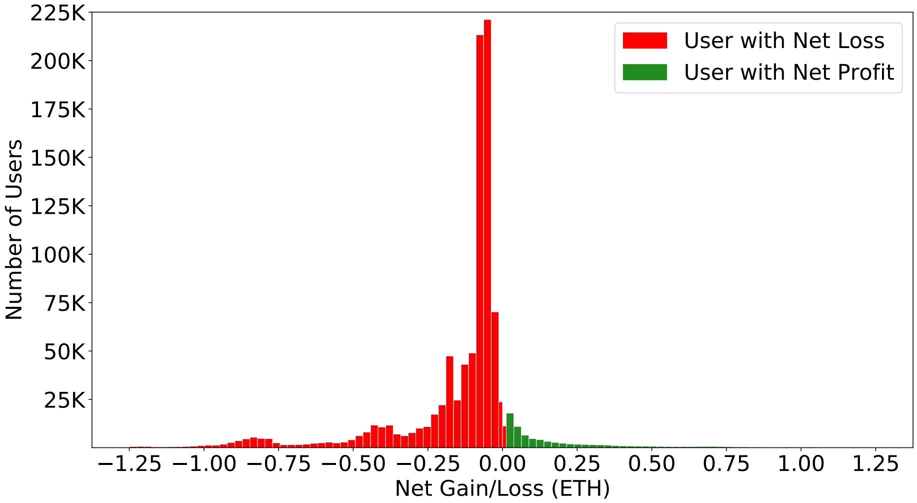


Fig. 7. Profit/loss histogram of Ethereum accounts that interacted with the Forsage smart contract, centered around 0 and on a linear scale. The vast majority of user accounts that interacted with Forsage lost between 0 and 0.25 ETH, with the peak occurring between 0.038 and 0.063 ETH.

on members of Forsage-related Facebook groups, we found 771 users that publicly listed a country location on their Facebook profile. We also found 10,200 unique Twitter accounts that publicly posted their geographic location. YouTube does not expose information about geographic location of the consumers of YouTube videos, but YouTube channels that produce videos can choose to include country location in their channel profile. We summarize this data for the five countries with the highest number of active users in Table 6. Despite having a substantial population and being the nationality of the founders of Forsage, Russia was not a large source of Twitter or Facebook content, although the country did produce a large number of YouTube videos and content about Forsage.

The high number of Forsage users in the Philippines may explain why the Philippines SEC was first to take action to raise awareness about the malicious intent behind Forsage [25,24]. Likewise, Nigeria has high penetration rates for both cryptocurrency and Forsage, and has recently banned cryptocurrency payments from its banking sector [3]. While each of these five countries had high Forsage activity in absolute terms, they also have large populations. We thus normalized our Facebook and Twitter data relative to the specific populations on each service for each country (i.e., the number of people per country divided by a public estimate of the number of Facebook and Twitter users in that country) to get a sense of the number of Facebook and Twitter users, per 100,000 users, that interacted on each platform with the Forsage topic. Statistics for the number of Facebook and Twitter users per country came from Miniwatts Marketing Group, WeAreSocial, and Hootsuite [13,16]. We did not include the YouTube data because the sample size was too small. We gave equal weight to the numbers for Facebook and Twitter to produce the heat map in Figure 8.

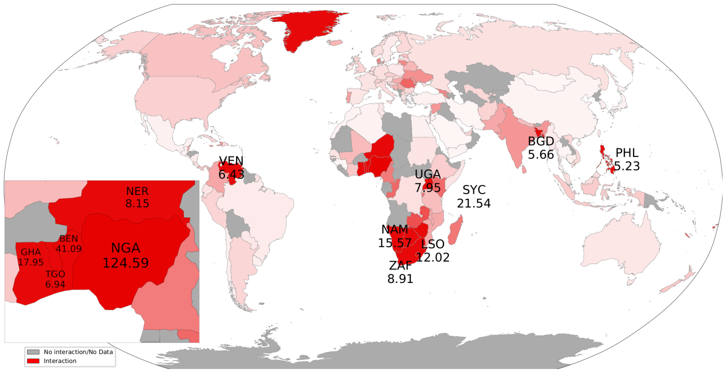


Fig. 8. Forsage social media interaction heat map by country. Country labels indicate the ISO-alpha-3 name of the country and the number of Forsage users per 100k people in that country. The data reflects the public location of members in a popular Forsage Facebook group and Twitter users that tweeted about Forsage. Countries depicted in gray had no Forsage interaction. The intensity of color from white to red is scaled linearly from the 0th percentile of data to the 90th percentile, and everything above 90% of the data is colored the same shade of dark red. This slightly understates the relative depth of penetration in outlier countries like Nigeria.

Our normalized data showed that Forsage is most popular in Nigeria and the African continent, the Philippines, and Venezuela. Greenland, the Seychelles, and some Caribbean islands may be outliers due to small population sizes. Google Trends traffic and geographic data agree with our conclusions: Google Trends shows the greatest amount of population-adjusted search traffic in Nigeria and surrounding West African countries, and shows a peak in user search interest in July 2020, which is when we observed a similar peak in transactions involved Forsage in Figure 2.

Familiarity with cryptocurrency does not appear to have any correlation with interest in Forsage: The 2021 Statista Global Consumer Survey [8] lists the top countries globally with the reported highest number of cryptocurrency users. Vietnam (#2) and China (#3) both had relatively high levels of cryptocurrency use, but low levels of interest in Forsage. Similarly, familiarity with cryptocurrency does not appear to prevent people from falling for the Forsage scam, as in the case of Nigeria and the Philippines (#1 and #3 globally for cryptocurrency usage). Nigeria may be a special case, as Statista found that almost a third of Nigerians said they used cryptocurrency, far beyond most countries. It is also an outlier in the data for interest in Forsage.

6 Related Work

Previous measurement studies of particular attack instances have been critical to the community's understanding of adversarial behaviour. Examples include Antonakakis et al.'s analysis of the Mirai botnet [4] and Pearce et al.'s characterisation of the ZeroAccess click-fraud botnet [30]. Case studies of other topics, including [45,18,22], have also been impactful to the security community.

Past research has examined scams running on Ethereum and Bitcoin. For Ethereum-based scams, Chen et al. [10] used data mining and machine learning to detect Ponzi schemes while Yu et al. [44]modeled Ponzi scheme identification and detection as a node classification task. Bartoletti et al. [6] compared the code and promotion of Ethereum Ponzi schemes, finding that scammers use the public nature of Ethereum to inspire confidence in their victims. Vasek et al. [39] and Bartoletti et al. [5] both worked to detect and model Bitcoin-based scams. These included Ponzi schemes that collect Bitcoin from victims, the former finding that most scams last less than one week. Paquet-Clouston et al. [29] and Xia et al. [41] studied specialized scams that leverage Bitcoin payments, namely threats of revealing intimate data and fake fundraising for COVID-19 research and relief.

Apart from our work, studies of existing scams' migration onto blockchains include [42,15,17], which examine chat-service based pump-and-dump schemes on cryptocurrencies. Some scams are new to blockchains, such as honeypot smart contracts, which include financial traps within the contract itself [36].

In past work characterizing the victims of blockchain-enabled scams, Phillips et al. [32] showed that victims tend to send funds from fiat-accepting cryptocurrency exchanges, making the scams accessible to novice cryptocurrency users. They also found that scammers often create multiple similar scams running in parallel. Yousaf et al. showed that scammers use shifting services to convert Ether into other coins to thwart tracking by law enforcement [43].

7 Conclusion

We presented an in-depth measurement study of Forsage, at one time the second most actively used contract in Ethereum. Our study required multiple data-gathering approaches and the creation of new open source tools to analyze the Forsage contract. These tools enabled us to provide detailed insights into the mechanism design, transaction costs, and other features of Forsage.

A key finding is that the vast majority of Forsage accounts—over 88%—incurred losses, for a combined total loss of 305,785 ETH. The contract owner and a few other accounts at the top of the pyramid earned over 5000 ETH (well over 1M USD). Social media analysis led us to discover the existence of geographically distinct communities, with scammers based mainly in Russia and victims mainly in Nigeria, the Philippines, Venezuela, Indonesia, and India.

Public warnings about Forsage by entities such as the Philippines SEC appeared to have little effect, as the creators continued to launch new lucrative variants, some on blockchains other than Ethereum. On August 1, 2022, some months after the initial release of our work, the SEC charged eleven members of Forsage including the founder [34] for operating a pyramid scheme. Since then, the website has been partially blocked. At present, it is inaccessible in some countries, such as the United States and United Kingdom, but still accessible in others, such as Switzerland.

Acknowledgements. This work was funded by NSF grants CNS-2112751 and CNS-1933655 as well as generous support from IC3 industry partners.

References

1. MLM law of China: 'Prohibition of Chuanxiao'. http://www.gov.cn/zwgk/2005-09/03/content_28808.htm, 2005.
2. Investor alerts and bulletins:beware of pyramid schemes posing as multi-level marketing programs. https://www.sec.gov/oiea/investor-alerts-bulletins/investor-alerts-ia_pyramidhtm.html, Oct 2013.
3. Hannah Akuiyibo. Nigeria's crypto ban fuels mistrust in government. *Coindesk*.
4. Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In *26th {USENIX} security symposium ({USENIX} Security 17)*, pages 1093–1110, 2017.
5. M. Bartoletti, B. Pes, and S. Serusi. Data mining for detecting bitcoin ponzi schemes. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 75–84, 2018.
6. Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, and Roberto Saia. Dissecting ponzi schemes on ethereum: Identification, analysis, and impact. *Future Generation Computer Systems*, 102:259 – 277, 2020.
7. Nick Bel. The most famous financial pyramids in the crypto world. https://cointelegraph.com/news/the-most-famous-financial-pyramids-in-the-crypto-world, Jul 2020.
8. Katharina Buchholz. How common is crypto? https://www.statista.com/chart/18345/crypto-currency-adoption/, 2021. Online; accessed 21 March 2021.
9. Vitalik Buterin and Vitalik Buterin. A next-generation smart contract and decentralized application platform. ethereum white paper. 2014.
10. Weili Chen, Zibin Zheng, Jiahui Cui, Edith Ngai, Peilin Zheng, and Yuren Zhou. Detecting ponzi schemes on ethereum. *Proceedings of the 2018 World Wide Web Conference on World Wide Web - WWW 18*, 2018.
11. John Ellson, Emden Gansner, Lefteris Koutsofios, Stephen North, Gordon Woodhull, Short Description, and Lucent Technologies. Graphviz — open source graph drawing tools. In *Lecture Notes in Computer Science*, pages 483–484. Springer-Verlag, 2001.
12. Tron Foundation. Tron: Advanced decentralized blockchain platform. whitepaper version: 2.0. 2018.
13. Miniwatts Marketing Group. Internet world stats: Usage and population statistics. https://www.internetworldstats.com/, 2021.
14. Samuel Haig. Plustoken scammer implicated in china's second ten-figure crypto ponzi. https://cointelegraph.com/news/plustoken-scammer-implicated-in-chinas-second-ten-figure-crypto-ponzi, May 2020.
15. JT Hamrick, Farhang Rouhi, Arghya Mukherjee, Amir Feder, Neil Gandal, Tyler Moore, and Marie Vasek. The economics of cryptocurrency pump and dump schemes. *SSRN Electronic Journal*, 01 2018.
16. Hootsuite and WeAreSocial. Digital in 2021: National reports. https://datareportal.com/library, 2021.
17. Josh Kamps and Bennett Kleinberg. To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science*, 7, 11 2018.
18. Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav

Shacham, and Stefan Savage. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*, pages 447–462, 2010.

19. António Madeira. Onecoin: A deep dive into crypto's most notorious ponzi scheme. https://cointelegraph.com/news/onecoin-a-deep-dive-into-crypto-s-most-notorious-ponzi-scheme, Sep 2020.
20. Damon McCoy, Andreas Pitsillidis, Jordan Grant, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey Voelker, Stefan Savage, and Kirill Levchenko. Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs. In *21st USENIX Security Symposium (USENIX Security 12)*, pages 1–16, Bellevue, WA, August 2012. USENIX Association.
21. Malte Möser and Arvind Narayanan. Effective cryptocurrency regulation through blacklisting. *Preprint*, 2019.
22. Keaton Mowery, Eric Wustrow, Tom Wypych, Corey Singleton, Chris Comfort, Eric Rescorla, J. Alex Halderman, Hovav Shacham, and Stephen Checkoway. Security analysis of a full-body scanner. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 369–384, San Diego, CA, August 2014. USENIX Association.
23. US Department of Justice Office of Public Affairs. Three north korean military hackers indicted in wide-ranging scheme to commit cyberattacks and financial crimes across the globe. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and, 2021.
24. Republic of the Philippines Securities and Exchange Commission. Forsage. https://www.sec.gov.ph/advisories-2020/forsage/, June 2020.
25. Republic of the Philippines Securities and Exchange Commission. Sec warns against forsage, other schemes. https://www.sec.gov.ph/pr-2020/sec-warns-against-forsage-other-schemes/, July 2020.
26. FORSAGE Official. Forsage overview: Earn ethereum daily! https://www.youtube.com/watch?v=m0NzYwFfGH4, 5 2020.
27. FORSAGE Official. Forsage.io - big special event. https://www.youtube.com/watch?v=NMfcDSCXLK8, 8 2020.
28. Daniel Palmer. Chinese authorities have seized a massive $4b in crypto from plustoken scam. https://www.coindesk.com/chinese-authorities-have-seized-a-massive-4-billion-in-crypto-from-plustoken-scam, Nov 2020.
29. Masarah Paquet-Clouston, Matteo Romiti, Bernhard Haslhofer, and Thomas Charvat. Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, AFT '19, page 76–88, New York, NY, USA, 2019. Association for Computing Machinery.
30. Paul Pearce, Vacha Dave, Chris Grier, Kirill Levchenko, Saikat Guha, Damon McCoy, Vern Paxson, Stefan Savage, and Geoffrey M Voelker. Characterizing large-scale click fraud in zeroaccess. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 141–152, 2014.
31. R. Phillips and H. Wilder. Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites, 2020.
32. Ross Phillips and Heidi Wilder. Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites. *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020.
33. Mohsen Sayyadiharikandeh, Onur Varol, Kai-Cheng Yang, Alessandro Flammini, and Filippo Menczer. Detection of novel social bots by ensembles of specialized

classifiers. *Proceedings of the 29th ACM International Conference on Information & Knowledge Management*, Oct 2020.
34. United States Securities and Exchanges Commission. Sec charges eleven individuals in $300 million crypto pyramid scheme.
35. United States Securities and Exchanges Commission. Sec charges eleven individuals in $300 million crypto pyramid scheme. https://www.sec.gov/news/press-release/2022-134, 2022.
36. Christof Ferreira Torres, Mathis Steichen, and Radu State. The art of the scam: Demystifying honeypots in ethereum smart contracts. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1591–1607, Santa Clara, CA, August 2019. USENIX Association.
37. U.S. Securities and Exchange Commission (SEC). SEC charges eleven individuals in $300 million crypto pyramid scheme. SEC Press Release; https://www.sec.gov/news/press-release/2022-134, 1 Aug. 2022.
38. Onur Varol, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, and Alessandro Flammini. Online human-bot interactions: Detection, estimation, and characterization, 2017.
39. Marie Vasek and T. Moore. There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams. In *Financial Cryptography*, 2015.
40. Gavin Wood. Ethereum: A secure decentralized generalized transaction ledger. 12 2020.
41. Pengcheng Xia, Haoyu Wang, Xiapu Luo, Lei Wu, Yajin Zhou, Guangdong Bai, Guoai Xu, Gang Huang, and Xuanzhe Liu. Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams, 2020.
42. Jiahua Xu and Benjamin Livshits. The anatomy of a cryptocurrency pump-and-dump scheme. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1609–1625, Santa Clara, CA, August 2019. USENIX Association.
43. Haaroon Yousaf, George Kappos, and Sarah Meiklejohn. Tracing transactions across cryptocurrency ledgers. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 837–850, Santa Clara, CA, August 2019. USENIX Association.
44. Shanqing Yu, Jie Jin, Yunyi Xie, Jie Shen, and Qi Xuan. Ponzi scheme detection in ethereumtransaction network, 2021.
45. Leah Zhang-Kennedy, Hala Assal, Jessica Rocheleau, Reham Mohamed, Khadija Baig, and Sonia Chiasson. The aftermath of a crypto-ransomware attack at a large academic institution. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1061–1078, Baltimore, MD, August 2018. USENIX Association.
46. Xiangfu Zhao, Zhongyu Chen, Xin Chen, Yanxia Wang, and Changbing Tang. The dao attack paradoxes in propositional logic. pages 1743–1746, 11 2017.

A Forsage Contract Deconstruction

Forsage promotional materials imply that the system is trustworthy because its code is open-source, e.g., the promotional materials claim that the contract “guarantees the purity of conditions.” We took advantage of the availability of the source code to conduct an in-depth analysis of the smart contract’s logic and data structures.

Methodology and data collection: The code for the Matrix smart contract is published on Etherscan.[5] We first attempted manual source code review, but found the logic too confusing to follow without visualization. We then built a simulator in Python that deployed the contract to a local private test network of Go-Ethereum (Geth) nodes,[6] and used Web3.py[7] to send sample transactions. We also wrote a visualizer for the contract’s state machine using GraphViz [11]. The output of that visualizer assisted in creating Figure 9, which depicts the data stored in the contract. Although the open source code is pointed to as a source of legitimacy by Forsage promotional materials, our analysis of the contract took weeks of focused effort by a professional research engineer. Our source code for the visualizer and simulator tools is released as open source software[8].

When the Forsage team launched their Tron implementation of the Matrix smart contract, they also released its source code. We found this Tron code to be nearly identical to the Ethereum original, so we did not specifically analyze it. The more recently released Forsage xGold contract has no publicly available source code.

The Ethereum and Tron blockchains include the data for all transactions performed by Forsage users. We mined this publicly available data to perform further analysis. To obtain Ethereum data we ran the Go-Ethereum (Geth)[9] and TurboGeth[10] full-node and archive-node software packages, and downloaded the entire blockchain up to January 14, 2021.

We then used the Ethereum-ETL[11] package to retrieve this data from Geth and store the 345 million transactions included in the Ethereum blockchain between the launch of Forsage (January 31, 2020) and January 14, 2021. We wrote custom Python scripts to analyze this data and found 222,516,680 transactions that involved function calls on smart contracts, of which 3,266,722 were to the Forsage smart contract. To profile user transactions outside Forsage, we used the Chainalysis Reactor tool.[12] Chainalysis Reactor is a web-based investigation platform that connects cryptocurrency transactions to real-world entities, using

[5] etherscan.io/address/0x5acc84a3e955Bdd76467d3348077d003f00fFB97

[6] https://github.com/ethereum/go-ethereum

[7] https://github.com/ethereum/web3.py

[8] https://github.com/anonnotamouse/forsage-anon

[9] https://github.com/ethereum/go-ethereum

[10] https://github.com/ledgerwatch/turbo-geth

[11] https://github.com/blockchain-etl/ethereum-etl

[12] https://www.chainalysis.com/chainalysis-reactor/

tags that are either internal to Chainalysis or gathered from public websites and documents.

To collect Tron transaction data we scraped the TronScan API[13] and parsed the results directly into CSV form.

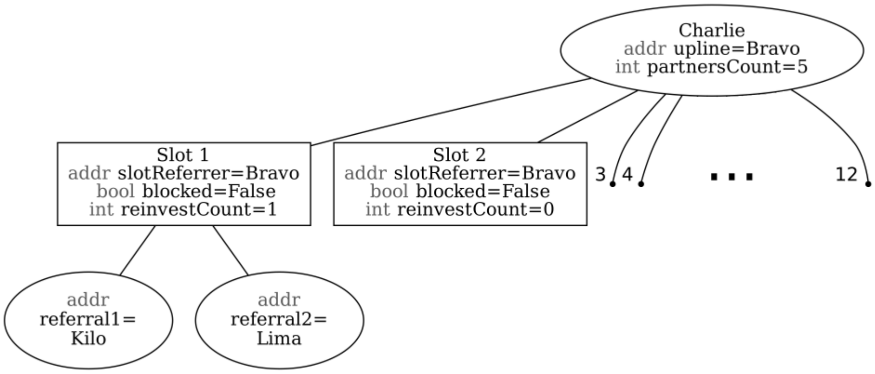


Fig. 9. A visualization of the state the contract keeps for each user in the X3 matrix, focusing on a user Charlie. The `addr` variables point to Ethereum addresses, here given NATO-phonetic names. Matrix slots that have not yet been opened are depicted with a numbered dot, instead of a box.

Forsage data structures: As noted in Section 3, Forsage consists of two matrix systems, X3 and X4, each consisting of 12 slots. These two matrices differ in the number of users needed to fill each matrix level (three for X3, six for X4) and the logic for how nodes propagate through them over time.

The data for each user is stored in a hashtable (Solidity mapping) on the Ethereum blockchain, with the key being the user's address and the value being a Solidity `struct` with the data for that user's state tree and arrays of pointers to its children. Figure 9 visualizes this mapping for a user's X3 tree, with some minor metadata variables omitted. Each user also has an X4 tree, whose structure is largely similar. As seen in this figure, each user has an *upline*, which is the user that referred them to the contract. This is distinct from slotReferrer, a variable used per slot as part of the payment logic. The slotReferrer variable is initialized to the upline, but changes over time as users refer each other. The reinvestCount variable records the number of times a slot has been filled. In our example, Charlie has filled his first matrix slot once (and then unblocked it by buying a slot at level 2), meaning he has referred $3 \times \text{reinvestCount} + 2 = 5 = \text{partnersCount}$ users.

External API: The contract exposes 15 functions to read its state, and two state-changing functions, `registrationExt` and `buyNewLevel`. The first registers new

[13] https://tronscan.org/

users and thus adds them to the contract state. The second changes contract state for an existing user to allow them to continue to gain money from new referrals.

The placement of new users in the contract state depends on the X3 and X4 slots for the user that referred them (their upline). The logic of the contract *scrambles* positions in the upline's matrices and in the matrices of the upline's parent when an upline's slot becomes full, i.e. every time the upline refers a multiple of three users to a given X3 slot ($\mathsf{partnersCount} \bmod 3 = 0$), or a multiple of six users to a given X4 slot. The logic of scrambling leaf nodes in the pyramid depends on the state of the slot `referrer` variable for the affected matrix slot, as well as the `blocked` variable for that slot, and in the X4 system an additional `closedPart` variable for each slot. Scrambling the positions of the existing users in the system helps to make payments through Forsage (falsely!) appear more random. It benefits older users in the pyramid, as users are usually scrambled "up" the pyramid to become children of older users rather than newer ones.

Opcode	Avg num per tx (all)	Median (all)	Avg num per tx (Forsage)	Median (Forsage)
`SSTORE`	4.54 ± 8.10	2	10.76 ± 9.57	6
`SLOAD`	17.84 ± 51.6	7	36.86 ± 26.21	29

Table 3. Average number of instruction operations per transaction, with standard deviation, for both all transactions and only those that interact with Forsage. Due to the intensive computation requirements, this table covers only between block heights 10,600,000 and 10,601,000 (Roughly 13:00-18:00 UTC on August 5th, 2020) rather than our larger dataset with all transactions from 2020. This smaller dataset still contains 188,920 transactions that interact with smart contracts, 5667 of which interact with Forsage.

Transaction fees: The fact that Forsage has so much persistent on-chain storage means that its users pay higher gas fees than the average for Ethereum contracts, due to the heavy usage of the (expensive) `SLOAD` and `SSTORE` opcodes. These fees are higher even when comparing Forsage transactions only to other contract function calls in Ethereum (so in particular ignoring simple sends of ETH). In our collected dataset of Ethereum network transactions, we found that the mean transaction fee for all Ethereum transactions that interacted with a contract was 0.00632 ETH with a standard deviation of 0.0618 ETH and a median of 0.00257 ETH. Forsage transactions paid a higher average transaction fee of 0.0116 ETH with a standard deviation of 0.0108 ETH and a median of

0.00883 ETH. Forsage users pay more than four times as much on average as other smart contract users.

The most gas-expensive EVM operations/opcodes are those that create a new contract (`CREATE`, `CREATE2`); store, change, and access data into persistent on-chain state (`SSTORE`, `SLOAD`), and call contract functions or send money to other users in the network (`CALL`) [40]. Every transaction that interacts with Forsage through its two main functions, `registrationExt` and `buyNewLevel`, uses two of these three most expensive categories, often multiple times: they make use of persistent storage via `SSTORE` and `SLOAD` operations, and send money to other users on the network using Solidity operations that compile to the `CALL` opcode. Forsage uses an average number of `CALL` operations, but makes heavy use of `SSTORE` and `SLOAD`, as shown in Table 3.

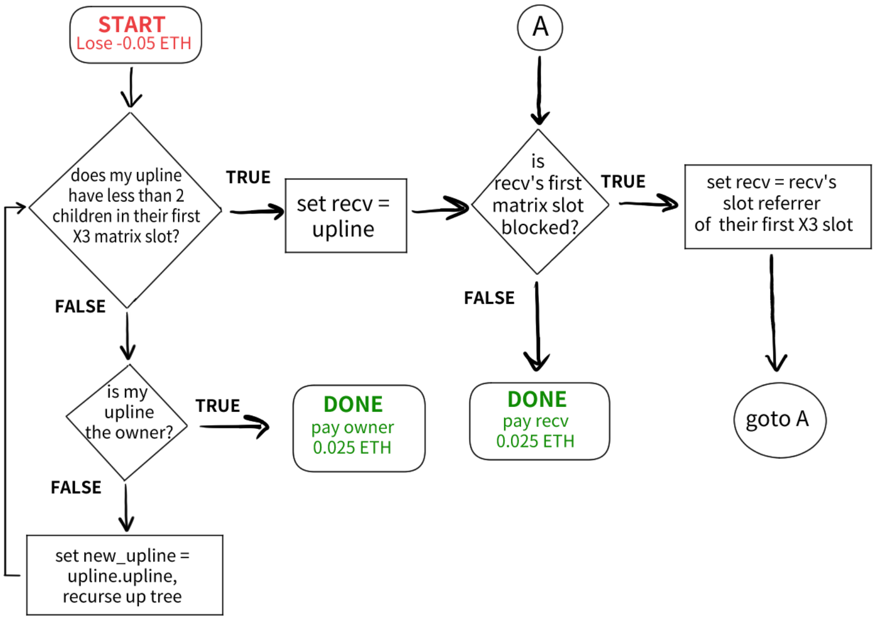

START
Lose -0.05 ETH
does my upline have less than 2 children in their first X3 matrix slot?
TRUE
set recv = upline
FALSE
is my upline the owner?
TRUE
DONE
pay owner
0.025 ETH
FALSE
set new_upline = upline.upline, recurse up tree
A
is recv's first matrix slot blocked?
TRUE
set recv = recv's slot referrer of their first X3 slot
FALSE
DONE
pay recv
0.025 ETH
goto A

Fig. 10. Flow chart for the logic of who gets paid when a new user registers, in the X3 system. The `BuyNewLevel` function follows similar logic, but conditioned on the matrix slot being purchased, rather than the first slot.

Payment logic: There are three ways for a user to get paid in Forsage: (1) by referring new users to the system; (2) when users they have referred in the past buy an additional matrix slot at a level corresponding to one previously purchased by the referrer; and (3) when *spillover* occurs, a condition in the X4 matrix resulting from the slots of another user downstream in the pyramid being blocked. Whenever money is sent to the smart contract by one user, the contract atomically (i.e., in the same transaction) sends those funds to other users based

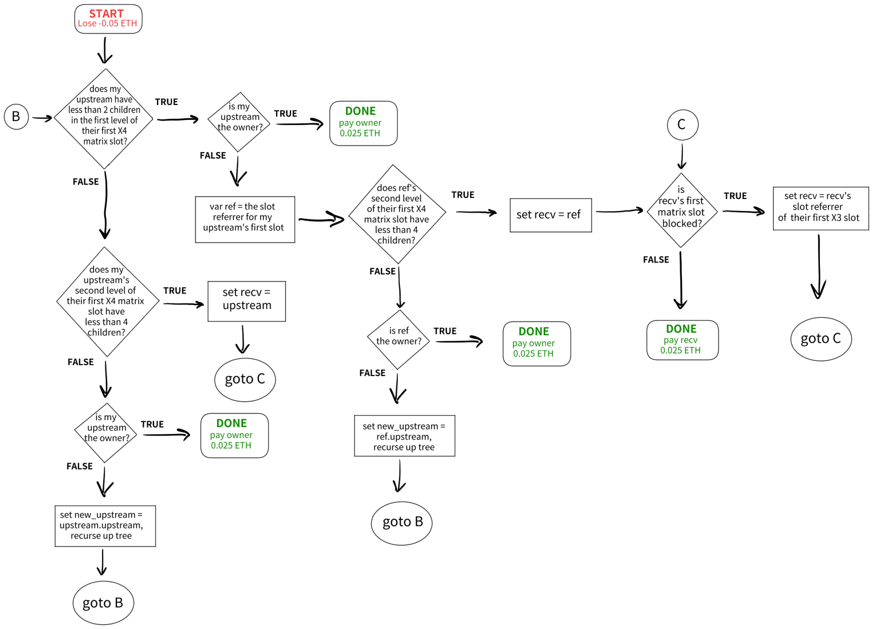

START
Lose -0.05 ETH
B
does my upstream have less than 2 children in the first level of their first X4 matrix slot?
TRUE
is my upstream the owner?
TRUE
DONE
pay owner
0.025 ETH
FALSE
var ref = the slot referrer for my upstream's first slot
does ref's second level of their first X4 matrix slot have less than 4 children?
TRUE
set recv = ref
C
is recv's first matrix slot blocked?
TRUE
set recv = recv's slot referrer of their first X3 slot
goto C
FALSE
DONE
pay recv
0.025 ETH
FALSE
is ref the owner?
TRUE
DONE
pay owner
0.025 ETH
FALSE
set new_upstream = ref.upstream, recurse up tree
goto B
FALSE
does my upstream's second level of their first X4 matrix slot have less than 4 children?
TRUE
set recv = upstream
goto C
FALSE
is my upstream the owner?
TRUE
DONE
pay owner
0.025 ETH
FALSE
set new_upstream = upstream.upstream, recurse up tree
goto B

Fig. 11. Flow chart for the logic of who gets paid when a new user registers, in the X4 system. The `BuyNewLevel` function follows similar logic, but would operate on the matrix slot being purchased for conditionals, rather than the first slot.

on the logic described below. This allows Forsage promotional materials to claim that the contract "never stores users' funds."

When a user buys a new slot, the money they pay typically routes to the first found upline that also has that same slot open. Users are thus incentivized to buy new levels in order to refer users underneath them, which means a user can be generally successful by adding additional matrix slots just before referring additional users, and in general by recruiting as many users as possible.

Figures 10 and 11 show the logic determining who gets paid when a new user registers with the Forsage contract, for both the X3 and X4 matrices. The logic for purchases of new slots (`buyNewLevel`) is largely similar but depends on the slot purchased rather than the first one (e.g., if a user buys the third slot then the logic is conditioned on the status of their upline's third slot).

The flowcharts in these figures show that uplines must keep their slots from becoming blocked, or payments will skip over them. To prevent a slot from becoming blocked, a user must buy the slot at the next level. This will also unblock an existing slot if it already has become blocked, and prevent the slot at $level - 1$ from ever becoming blocked again. Figure 1 shows the distribution of levels purchased in aggregate for all Forsage users, as well as the summed profitability for the group of users that purchased that many slot levels. In general, users that purchased more levels also gained the most profit: The average user of the contract purchased 2.13 levels, with a standard deviation of 2.89 and a median of 1 level purchased.

When a new user joins the system, their payment is split into two equal parts and the logic in the flowchart is applied to each half, with one half going through the X3 flowchart and one half through the X4 flowchart, to determine which other user(s) should get each half of the payment. If the direct upline of this new user is not blocked, then the upline gets the payment. If the upline has a blocked slot, the contract checks the upline's upline for that matrix slot level to see if it is blocked. The contract checks slots until it finds one that is unblocked, which it then pays. The contract owner (i.e., user that created the contract) is always unblocked, so the contract always finds a user to pay. This can result in the same user being payed twice (once by each half), or uncles and aunts being paid by their nephews and nieces in the tree if it has been previously scrambled. This condition is called *spillover*.

Spillover means that it is possible to earn money by receiving payments that should have gone to another user who had blocked slots. This passive earning is possible only in the X4 system, and only if a spillover recipient's upline is blocked and cannot currently receive payment. A given user's chance of spillover is unpredictable, because it depends on the actions of other users. In our analysis of the transactions to Forsage from its conception until January 14th, 2021, we found that 35,251 transactions (only 1.08%) contained spillover payments. Of those transactions 63% were registrations, and the remaining 37% resulted from buying new levels.

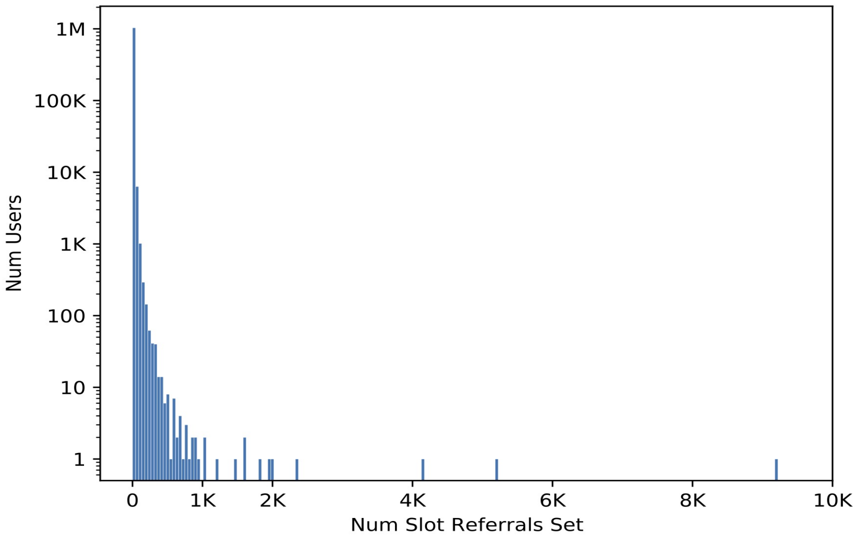


Fig. 12. On a log scale, the total number of users (on the y-axis) acting as slot referrer for a given number of *other* users (on the x-axis), for both the X3 and X4 matrices. For example, one user (the contract owner, *0x81...*) is slot referrer for 9220 other users.

Each interaction with the Forsage smart contract incurs Ethereum transaction costs that eat into users' profits. Any claims about user profit must thus take gas costs into account.

The privileged role of the owner: The Forsage contract is initialized so that the owner account (i.e., the creator of the contract, 81ca...) has all matrix slots for both X3 and X4 opened for free. The owner's slots can also never become blocked. The owner thus has ample opportunity to profit from the contract, which we confirm empirically in Section 4.

Beyond the ability to earn money by referring users, the owner also has additional opportunities to earn money passively. If a user sends the contract exactly 0.05 ether for registration without specifically calling the registration function, or calling a function that does not exist, that function call is rerouted to the registration function with the owner set as the user's upline. Likewise, if the upline gets replaced as the referrer, it is always replaced with a user further up in the pyramid. Thus, as users refer others and have their slots blocked as a result, the upline for all users eventually converges to the owner of the contract. Finally, the logic that prevents the owner's slots from becoming blocked also means that the owner's children do not change once set. This means that the owner maintains the oldest users in the pyramid as children, which results in high spillover in the X4 matrix.

We found that the slotReferrer variable was set to the contract owner for 9220 slots in the Forsage contract. By comparison, the average Forsage user was set as the referrer for 4.14 other accounts (with a standard deviation of 15.92); the median account was set as the referrer for one other account. Figure 12 shows the distribution of referrers for all accounts.

B Analysis of Forsage YouTube Promotions

We manually watched YouTube videos to understand the claims that Forsage promotional videos make, as discussed in Section B, and made requests to the public YouTube API for view count and other popularity-related data.[14] To get a sense of Forsage's Facebook and Instagram presence, we manually browsed various Facebook groups and official Instagram accounts and leveraged the Facebook and Instagram Graph APIs.[15] Facebook group data is not available on the Graph API so we wrote a custom Python script leveraging the Selenium WebDriver browser automation tool to collect more in-depth data about Forsage Facebook groups and their users.[16] This yielded a dataset of just over 5000 of the most recent members from the largest Facebook group dedicated to Forsage.[17] Using the Twitter API for academic researchers,[18] we were able to scrape all tweets with the word "Forsage" from January 1, 2020 until February 13, 2021. We used the official Telegram API [19] to collect information about telegram groups related to Forsage.

Community size: Forsage has a substantial presence on the social network sites that they target. This includes:

- *Facebook:* 131 active Facebook groups with titles or descriptions including "Forsage," containing 403,029 distinct Facebook members.
- *Instagram:* 24 Instagram accounts with Forsage in the username, disseminating information about Forsage to 24,747 followers of these accounts, with an additional 78,220 posts on the Instagram #forsage hashtag.
- *Telegram:* 285,788 people spread across 49 different channels on Telegram dedicated to Forsage.
- *Twitter:* Our collected Twitter dataset included 85,085 tweets from 21,746 unique accounts, including 513 accounts on Twitter with Forsage in their name.
- *YouTube:* 57,551 video results from 325 different YouTube channels.

The Forsage website also features a "community" subdomain[20] that hosts a tips and tricks section, blog-post style news, a frequently asked questions section, "academy courses" that include video lectures on how to be an effective multi-level-marketer, and a Stack-Overflow-like site where users can ask questions and "Forsage Community Authors" answer.

A substantial amount of the Forsage online social media ecosystem may be driven by bots. We ran the University of Indiana's Observatory on Social Media

[14] https://developers.google.com/youtube/v3/docs/search/list
[15] https://developers.facebook.com/docs/graph-api/
[16] https://www.selenium.dev/
[17] https://www.facebook.com/groups/forsageinformationgroup
[18] https://developer.twitter.com/en/docs/twitter-api/tweets/search/introduction
[19] https://core.telegram.org/
[20] https://community.forsage.io/

(OSoMe) Botometer tool [33] on our collected dataset of tweets and found that the tool identified roughly 47% of the Forsage-related tweets we collected as coming from likely bot accounts. For comparison, in March of 2017, Varol et al. [38] used an earlier version of the Botometer tool to perform a measurement study across all of Twitter and found that “between 9 and 15% of active Twitter accounts are bots."

Rank	Title	Views	Link
1	Forsage Overview: Earn Ethereum Daily!	267008	https://www.youtube.com/ watch?v=m0NzYwFfGH4
2	Forsage Presentation - How does Forsage work	120425	https://www.youtube.com/watch?v=NoAh57M-Dak
3	Forsage Smart Contract- $735 Made Without Referring Anyone	113677	https://www.youtube.com/watch?v=PqsfdcLvlIQ
4	FORSAGE: HOW TO EARN WITHOUT RECRUITING ANYONE IN FORSAGE	117931	https://www.youtube.com/watch?v=zCvj_zZZmOI
5	Forsage Smart Contract Review - Is It A SCAM Or Legit Ethereum MLM?	106261	https://www.youtube.com/watch?v=7YUWfl0looY
6	FORSAGE.io - BIG SPECIAL EVENT	91973	https://www.youtube.com/watch?v=NMfcDSCXLK8
7	Forsage Smart Contract $1,778 Made Without Referring a Single Person	91188	https://www.youtube.com/watch?v=N-Qem777Qis
8	Forsage Review - Is Forsage a Scam or Legit?	79264	https://www.youtube.com/watch?v=WVsLIVCqJbc
9	Smartway Forsage REVIEW - First Ever SCAM PROOF Program	64923	https://www.youtube.com/watch?v=TmVp2ViU0Ro
10	how to make money on forsage without referring anyone	61996	https://www.youtube.com/watch?v=qTVMCjuipho

Table 4. Top Youtube videos for Forsage.

Type	Claim	Appearances	Cumulative Views
Wealth	Forsage users make money forever.	3/10	425,356
	Forsage users make unlimited income.	3/10	449,429
	Forsage users make passive income.	3/10	247,344
	Forsage users can earn hundreds of ETH in the first few weeks or months.	4/10	558,617
Risk	Forsage is risk-free for users.	3/10	393,927
	No one can stop Forsage.	4/10	558,617
	Forsage is safe because the contract does not store funds.	4/10	530,165
	Forsage is scam-proof.	3/10	393,927
Ethereum Education	The video explains what Ethereum is for new users.	5/10	637,881
	The video explains what a smart contract is for new users.	5/10	637,881
How to Use Forsage	Successful Forsage users open at least 3 slots per program to start (0.2 ETH).	6/10	745,960
	Users should buy more slots (send Forsage more money) as soon as they earn.	5/10	654,727
	The more slots you open (money you send Forsage), the more you will earn.	4/10	511,858
	If you do not keep opening slots (sending money to Forsage), you will not earn.	5/10	444,539

Table 5. Results of coding repeated claims that appear across the top 10 most viewed, English language videos on YouTube mentioning “Forsage” in their title. These claims offer a perspective on user expectations when joining Forsage.

Country	Facebook	Twitter	YouTube
Nigeria	84	4878	3
Philippines	272	668	14
India	97	488	88
United States	45	1019	26
Indonesia	17	203	8
TOTAL	771	10200	216

Table 6. Top five countries with the highest absolute level of Forsage user engagement. User engagement here is measured as a country's total number of Facebook observed users in the most popular Forsage Facebook group, plus its analogous number of Twitter observed users that tweeted about Forsage in 2020, and YouTube data for the number of YouTube channels with geo-tagged locations that produced videos with Forsage in the title of the video.

Forsage promotional materials offer a window into users' expectations for the contract and insight into how the technical properties of blockchain technology are represented to manipulate novice users.

YouTube is the main promotional channel for Forsage. Participants joining Forsage are referred to an official YouTube video explaining the program [26]. We searched YouTube for English language videos with "Forsage" in the title and tracked the claims that repeat across videos to measure user expectations for Forsage. The search for most viewed videos about Forsage also returned promotional videos in Tagalog, Russian, Hindi, Tamil, Bangala, Telugu, Indonesian, and Spanish. Quasi-official (they share the same branding) Telegram chat groups for Forsage news exist in English, Spanish, French, Italian, Russian, Arabic, Portuguese, Hindi, Tamil, German, Azerbaijani, and Turkish.

Recommendation algorithms, like the one used by YouTube for search results, work in terms of popularity measured in views. The most viewed videos on YouTube are the most likely to be seen by users. We selected the top ten videos by views to qualitatively measure what users who search for informational videos about Forsage would see and hear about the program and gain a sense of participant expectations. We did so by coding the claims asserted about Forsage in these videos. We focused on just the top ten videos because coding claims is a labor-intensive, manual process. A researcher watched each video and noted if each video contained any instance of certain claims (see Table 5 and Appendix **??**). Each video was watched and coded twice to ensure accuracy.

The top ten YouTube videos we coded had between 267,008 views (1st) and 61,996 views (10th). Beyond the videos we coded, the 11th most viewed video had just over 50,000 views[21] and the 20th had 33,000 views.[22]

The top 10 "Forsage" YouTube videos by views as of December 14, 2020 (see Appendix **??**) [Ari: Broken link.] fit into three categories: official promotion, user-led recruitment, and user reviews. Two of the videos were official promotion

[21] https://www.youtube.com/watch?v=aGi5G5mTCUM

[22] https://www.youtube.com/watch?v=9vlOYRSLaHI

posted to Forsage's YouTube channel [26,27]. Table 5 shows the repeated claims across the top ten videos.

In recruiting new users, Forsage promoters pointed to users who earned large sums of money, showing, e.g., images of monthly six-figure returns on successful users' Forsage dashboards. Forsage official promotion videos highlight the immutable nature of the smart contract and the transparency of Ethereum as proof that Forsage cannot be a scam. They also make claims about the life-changing wealth and unstoppable, passive income that users could gain from Forsage.

Forsage promotional videos also provide basic explanations of blockchains, Ethereum, smart contracts, and how to use a cryptocurrency wallet, implying that they expect users to be cryptocurrency novices. Only one of the top ten videos identifies Forsage as a scam and warns users against using it.

Many incorrect claims made in the Forsage promotional YouTube videos also appear on the Forsage website and in the questions section of the official Forsage Community website.

C Proposed Solutions to Prevent Further Scams

Targeted education: From our analysis of Forsage user locations in Section 5.1, the majority of Forsage victims are located in only a few countries. This concentration lends itself well to targeted education campaigns and warnings from local authorities. For example, a simple user dashboard showing the number of Forsage users who lose money from the contract—more than 88% as of January 15th, 2020—could serve as an effective tool to combat disinformation from Forsage promoters more effectively than general warnings such as that issued by the Philippines SEC (see below).

Law enforcement and regulation: Past cryptocurrency pyramid schemes, including Plustoken, Wetoken, Onecoin, and Bitconnect, have collapsed as a result of government sanctioning, which included the arrest or warrants for the arrest of the founders and leadership [28,14,7,19]. Similar attempts have been made around the world in regards to Forsage. On June 30, 2020, The Philippines Securities and Exchange Commission (PSEC) issued numerous warnings declaring that Forsage was not a registered entity within their jurisdiction and was operating without a license.

On the 1st August 2022 the SEC filed charges against eleven members of the Forsage scheme, including the four founders and seven promoters, for operating a $300 million pyramid scheme and violating multiple acts of US securities law [35,34]. The case demands a trial by jury and alleges that the members frauded and deceited their investors by operating a 'textbook pyramid and Ponzi scheme.' The SEC calls the court to serve permanent injunctions to the members against violating the laws, against further conduct and asks to pay disgorgement with interest and civil money penalties. Since, the website has been partially blocked, at present is inaccessible in the United States and United Kingdom but accessible in Switzerland.

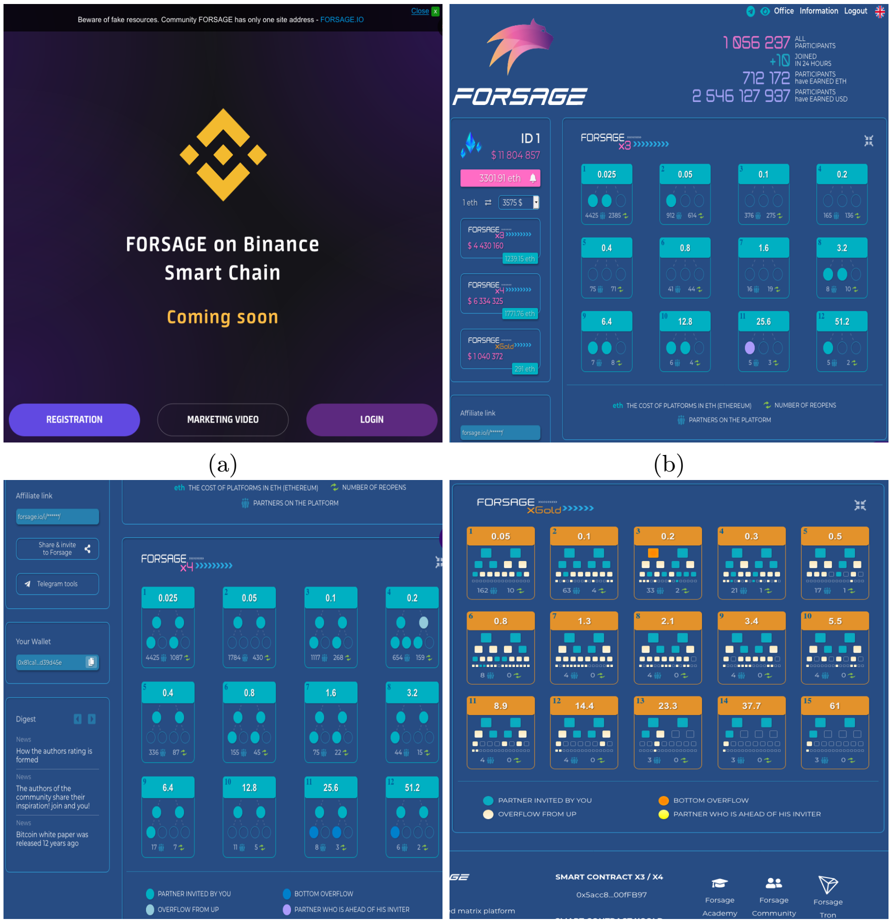
Voluntary blocklisting: Previous research has shown blocklisting can effectively combat scams and illicit activity. Moser et al. found that blocklisting of illicit cryptocurrency funds is an effective additional layer above existing anti-money laundering (AML) and know-your-customer (KYC) requirements for cryptocurrencies [21]. Previous research in illicit online pharmaceutical sales found that payment processing services—analogous to cryptocurrency exchanges for Forsage—are the most fragile part of the scam [20]. Their work suggests that blocklisting access to exchanges may impact the most fragile part of pyramid schemes. Crypto Defenders Alliance (CDA)[23] and CryptoSafe Alliance[24] are two examples of groups that operate a blocklist.

On the other hand, blocklists can be biased and enable forms of censorship, and addresses that are blocked in one region may not be considered suspicious or criminal in other regions. To understand how professionals navigate these tensions, we spoke to an anti-money laundering cryptocurrency investigator at a high profile exchange. This expert expressed a belief that it is the responsibility of law enforcement and regulators to comment on whether or not an address should be blocked, and that it would be unfair and unjust to hold a user's funds without an explicit request from law enforcement or a court of competent jurisdiction. Nevertheless, some exchanges have joined the alliances mentioned above, due to the time and resources required to maintain a dedicated list of blocked addresses by themselves.

[23] https://cryptodefendersalliance.com/

[24] https://www.cryptosafe.org/

D Forsage Website Screenshots



(a) (b)

(c) (d)

Fig. 13. Four screenshots of the forsage.io website. (a) Homepage of forsage.io as of May 6th, 2021. The website is marketing the arrival of the new scheme that will be used on the Binance Smart Chain. (b) Landing page of the most profitable user showing the progress page of the X3 matrix and other macro statistics. (c) Progress page of the user's X4 matrix. (d) Progress page of the user's xGold matrix.