Buy Crypto, Sell Privacy: Investigating the Cryptocurrency Exchange Evonax

Anonymous Authors
Anonymous Institution

***Abstract*—In their study of the cryptocurrency exchange *ShapeShift*, Yousaf et al. (USENIX Security, 2019) have demonstrated that information provided by the APIs of exchange platforms can facilitate cross-chain traceability and thus severely hurt user privacy. Unfortunately, little empirical research on exchanges is available otherwise.**

In this paper, we replicate and extend the approach of Yousaf et al. by developing new methods to extract transactions using the public blockchain and the interface of the cryptocurrency exchange *Evonax*. We are able to identify $30,402$ transactions between the launch of Evonax in February 2018 and December 31, 2022, which should be close to a complete set of all transactions. This allows us to generate deep insights into the operations of the platform as well as the behavior of its users.

***Index Terms*—cryptocurrency exchange measurement, blockchain privacy, cryptocurrency forensics**

I. Introduction

Cryptocurrency exchanges nowadays constitute a multi-billion dollar industry with hundreds of competing platforms: As of January 2024, CoinMarketCap lists over 200 spot exchanges and approximately 450 decentralized exchanges[1].

This inevitably raises the question of how cryptocurrency exchanges operate and what they are being used for. Unfortunately, there is only little research on cryptocurrency exchanges available that relies on direct empirical evidence.

In a pioneering study using the APIs of ShapeShift, Yousaf et al. demonstrated that the interfaces of exchange platforms might inadvertently facilitate the cross-chain traceability of transactions. Their analysis identified corresponding cryptocurrency transactions for $70\% - 90\%$ of exchanges made on the platform over a 13-month period [7].

In this study, we add fresh insights to the line of research started by [7]: We develop a new method for identifying exchange-related cryptocurrency transactions for the exchange platform Evonax[2] and perform an in-depth analysis of the acquired data. Our key contributions are as follows:

- We present a novel method for extracting cryptocurrency trade data from an exchange platform. By reverse-engineering the way Evonax handles payments on the blockchain, we obtain information that can be used to acquire trade data from an interface provided by Evonax.
- Employing this method, we compile a dataset containing detailed information on $30,402$ exchange trades spanning from the platform's launch on February 16, 2018, to December 31, 2022.
- We attain a deep understanding of Evonax's internal operations and investigate the behavior of its users. For instance, we identify a unique trading pattern involving intra-currency "coin swaps", and provide evidence of its use for obscuring the flow of funds obtained from illicit activities.

The paper is organized as follows: Section II provides an overview of related work.Technical background information is presented in Section III. Section IV details the methodology for acquiring Evonax trades using the blockchain and the Evonax *track exchange* form. Platform operations of Evonax are analyzed in Section V, and interesting use cases are discussed in Section VI. A critical discussion of our findings is presented in Section VII.

II. Related Work

Within the cryptocurrency exchange domain, studies, including those from non-computer science fields, tend to concentrate on regulation ([1]) and criminal activities like wash trading ([2]–[4]) and money laundering ([5], [6]).

To our knowledge, [7] is the sole work investigating trading behavior on cryptocurrency exchanges using actual trading data from blockchain analysis and exchange APIs: Yousaf et al. leverage ShapeShift's API to derive trading information, identifying corresponding cryptocurrency transactions with success rates ranging from 70% to 90% of exchanges on the platform. They define three cross-currency transaction patterns and conduct case studies to uncover potential criminal activities.

Our study complements and expands [7] in several aspects. We delve into an exchange's internal payment processing mechanisms and corresponding blockchain transaction patterns, allowing us to extract a comprehensive dataset of nearly the entire trade history. Using this dataset, we investigate exceptional use cases, notably identifying a novel trading pattern termed "coin swaps" and linking some trades to criminal activities.

III. Background

We assume that readers are familiar with cryptocurrencies and provide a brief overview of our notation for key concepts only.

A. Transactions

Formally, a transaction t in currency $\mathcal{C}$ involves a set of input addresses A_t^{in} and output addresses A_t^{out}. A value v_a

[1]https://coinmarketcap.com/rankings/exchanges/
[2]https://www.evonax.com/

exists for each $a \in A_t^{in}$, denoting the amount spent in the transaction, and similarly for each $a \in A_t^{out}$ indicating the received amount. This paper primarily focuses on addresses, defining a transaction t by the parameters:

$$t = (\mathcal{C}, A_t^{in}, A_t^{out}). \tag{1}$$

Transactions on the blockchain are uniquely identified by their transaction ID (TXID). For simplicity, we use t to refer to both a transaction and its TXID.

B. Cryptocurrency Exchanges

In our model, a cryptocurrency exchange facilitates the sale of a specified amount v_{in} of currency $\mathcal{C}_{in}$ in exchange for an amount v_{out} of currency $\mathcal{C}_{out}$, where at least one currency involved is a cryptocurrency. The received v_{out} is determined by the exchange rate of the currency pair and an optional fee.

We generically term this process an exchange trade e, even if $\mathcal{C}_{in} = \mathcal{C}_{out}$. To avoid confusion with the terms *transaction* and *(exchange) trade*, we clarify their usage: Transaction t refers to the concept of transactions in the context of cryptocurrencies (cf. Section III-A), while trade e describes the act of exchanging one cryptocurrency for another using a cryptocurrency exchange platform.

1) Structure of a Trade: Irrespective of their specific implementation, exchange platforms typically manage cryptocurrency trading through three transactions:

Pay-in transaction t_{in}: Users initiate a transaction t_{in}, transferring v_{in} within currency $\mathcal{C}_{in}$ from user address a_u to an exchange-owned deposit address a_{dep}. Deposit addresses are used to link payments to customers, especially for cryptocurrencies lacking reference fields in their transaction data.

Deposit transaction t_{dep}: As user deposits are usually resold in other trades, accumulated funds in a_{dep} are eventually withdrawn in an exchange-issued transaction t_{dep}.

Pay-out transaction t_{out}: Upon confirming the user's transfer of v_{in} to a_{dep}, the exchange initiates a pay-out transaction t_{out}, transferring v_{out} from an exchange-owned wallet to the user's payout address a_{out}.

In this study, we focus on transactions issued by the exchange service: t_{dep} and t_{out}. t_{in} is user-initiated and not part of the trade. Thus, a trade e is associated with the following parameters:

$$e = (\underbrace{\mathcal{C}_{in}, a_{dep}, v_{in}, t_{dep}}_{\text{deposit transaction}}; \underbrace{\mathcal{C}_{out}, a_{out}, v_{out}, t_{out}}_{\text{pay-out transaction}}). \tag{2}$$

The deposit transaction t_{dep} and pay-out transaction t_{out} are transactions in $\mathcal{C}_{in}$ and $\mathcal{C}_{out}$, respectively. Notably, only "half" of each transaction is involved in a given trade, signifying that for t_{dep}, an input address $a_{dep} \in A_{t_{dep}}^{in}$ is known, and for t_{out}, an output address $a_{out} \in A_{t_{out}}^{out}$ is known. Additionally, t_{dep} may occur after t_{out}, indicating that a user might receive their bought coins before their sold ones are swept off a_{dep}.

C. Evonax

Evonax is a cryptocurrency exchange supporting the crypto-to-crypto exchange of nine native cryptocurrencies (Bitcoin, Bitcoin Cash, Bitcoin Gold, Dash, Dogecoin, Ether, Litecoin, Monero, ZCash) and nine ERC-20 tokens (0x, Chainlink, Compound, Dai, Maker, Shiba Inu, Tether, Uniswap, Wrapped Bitcoin). Initial support for Bitcoin SV was discontinued. The platform claims no registration or know-your-customer (KYC) checks are required for its use. Initially offering exchanges to and from fiat currencies, Evonax allowed deposits via bank transfer and payouts through PayPal. After PayPal terminated its business relationship with Evonax, the service shifted to *AdvCash* as a payment provider [8]. Crypto-to-fiat trades using AdvCash were also discontinued in February 2022.

Trades on Evonax are initiated via a simple form on the website, with no need for user account creation. Users interested in the service first select $\mathcal{C}_{in}$ and $\mathcal{C}_{out}$. Evonax then sets an exchange rate and prompts the user to specify either the amount to sell (v_{in}) or the amount to buy (v_{out}). Once one amount is entered, the other is automatically calculated based on the exchange rate. After providing a valid pay-out address a_{out} in $\mathcal{C}_{out}$, the exchange can be started. Users may opt to supply an email address for status updates.

Interestingly, users can choose the same currency for $\mathcal{C}_{in}$ and $\mathcal{C}_{out}$. From a trading standpoint, this may seem futile, as the user incurs network and exchange fees but ends up with the same currency. Possible use cases are explored in Section VI-B.

Evonax lacks an order book, advanced trading interface, or trading API. The website interface serves as the sole means to initiate a trade.

IV. Data Acquisition

Let $\mathcal{E}$ denote the complete set of all trades executed by Evonax. Our objective is to capture as many trades in $\mathcal{E}$ as possible, achieved through Extract procedures that extract additional trades from a given set of trades using the blockchain and the Evonax interface. More detailed descriptions of these procedures are provided below. The initial step is to identify a "starting" set of trades, obtained from our own test trades and by extracting cryptocurrency addresses from user reviews on Trustpilot[3]. Subsequently, the Extract procedures are repeatedly applied to the known set until no new trades are found.

These procedures leverage two sources of information: the public blockchain and a web interface provided by Evonax.

The blockchains of Bitcoin Cash, Bitcoin Gold, Bitcoin SV, Monero, and Zcash are excluded from the acquisition process due to low trading volume and/or privacy-centric design. However, information on trades involving these coins is still acquired as a byproduct, for instance, if the other involved currency is part of the analysis or the trade has a known email address associated with it.

[3]https://www.trustpilot.com/review/www.evonax.com

Blockchain: As the blockchain contains all transactions, it is possible to directly derive the input and output addresses of a given transaction t (cf. Equation (1)):

$$t \overset{\text{Blockchain}}{\mapsto} (A_t^{in}, A_t^{out}) \tag{3}$$

Additionally, the blockchain can be searched for transactions where only partial information is known. More precisely, given an address a, one can extract all transactions t where a is either an input or output address:

$$a \overset{\text{Blockchain}}{\mapsto} \left\{t \mid a \in A_t^{in}\right\} \tag{4}$$

$$a \overset{\text{Blockchain}}{\mapsto} \left\{t \mid a \in A_t^{out}\right\} \tag{5}$$

Evonax web interface: Evonax facilitates the querying of exchange transaction status through a *track exchange* form[4]. This page is publicly accessible, and requests are not authenticated. Trades are identified by either the deposit address a_{dep}, the pay-out address a_{out}, or an (optionally provided) e-mail address $@mail$.

Entering any of these three identifiers will prompt the website to display status information for all exchanges involving the specified search key. The status data includes the TXIDs of the pay-in transaction t_{in} and the pay-out transaction t_{out}, the deposit address a_{dep}, the pay-out address a_{out}, a timestamp, the exchanged currencies $\mathcal{C}_{in}$ and $\mathcal{C}_{out}$ with the corresponding amounts and the exchange rate and, optionally, an e-mail address $@mail$.

In essence, the Evonax interface allows the use of partial trade information as input and provides nearly the full data about a trade (cf. Equation (2)) in return. Only t_{dep} is not directly provided. However, as the deposit address a_{dep} is trade-specific and under the control of Evonax, t_{dep} can be reliably identified with the help of the public blockchain and Procedure (4).

To summarize, the Evonax track exchange form offers two procedures for deriving trade information:

$$@mail^* \overset{\text{Evonax}}{\mapsto} \{(e, @mail) | @mail^* = @mail\} \tag{6}$$

$$a \overset{\text{Evonax}}{\mapsto} \{(e, @mail) | a = a_{dep} \vee a = a_{out}\} \tag{7}$$

Procedures (6) and (7) directly produce (potentially) new trades if $@mail$, a_{dep} or a_{out} is provided. This allows us to derive all trades associated with a given e-mail, deposit or pay-out address. This approach is part of the Extract procedures for both account-based and UTXO-based currencies.

The subsequent part of this section describes the Extract procedures for the case of account-based cryptocurrencies (Section IV-A) and UTXO-based cryptocurrencies (Section IV-B). Each procedure, applied to a trade as displayed in Equation (2), identifies (potentially) new trades. Note that each procedure can be applied to either t_{dep} *or* t_{out}, but not both. Thus, cases in which $\mathcal{C}_{in}$ is an account-based currency and $\mathcal{C}_{out}$ is a UTXO-based currency, and vice versa, can be handled by combining the appropriate procedures.

[4]https://www.evonax.com/status

A. Account-Based Cryptocurrencies

Evonax employs a dedicated hot wallet with a single address[5] a_{hot} for handling payments in account-based currencies. Trades involving at least one of $\mathcal{C}_{in}$ and $\mathcal{C}_{out}$ as an account-based currency or ERC-20 token trigger transactions involving the hot wallet.

Users exchanging Ether on Evonax send funds to an exchange-owned deposit address a_{dep}. After trade execution, Evonax initiates transaction t_{dep}, forwarding funds from a_{dep} to a_{hot}. Similarly, when users exchange other currencies for Ether or an ERC-20 token, transaction t_{out} transfers funds from a_{hot} to the user-specified pay-out address a_{out}.

For ERC-20 token deposits, additional transactions are required due to gas fees for t_{dep}. Following the ERC-20 token deposit, a small amount of Ether is transferred from a_{hot} to a_{dep} to cover gas fees. Subsequently, t_{dep} transfers the ERC-20 tokens to a_{hot}, utilizing the previously transferred Ether for gas fees. The remaining Ether is returned to a_{hot}. Identifying t_{dep} is possible as it is the sole transaction transferring tokens off a_{dep}.

The extraction procedures for trades involving Ether or an ERC-20 token are defined as follows:

Approach 1: Pay-out transaction t_{out} transfers funds from a_{hot} to a_{out}. Procedure (3) yields $A_{t_{out}}^{in} = \{a_{hot}\}$, the hot wallet address. Subsequently, approach 3 is applied.

Approach 2: Deposit transaction t_{dep} forwards deposited funds from a_{dep} to a_{hot}. If a_{dep} is known, Procedure (4) retrieves t_{dep}, and Procedure (3) yields $A_{t_{dep}}^{out} = \{a_{hot}\}$. Extraction then proceeds with approach 3.

Approach 3: With the hot wallet address a_{hot}, trades can be retrieved in a two-step process. First, Procedure (5) is employed to query the blockchain for transactions transferring funds to the hot wallet:

$$a_{hot} \overset{\text{Blockchain}}{\mapsto} \left\{t \mid a_{hot} \in A_t^{out}\right\} =: T. \tag{8}$$

For each transaction $t \in T$, Procedure (3) provides A_t^{in}, the potential deposit addresses. To verify if an address $a \in A_t^{in}$ is a deposit address, the Evonax track exchange page is consulted: a is a deposit address if and only if Procedure (7) returns a trade when queried for the address. Otherwise, the address is flagged for further inspection.

In the second step, transactions transferring funds from the hot wallet are obtained using Procedure (4):

$$a_{hot} \overset{\text{Blockchain}}{\mapsto} \left\{t \mid a_{hot} \in A_t^{in}\right\} =: T. \tag{9}$$

Similarly, for each transaction $t \in T$, Procedure (3) provides a potential pay-out address. True pay-out addresses in A_t^{out} are identified through Evonax's track exchange page, while non-pay-out addresses are collected for further analysis.

B. UTXO-Based Cryptocurrencies

Similar to account-based currencies, new trades can be obtained using either the pay-out transaction t_{out} or the deposit address a_{dep} in the deposit transaction.

[5]0x2ab5a95e5881ba190434bd2ca423f7f1e2106747

Approach 1: The first approach leverages the fact that a trade specifies a pay-out transaction t_{out}. Procedure (3) identifies the set of its input addresses $A^{in}_{t_{out}}$ and output addresses $A^{out}_{t_{out}}$. Further trades can be derived from these sets.

Notably, the same transactions can be involved in multiple trades. A transaction t_{out} can serve as the pay-out transaction for several trades simultaneously. In other words, two distinct trades $e \neq e'$ may exist such that

$$\begin{aligned} e &= (\ldots; \mathcal{C}_{out}, a_{out}, v_{out},\ t_{out}), \\ e' &= (\ldots; \mathcal{C}_{out}, a'_{out}, v'_{out},\ t_{out}). \end{aligned}$$

Pay-out addresses of additional trades can be derived from the set $A^{out}_{t_{out}}$ using Procedure (3). Distinguishing pay-out addresses from other elements in $A^{out}_{t_{out}}$, such as change addresses, is crucial. The Evonax interface serves this purpose: $a^* \in A^{out}_{t_{out}}$ is a pay-out address if and only if the Evonax interface returns a trade (cf. Procedure (7)) when queried for a^*.

If $a^* \in A^{out}_{t_{out}}$ is not a pay-out address, Procedure (4) is used to find a transaction t^* that has a^* as an input address, i.e., $a^* \in A^{in}_{t^*}$. a^* is a change address if and only if there exists at least one $a \in A^{out}_{t^*}$ for which Procedure (7) returns a trade. In case a^* is a change address, it is treated as a deposit address in approach 2. If a^* is neither a change address nor a pay-out address, it is likely part of the liquidity management process.

Approach 2: The second approach employs the trade-specific deposit address a_{dep}. Extracting the corresponding deposit transaction t_{dep} from the blockchain is straightforward using Procedure (4). Similar to $A^{out}_{t_{out}}$ referring to multiple users' pay-out addresses, $A^{in}_{t_{dep}}$ may include deposit addresses for several trades. Formally, two distinct trades $e \neq e'$ may exist such that

$$\begin{aligned} e &= (\mathcal{C}_{in}, a_{dep}, v_{in},\ t_{dep}; \ldots), \\ e' &= (\mathcal{C}_{in}, a'_{dep}, v'_{in},\ t_{dep}, \ldots). \end{aligned}$$

Observationally, $A^{in}_{t_{dep}}$ comprises three types of addresses: deposit addresses, change addresses, and others. To distinguish between these types, the Evonax interface is employed as described in approach 1.

Approach 3: Exploiting the fact that an input transaction t_{dep} may combine multiple deposit addresses as inputs and, similarly, an output transaction t_{out} may comprise several user addresses as outputs has been discussed. In the context of Evonax, a transaction t_{out} can serve as the pay-out transaction for one trade e and, simultaneously, the deposit transaction for another trade e', i.e.,

$$\begin{aligned} e &= (\ \ldots\ ;\ \mathcal{C}_{out}, a_{out}, v_{out},\ t_{out}\ ) \\ e' &= (\ \mathcal{C}_{in}', a_{dep}', v_{in}',\ t_{out}\ ;\ \ldots\ ) \end{aligned}$$

Therefore, the inputs $A^{in}_{t_{out}}$ of a pay-out transaction t_{out} typically reveal further deposit addresses (and hence trades).

Similarly, a transaction t_{dep} can simultaneously be the deposit transaction for one trade e and the pay-out transaction for another trade e', i.e.,

$$\begin{aligned} e &= (\ \mathcal{C}_{in}, a_{dep}, v_{in},\ t_{dep}\ ;\ \ldots\ ) \\ e' &= (\ \ldots\ ;\ \mathcal{C}_{out}', a_{out}', v_{out}',\ t_{dep}\ ) \end{aligned}$$

This property allows us to combine the first two approaches: By applying approach 2 to the hitherto unused input addresses of the pay-out transaction obtained in approach 1, $A^{in}_{t_{out}}$, further trades may be discovered. Correspondingly, approach 1 is applied to $A^{out}_{t_{dep}}$ of the deposit transaction t_{dep} that has already been processed in approach 2.

V. Exchange Operations

We use a dataset containing $30,402$ trades from February 16, 2018 (the first observed trade) to December 31, 2022 to analyze and measure the operations of Evonax. Among the captured trades, $23,600$ were successful, while the remaining trades either failed or had an unclear status. Conversions between cryptocurrencies and US-Dollar are calculated based on data from CoinGecko[6], using the historical exchange rate at the time of each trade or transaction.

A. Trading Volume

Trading volume, the total value of executed trades within a given time period, is a crucial indicator of an exchange's popularity. Many exchanges report their trading volume to data aggregators like CoinMarketCap. While there is no public information available on Evonax's trading volume, it can be calculated based on our data. The total trading volume during the investigated timeframe amounts to approximately $\$19,450,000$. A yearly breakdown of successful trades, including the average volume per trade and the number of trades, is presented in Table I.

TABLE I
Total and average yearly trading volume

Year	Trades	Total Volume	Average	Median
2018	1,815	$ 485,375.99	$ 267.42	$ 11.30
2019	2,307	$ 386,830.42	$ 167.68	$ 8.23
2020	6,601	$ 2,507,694.79	$ 379.90	$ 35.22
2021	11,030	$ 14,666,685.61	$ 1,329.71	$ 61.32
2022	1,847	$ 1,402,123.84	$ 759.14	$ 71.30
Total	**23,600**	**$ 19,448,71**	**$ 824.10**	**$ 44.20**

As shown in Figure 1, the number of trades reached its peak in January 2021 and maintained a relatively high level throughout the first half of the year. However, there was a temporary drop in trading count in March. Regarding trading volume, a distinct peak is evident in August 2021, where the total traded value was approximately $\$6,770,000$, constituting around $\approx 35\%$ of the entire trading volume on the platform. This outlier results from a low number of very high-value trades, contributing to the unusual difference between median and average trading values in 2021. This anomaly raises suspicions of an individual or group utilizing Evonax for coin laundering, aiming to obscure the on-chain traceability of their payments. Further details are discussed in Section VI-A.

[6]https://www.coingecko.com/

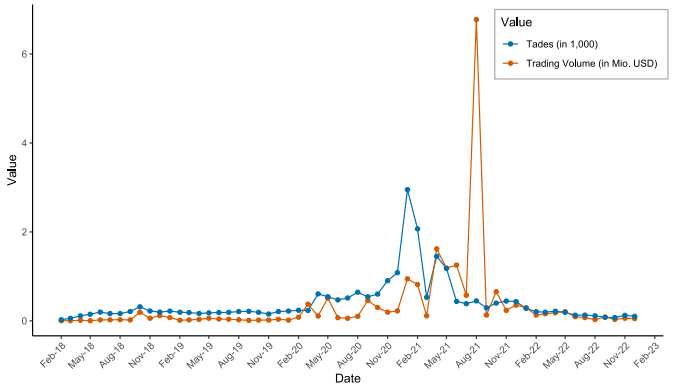

Fig. 1. Monthly trading volume and trading activity

B. User Statistics

To analyze user behavior, we cluster trades in the dataset into entities based on common pay-out addresses a_{out} or shared e-mail addresses $@mail$. This clustering process is repeated until no new trades are assigned to a cluster. It's crucial to note that entities may not correspond to individual users, as a user with two trades using different pay-out addresses without supplying an e-mail address would be assigned to two entities.

A total of $10,484$ entities were identified, with an average of 2.25 trades per entity (median 1) and an average exchanged value of $\$1,855.09$ (median $\$68.35$). The data suggests that a small group of entities dominates Evonax's trading activity, both in terms of executed trades and exchanged value. Figure 2 displays the cumulative share of overall trading volume and activity, ranking entities by the number of trades and the sum of exchanged value. Notably, 39 entities (or 0.37%) accounted for over half of the overall trading volume, while $1,135$ entities (or 10.83%) executed half of the trades.

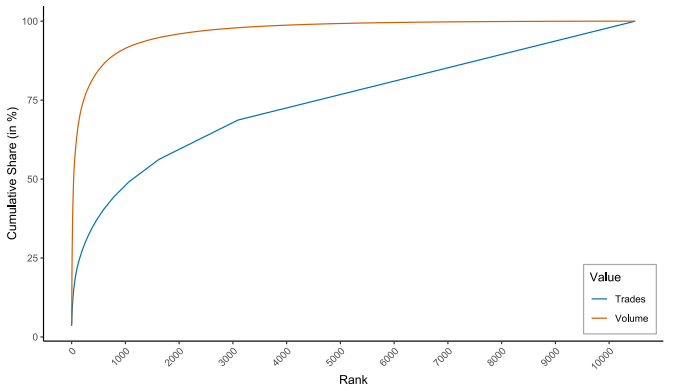

Fig. 2. Cumulative share of trading activity and volume

A similar disparity exists in the popularity of trading pairs among the 171 observed pairs. The top 10 pairs, ranked by exchanged value, collectively represent $\approx 77.5\%$ of the overall trading volume (refer to Table II). Notably, exchanges from Ether to Monero stand out as an outlier within the pairs, constituting over a quarter of the value exchanged on Evonax. This aligns with the trading peak observed in January 2021, where a significant portion of these trades occurred.

TABLE II
MOST POPULAR TRADING PAIRS

Pair	Total Volume	Median	Count
ETH → XMR	$ 5,019,394.95	$ 213.48	313
DOGE → BTC	$ 1,694,832.02	$ 157.03	755
BCC → BTC	$ 1,563,163.82	$ 46,656.89	48
BTC → XMR	$ 1,497,182.09	$ 144.21	2,947
LTC → XMR	$ 1,428,920.31	$ 125.59	391
ETH → BTC	$ 1,092,772.68	$ 478.71	288
BTC → PAYPAL	$ 798,980.40	$ 56.18	4,498
XMR → ETH	$ 748,816.41	$ 150.27	261
BTC → DOGE	$ 640,636.03	$ 21.57	4131
XMR → BTC	$ 592,118.26	$ 788.68	159

VI. CASE STUDIES

In this section we investigate unusual observations included in our data, aiming to provide explanations for outliers and noteworthy events.

A. Trading Peak in August 2021

In late August 2021, Evonax witnessed a substantial surge in trading volume, with total trades reaching $\approx \$6,800,000$, before sharply dropping to $\approx \$130,000$ in September 2021. Our investigation traced this spike back to 68 high-value trades between August 20 and September 01, 2021, involving Ether and Litecoin exchanged for Monero, ZCash, Dash, Dogecoin, and Bitcoin Cash. A total of 54 Ether trades sold $1,604.05$ ETH ($\approx \$5,160,000$), and 16 Litecoin trades sold $10,47.269$ LTC ($\approx \$1,760,000$).

All these trades seemed closely linked, with Ether deposits originating from 13 addresses, ultimately connected to a single Ethereum address[7], accumulating $\approx 5,360.6$ ETH ($\approx \$16,970,000$). The funds were then split into batches, each up to 122 ETH, and deposited on various exchanges.

Litecoin deposits stemmed from addresses in two peeling chains, both originating from addresses accumulating $18,201$ LTC ($\approx \$2,720,000$)[8]. Common email addresses and a shared Monero payout address further suggested a connection between the Ether and Litecoin trades.

Attempts to trace the origin of funds and the whereabouts of exchanged funds were inconclusive. Payouts in ZCash, Dash, Dogecoin, and Bitcoin Cash were forwarded to other addresses, presumably for storage, and have not been moved as of February 05, 2023. Tracking the exchanged Monero coins proved impossible due to Monero's privacy-preserving design.

Between October 06 and October 09, 2021, trading activity resumed with 5 trades exchanging 39 ETH ($\approx \$140,000$) for Monero, Bitcoin, and Dogecoin. Subsequent transactions using the Dogecoin and Bitcoin payouts showed no interactions with known addresses.

[7]0xbebb0ce4b28403c1b05ecd28e300c4db6b418032

[8]ltc1qzj69lwnjea99dkjgyy7rf5wx0vrx72g3lml0nc and LfQysUPZQu6otwFQwEP7DCZfSzgQTZ6nUT

TABLE III
COIN SWAPS BY CURRENCY

Currency	Count	Total Amount	Total Value
Ether	13	13.15206	$ 53,588.45
Litecoin	745	149.6992	$ 24,318.17
Bitcoin	36	0.827579	$ 9,523.45
Dogecoin	75	134,865.5	$ 2,840.00
Bitcoin Cash	2	0.1659801	$ 155.73
Tether	1	90.04	$ 89.99
Dash	5	0.26288	$ 69.30
Monero	2	0.1871228	$ 36.23
Total	**933**		**$ 90,621.37**

B. Coin Swaps

Certain exchanges, such as ChangeNOW and Evonax, offer "coin swaps", allowing users to exchange funds within the same currency, i. e. $\mathcal{C}_{in} = \mathcal{C}_{out}$. Despite the initial counterintuitiveness of trading money for a smaller amount of the same currency, Evonax's handling of the swaps hints towards possible use cases. Instead of merely forwarding deposited funds from the user's deposit address a_{dep} to the pay-out address a_{out}, coin swaps draw funds from *other* users' deposit addresses or, for account-based currencies, Evonax's hot wallet. This process conceals the true sender's address from the recipient, as $a_{dep} \notin A^{in}_{t_{out}}$. Consequently, coin swaps can serve as a means to obscure currency flows, making it challenging for external observers to trace fund movements.

To ascertain evidence of coin swaps being employed for currency flow obfuscation, we analyze relevant trades on Evonax, observing 933 coin swaps across 8 different currencies. Table III reveals Litecoin as the primary currency for coin swaps, with Ether standing out due to infrequent but high-value swaps. Subsequently, we focus on inspecting coin swaps in Ether, as it is the currency with the largest swapped values.

Ethereum Ethereum addresses engaged in swaps were manually inspected via Etherscan and its database of known addresses. The analysis identified a single source responsible for the majority of swapped Ether: On October 21, 2021, a total of around 12.93 ETH ($\approx$ $\$53,280$) were swapped in three trades. Strong evidence links these swaps to a *rug pull*, a fraudulent scheme involving the creation and listing of a worthless ERC-20 token on a (decentralized) exchange, followed by the removal of liquidity, deceiving victims into buying worthless tokens [9].

- 1^{st} swap: On October 21, 2021, an ERC-20 token named "DIO INU" was created, and one trillion DIO tokens and 2 ETH were supplied to a Uniswap v2 liquidity pool. Shortly afterward, the majority of the liquidity pool was drained, transferring around 327 billion DIO tokens and approximately 6.15 ETH back to the creator's address. Around 3.35 ETH were sent to Evonax, swapped, and paid to a deposit address[9] of the now-defunct exchange FTX.
- 2^{nd} swap: Approximately six hours later, 4 ETH from the FTX hot wallet were observed being sent to an Evonax deposit address[10], swapped, and paid to another Ethereum address[11].
- 3^{rd} swap: Using the same address, an ERC-20 token named "MADARA INU" was created, mirroring the first rug pull's procedure. Around 50 minutes after the second swap, 5.58 ETH were transferred to Evonax, swapped, and paid to the same FTX deposit address as the funds from the first rug pull. This suggests that Evonax was used to conceal the FTX user from rug pull victims and the rug pulls from FTX.

For the six other Ethereum swaps interacting with known addresses, no criminal activity was observed: Two swaps were part of a round-trip trade, exchanging currency for Ether, swapping Ether, and ultimately exchanging back to the original currency (BTC and USDT). In another two swaps, the swapped funds were forwarded to the same address initiating the swap. Two swaps involved other exchanges, with funds obtained from HitBTC and Kraken being swapped and, in one case, immediately deposited to Coinbase.

VII. DISCUSSION

Despite the powerful insights gained from our data analysis, generalizing our findings is challenging due to Evonax's small scale compared to industry leaders. Binance, for instance, had an hourly trading volume approximately 50 times greater than Evonax's total trading volume during the study period.

A fundamental challenge is the lack of a ground truth to assess dataset completeness. Trades exchanging funds between two currencies that were ignored in the blockchain analysis, and that were not otherwise connected to known trades, may not have been captured during data collection. Hypothetically, there could exist a set of trades entirely disconnected from all known trades, thus escaping our methodology. We rely entirely on Evonax's track exchange functionality, and any inaccuracies in its data, intentional or due to software bugs, would impact our dataset. However, there is no evidence of widespread issues. The initial trade in our dataset, by Evonax's owner on February 16, 2018, predates the service's first Internet Archive capture (May 23, 2018). Evonax's predecessor, *ExchangeMyCoins.com*, reported an average of 372 trades per month when sold in 2017, aligning with the 400 trades per month we observed [10]. This suggests our approach retrieved most trades until the service's inception.

Ultimately, the success of our analysis is constrained by available data, especially when exploring fund origin and destination, given the scarcity of reliable sources for identified cryptocurrency addresses. Researchers with access to more comprehensive data could potentially yield further insights.

[9] 0xb9df6eAeAA5238b3f64827a967cE5b9Fac215928

[10] 0x198207bcc810a4c653cc0ce0ca3b3cf6df06c737

[11] 0xd48049d09530356B169523243e44c8F982e4D062

REFERENCES

[1] K. N. Johnson, "Decentralized finance: Regulating cryptocurrency exchanges," *Wm. & Mary L. Rev.*, vol. 62, p. 1911, 2020.

[2] G. Le Pennec, I. Fiedler, and L. Ante, "Wash trading at cryptocurrency exchanges," *Finance Research Letters*, vol. 43, p. 101982, 2021.

[3] F. Victor and A. M. Weintraud, "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in *Proceedings of the Web Conference 2021*, ser. WWW '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 23–32. [Online]. Available: https://doi.org/10.1145/3442381.3449824

[4] J. Chen, D. Lin, and J. Wu, "Do cryptocurrency exchanges fake trading volumes? An empirical analysis of wash trading based on data mining," *Physica A: Statistical Mechanics and its Applications*, vol. 586, p. 126405, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378437121006786

[5] S. Bistarelli, I. Mercanti, and F. Santini, "A Suite of Tools for the Forensic Analysis of Bitcoin Transactions: Preliminary Report," in *Euro-Par 2018: Parallel Processing Workshops*, G. Mencagli, D. B. Heras, V. Cardellini, E. Casalicchio, E. Jeannot, F. Wolf, A. Salis, C. Schifanella, R. R. Manumachu, L. Ricci, M. Beccuti, L. Antonelli, J. D. Garcia Sanchez, and S. L. Scott, Eds. Cham: Springer International Publishing, 2019, pp. 329–341.

[6] A. Faccia, N. R. Moşteanu, L. P. L. Cavaliere, and L. J. Mataruna-Dos-Santos, "Electronic money laundering, the dark side of fintech: An overview of the most recent cases," in *Proceedings of the 2020 12th International Conference on Information Management and Engineering*, ser. ICIME 2020. New York, NY, USA: Association for Computing Machinery, 2020, p. 29–34. [Online]. Available: https://doi.org/10.1145/3430279.3430284

[7] H. Yousaf, G. Kappos, and S. Meiklejohn, "Tracing Transactions Across Cryptocurrency Ledgers," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, 8 2019, pp. 837–850. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/yousaf

[8] Evonax, "Trade bitcoin for cash - btc to advanced cash - evonax," https://www.evonax.com/exchange/btc/paypal, 2023, accessed: 2023-02-08.

[9] P. Xia, H. Wang, B. Gao, W. Su, Z. Yu, X. Luo, C. Zhang, X. Xiao, and G. Xu, "Trade or trick? detecting and characterizing scam tokens on uniswap decentralized exchange," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 5, no. 3, dec 2021. [Online]. Available: https://doi.org/10.1145/3491051

[10] CryptoNinjas.net, "Danish bitcoin exchange exchangemycoins.com goes up for sale," https://www.cryptoninjas.net/2017/05/06/danish-bitcoin-exchange-exchangemycoins-com-goes-sale/, Jul 2019, accessed: 2023-02-08.