International Journal of Network Management

WILEY

SPECIAL ISSUE PAPER OPEN ACCESS

Buy Crypto, Sell Privacy: An Extended Investigation of the Cryptocurrency Exchange Evonax

Alexander Brechlin | Jochen Schäfer | Frederik Armknecht

Chair for Dependable Systems Engineering, University of Mannheim, Baden-Württemberg, Germany

Correspondence: Jochen Schäfer (jochen.schaefer@uni-mannheim.de)

Received: 13 August 2024 | **Revised:** 18 November 2024 | **Accepted:** 7 January 2025

Keywords: blockchain privacy | cryptocurrency exchanges | cryptocurrency forensics

ABSTRACT

Cryptocurrency exchanges have become a multi-billion dollar industry. Although these platforms are not only relevant for economic reasons but also from a privacy and legal perspective, empirical studies investigating the operations of cryptocurrency exchanges and the behavior of their users are surprisingly rare. A notable exception is a study analyzing the cryptocurrency exchange *ShapeShift*. While this study described new heuristics to retrieve a significant fraction of trades made on the plaform, its approach relied on identifying cryptocurrency transactions based on previously scraped trade data. This limited the analysis to the timeframe for which data had been acquired and likely led to false negatives in the transaction identification process. In this paper, we replicate and extend previous work by conducting an in-depth investigation of the cryptocurrency exchange *Evonax*. Our analysis is based on actual trading data acquired by using a novel methodology allowing to extract detailed information from the public blockchain and the interface of the exchange platform. 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 not only to analyze the business practices of a cryptocurrency exchange but also to identify a number of interesting use cases that are likely to be associated with illegal activity. This paper is an extended version of a research article previously accepted at the CryptoEx Workshop at IEEE ICBC 2024.

1 | Introduction

Cryptocurrency exchanges nowadays constitute a multi-billion dollar industry with hundreds of competing platforms: As of August 2024, CoinMarketCap lists around 250 spot exchanges and approximately 500 decentralized exchanges.[1] These services are relevant not only for economic reasons but also from a privacy and legal perspective, as cryptocurrency payments are often perceived to be more private due to their pseudonymous nature.

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

One of the few examples is the study of Yousaf et al. which demonstrates that the interfaces of exchange platforms might inadvertently facilitate the cross-chain traceability of transactions. In their analysis, which is built on information acquired from the API of ShapeShift, they were able to identify the corresponding cryptocurrency transactions for 70%–90% of observed exchanges made on the platform [1]. However, their analysis was limited to the 13-month period during which they scraped the ShapeShift API and analysis of their data suggested that not all trades were correctly captured.

In summary, the sheer size of the cryptocurrency exchange industry, combined with its potential relevance to criminal activity, makes exchange platforms highly interesting and relevant, yet understudied subjects of scientific research.

In this study, we add fresh insights to the line of research started by Yousaf et al.: We conduct an in-depth investigation of the exchange Evonax,[2] analyzing the platform's internal workings, operations and business practices. Our case study is based on empirical data acquired from a newly developed method for identifying cryptocurrency transactions related to Evonax. Our key contributions are as follows:

- We reverse-engineer the way Evonax handles payments on the blockchain and thereby obtain information that can be used to acquire trade data from an interface provided by the platform. We turn this into a novel, fully automated and error-resistant method for extracting cryptocurrency trade data from Evonax.
- Employing this methodology, 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. This dataset is expected to encompass nearly all trades executed on the platform, as discussed in Section 8.
- We gain an understanding of the internal workings of Evonax. This includes information on the overall state of the platform like trading activity over time and also the sources of liquidity, the extent of liquidity reserves held by Evonax, and estimates of profit generated.
- We conduct case studies investigating particularly interesting findings in greater detail. More precisely, we identify a novel trading pattern in which funds are "exchanged" within the same currency. As these *coin swaps* always incur cost to the user, there is no obvious legitimate use for such trades and they might be indicative of money laundering or wash trading. Indeed, we find evidence that Evonax is being used to launder funds obtained from criminal activity, such as darknet markets, rug pulls, and hacking.

This paper is structured as follows. Section 2 gives an overview of related work. In Section 3, we discuss ethical aspects of our research. Technical background is provided in Section 4. In Section 5, we explain how Evonax trades have been acquired, using the blockchain and the Evonax *track exchange* form. Section 6 describes the analysis of the business practices of Evonax. In addition, several interesting use cases including the use of Evonax to launder money are discussed in Section 7. A critical discussion of our findings is conducted in Section 8, while Section 9 concludes the paper.

2 | Related Work

Most studies dealing with cryptocurrency exchanges, particularly those from noncomputer science fields, tend to concentrate on regulation [2] and criminal activities like wash trading [3–5] and money laundering [6, 7].

To our knowledge, 2019 paper of Yousaf et al. is the sole work investigating trading behavior on cryptocurrency exchanges using actual trading data from blockchain analysis and exchange APIs [1]: 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 nicely complements the work of Yousaf et al. by performing a similar analysis for a different exchange platform. We reverse-engineer the internal payment processing mechanisms of the exchange platform Evonax, allowing us to extract a comprehensive dataset of nearly the entire trade history. Using this dataset, we investigate possible use cases, notably identifying a novel trading pattern termed "coin swaps" and linking some trades to criminal activities. We also gain insights into operational details such as sources and extent of liquidity reserves and user statistics. Additionally, our study addresses the key limitations Yousaf et al. identified with their approach (See Section 5.1 of their paper):

- False positives, that is, addresses being identified as belonging to a ShapeShift trade when they are actually unrelated, may occur when users reuse deposit addresses shortly after completing trades. This can happen because the ShapeShift API only returns data on the most recent trading activity associated with an address. In such a scenario, transactions might be matched to the wrong trade. Our approach addresses this limitation by using the Evonax interface, which not only provides all trades associated with each deposit address but also uniquely matches these trades to specific cryptocurrency transactions. This effectively eliminates the possibility of false positives resulting from address reuse.
- False negatives, that is, transactions that belong to a trade but are not captured by their heuristics, may arise from the need to match transactions using nonunique criteria such as value and timestamps, which requires searching the blockchain for potential matches. Our approach avoids this problem by deriving candidate addresses directly from the information provided by the Evonax interface as well as the deterministic structure of Evonax-related cryptocurrency transactions.
- Yousaf et al. search for matching cryptocurrency transactions based on the trade information returned by the ShapeShift API. Trades not included in the API response cannot be identified by their methodology, as their characteristics are not known. This can be problematic, because API only returns the 50 most recent trades made on the platform and does not allow retroactive queries. Consequently, the analysis of Yousaf et al. was limited to the timeframe in which they consistently queried the API (November 2017 to December 2018). Evidence suggests that even during this time, not all ShapeShift trades were actually captured, presumably due to situations in which more than 50 trades occurred between two consecutive API calls. Our approach, however, is not bound by these limitations, as we can retroactively generate candidate

addresses through the Evonax interface and blockchain data, ensuring comprehensive trade activity coverage and avoiding dataset gaps.

Our study also takes a security and privacy perspective, as it highlights potential privacy issues that can arise from granting access to exchange trade data too freely. Here, our work is embedded in a corpus of existing literature that exploits meta-information to identify blockchain transactions. Such information is recurring transaction patterns from cryptocurrency services such as darknet markets [8, 9] and exchanges [10].

Disclosure and Ethical Considerations

Our study involves the analysis of financial and usage data of exchange customers without their explicit consent, raising ethical and legal questions. The research design received approval from our institution's internal review board and adheres to the ethical framework provided by the *Menlo Report* [11], a widely used framework in IT security research.

Respect for Persons: While obtaining informed consent from all affected individuals was desirable, it was not feasible due to the specifics of our research. Contacting users would only have been possible through email addresses, known for only ≈ 66% of users, and finding these addresses was a byproduct of the analysis itself. Consequently, seeking consent before analysis was not possible. Research without consent can be justified if the risk is minimal and lacking consent does not adversely affect subjects' rights and welfare. Therefore, we report findings in a manner preventing the identification of individual users.

Beneficence: Our research aims to raise awareness of privacy implications of cryptocurrency-based services. Its publication is intended to help platform operators avoid similar errors, contributing to improved user security. To balance scientific interests and user privacy, associated data and code will not be publicly released, with conditional or limited access provided to other researchers.

Justice: Our research is focused on the small population of Evonax users, which are also the primary beneficiary. We believe that the risks and benefits to the target population are well balanced.

Respect for Law and Public Interest: Our research adheres to applicable laws, as confirmed through consultation with our institution's internal review board.

Responsible Disclosure We have disclosed our research, including the methodology, to Evonax via their customer support e-mail address on February 14, 2023. We have not received any response.

4 | Background

4.1 | Cryptocurrencies

Following the creation of Bitcoin, numerous different cryptocurrencies have emerged. While they all rely on publicly distributed ledgers to store the transaction history and thus, implicitly, the state of the system, there are differences in the way the information is stored and processed. We assume that readers are familiar with cryptocurrencies in general and only shortly outline the most relevant concepts.

4.1.1 | Transactions

In cryptocurrencies, the transfer of value is facilitated by transactions. Formally, a transaction t in currency C involves a set of input addresses A_t^{in} and output addresses A_t^{out}. A value v_a 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:

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

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.

4.1.2 | Account-Based Currencies and ERC-20 Tokens

In account-based cryptocurrencies like Ethereum, addresses are associated with accounts and account balances are explicitly stored as part of the global state. User addresses typically encode a public key and only transactions signed with the corresponding private key are authorized to withdraw currency from the account. Once a transaction is confirmed, the balances of the sending and receiving accounts are updated accordingly [12].

ERC-20 is a standard introduced in 2015 that defines common design criteria for fungible tokens on the Ethereum blockchain [13]. ERC-20 tokens, such as Maker, Dai Stablecoin or Uniswap, are implemented in smart contracts deployed on the Ethereum blockchain. They can be seen as a kind of meta-currency built on top of an existing blockchain ecosystem. Transaction fees resulting from the transfer of these tokens must still be paid in the underlying blockchain's native currency, which in the case of ERC-20 tokens is Ether. While different tokens may provide additional program logic, the basic functionality for token transfer is identical and defined in the standard. Software developed against the ERC-20 standard should be universally compatible with all ERC-20 tokens. Therefore, we will not distinguish between different ERC-20 tokens in this paper unless we are talking about observations specific to an individual token.

4.1.3 | UTXO-Based Currencies

In cryptocurrencies such as Bitcoin, Litecoin or Monero, value is stored in *unspent transaction outputs* (UTXOs). These outputs are generated by transactions and are associated with an amount of currency and a set of locking conditions. Addresses are a standardized and human-friendly way of encoding certain standard locking conditions. Subsequent transactions can consume a UTXO by referencing it in the transaction input and providing data that satisfies the locking conditions of the UTXO (typically a digital signature that matches a public key defined in the UTXO). Once the spending transaction is confirmed, the UTXO is spent and can no longer be used as a transaction input [14]. Unlike in account-based currencies, addresses do not

exist as entities on the blockchain and have no explicit balance associated with them. However, the balance equivalent can be calculated by summing the value of all UTXOs that are tied to the locking conditions specified by a given address. To keep the terminology simple, we will refer to this value as the address balance.

Importantly, UTXOs can only be spent as a whole. If the value of the spent UTXO does not match the desired value of the output, a second output storing the leftover funds is created. This so-called change output or change address can be used as an input to a subsequent transaction, which might itself produce change. A repeated occurrence of this pattern is commonly known as a *peeling chain* [15], since every transaction effectively "peels off" the initial, high-value UTXO.

4.2 | Cryptocurrency Exchanges

A cryptocurrency exchange facilitates the sale of a specified amount v_{in} of currency C_{in} in exchange for an amount v_{out} of currency 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 $C_{in} = C_{out}$. 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 4.1.1), while trade e describes the act of exchanging one cryptocurrency for another using a cryptocurrency exchange platform.

4.2.1 | Structure of a Trade

Regardless of their specific implementation, exchange platforms typically handle the trading process of cryptocurrencies in a similar way. This involves three transactions:

Pay-in transaction t_{in}: Users initiate a transaction t_{in}, transferring v_{in} within currency 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}.

Figure 1 provides an overview of these transactions, emphasizing the connection between them. 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:

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

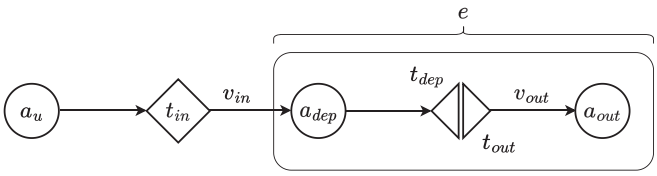

FIGURE 1 | Currency flow on a cryptocurrency exchange, trade highlighted.

The deposit transaction t_{dep} and pay-out transaction t_{out} are transactions in C_{in} and C_{out}, respectively. Notably, only "half" of each transaction is involved in a given trade, signifying that for t_{dep}, an input address $a_{dep} \in A^{in}_{t_{dep}}$ is known, and for t_{out}, an output address $a_{out} \in A^{out}_{t_{out}}$ is known. This is visualized in Figure 1 by the use of halved rhombs.

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}.

4.2.2 | Hot and Cold Wallets

While Figure 1 is an accurate description of a trade from a user's perspective, it does not make any statements about how the exchange internally processes the payments: The role of the addresses on the second half of the rhombs, that is, the addresses in $A^{out}_{t_{dep}}$ and $A^{in}_{t_{out}}$, might vary between exchanges or even among currencies on the same exchange, depending on their implementation of hot and cold wallets [10].

The *hot wallet* is a collection of cryptocurrency addresses actively used by the exchange for handling daily operations and short-term liquidity. Specifically, a pay-out transaction uses the hot wallet as an input [10]. User deposits are typically forwarded from deposit addresses to dedicated hot wallet addresses, although using deposit addresses as a hot wallet is also feasible.

On the contrary, *cold wallets* are reserved for long-term storage of an exchange's funds. Usually air-gapped from the internet, cold wallets offer a more secure storage solution compared to hot wallets connected to platform systems [10]. For security reasons, excess liquidity is regularly transferred to the cold wallet. Transactions spending from cold wallets are infrequent but may occur, such as when exchanges need to replenish liquidity in a hot wallet.

4.3 | Evonax

Evonax is a cryptocurrency exchange supporting crypto-to-crypto exchange of 10s native cryptocurrency coins and nine ERC-20 tokens. 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 [16].

Crypto-to-fiat trades using AdvCash were also discontinued in February 2022. Table 1 provides an overview of currencies and payment methods once supported by Evonax, indicating whether they could be used for deposits (sell), payouts (buy), and their current status as of August 2024.

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 C_{in} and 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 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 C_{in} and 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 7.3.

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

5 | 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.

TABLE 1 | Payment methods supported by Evonax.

Name	Ticker	Type	Sell	Buy	Active
0x	ZRX	ERC-20	✓	✓	✓
Bitcoin	BTC	UTXO	✓	✓	✓
Bitcoin Cash	BCC	UTXO	✓	✓	✓
Bitcoin SV	BSV	UTXO	✓	✓	✗
Bitcoin Gold	BTG	UTXO	✓	✓	✓
Chainlink	LINK	ERC-20	✓	✓	✓
Compound	COMP	ERC-20	✓	✓	✓
Dai	DAI	ERC-20	✓	✓	✓
Dash	DASH	UTXO	✓	✓	✓
Dogecoin	DOGE	UTXO	✓	✓	✓
Ether	ETH	Account	✓	✓	✓
Litecoin	LTC	UTXO	✓	✓	✓
Maker	MKR	ERC-20	✓	✓	✓
Monero	XMR	UTXO	✓	✓	✓
Shiba Inu	SHIB	ERC-20	✓	✓	✓
Tether	USDT	ERC-20	✓	✓	✓
Uniswap	UNI	ERC-20	✓	✓	✓
Wrapped Bitc.	WBTC	ERC-20	✓	✓	✓
Zcash	ZEC	UTXO	✓	✓	✓
Bank Transfer	—	—	✓	✗	✗
PayPal	—	—	✗	✓	✗
Advcash	—	—	✗	✓	✗

(Continues)

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.

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:

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

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

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 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 include 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 C_{in} and C_{out} with the corresponding amounts and exchange rate, and optionally, an e-mail address $@mail$. Figure 2 illustrates the information available for a test transaction issued by us.

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:

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

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

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.

FIGURE 2 | Trade information shown in "Track Exchange"

This approach is part of the Extract procedures for both account-based and UTXO-based currencies.

As shown in Figure 3, it is possible to alternate between the blockchain- and interface-based procedures to iteratively discover additional trades made on the Evonax platform. Each procedure, applied to a trade as displayed in Equation (2), identifies (potentially) new trades: Given a deposit address, blockchain analysis reveals the output address of another trade, which can be used as a search key for the Evonax track exchange form. In turn, the trade information returned by the web interface includes a deposit address, which can again serve as the starting point for another blockchain analysis.

Note that each procedure can be applied to either t_{dep} *or* t_{out}, but not both. Thus, cases in which C_{in} is an account-based currency and C_{out} is a UTXO-based currency, and vice versa, can be handled by combining the appropriate procedures.

The subsequent part of this section describes exact implementation of the Extract procedures for the case of account-based cryptocurrencies (Section 5.1) and UTXO-based cryptocurrencies (Section 5.2).

5.1 | Account-Based Cryptocurrencies

In account-based currencies, Evonax uses a dedicated hot wallet consisting of a single address[5] a_{hot} to handle payments. All trades in which at least one of C_{in} and C_{out} is an account-based currency or ERC-20 token will cause transactions involving the hot wallet.

Users wishing to exchange Ether on Evonax have to send funds to an exchange-owned deposit address a_{dep}. Upon execution of the trade, Evonax issues a transaction t_{dep}, forwarding the funds to a_{hot}. Correspondingly, whenever a user exchanges other currencies for Ether or an ERC-20 token, a transaction t_{out} transferring funds from a_{hot} to the user-specified pay-out address a_{out} occurs. This process can also be seen in Figure 4, which visualizes the cryptocurrency transactions corresponding to a trade between two account-based currencies. In this figure, colors are used to highlight the two currencies involved.

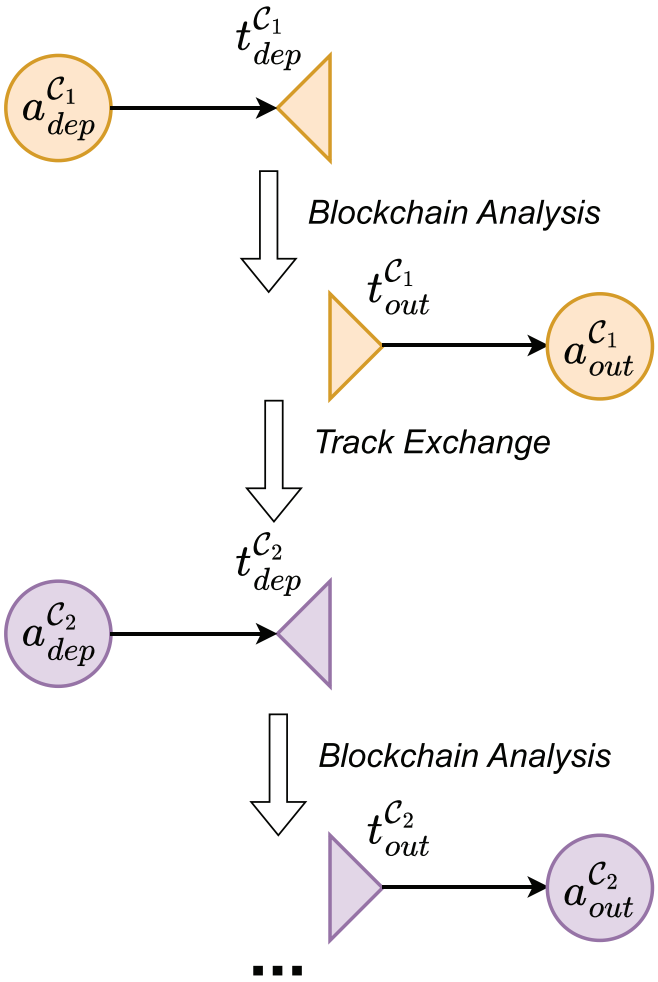

FIGURE 3 | Iterative data acquisition using blockchain and exchange interface (Color indicates currency).

In principle, the same transaction pattern also applies if an ERC-20 token is deposited. However, as the gas fees for t_{dep} have to be paid in Ether, two more transactions are necessary: After the user has deposited the ERC-20 tokens, a small amount of Ether gets transferred from a_{hot} to a_{dep} to cover gas fees. Afterwards, t_{dep} forwards the ERC-20 tokens to a_{hot}, using the previously transferred Ether for the gas fee. Finally, the remaining Ether are transferred back to a_{hot}. t_{dep} can still be identified, as it is the only transaction transferring tokens off a_{dep}.

Using this knowledge, the Extract procedures for trades involving Ether or an ERC-20 token are defined as follows:

Approach 1: Using t_{out}. Recall that the pay-out transaction t_{out} (the yellow transaction to the right of Figure 4) transfers funds from a_{hot} to a_{out}. Hence, Procedure (3) can be employed to obtain $A^{in}_{t_{out}} = \{a_{hot}\}$, which consists of a single address, namely, the hot wallet. From here on, we can proceed with approach 3, explained below.

Approach 2: Using a_{dep}. The deposit transaction t_{dep} (the green transaction to the left of Figure 4) will forward the deposited funds from $a_{dep} to a_{hot}$. If a_{dep} is known, we can thus use Procedure (4) to retrieve t_{dep}. Procedure (3) will then yield $A^{out}_{t_{dep}} = \{a_{hot}\}$. Extraction then proceeds with approach 3.

Approach 3: Using the hot wallet. Given the address a_{hot} of a hot wallet, new trades can be obtained in a two-step-procedure. First, the blockchain is queried according to Procedure (5), which outputs all transactions that transferred funds to the hot wallet:

$$a_{hot} \overset{\text{Blockchain}}{\mapsto} \left\{t \,|\, a_{hot} \in A^{out}_t\right\} =: T. \tag{8}$$

For each of those transactions $t \in T$, we apply Procedure (3) to get A^{in}_t, the potential deposit addresses. To decide for an address $a \in A^{in}_t$ if it is a deposit addresses, Evonax's track exchange page can be used: a is a deposit address if and only if Procedure (7) returns a trade when queried for the address. Otherwise, the address might serve a different purpose and is stored for further inspection.In the second step, the transactions transferring funds from the hot wallet are retrieved via Procedure (4):

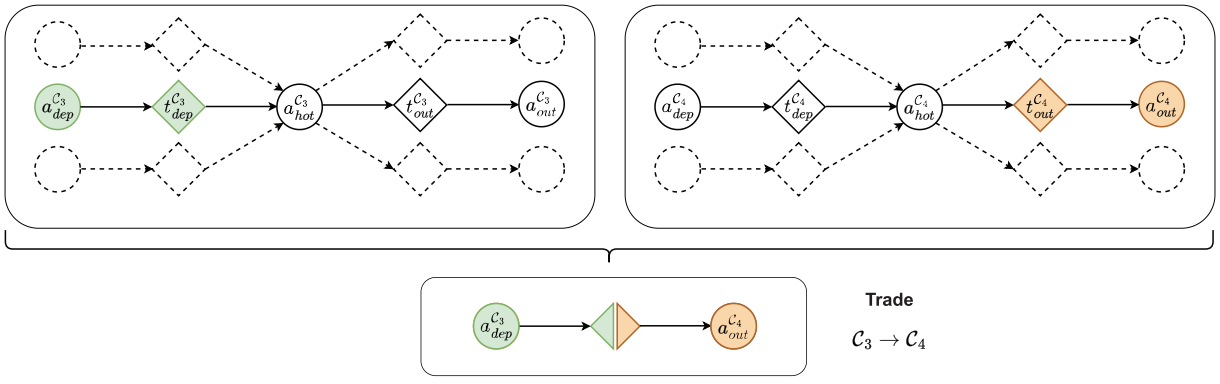

FIGURE 4 | Transaction structure of Evonax trades involving account-based currencies (color indicates currency).

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

Similar to the previous step, we get a potential pay-out address for each transaction $t \in T$ by applying Procedure (3). Again, true pay-out addresses in A_t^{out} are identified through Evonax's track exchange page and non–pay-out addresses are collected for further analysis.

5.2 | UTXO-Based Cryptocurrencies

For account-based currencies, our data acquisition methodology exploited the fact that Evonax uses a single hot wallet that is connected to all deposit- and pay-out-addresses. In UTXO-based currencies however, Evonax does not maintain such a dedicated hot wallet. Instead, all deposit addresses collectively serve as a kind of hot wallet, meaning that they are used as inputs to a pay-out transaction. Note that this design implies that each transaction simultaneously serves as a deposit transaction for one trade and a pay-out transaction for another trade. Given an Evonax trade, this allows us to derive additional trades using the pay-out transaction t_{out} or the deposit address a_{dep}. Figure 5 is a graphical representation of the transactions relating to trade between a pair of UTXO-based currencies, where the different colors once again represent the two currencies involved.

Approach 1: Using t_{out}. The first approach makes use of the fact that a trade specifies a pay-out transaction t_{out}. Procedure (3) allows to determine the set of all input addresses $A_{t_{out}}^{in}$ sending funds to and output addresses $A_{t_{out}}^{out}$ receiving funds from the transaction. From these sets, further trades can be derived.Here, we take advantage of the fact that the same transactions can be involved in multiple trades. More precisely, a transaction t_{out} can be the pay-out transaction for several trades at the same time, that is, there can be two different trades $e \neq e'$ such that

$$\begin{aligned} e &= (\ldots; C_{out}, a_{out}, v_{out}, t_{out}), \\ e' &= (\ldots; C_{out}, a_{out}{}', v_{out}{}', t_{out}). \end{aligned}$$

This is indicated by the dashed lines to the *right* of the transactions in Figure 5. We may derive pay-out addresses of additional trades from the set $A_{t_{out}}^{out}$ with Procedure (3). This requires distinguishing pay-out addresses from other elements of $A_{t_{out}}^{out}$, such as change addresses. To this end, one can use the Evonax interface again: $a^* \in A_{t_{out}}^{out}$ is a pay-out address if and only if the Evonax interface returns a trade (cf. Procedure (7)) when queried for a^*.If $a^* \in A_{t_{out}}^{out}$ is not a pay-out address, Procedure (4) is used to find a transaction t^* that has a^* as an input address, that is, $a^* \in A_{t^*}^{in}$. a^* is a change address if and only if there exists at least one $a \in A_{t^*}^{out}$ for which Procedure (7) returns a trade. In case a^* is a change address, it can be treated as a deposit address in approach 2. If a^* is neither a change address, nor a pay-out address, it probably forms part of the liquidity management process and is further investigated in Section 6.4.

Approach 2: Using a_{dep}. The second approach uses the deposit address a_{dep} specified in a trade. As a_{dep} is trade-specific, one can extract the corresponding deposit transaction t_{dep} from the blockchain. Similar to the fact that $A_{t_{out}}^{out}$ may refer to the pay-out addresses of several users, it holds that $A_{t_{dep}}^{in}$ may refer to the deposit addresses of several trades. This is indicated by the dashed lines to the *left* of the transactions in Figure 5. Formally, there can be two different trades $e \neq e'$ such that

$$\begin{aligned} e &= (C_{in}, a_{dep}, v_{in}, t_{dep}; \ldots), \\ e' &= (C_{in}, a_{dep}{}', v_{in}{}', t_{dep}, \ldots). \end{aligned}$$

In fact, we observed that three different types of addresses can be found in $A_{t_{dep}}^{in}$: deposit addresses, change addresses, and other. To distinguish between these types, one can use the Evonax interface again in a way analogous to the procedure described in approach 1.

Approach 3: Using transactions shared across trades. So far, we exploited that an input transaction t_{dep} may combine multiple deposit addresses as inputs and likewise an output transaction t_{out} may combine several user addresses as outputs. In the case of Evonax, however, a transaction t_{out} can be the pay-out transaction of some trade e and, at the same time, the deposit transaction of another trade e', that is,

$$\begin{aligned} e &= (\quad \ldots \quad ; \quad C_{out}, a_{out}, v_{out}, t_{out}) \\ e' &= (\, C_{in}{}', a_{dep}{}', v_{in}{}', t_{out} \, ; \quad \ldots \quad). \end{aligned}$$

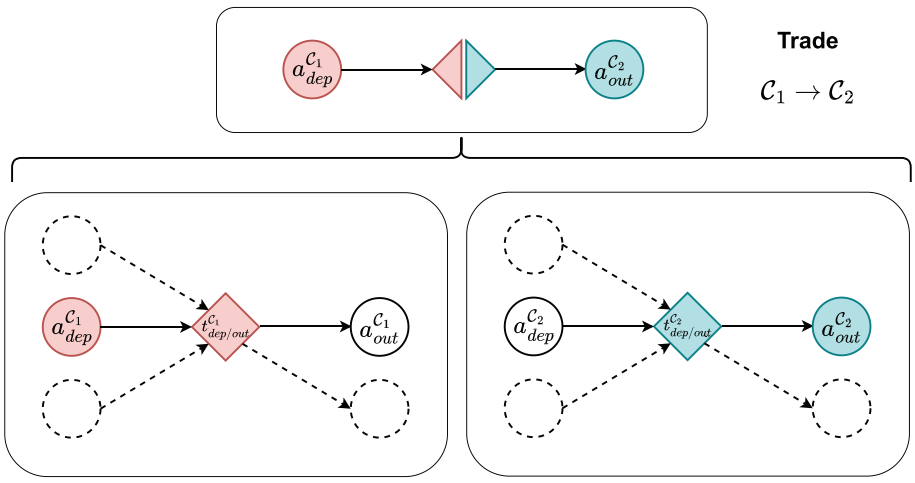

FIGURE 5 | Transaction structure of Evonax trades involving UTXO-based currencies (Color indicates currency).

That is, the inputs $A^{in}_{t_{out}}$ of a pay-out transaction t_{out} typically reveal further deposit addresses (and hence trades).Likewise, a transaction t_{dep} can simultaneously be the deposit transaction of some trade e and the pay-out transaction of one another trade e', that is,

$$\begin{aligned} e &= (\, C_{in}, a_{dep}, v_{in}, t_{dep} \;\; ; \;\; \dots \;\;) \\ e' &= (\, \dots \;\; ; \;\; C_{out}{}', a_{out}{}', v_{out}{}', t_{dep}). \end{aligned}$$

In Figure 5, this is represented by the white deposit- and pay-out-addresses that are connected to the transactions, but not part of the specified trade. This property allows us to combine the first two approaches:By applying approach 2 to the so-far unused input addresses of the pay-out transaction obtained in approach 1, $A^{in}_{t_{out}}$, we may find further trades. Correspondingly, we may apply approach 1 to $A^{out}_{t_{dep}}$ of the deposit transaction t_{dep} that is already processed in approach 2.

6 | Exchange Operations

While all exchange platforms offer similar services, they can be operated in various ways. This section reconstructs the business decisions made by the Evonax operators and the behavior of its user base.

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 carried out successfully, while Evonax reported a failure or an unclear status for the remaining ones. 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.

6.1 | 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 2.

As shown in Figure 6, 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 7.2.

TABLE 2 | Total and average yearly trading volume.

Year	Trades	Total volume	Average	Median
2018	1815	$ 485,375.99	$ 267.42	$ 11.30
2019	2307	$ 386,830.42	$ 167.68	$ 8.23
2020	6601	$ 2,507,694.79	$ 379.90	$ 35.22
2021	11,030	$ 14,666,685.61	$ 1329.71	$ 61.32
2022	1847	$ 1,402,123.84	$ 759.14	$ 71.30
Total	23,600	$ 19,448,71	$ 824.10	$ 44.20

6.2 | 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 is 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 $1855.09 (median $68.35). The data suggest that a small group of entities dominates Evonax's trading activity, both in terms of executed trades and exchanged value. Figure 7 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 1135 entities (or 10.83%) executed half of the trades.

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 3). 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.

6.3 | Revenue Through Fees

Evonax promotes its service as “fee-free” [17], instead incorporating a markup into the exchange rate. A comparison with Google Finance data reveals that Evonax rates are consistently $\approx 5\%$ below the reference rate. Similar services, which also include fees in exchange rates and offer instant exchanges with fixed rates, such as Changelly and Simpleswap, offer rates between 1.3% and 1.9% below the reference rate. Even when compared with these competitors, Evonax stands out as relatively expensive.

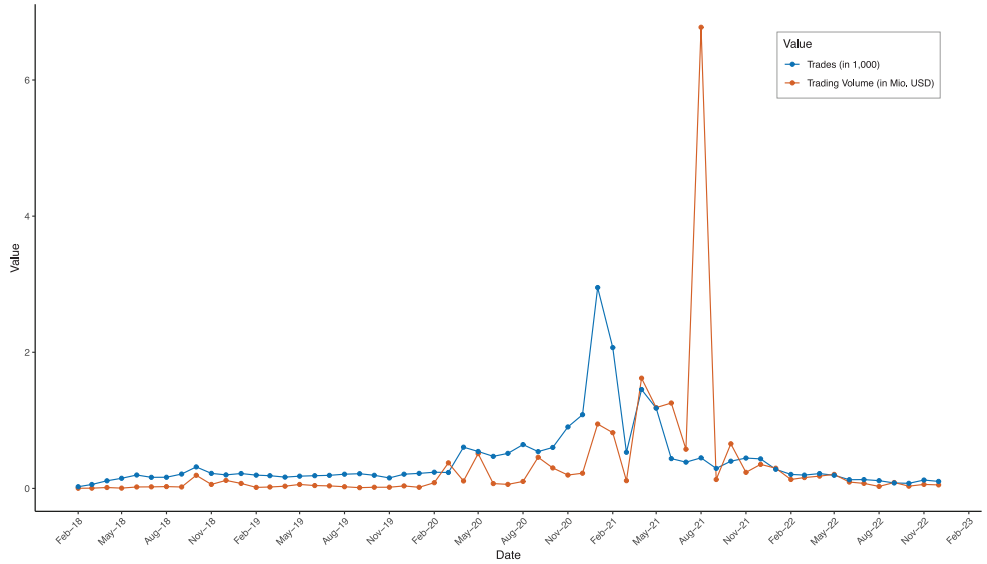

FIGURE 6 | Monthly trading volume and trading activity.

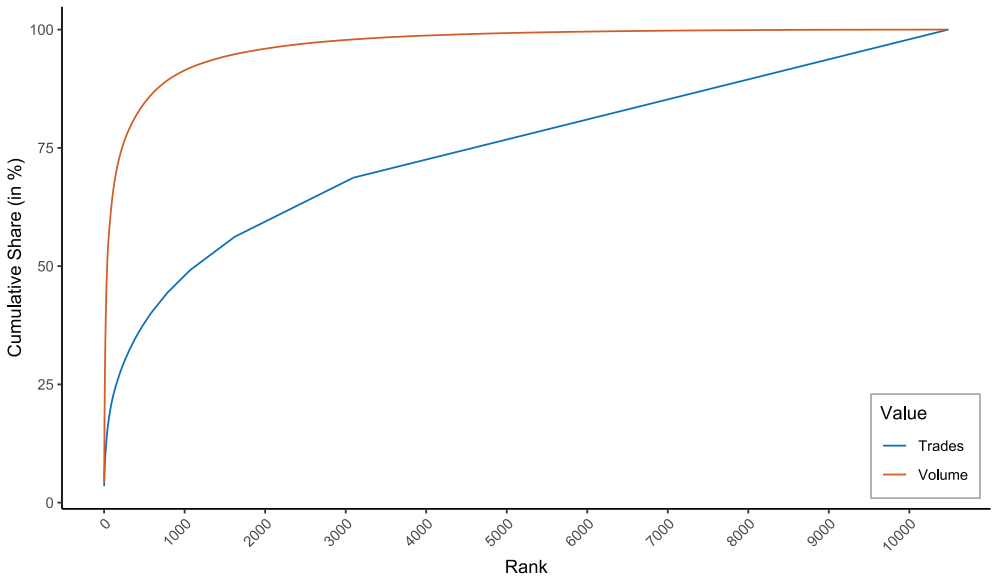

FIGURE 7 | Cumulative share of trading activity and volume.

For intracurrency exchanges, Evonax charges an effective fee at $\approx 1\%$ of the trading volume. Transactions from cryptocurrencies to fiat (via PayPal or AdvCash) incur a 10% fee.

Considering this information alongside trading volume data, we estimate Evonax's overall revenue from trades. The effective fee for each trade in the database is calculated and converted to US dollars based on the market exchange rate at the time of the trade. The estimated lifetime revenue totals $\approx \$1{,}000{,}000$, with a breakdown by year and transaction type shown in Table 4. Swap trades, where $C_{in} = C_{out}$, are further explained in Section 7.3. It is important to note that this represents the income generated from the markup on the exchange rates only.

6.4 | Liquidity

In our context, liquidity refers to the exchange's "cash reserve", specifically the amount of cryptocurrency stored on addresses under Evonax's immediate control. Sufficient liquidity is vital for seamless exchange operations. However, maintaining substantial cryptocurrency holdings inherently introduces volatility risks. To mitigate this, exchanges may aim to minimize reserves by converting excess cryptocurrency into more stable assets like fiat currencies, with the option of relying on other platforms as liquidity providers when needed. While this approach partially addresses volatility risks, it comes with added operational costs and dependence on competitors. This section explores how Evonax deals with this trade-off.

TABLE 3 | 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

TABLE 4 | Generated revenue grouped by trade type.

Year	Swap	Other
2018	$ 8.42	$ 7269.08
2019	$ 11.68	$ 16,723.39
2020	$ 34.98	$ 152,165.90
2021	$ 757.75	$ 749,496.18
2022	$ 91.19	$ 69,650.22
Sum	$ 904.02	$ 1,012,167.03
Total	$ 1,013,071.05	

Ethereum Liquidity for Ether and ERC-20 Tokens is equivalent to the balances stored in the hot wallet. Figure 8 shows the development of the hot wallet's Ether balance over time. To test the hypothesis of Evonax utilizing other exchanges for liquidity management, we examined addresses sending funds to Evonax's hot wallet via Etherscan.[7] This analysis revealed 14 addresses associated with Binance, Kraken, and Kucoin, suggesting these exchanges contribute to Evonax's liquidity. To gather additional evidence, a test trade exchanging Litecoin for 0x (an ERC-20 token) was conducted. As the trade exceeded Evonax's 0x balence, the platform had to obtain additional funds to fulfill the trade. Indeed, the deposit transaction got confirmed,[8] but the trade was halted with a notice that technical support must transfer funds from a "cold wallet". A transaction[9] sending 0x tokens from a Binance address[10] to the Evonax hot wallet could be observed a few hours later. We see this as proof that Evonax obtains liquidity from competing exchanges.

In a subsequent step, addresses receiving payments from the Evonax hot wallet, excluding customer payout or deposit addresses, were analyzed. This uncovered deposit addresses for Binance, Kraken, Kucoin, Bittrex, and Coinbase. Over 130 transactions, featuring sizable amounts like 50 ETH or 100 ETH, indicated Evonax's potential sale of Ether to these exchanges. No fixed threshold triggering fund sale was identified, hinting at a potentially manual liquidity management process.

UTXO-based currencies: Liquidity analysis for UTXO-based currencies faces challenges due to Evonax's wallet structure, where liquidity is the aggregate balance of deposit and change addresses. Approximately 99.43% of Evonax addresses engaged in precisely two transactions, allowing the calculation of address balances at various timestamps. The exchange's overall liquidity is the sum of these balances, calculated daily at 00:00 UTC (cf. Figure 9).

To further analyze liquidity management, addresses not designated as deposit, change, or payout addresses are investigated. This examination uncovered addresses linked directly to major exchanges like Binance[11] and Kraken.[12] Using these addresses as inputs in a deposit transaction t_{dep}, funds were injected into Evonax's payment system, hinting towards their role for liquidity management. Similar connections to Binance[13] and Kraken[14] were identified on the output side of Evonax transactions, where these addresses received larger, smooth amounts of currency.

When multiple potential liquidity management addresses were found for a currency, their usage time frames aligned: one address's funds depleted through current operations while newly obtained liquidity was sent to another. After an overlap of about 1 month, the old address was entirely replaced by the new one.

6.5 | Payment Processing

Requiring a certain number of confirmations, defined as blocks mined on top of the one containing a transaction, is a standard practice to enhance security against double-spending attacks and address nonmalicious chain splits [18]. Evonax displays the confirmation threshold to users post-trade, detailed in Table 5 by currency.

Notably, the universal confirmation settings are one block for UTXO-based currencies and six blocks for Ethereum and ERC-20 tokens, considerably fewer than competitor exchanges [19, 20].

There exists a minimum value threshold for trades, determined by C_{out}. Generally, currencies with lower network fees (e.g., Litecoin) have lower thresholds than ERC-20 tokens and especially Bitcoin. However, some thresholds are not plausible. As of January 26, 2023, swapping 1.768 USDT for 1.50 USDT could potentially incur Ethereum transaction gas fees surpassing the trade's profit: In the month prior to our analysis, USDT-Transactions transferring funds from deposit addresses to Evonax's hot wallet and from the hot wallet to the pay-out addresses were found to cost between $0.82 and $1.44 in gas fees.

7 | Case Studies

This section investigates cases that were either outliers in the data or could be evidence of criminal activity.

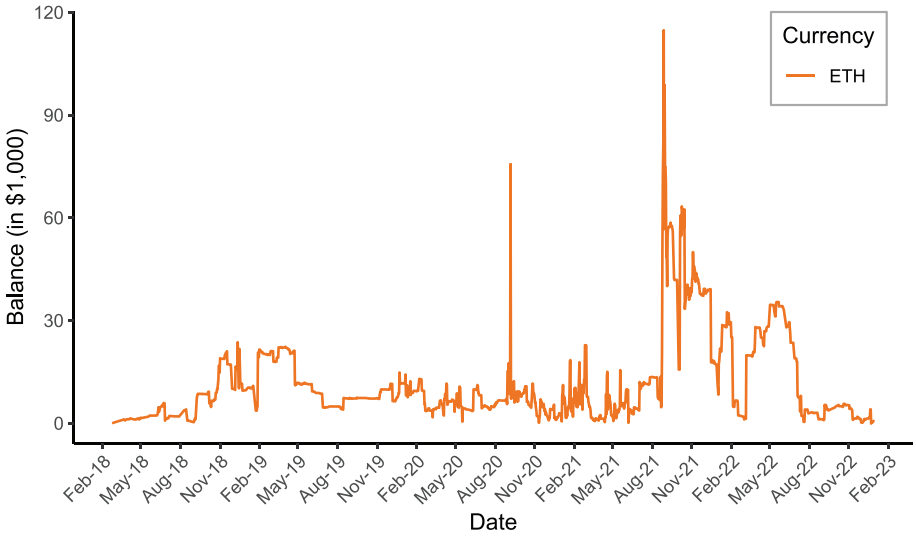

FIGURE 8 | Balance of Evonax's ETH hot wallet over time (in 1000 US dollar).

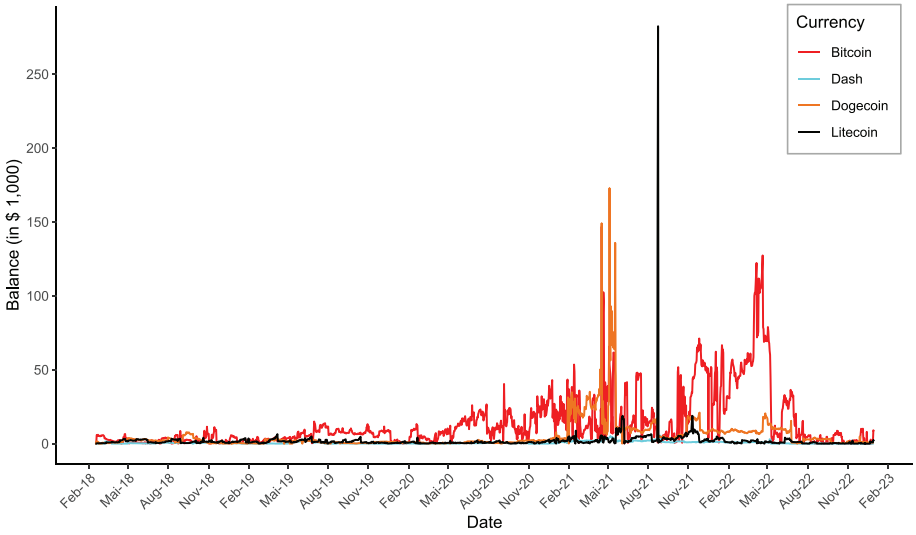

FIGURE 9 | Evonax's balance in select UTXO-based currencies over time (in 1000 US Dollar).

7.1 | Upbit-Hack

Addresses interacting with Evonax were cross-referenced with databases of known criminal and malicious activity, including the Bitcoin Abuse Database[15] and Etherscan's[16] set of labeled addresses.

This revealed a potential link between deposits on Evonax and an address associated with the hack of *Upbit*. On November 27, 2019, 342,000 ETH (≈ $45,000,000) were stolen from the south korean exchange platform [21]. Blockchain research by Cylynx traced the movement of the stolen funds across various wallets, with attempts being made to launder the money through exchanges [22]. At least 255,000 of the stolen Ether were sent to various exchanges. On December 21, 2019, two Evonax trades were observed, exchanging 50 ETH (≈ $6,360) for Bitcoin. The address[17] depositing the Ether in two trades to Evonax was flagged as being connected to the *Upbit hack*. Both trades use unique deposit addresses[18] but used the same Bitcoin payout address.[19] Further analysis of the receiving Bitcoin address, which was not present in relevant databases, indicated payments to Binance deposit addresses, suggesting yet another exchange of funds.

7.2 | Trading Peak in August 2021

In late August 2021, Evonax witnessed a substantial surge in trading volume, with total trades reaching ≈ $6,800,000, sharply dropping to ≈ $130,000 in September 2021. Our investigation traced this spike 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 (≈ $5,160,000), and 16 Litecoin trades sold 10,47.269 LTC (≈ $1,760,000).

All these trades seemed closely linked, with Ether deposits originating from 13 addresses, ultimately connected to a single Ethereum address,[20] accumulating ≈ 5,360.6 ETH

TABLE 5 | Block confirmations until deposit is confirmed and minimum exchange value (as of February 6, 2023).

Currency	Blocktime	Confirmations	Min value
Bitcoin	10:00	1	$84.10
Dash	02:30	1	$0.47
Dogecoin	01:00	1	$0.68
Litecoin	02:30	1	$1.43
Bitcoin Cash	10:00	1	$0.50
Ethereum	00:14	6	$4.80
ERC-20 token	00:14	6	—
Zcash	01:15	1	$0.17
Monero	02:00	1	$3.65

(≈ $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 (≈ $2,720,000).[21] 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.

Between October 6 and October 9, 2021, trading activity resumed with 5 trades exchanging 39 ETH (≈ $140,000) for Monero, Bitcoin, and Dogecoin. Subsequent transactions using the Dogecoin and Bitcoin payouts showed no interactions with known addresses.

7.3 | Coin Swaps

Certain exchanges, such as ChangeNOW and Evonax, offer "coin swaps", allowing users to exchange funds within the same currency, i. e. $C_{in} = C_{out}$. 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 6 reveals Litecoin as the primary currency for coin swaps, with Ether standing out due to infrequent but high-value swaps.

TABLE 6 | 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	$ 9523.45
Dogecoin	75	134,865.5	$ 2840.00
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

Subsequently, we focus on inspecting coin swaps in Litecoin, Ether, and Bitcoin, as they represent the currencies 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 (≈ $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 [23].

- First 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[22] of the now-defunct exchange FTX.
- Second swap: Approximately 6 h later, 4 ETH from the FTX hot wallet were observed being sent to an Evonax deposit address,[23] swapped, and paid to another Ethereum address.[24]
- Third swap: Using the same address, an ERC-20 token named "MADARA INU" was created, mirroring the first rug pull's procedure. Around 50 min 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.

Litecoin Out of 745 Litecoin swaps occurring from May 27, 2021, to January 30, 2022, 699 were initiated by the same entity, swapping a total of $23,275 to four different pay-out addresses. The individual trades ranged between $1.46 and $167.14. Three of these pay-out addresses exhibited transactional patterns suggestive of institutional ownership, with funds sent to these addresses being combined with hundreds of other inputs in transactions transferring large quantities of Litecoin to one or two recipients. Due to the scarcity of publicly identified Litecoin addresses, confirming whether these addresses belonged to exchanges or other services proved challenging. The associated e-mail address could be linked to a real-world identity, including name and place of residence. The remaining Litecoin swaps were not investigated due to their low volume.

Bitcoin While examining Bitcoin swaps, transactions sending to the deposit address and spending from the pay-out address were manually checked for known addresses using KYCP.org/oxt.me. Peeling chains were considered to determine the actual origin of deposits and additional recipients of swapped funds. This identified 20 swaps with at least one side having a clear connection to known addresses. Seven trades had deposited coins originating from other exchanges: Paxful (five), Bitstamp, and Coinbase (one each). In nine cases, swapped funds were (partially) sent to Cryptonator (three), Binance (two), Bitstamp (two), Bitfinex, and Coinbase (one each). One trade was found that swapped coins bought on Paxful and deposited the received funds to Bitstamp. Additionally, three swaps had a connection to Hydra Market, a now-defunct darknet market (two on input, one on output).

8 | 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. Replicating our study is hindered by the absence of similar cryptocurrency exchanges offering data comparable to Evonax's track exchange page. Nevertheless, we believe our work contributes significantly to the limited research on cryptocurrency exchanges, especially concerning criminal use. The suspicious trading behavior observed on a lesser-known, high-fee exchange like Evonax may signal an industry-wide phenomenon.

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 [24]. 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.

8.1 | Generalizability

In theory, the data acquisition methodology presented in this paper could be applied to other cryptocurrency-based services or exchanges as well. This would require that the service in question fulfills three main criteria:

Deterministic transactions patterns: Certain actions on the platform, for example, executing a trade, must trigger cryptocurrency transactions that are observable on the blockchain. These transactions must be deterministic, meaning that the same type of action will always cause a transaction with the same general structure. This enables the reverse-engineering of the payment processing.

Linkability: Once the payment process is known, transactions triggered by actions on the platform must be linkable. Such a link can either manifest in the blockchain, for example, if a service routes all payments through a singular hot wallet or in off-chain data provided by the service. An example of the latter would be the link between the deposit transaction and the pay-out transaction of a trade provided by the Evonax interface that could not be derived from blockchain data alone. This is crucial for iteratively retrieving additional addresses potentially belonging to the service.

API availability: The platform must provide an API that allows to decide whether a given address or transaction is related to the service. Without such an API, address identification is prone to false positives. Ideally, the API should also return additional information on the action that triggered the transaction, as this allows for a more detailed investigation of the service.

Currently, we are not aware of any active services or platforms that fulfill all three criteria. However, adapted versions of our approach might be applicable even if not all conditions are met, likely at the cost of increased uncertainty.

9 | Conclusion

In this paper, we acquired a near-complete dataset of the trades carried out on the cryptocurrency exchange Evonax. Based on this data, platform operations and user behavior were analyzed. We were able to show that Evonax uses competing exchange services for liquidity management. The distribution of trading activity turned out to be rather skewed: A small share of users is responsible for the majority of activity on the platform, both in terms of volume and transaction count. A closer analysis of

individual phenomena produced evidence of the involvement of Evonax users in criminal activities: Not only did Evonax exchange funds supposedly originating from a hack, it was also used to hide currency flows related to rug pull scams. Very high volume trades exchanging Ether and Litecoin for Monero could also be an attempt to break the traceability of currency flows, although no definitive proof was found. Overall, our research supports claims that cryptocurrencies and cryptocurrency exchanges have ties to criminal activities. While this undoubtedly also holds for fiat currencies and traditional banks, future research could use our data and methodology to estimate the extent of the problem.

Acknowledgments

Open Access funding enabled and organized by Projekt DEAL.

Endnotes

[1] https://coinmarketcap.com/rankings/exchanges/.

[2] https://www.evonax.com/.

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

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

[5] 0x2ab5a95e5881ba190434bd2ca423f7f1e2106747.

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

[7] https://etherscan.io/.

[8] 2e8e581ac09646c5b2f533b546520f9dbfbfcee9f3417959fe8c9ad269a9f04e.

[9] 0xaf3da1c3cc0a5e1e2a3766435cf01acfed0bd355732d85d8113bc9678bd391ec.

[10] 0xdfd5293d8e347dfe59e90efd55b2956a1343963d.

[11] 3QAhqEKfugbFgyCn2ytmssn6LmVqUQx9RS.

[12] 16pQuacyotCknHaLNfQSg9rtYAxJRUdy51.

[13] 18bxPVpUZudJC43HPeQsGrzQnhJaxYqoor.

[14] 32zQJUJjkNkDKPsPXcXU1At2MAgNc9jN5g.

[15] https://www.bitcoinabuse.com/.

[16] https://etherscan.io/.

[17] 0xaf6d891deb703e6bd9d1f779578fb18c92a6852f.

[18] 0x7ae639e56d43d7fb2eab7722410e887ff2091006 and 0x87d56b85295a544c387498ca265b91771561c1d7.

[19] 1ER1Jkak265zRFiiB6yn7Xqd3iyakrEeLK.

[20] 0xbebb0ce4b28403c1b05ecd28e300c4db6b418032.

[21] ltc1qzj69lwnjea99dkjgyy7rf5wx0vrx72g3lml0nc and LfQysUPZQu6otwFQwEP7DCZfSzgQTZ6nUT.

[22] 0xb9df6eAeAA5238b3f64827a967cE5b9Fac215928.

[23] 0x198207bcc810a4c653cc0ce0ca3b3cf6df06c737.

[24] 0xd48049d09530356B169523243e44c8F982e4D062.

References

1. 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, 2019): 837–850.

2. K. N. Johnson, "Decentralized Finance: Regulating Cryptocurrency Exchanges," *William & Mary Law Review* 62 (2020): 1911.

3. G. Le Pennec, I. Fiedler, and L. Ante, "Wash Trading at Cryptocurrency Exchanges," *Finance Research Letters* 43 (2021): 101982.

4. F. Victor and A. M. Weintraud, "Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges," WWW '21, *Proceedings of the Web Conference 2021*, (New York, NY, USA: Association for Computing Machinery, 2021): 23–32.

5. 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* 586 (2022): 126405, https://doi.org/10.1016/j.physa.2021.126405.

6. S. Bistarelli, I. Mercanti, and F. Santini, "A Suite of Tools for the Forensic Analysis of Bitcoin Transactions: Preliminary Report," in *Europar 2018: Parallel Processing Workshops*, eds. 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 (Cham: Springer International Publishing, 2019): 329–341.

7. 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*, ICIME 2020, (New York, NY, USA: Association for Computing Machinery, 2020): 29–34.

8. X. Chen, M. A. Hasan, X. Wu, P. Skums, M. J. Feizollahi, M. Ouellet, et al., "Characteristics of Bitcoin Transactions on Cryptomarkets," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, eds. G. Wang, J. Feng, M. Z. A. Bhuiyan, and R. Lu (Cham: Springer International Publishing, 2019): 261–276.

9. J. Schäfer, C. Müller, and F. Armknecht, "If You Like Me, Please Don't "Like" Me: Inferring Vendor Bitcoin Addresses From Positive Reviews," *Proceedings on Privacy Enhancing Technologies* 2022, no. 1 (2022): 440–459.

10. G. Xue, Y. Li, and Z. Zheng, "Transparency to the Extreme: An In-Depth Study of the Bitcoin Exchange Ecosystem," in *Blockchain and trustworthy systems*, eds. H.-N. Dai, X. Liu, D. X. Luo, J. Xiao, and X. Chen (Singapore: Springer Singapore, 2021): 257–271.

11. D. Dittrich and E. Kenneally, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," U.S. Department of Homeland Security, (2012).

12. V. Buterin, "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform," (2013), https://github.com/ethereum/wiki/wiki/White-Paper.

13. F. Vogelsteller and V. Buterin, "Eip-20: Token Standard," *Ethereum Improvement Proposals* 20 (2015).

14. A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 1st ed. (O'Reilly Media, Inc., 2017).

15. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men With No Names," *Communications of the ACM* 59, no. 4 (2016): 86–93, https://doi.org/10.1145/2896384.

16. Evonax, "Trade Bitcoin for Cash - BTC to Advanced Cash - Evonax," Evonax, (2023), https://www.evonax.com/exchange/btc/paypal. Accessed: 2023-02-08.

17. Evonax.com, "Easy Crypto Coin Exchange - Evonax," (2023), https://www.evonax.com/. Accessed: 2023-02-08.

18. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (2008).

19. Coinbase, "Coinbase Help Center," Coinbase, (2023), https://help.coinbase.com/en/coinbase/getting-started/crypto-education/glossary/confirmations. Accessed: 2023-02-08.

20. Kraken, "Cryptocurrency Deposit Processing Times – Kraken," Kraken, (2023), https://support.kraken.com/hc/en-us/articles/

203325283-Cryptocurrency-deposit-processing-times. Accessed: 2023-02-08.

21. S. Lee, "Upbit - Press Release Suspension of Deposits," (2019), https://upbit.com/service_center/notice?id=1085.

22. Cylynx, "Tracing the Trail of the Upbit Hack," (2020), https://www.cylynx.io/blog/tracing-the-trail-of-the-upbit-hack/. Accessed: 2023-02-08.

23. P. Xia, H. Wang, B. Gao, W. Su, Z. Yu, X. Luo, et al., "Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange," *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 5, no. 3 (2021): 1–26, https://doi.org/10.1145/3491051.

24. CryptoNinjas.net, "Danish Bitcoin Exchange Exchangemycoins.com Goes Up for Sale," CryptoNinjas, (2019), https://www.cryptoninjas.net/2017/05/06/danish-bitcoin-exchange-exchangemycoins-com-goes-sale/. Accessed: 2023-02-08.