OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

WORKING PAPER 248

Assessing the Solvency of Virtual Asset Service Providers: Are Current Standards Sufficient?

Pietro Saggese, Esther Segalla, Michael Sigmund, Burkhard Raunig, Felix Zangerl, Bernhard Haslhofer

The *Working Paper series of the Oesterreichische Nationalbank* is designed to disseminate and to provide a platform for discussion of either work of the staff of the OeNB economists or outside contributors on topics which are of special interest to the OeNB. To ensure the high quality of their content, the contributions are subjected to an international refereeing process. The opinions are strictly those of the authors and do in no way commit the OeNB.

The Working Papers are also available on our website (http://www.oenb.at) and they are indexed in RePEc (http://repec.org/).

Publisher and editor *Oesterreichische Nationalbank*
Otto-Wagner-Platz 3, 1090 Vienna, Austria
PO Box 61, 1011 Vienna, Austria
www.oenb.at
oenb.info@oenb.at
Phone (+43-1) 40420-6666
Fax (+43-1) 40420-046698

Editor *Martin Summer*

Cover Design *Information Management and Services Division*

DVR 0031577

ISSN 2310-5321 (Print)
ISSN 2310-533X (Online)

Assessing the Solvency of Virtual Asset Service Providers: Are Current Standards Sufficient?

Pietro Saggese[1], Esther Segalla[2], Michael Sigmund[2], Burkhard Raunig[2], Felix Zangerl[3], Bernhard Haslhofer[4]

Abstract

Centralized cryptocurrency exchanges, which manage annual trading volumes on the scale of trillions of US dollars worldwide, are classified as virtual asset service providers (VASPs). They facilitate the exchange, custody, and transfer of cryptoassets organized in wallets across distributed ledger technologies (DLTs). As any corporation, VASPs can become insolvent. Despite the public availability of DLT transactions, their cryptoasset holdings are not yet subject to systematic auditing procedures. In this paper, we propose an approach to assess the solvency of a VASP by cross-referencing data from three distinct sources: cryptoasset wallets, balance sheets, and supervisory entity data. We investigate 24 VASPs registered with the Financial Market Authority in Austria. Regulatory data insights show that their yearly incoming and outgoing transaction volume amounts to 2 billion EUR for 1.8 million customers; the financial services they provide position them closer to brokers, money exchanges, and funds, rather than banks. Next, we empirically measure DLT transaction flows of four VASPs and compare their cryptoasset holdings to balance sheet entries. Data are only partially consistent; this enables us to identify gaps in the data collection and propose strategies to address them, towards achieving a more systematic, reliable, and automated assessment of VASPs solvency.

JEL Classification: C81, F31, G15, G20, G33, M41, 033
Keywords: *Blockchain, Solvency, Virtual Asset, VASP, Accounting, Auditing*

Email addresses: saggese@csh.ac.at (Pietro Saggese), esther.segalla@oenb.at (Esther Segalla), michael.sigmund@oenb.at (Michael Sigmund), burkhard.raunig@oenb.at (Burkhard Raunig), felix.zangerl@fma.gv.at (Felix Zangerl), haslhofer@csh.ac.at (Bernhard Haslhofer)

[1]Complexity Science Hub Vienna (CSH), Josefstaedter Strasse 39, 1080 Vienna, Austria and AIT - Austrian Institute of Technology, Giefinggasse 4, 1210 Vienna, Austria. *Corresponding author.*

[2]Oesterreichische Nationalbank (OeNB), Otto-Wagner-Platz 3, 1090 Vienna, Austria.

[3]Austrian Financial Market Authority (FMA), Otto-Wagner-Platz 5, 1090, Vienna, Austria.

[4]Complexity Science Hub Vienna (CSH), Josefstaedter Strasse 39, 1080 Vienna, Austria.

Non technical summary

Virtual asset service providers (VASPs) like centralized cryptocurrency exchanges are companies that facilitate financial activity involving virtual assets (VAs, also called cryptoassets), by enabling their exchange for other VAs or fiat currencies, their custody and transfer via cryptoasset wallets, and portfolio management services (FMA, 2021; EC, 2022; FATF, 2021).

Two major incidents that unfolded within the cryptoasset sector in 2022 highlight that the lack of proper accounting and business continuity concepts are a critical aspect of this industry (Zetzsche et al., 2023). In May, a bank run on the stablecoin Terra, a cryptoasset whose value was supposed to be pegged to the US dollar, contributed to the collapse of the companies Celsius and Voyager, and the hedge fund Three Arrows Capital. In November, the crypto trading platform FTX collapsed and filed for bankruptcy, leading to BlockFi's downfall and bankruptcy consideration for Aax and Genesis (The Economist, 2022). While VASPs activities involving fiat currencies are audited according to generally accepted accounting principles, cryptoassets are held in pseudo-anonymous wallets across multiple distributed ledgers (ElBahrawy et al., 2017) and are not yet systematically audited. However, transactions executed on distributed ledgers such as Bitcoin and Ethereum are public and can be observed, potentially opening new opportunities to enhance and automate the current auditing procedures.

Our paper aims to propose an approach for determining a virtual asset service provider's solvency status by measuring their cryptoasset holdings, to identify the limits of the current auditing and accounting procedures, and to suggest potential improvements. We investigate 24 VASPs registered with the Financial Market Authority in Austria and cross-reference data from three distinct sources: their cryptoasset wallets, balance sheet data from the commercial register, and information from supervisory entities.

Using information from the Austrian Financial Market Authority (FMA), we describe what cryptoassets VASPs support and what financial services they provide. We find that they typically operate using multiple cryptoassets, such as bitcoin (N = 20), ether (N = 16), and stablecoins (N = 12). Regarding their service offering, we note that the VASPs we analyzed do not provide saving deposits and loans as traditional banks do. Most of them facilitate the exchange of virtual assets for fiat currency (N = 20) or virtual assets (N = 9), and keep them in custody for their customers (N = 15). By comparing their activity to traditional financial intermediaries, we find that they are most similar to brokers, money exchanges, and funds, rather than banks.

Next, we concentrate the empirical analysis on four VASPs that have published their balance sheets, allowing to compare their cryptoasset holdings on Bitcoin and Ethereum wallets to their balance sheets. Their market share is around 99% of the total market share; the remaining VASPs are rather small companies. We find that data are consistent for two VASPs only.

This enables us to identify gaps in the data collection and propose strategies to address them. First, VASPs employ diverse approaches to manage their cryptoasset transfers, making more challenging to identify their cryptoasset holdings; second, even using a dataset containing more than 265,000,000 deanonymized Bitcoin addresses and 278,244 tagged Ethereum addresses, and having conducted manual transactions with the VASPs investigated, the resulting data only provide a partial view of their holdings; third, not all VASPs report balance-sheet items for crypto and fiat asset holdings separately, and VASPs may be subsidiaries of larger corporations and operate under multiple jurisdictions.

We therefore sketch out our vision for a more systematic, reliable, and highly automated assessment of proof of solvency. On the cryptoasset side, we remark that any entity in charge of auditing requires proof that a VASP actually controls the funds associated with its on-chain wallets. VASPs should disclose their cryptoasset wallets and provide additional metadata describing the use of these wallets. On the balance sheet side, reporting requirements for a VASP should report fiat and crypto asset and liability positions broken down by asset types at a reasonable frequency. We conclude by discussing how using cryptographic primitives and automation could improve the current assessment process.

1. Introduction

In 2022, the cryptoasset sector experienced a crash driven by two major incidents that exposed the repercussions of inadequate regulation and accountability in the industry. In May, Terra's algorithmic stablecoin protocol experienced a stablecoin run, similar to a bank run, on its associated cryptoassets LUNA and UST (Briola et al., 2022). This triggered the bankruptcy of the crypto lenders Celsius and Voyager, and the hedge fund Three Arrows Capital. In November, the crypto trading platform FTX filed for bankruptcy, leading to BlockFi's downfall and bankruptcy consideration for Aax and Genesis. Even more recently, in June 2023, the U.S. Security and Exchange Commission (SEC) brought forward charges against some of the largest U.S.-based VASPs (SEC, 2023).

These companies, and other centralized cryptoasset exchanges (CEXs) like FTX, fall under the broader definition of virtual asset service providers (VASPs). They facilitate financial activity involving virtual assets (VAs), such as their exchange for other VAs or fiat currencies, their custody and transfer via cryptoasset wallets, and portfolio management services for their customers (FMA, 2021).

As Figure 1 shows, VASPs lie at the interface of the traditional and the crypto financial ecosystems, respectively called *off-chain* and *on-chain* financial activity in jargon. The aforementioned and other (Moore et al., 2018) incidents that affected cryptoasset exchanges highlight a critical aspect of VASPs, i.e., the lack of proper accounting and business continuity concepts (Zetzsche et al., 2023). While their *off-chain* activities are audited according to generally accepted accounting principles, *on-chain* assets are held in pseudo-anonymous cryptoasset wallets across multiple, possibly privacy-preserving DLTs and are not yet systematically audited.

Whilst VASPs share several characteristics with traditional financial intermediaries, they are less regulated and their activities often lack transparency. Whether and how regulating them is an ongoing, highly controversial debate. A clear understanding of the financial functions VASPs provide, how they operate, and what risks are involved may provide guiding principles for regulators and policymakers.

This paper proposes an approach for determining a virtual asset service provider's solvency status by measuring their cryptoasset holdings. By solvency, we mean that the total amount of assets held in custody is larger than the total amount of liabilities, whereby the difference is equity. We investigate the VASPs registered with the Financial Market Authority (FMA) in Austria in the context of the Anti-Money Laundering Act. We compare data from three distinct sources: we rely on publicly available DLT transaction records from the Bitcoin and Ethereum DLTs and use established algorithms (Meiklejohn et al., 2016) to identify and cluster cryptoasset wallets likely controlled by the same entity. Then we reconstruct the VASPs' cryptoasset flows, compare their net positions to balance sheet data from the commercial register, and complement them with supervisory data from FMA.

To the best of our knowledge, our work is the first that combines these distinct sources in a unified framework. Also, a consolidated approach to measuring the types of cryptoassets held by VASPs against their liabilities to customers still does not exist, although their activity is based on DLTs whose transactions are publicly auditable by design.

Moreover, we position VASPs in the landscape of financial intermediaries, by systematically comparing the services they offer to those of traditional financial service providers. While previous research has compared VASPs to banks (Anderson et al., 2019), we discuss why this can be misleading. Our work provides the following contributions:

- We study 24 Austrian VASPs and systematize the services they offer. We find that they are most similar to *brokers*, *money exchanges*, and *funds*, rather than to *banks*;
- We provide regulatory data insights showing that their yearly incoming and outgoing transaction volume in 2022 amounted to 2 billion EUR for around 1.8 million users;

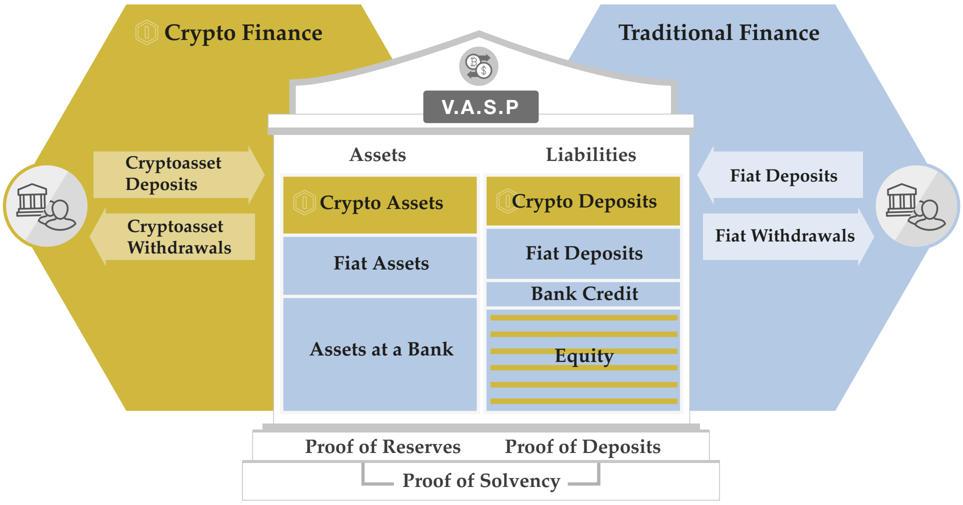


Figure 1: ***Virtual Asset Service Provider.*** *VASPs hold virtual assets in custody, transfer them, and facilitate their purchase and sale against fiat currencies and other virtual assets. Customers can interact with them by depositing or withdrawing cryptoassets through DLT-based transactions, or fiat currency via commercial banks.*

- We measure on-chain transaction flows for four VASPs and compare their holdings to balance sheet data from the commercial register. Data are consistent for two VASPs only;
- We identify gaps in data collection practices and propose strategies to fill them: any entity in charge of auditing requires proof that a VASP actually controls the funds associated with its on-chain wallets; it is also important to report fiat and crypto asset and liability positions broken down by asset types, and at a reasonable frequency.

Currently, supervisory auditing of VASPs does not fully exploit the public availability of DLT transactions. We believe our work provides valuable insights toward a better and more systematic assessment of their solvency, and might help make the process more effective and less error-prone. By comparing the VASPs cryptoasset holdings to balance sheet data, we show that the major issues are related to the different management of cryptoasset wallets in different DLTs, the lack of wallet addresses attribution data for VASPs, and the absence of breakdowns by cryptoasset types in balance sheets.

2. Background and Related Literature

2.1. Definitions - what is a VASP?

While the term VASP has become increasingly common, its precise meaning and the specific activities that fall under this term still need to be clarified. We provide the definition of VASPs according to the FMA (2021), which follows the 5*th* EU AML directive (EC, 2018) and the Financial Action Task Force guidelines (FATF, 2021). According to it, a **Virtual Asset**, implemented on a distributed ledger technology, is:

> *[...] a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.*

In the "Market in Crypto Asset Regulation" (MiCA), the term "crypto asset" is used instead of virtual asset. In our context, the two terms can be considered equivalent.

Virtual Asset Service Providers are any natural or legal person that, as a business, conducts activities or operations for or on behalf of another natural or legal person. They offer "*[...] one or more services*" (FMA, 2021, p. VIII), which we summarize in Table 1.

Service	Description
Custodian	Services to safeguard private cryptographic keys, to hold, store and transfer virtual assets on behalf of a customer (custodian wallet providers)
V2F-Exchange	Exchanging of virtual assets into fiat currencies and vice versa
V2V-Exchange	Exchanging of one or more virtual assets between one another
Payment	Transferring of virtual assets
Issuance	Provision of financial services for the issuance and selling of virtual assets

Table 1: ***Services provided by Austrian VASPs.***

VASPs lie at the interface of the traditional and the crypto financial ecosystems. The former encompasses financial activity with fiat currencies, i.e., legal tender money, and fiat assets, i.e., assets denominated in fiat currencies (similarly to cryptoassets being assets denominated in a cryptocurrency). The latter entails financial activity executed on Distributed Ledger Technologies (DLTs) like the Bitcoin and Ethereum blockchains, and with cryptoassets such as Bitcoin, Ether, and the stablecoins Tether (USDT), USD coin (USDC), or DAI.

On the off-chain side, VASPs and customers interacting with them have strong identities; that is, the former need to register with regulatory bodies and the latter undergo identification processes such as KYC and AML5 compliance. On the on-chain side, activities involve weak identities (Möser et al., 2013): transactions, enabled by cryptographic keys, occur among pseudonymous counterparts, and the same entity can control multiple addresses.

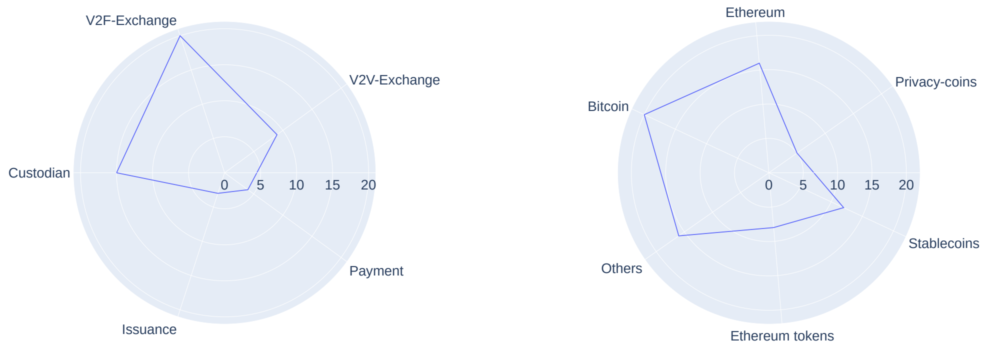
We note that VASPs differ from decentralized finance (DeFi) actors. This term indicates an emerging financial ecosystem built on DLTs that is non-custodial and does not require a central organization to operate (Auer et al., 2023), while VASPs are centralized intermediaries, and transactions can be stored in private ledgers rather than on DLTs.

2.2. Proof of solvency

A company is solvent if the total amount of assets held in custody is larger than the total amount of liabilities, whereby the difference is equity. Substantial documentation exists regarding incidents and exchange closures of VASPs (Moore et al., 2018), including recent events such as FTX's bankruptcy filing. Several VASPs have recently disclosed lists of cryptoasset wallet addresses as a *proof of reserve*, i.e., proof that they hold a given amount of assets. However, such an approach alone does not constitute a valid *proof of solvency* because it does not guarantee that VASPs have the financial resources to meet their current and future obligations[1]. First, a *proof of deposits*, i.e., a verification of the customers' deposit amount, is needed as well. Second, in addition to revealing the existence of an address, it is necessary to prove control over the corresponding private key. Third, even this might not be sufficient, as colluding actors could lend each other cryptoassets to conduct one-time proof of reserves.[2]

[1] *proof of reserves* and *proof of solvency* are terms adopted in jargon. Proof of reserves were collected by projects such as DefiLLama, which gathered several CEX wallet addresses: `https://bit.ly/3KpdnHT`.

[2] See e.g., `https://bit.ly/3XXBlgP`.



(a) (b)

Figure 2: ***The Austrian VASP landscape***. *Subfigure (a) shows the number of VASPs registered for each of the five service categories described in Table 1. Most of the VASPs offer V2F-Exchange (N = 20), and offer more than one service, such as custody (N = 15). Subfigure (b) reports how many VASPs offer services related to Bitcoin (N = 20), Ether (N = 16), and other relevant cryptoassets.*

As balance sheets report information on the asset and liability side, and the fiat assets are audited according to accepted accounting principles, in our context it is sufficient to verify that the asset side is consistent with the cryptoasset holdings of a VASP to prove its solvency.

2.3. Literature

The academic literature on VASPs primarily focuses on cryptoasset exchanges, highlighting the central role they have in the crypto ecosystem. Cryptoasset trading happens mostly off-chain on CEXs (Auer et al., 2022), and 75% of Bitcoin transactions involve exchanges or exchange-like providers (Makarov & Schoar, 2021). Scholars exploited price time series from the largest exchanges to investigate the price formation dynamics (Ciaian et al., 2016), estimate the fundamental value of cryptoassets (Cheah & Fry, 2015), investigate market (in)efficiency (Urquhart, 2016; Wu & Chen, 2020) and the related arbitrage opportunities (Saggese et al., 2023).

The literature closer to our work is more limited. Previous studies have categorized crypto financial intermediaries (Kazan et al., 2015) and compared them to traditional ones (Aramonte et al., 2021). Regarding solvency-related issues, Decker et al. (2015) and Dagher et al. (2015) implemented a software-based solution to automate the audit of centralized Bitcoin cryptoasset exchanges. Other works focused instead on proof of reserves for less relevant DLTs (Dutta & Vijayakumaran, 2019a,b). Our study is based instead on an empirical approach that focuses on the two most relevant DLTs, Bitcoin and Ethereum, and can be extended to others.

3. VASPs: A Closer Examination

Using information from the Austrian Financial Market Authority (FMA), we describe what financial services VASPs offer and what cryptoassets they support. Next, we complement the FMA data with additional public information collected from the VASPs websites to group them based on similarity scores. Finally, we compare their economic functions highlighting similarities and differences to traditional financial intermediaries.

3.1. The Austrian VASP landscape

VASPs in Austria are supervised by the Financial Market Authority (FMA) under the Anti-Money Laundering Act. In December 2022, 24 VASPs were registered in the FMA database[3]. Figure 2a shows the aggregate number of VASPs registered for each service described in Table 1.

[3] `https://bit.ly/3kMUkwg`

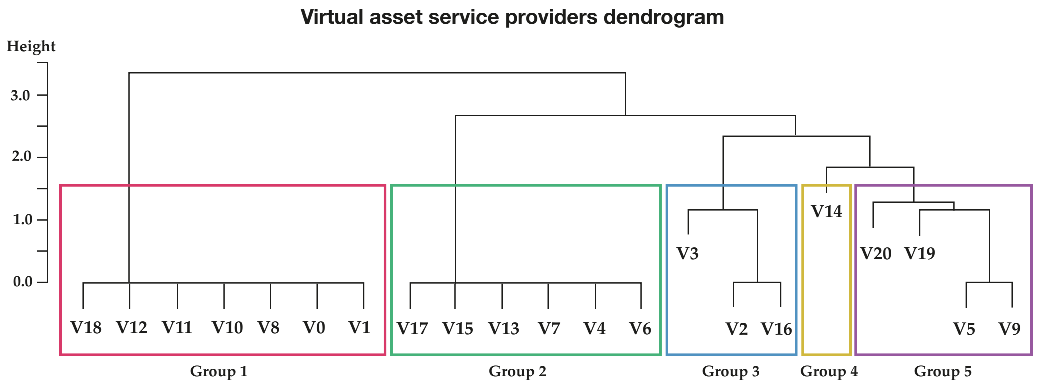


Figure 3: ***VASPs categorization by their service offering.*** *We use a hierarchical agglomerative clustering approach to categorize VASPs. The largest group comprises VASPs that facilitate the exchange of virtual assets without offering custody ( ). The others offer custody and consulting ( ) or exchange services ( ), are payment processors ( ), or implement trading platforms ( ).*

The vast majority of them ($N = 20$) offers *V2F-Exchange*, i.e., services to exchange virtual assets and fiat currencies; nine also facilitate the exchange from and to other virtual assets (*V2V-Exchange*). In most cases, customer funds are or can be kept in custody by the VASP ($N = 15$). Only a few of them are legally authorized to transfer virtual assets and to issue and sell them (respectively services *Payment*, $N = 4$, and *Issuance*, $N = 3$). Additional details on the number of services offered per VASP are reported in Appendix A.

Figure 2b shows what virtual assets are used by the Austrian VASPs. We follow the taxonomy described in Auer et al. (2023) to aggregate cryptoassets into five categories. We could retrieve reliable information for 20 VASPs out of the 24 in the FMA database. Notably, all VASPs offer services related to Bitcoins ($N = 20$). More than 75% support Ethereum ($N = 16$), and the latter typically also support Ethereum tokens, i.e., ERC-20 and ERC-721 compatible non-native tokens, and stablecoins (respectively $N = 8$ and $N = 12$). A limited number of VASPs also provide services related to privacy-focused cryptoassets (i.e., Monero, Dash, Zcash). Finally, several VASPs also support tokens native to other DLTs (e.g., Litecoin or Cardano).

In addition to FMA data, we collect online public information on VASPs. Our aim is to categorize them by their service offering. We construct categorical variables that indicate whether they offer custody services, facilitate payments, allow users to exchange cryptoassets, implement a trading platform, or offer consulting or investment services. We could gather sufficient information for 21 VASPs (data are reported anonymously in Appendix A). To ensure consistency and objectivity in categorizing VASPs we exploit an unsupervised learning method, i.e., the hierarchical agglomerative clustering (HAC, Murtagh & Contreras 2012). With this bottom-up approach, objects are iteratively clustered based on their similarity. In our setting, we choose the Euclidean distance and Ward metric respectively for the distance among objects and as linkage method, and distances are iteratively computed using the Lance–Williams update formula.

We report our classification in Figure 3. It categorizes VASPs into five clusters: the first, denoted as “Group 1” (red rectangle, $N = 7$), comprises VASPs that solely facilitate virtual asset exchanges, at times using vending machines, without custody services. The first branch mainly separates VASPs that offer custody from those that do not. “Group 2” (green rectangle, $N = 6$) identifies VASPs that, in addition to custody services, provide investment advice and/or portfolio management, and in some cases lend customer funds.

“Group 5” (purple rectangle, N = 4) aggregates VASPs that act as cryptoasset custodians and facilitate the exchange of cryptoassets. They are similar to VASPs in “Group 3” (blue rectangle, N = 3), but the latter in addition provide customers with an internal trading platform and manage and match orders in a private limit order book. Such VASPs play an essential role

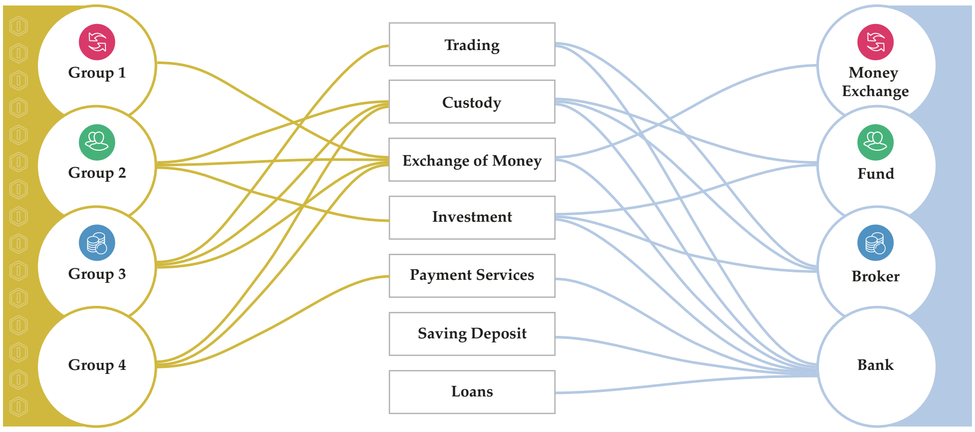


Figure 4: ***Comparison of traditional financial intermediaries with VASPs.*** *Circles on the left represent VASPs, divided into groups as described in Figure 3, while on the right are traditional financial intermediaries. Links point to the financial functions offered by each financial intermediary. VASPs are most similar to money exchanges, brokers, and funds, rather than banks. The colors in the circles highlight what traditional intermediary each group is most similar to.*

in the crypto-financial system. As a result of the matching mechanism for demand and supply, these are the platforms where price formation takes place. The other VASPs derive their offered prices from other platforms as an exogenous variable.

All the VASPs in the groups described above are cryptoasset centralized exchanges. The remaining VASP in the yellow rectangle is instead a payment processor service. It offers solutions to facilitate the purchase and sale of commodity goods with cryptoassets; such VASPs play a minor role in the crypto ecosystem.

3.2. A comparison with traditional financial intermediaries

Having outlined the landscape of VASPs in Austria, we are now interested in understanding how they differ from traditional financial intermediaries. Figure 4 stylizes the traditional financial intermediaries on the right and the VASPs on the left. In the middle, rectangles represent the primary economic services, and links indicate what services each intermediary category offers. The comparison shows that an analogy with traditional intermediaries exists for three out of the four groups described in Figure 3. More specifically, VASPs in Group 1 operate similarly to *money exchanges*, as they only allow customers to buy and sell virtual assets. VASPs in Group 2 provide investment services to their users, akin to *funds*. Third, Group 3 (and 5) include VASPs allowing users to trade, keep their funds in custody, and thus act as *brokers*, connecting buyers and sellers to facilitate a transaction. The last group that provides payment services can be compared to payment processor systems. Interestingly, we find that the comparison of VASPs to banks can be misleading: while the two share overall several financial services, such as exchanging money, trading, or investing, banks also enable customers to open loan positions with the funds they hold and to open savings and deposit positions. None of the VASPs we examined offers such services.

4. Measuring VASPs Cryptoasset Holdings

After describing the VASPs service offerings, we devise an approach to empirically assess their solvency by correlating data from multiple on-chain and off-chain sources. The underlying intuition is that, by quantifying the cryptoassets held on-chain by one VASP, we should be able to verify the numbers reported in the balance sheets. It is sufficient to measure the asset side, because on the liability side cryptoassets are either customer liabilities or equity. Since balance sheet assets minus liabilities are equal to equity, our approach serves as a first proof of solvency.

We first discuss which DLTs we analyze, motivate our choice, and document our approach to reconstruct the VASPs net positions by extracting the data from the two most relevant DLTs, Bitcoin and Ethereum. VASPs wallet addresses are extracted from a large collection of public attribution tags, or identified by executing manual transactions, and have not been revealed by the VASPs themselves. Next, we describe the balance sheet data from the commercial register. We concentrate our empirical analysis on four VASPs whose wallets appear in the attribution tag collection and that have published their balance sheets consistently over time, allowing to compare on-chain cryptoasset holdings to balance sheets. Their market share is around 99% of the total market share.

4.1. On-chain data

We begin by gathering the transaction history of the two most relevant DLTs, Bitcoin and Ethereum, from their origin to the 3^{rd} of April 2022[4]. We focus on them for the following reasons: first, as shown in Section 3, all VASPs operate with Bitcoins and in most cases also with Ether. Cryptoassets deployed on other DLTs are less relevant. Second, Bitcoin, Ether, and the stablecoins USDT and USDC alone account for more than 70% of the total cryptoasset market capitalization, and these are also the most traded and held cryptoassets by CEXs customers[5]. Third, while stablecoins like USDT are deployed on multiple smart contract-compatible ledgers[6] and currently deploy significant amounts of tokens also in other DLTs[7], Ethereum is historically the most relevant one.

We implement two approaches to extract on-chain VASP-related information for Bitcoin and Ethereum. Entities on the Bitcoin blockchain interact with each other as a set of pseudo-anonymous addresses; new transactions can generate new transactions. We exploit known clustering heuristics (Meiklejohn et al., 2016) to associate addresses controlled by the same entity. We use a collection of public attribution tags that associate addresses with real-world actors, expand the dataset by conducting manual transactions with the VASPs in our sample, and filter the clusters associated with the VASPs considered in our study. We identified 88 addresses and their corresponding clusters associated with four different VASPs, for a total of 1,574,125 Bitcoin transactions. We reconstruct their net positions from the Bitcoin transaction history by selecting only transactions where the sender or recipient is an address associated with the four VASPs. Further details are discussed in Appendix A.

We use a different approach for the Ethereum DLT. While approaches for address clustering have been devised for Ethereum as well (Victor, 2020), in practice, addresses are typically reused. We thus extract all relevant information by running a full Erigon Ethereum archive node. Similarly to the previous approach, we exploit attribution tags and manual transactions to identify the addresses associated with VASPs. In total, we identified nine relevant addresses associated with three different VASPs. We proceed by querying the balance of each account, from the beginning of the Ethereum transaction history (block 0) to the 3^{rd} of April 2022, every 10,000 blocks. In addition to the Ether balance, we collect data on the address balance for the tokens USDT, USDC, DAI, wETH, wBTC.

We remark that our attribution dataset contains more than 265,000,000 deanonymized Bitcoin addresses, covering more than 24% of the total number of existing Bitcoin addresses. In addition, 278,244 tagged Ethereum addresses cover 0.11% of the existing addresses. The former identifies around 3000 entities active in the Bitcoin ecosystem, the latter more than 25,000 Ethereum entities.

[4] The time frame can be extended to 2022 to include the balance sheet of upcoming years when available.
[5] See `https://coinmarketcap.com/charts/` and `https://coinmarketcap.com/rankings/exchanges/`
[6] see, e.g., USDT `https://bit.ly/3YSYNwR` and USDC `https://www.circle.com/en/multichain-usdc`
[7] `https://tether.to/en/transparency/`.

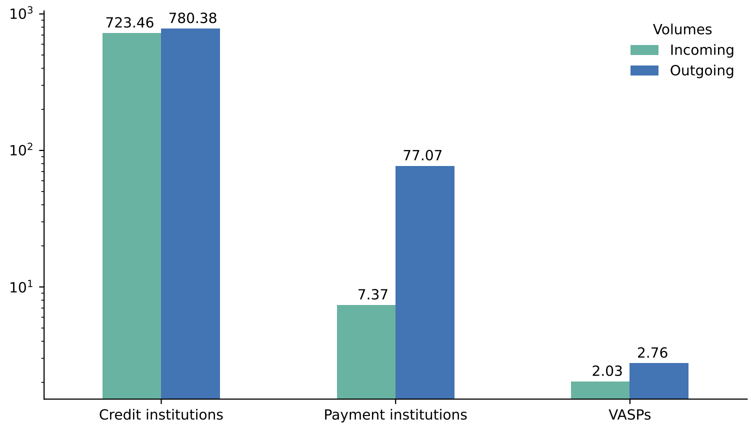


Figure 5: ***Transaction volumes of Austrian VASPs and other financial intermediaries.*** *The incoming and outgoing transaction volumes of VASPs are respectively one order and two orders of magnitude smaller than those of payment institutions and credit institutions.*

4.2. Off-chain data

We collect balance-sheet data for 17 Austrian VASPs through the Austrian Commercial Register. We construct an unbalanced panel data starting from 2014 to 2021. Ultimately, in our empirical analysis, we use the data of four Austrian VASPs for which we can identify on-chain and off-chain data. Our variable of interest is a firm-level measure of crypto asset holdings. Some firms describe their crypto asset holdings as explicit balance-sheet items; for other firms that aggregate them with other items we construct a variable that approximates the corresponding crypto asset holdings from their described asset items. The balance sheet does not allow us to distinguish between cryptoasset holdings such as Ether and Bitcoin. The variable *crypto asset holdings* represents those balance-sheet items in form of red markers in Figures 6, 7, 8 and 9.

4.3. Comparing on- and off-chain data

Supervisory data from FMA show that in a 12-month period (roughly 2021 until 2022 due to varying reporting dates for VASPs), the transaction volume of virtual assets converted to EUR conducted by VASPs registered in Austria amounts to 2.03 billion incoming transaction volume and 2.76 billion outgoing. The transaction volume is computed as the sum of the transactions related to customer relationships only. As Figure 5 shows, in comparison, during the same time we observed a transaction volume for credit institutions of 723.46 (incoming) and 780.38 (outgoing) billion and of 7.37 (incoming) and 77.07 (outgoing) billion for payment institutions.

Table 2 reports additional supervisory data from FMA on the number of VASP customers by residence and legal form. A VASP customer refers to a natural or legal person, who has opened an account and gone through a validated KYC process with the particular VASP. The rows distinguish natural persons, i.e., individuals, and legal persons, i.e., entities with legal rights. Customers are further divided by jurisdiction: the first column indicates the number of Austrian customers, while the second one reports the number of customers in the European Union, excluding Austrians (note that customers are never counted in two columns). The subsequent columns identify customers by jurisdictions that are respectively offshore financial centers (IMF, 2019), subject to embargo (WKO, 2020), and under increased monitoring (grey list; FATF, 2022). The last columns respectively aggregate all remaining countries and report the total number of users. Countries that appear in several lists are assigned to the group that bears the greater risk. The total customers, mainly natural persons, are 1.79 million. The vast majority are Austrian or European Union members (respectively N = 326,660 and N = 1,279,132). We note that this number might include customers who created an account but

	Austria	EU$^{(*)}$	Offshore	Embargo	Grey list	Other	Total
Natural persons	326,660	1,279,132	1160	1183	36,421	141,491	1,785,747
Legal persons	326	147	2	-	-	26	501

$^{(*)}$excluding Austrian customers

Table 2: ***VASP customers residency in different jurisdictions.*** *We report figures for natural persons (top) and legal persons (bottom). Customers are never double counted; e.g., the first column reports the number of Austrian customers, while the second reports European Union members excluding Austrians. We further distinguish customers by jurisdictions that are offshore, subject to embargo, and under increased monitoring ("grey list"). The last columns aggregate all other jurisdictions (Other) and report the total number of customers (Total).* Source: supervisory data from FMA.

never transacted, i.e. the count is not weighted by transaction number, and the same customers can have accounts at multiple VASPs. Customers from subsidiaries and inactive are excluded.

The four entities we study cover around 99% of the Austrian VASP transaction volumes measured in total assets. Consistently with the labels introduced in Figure 4, we denote them as VASP-2, VASP-5, VASP-9, and VASP-12. They are representative of different VASP groups (i.e., money exchanges, brokers, and brokers with trading platforms).

4.3.1. VASP-2

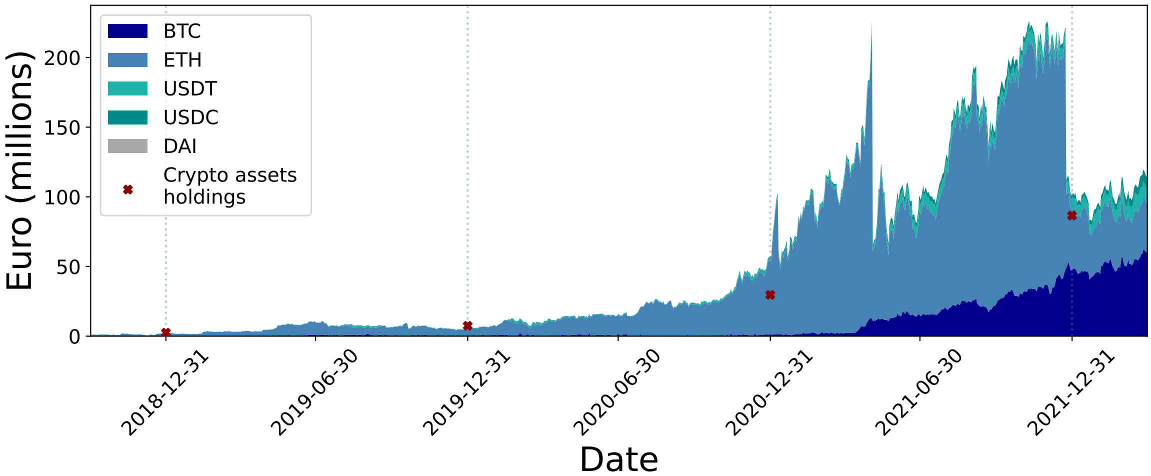


Figure 6: ***Estimation of the cryptoasset holdings of VASP-2.*** *Colors correspond to different cryptoassets: Bitcoin in dark blue, Ether in light blue, USDC in dark green, USDT in light green, and DAI in gray. Red markers indicate the cryptoasset holdings declared in the balance sheet data at the end of each year from 2018 to 2021.*

Observations. We report the values for VASP-2 in Figure 6. In this and the subsequent plots, the Bitcoin holdings are in dark blue, Ether in light blue, USDC in dark green, USDT in light green, and DAI in gray. The dots represent the cryptoasset holdings declared in the balance sheet data at the end of each year for the period 2018 to 2021. This VASP implements a trading platform and falls within group 3.

The cryptoasset holdings identified on-chain correspond to 75.59% of the cryptoassets declared in the balance sheet at the end of 2018, 66.68% at the end of 2019, 194.56% at the end of 2020, 116.79% at the end of 2021. The amount of Bitcoin increased significantly after April 2021, and the largest amount of tokens is held in Ether.

Findings. Overall, the two sources of information point in the same direction. After 2020, the on-chain activity is higher than what the balance sheet reports. A possible interpretation is that the cryptoassets in excess represent equity or private funds. VASP-2 reports well-separated balance sheet positions, allowing to compute precisely the amount of cryptoasset holdings.

4.3.2. VASP-12

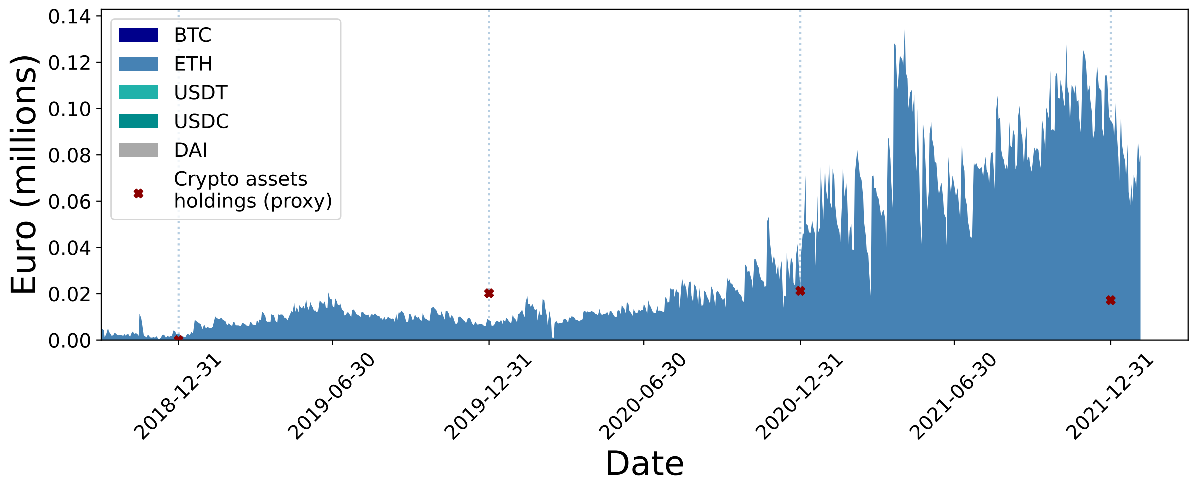


Figure 7: ***Estimation of the cryptoasset holdings of the VASP-12.*** *On-chain and off-chain data correspond until the end of 2020. All reported assets are Ether. Balance sheet data are a proxy, as cryptoassets are aggregated with other items in the balance sheet.*

Observations. Figure 7 shows the cryptoasset holdings of VASP-12. It is a non-custodial VASP that provides exchange services based both on Ether and Bitcoin. The cryptoassets measured on-chain are partially comparable with those reported on the balance sheets (42.59% at the end of 2019, 102.45% at the end of 2020, but 549.38% at the end of 2021).

Findings. Similarly to VASP-2, on-chain activity is higher than reported on the balance sheet after 2020. As expected, since the VASP is non-custodial, the amount of cryptoasset holdings is small and exceeds 100K EUR only after 2021. All reported assets are Ether: the absence of stablecoins is expected, as this VASP trades Bitcoin, Ether, and a few other cryptoassets. To identify the addresses associated with this VASP and collect additional attribution tags, we relied on manual transactions and re-identification attacks. While this strategy is effective for Ethereum accounts, the Bitcoin addresses we gathered identify the VASP activity dating back to November 2022 only, thus outside of the time frame we considered. Therefore, we could not identify Bitcoin flows from or to their wallets in the time frame we considered. Regarding balance sheet data, we note that the values, in this case, are a proxy: cryptoassets are aggregated with other items in the balance sheet.

4.3.3. VASP-9

Observations. VASP-9 is shown in Figure 8. It is categorized in group 5 in Subsection 3.1. Unlike the previous cases, the cryptoasset holdings cover only a tiny fraction of the funds declared in the balance sheets; in the best case, i.e., at the end of 2021, we can identify on-chain only 16.85% of the total cryptoassets reported in the balance sheet.

Findings. A possible explanation for the discrepancy is that our dataset might include only *hot wallets*, i.e., addresses used to conduct daily operations such as the deposit and withdrawal, but not the *cold wallets*, i.e., addresses that control the large majority of customers funds and that are subject to stricter security measures. An alternative explanation could be that the considered VASP is part of a larger company structure and that the company engages next to VASP activities also in non-VASP-related business activities. In that case, the reported balance sheet items might contain aggregated business activities, whereby it is difficult to disentangle the specific positions related to the crypto activities of the VASP-9. As a result, the proxy variable from the balance sheet might then overestimate the actual figure we are interested in.

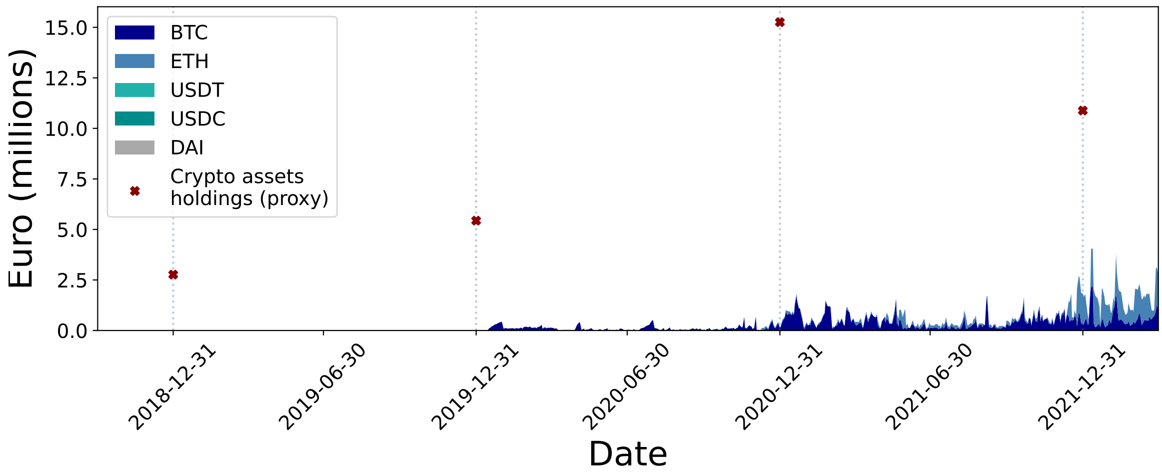


Figure 8: ***Estimation of the cryptoasset holdings of VASP-9.*** *The cryptoasset holdings cover only a small fraction of the funds declared in the balance sheets.*

Furthermore, this VASP operates with multiple DLTs and also exchanges stablecoins, but the cryptoasset wallets we analyzed do not hold any USDC, USDT, or DAI.

4.3.4. VASP-5

Observations. VASP-5 is the last we analyze; values are shown in Figure 9. This VASP bases its services on the purchase and sale of Bitcoins. For this VASP, using both attribution tags in the TagPack database mentioned above and re-identification strategies, we could only gather information for a few months in between 2014 and 2017 and after 2021. The results are consistent only for the years 2015 and 2016, when the VASP held very small amounts of cryptoassets, if compared to the subsequent years.

Findings. Similarly to VASP-9, we could not collect sufficient data to obtain comparable values to the figures reported in the balance sheets. As for VASP-12, the Bitcoin addresses we gathered through manual transactions identify clusters whose transaction history only dates back to a few months (mid-2021). Again, this highlights that re-identification is less effective for Bitcoin than Ethereum addresses.

The data gap between 2018 and 2020 reveals another issue: likely, after 2017, funds were moved to other addresses that are not reused with those in our sample. VASPs apply different strategies to organize their cryptoasset transfers and holdings, e.g., to create new addresses for each transaction, or reuse them. If they are not reused, cryptoasset holdings can be held at multiple apparently unrelated clusters that can change over time.

5. Closing The Data Gap

We presented an approach to measure the cryptoasset holdings of VASPs by correlating data from multiple on-chain and off-chain sources. Empirical analysis of four VASPs reveals that only two of them show consistent comparisons of on-chain and off-chain data, indicating potential data-related problems. In this section, we systematically discuss the encountered data issues and provide suggestions for possible improvements.

5.1. On-chain data collection issues

Different wallet management strategies. VASPs employ diverse approaches to manage their cryptoasset transfers and holdings. While some create new addresses for each user transaction, others might reuse addresses. Moreover, their approach varies when dealing with UTXO-based or

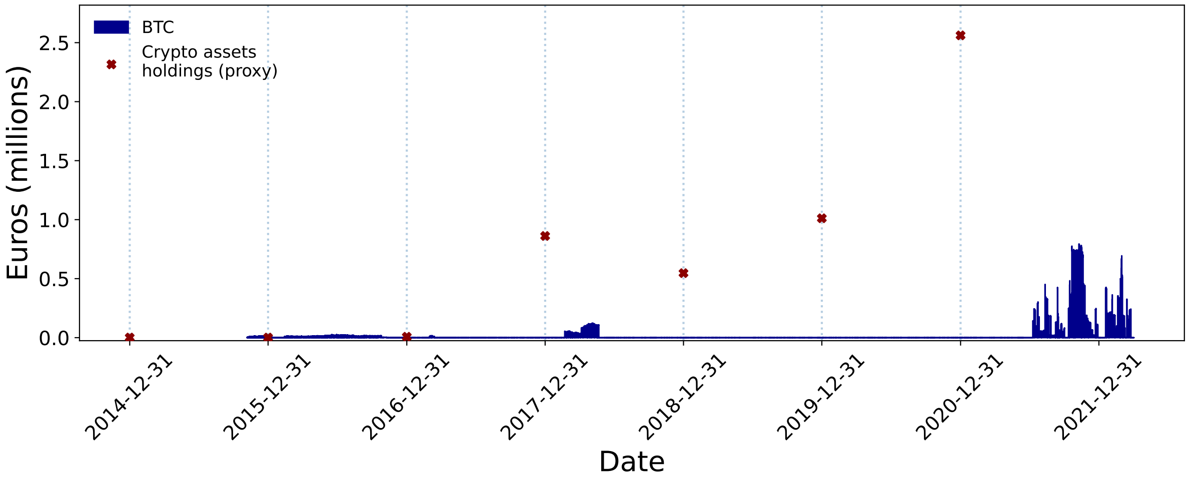


Figure 9: ***Estimation of the Bitcoin holdings in Euro of VASP-5.*** *On-chain and off-chain data are comparable only in 2015 and 2016.*

account-based ledgers. We observed that VASPs deploy user-specific Ethereum smart contracts wallets for each customer and subsequently forward the funds to a collector wallet. We did not observe this pattern with Bitcoin. This organization strategy makes it more challenging to identify cryptoasset holdings associated with VASPs. Identification largely relies on heuristics approaches, which can produce false positives and are often inadequately understood.

Lack of attribution data. Another issue concerns the lack of attribution data, i.e., associations of addresses with additional contextual information allowing the identification of their owner. Our attribution dataset contains more than 265,000,000 Bitcoin and 278,244 Ethereum tagged addresses. Furthermore, we have conducted additional manual transactions to identify and tag additional addresses associated with the VASPs investigated in our study. Despite this, the resulting data only provide a partial view of their holdings, as shown in the previous section.

Another issue associated with manual tagging is that it misses historical data. As we showed in Section 4 for VASP-12 and VASP-5, we could only trace the Bitcoin transaction history of a VASP back in time for a few months when using re-identification techniques.

Missing cross-ledger perspective. The data collected for both ledger types face a common issue — they may only represent a portion of the total cryptoassets holdings. This could be because manual transactions used to tag hot wallets, i.e. addresses used for daily deposit and withdrawal operations, may not successfully identify cold wallets, i.e., the addresses that manage most of the VASP funds. The latter are subject to stricter security measures that may prevent association with hot wallet addresses. Additionally, wallets such as VASP-2 and VASP-12 contain more funds than reported to authorities, making it difficult to differentiate between customers' funds and other cryptoassets managed under the same wallet, such as equity or private funds.

5.2. Off-chain data collection issues

In addition to on-chain data, we used all data sources currently available for VASPs in Austria: balance sheet data from the commercial register and data from the supervisory entities.

Long reporting periods. Balance sheets are only published yearly, and asset holdings might differ before and after the exact reporting due date. Thus, the balance sheet statements of VASPs are only partially suitable for assessing their solvency.

Missing breakdown by cryptoasset type. Nevertheless, it is important to outline the type of data and related good reporting practices to improve the transparency of virtual asset-providing companies. Not all firms report balance-sheet items for crypto and fiat asset holdings separately. In Section 4, we sometimes needed to use proxies for some VASPs that overestimate the actual cryptoasset holdings of a VASP, primarily due to the aggregation of multiple items within the same balance sheet entry. It is, therefore, essential that VASPs report their fiat and crypto asset and liability positions at a reasonable frequency and separately from other activities within a company's holding structure.

Subsidiary companies and different jurisdictions. VASPs may be subsidiaries of larger corporations. For VASP-9, we could not precisely determine the proportion of assets attributable to the subsidiary we examined. Moreover, many companies operate in several countries and fall under multiple jurisdictions, which adds another layer of complexity.

5.3. Limitations of our approach

Other limitations related to our approach stand out. First, data are extracted from the two major DLTs, Bitcoin and Ethereum, and only on a limited number of tokens supported by the latter. While these are the most relevant for market capitalization, including other DLTs and Ethereum tokens would be a straightforward improvement. Second, we gather Ethereum data by querying the account balances. Thus, we do not reconstruct balances from transactions, and we repeat the procedure on an interval of 10,000 blocks. We favor the approach based on querying the account states as it facilitates reproducibility at the cost of a lower granularity. We also note that this time interval can be easily changed with a shorter one. Third, our current approach is limited to end-year of 2021, but the analysis can potentially be extended to subsequent years.

5.4. Towards a systematic assessment of proof of solvency

Having discussed the data issues and limitations of our approach, we sketch out our vision for a more systematic, reliable, and highly automated assessment of proof of solvency.

Assessing proof of solvency today. Fiat assets and liabilities are held at traditional financial intermediaries and undergo audits based on established standards. Cryptoassets are instead held in cryptoasset wallets, scattered across various, potentially privacy-preserving DLTs, and are not subject to systematic and consistent audits. By measuring the cryptoassets held by one VASP, we can validate the amounts reported in the balance sheets. Given that the difference between assets and liabilities on a balance sheet equals equity, our method offers an initial, systematic validation and proof of solvency. However, balance sheets currently disclose crypto and fiat deposits from customers under one balance sheet position. Thus, we cannot answer whether the VASPs retain the customer funds in crypto or convert them to fiat (or vice-versa).

Improving on-chain data reporting. Regarding on-chain data, we note that determining the solvency of VASPs is unfeasible without knowledge of the crypto addresses they control. Hence, any auditing entity must be aware of the on-chain cryptoasset holdings each VASP manages. Furthermore, sharing a list of on-chain wallet addresses alone is insufficient. In a system with weak identities, anyone could hold the corresponding private keys and control the associated funds. VASPs need to prove they also control the funds they hold in custody for their users.

Revealing a list of on-chain wallet addresses and transferring funds proves that a VASP possesses and manages specific funds. However, this approach can create privacy, security, and operational efficiency concerns. One way to mitigate these issues is to share this information only with trusted entities such as certified auditors or regulatory authorities. Furthermore, this approach would not disclose any information on actual user deposits.

Finally, in addition to disclosing their on-chain wallets, VASPs should provide additional metadata describing the use of these wallets. Most importantly, they should differentiate between hot and cold wallets and customer and non-customer (corporate) wallets. With hot wallets, they could also distinguish between deposit and withdrawal wallets and specify whether they are used per customer or across customers.

Improving off-chain data reporting. On the off-chain side, reporting requirements for a VASP should include a breakdown of asset holdings differentiating between fiat and crypto holdings. Such a breakdown is necessary for items on the asset side but also for items on the liability side. A step towards even more granularity is to differentiate the crypto items according to major cryptoassets and to provide wallet information on the storage of crypto asset holdings and liabilities. To understand the implications of VASPs on financial stability, frequent and detailed reports on the distribution of who are the counter-parties of VASPs (private customers, companies, other VASPs, ...) and concepts of how and where crypto assets are stored are necessary information.

Enhancing VASP solvency assessment. One possible strategy to improve the assessment process is to use cryptographic primitives. The academic literature has already proposed cryptographically secure proof-of-concept implementations for proofing the solvency of cryptoasset exchanges. Decker et al. (2015) devised an audit process in a trusted computing environment that exploits digital signatures on the addresses for proofing reserves and Merkle trees to prove liabilities size without directly leaking user-specific information. This technique has already been implemented by several centralized exchanges (e.g., Binance[8]). However, an attacker that controls many accounts could still potentially learn a significant amount about the exchange's users. To improve the privacy and robustness of that approach, and to prove that all balances in the tree are non-negative, Buterin (2022) recently proposed to use ZK-SNARK technology.

A more forward-thinking strategy goes in the direction of automation. Given access to both on- and off-chain data with specific detail and granularity, the entire audit process could be streamlined and performed more systematically, frequently, and reliably than current methods allow. In line with this perspective, Auer (2019) introduced the concept of "embedded supervision" enabling automated monitoring of decentralized finance (DeFi) services to ensure compliance with regulatory objectives. Buterin et al. (2023) studied an automated privacy-enhancing protocol that utilizes smart contracts and ZK-SNARKS to prove that the users' assets were received from lawful sources. Additionally, Eichengreen et al. (2023) suggest that real-time audits carried out by independent proof-of-reserve systems and facilitated by smart contracts could effectively mitigate the threat of stablecoin devaluation.

Noteworthy, according to Article 29 (1) of the Austrian AML-Act, the FMA already possesses the authority and legal mandate to request essential data from all obliged entities (i.e., VASPs) at any time on all issues that are addressed in the Austrian AML-Act and Regulation (EU) 2015/847, e.g. a list of cryptoasset addresses under their control[9].

6. Conclusions

In this work, we investigate 24 VASPs registered with the Austrian Financial Market Authority (FMA) at the end of 2022. We aim to provide an empirical approach to assess their solvency status, by measuring their cryptoasset holdings across time and distributed ledgers. To do so, we cross-reference data from three distinct sources: publicly auditable cryptoasset wallets, balance sheet data from the commercial register, and information from supervisory entities. We begin by describing the financial services they offer, the virtual assets they support, and compare them to conventional financial intermediaries. Their core financial activity can

[8] https://www.binance.com/en/proof-of-reserves

[9] https://www.ris.bka.gv.at/eli/bgbl/i/2016/118/P29/NOR40189690, https://eur-lex.europa.eu/eli/reg/2015/847/oj

be compared to money exchanges, brokers, and funds, rather than to commercial banks. We provide regulatory data insights showing that their yearly incoming and outgoing transaction volume in 2022 amounted to 2 billion EUR for around 1.8 million users.

Next, we implement address clustering algorithms and entity identification techniques to reconstruct their cryptoasset flows on the Bitcoin and Ethereum blockchains and compare their net positions to balance sheet data from the commercial register. We focus on four VASPs for which we could gather information both on their cryptoasset transactions and balance sheets. These four entities cover around 99% of the Austrian VASP transaction volumes measured in total assets. With our approach, we find proof, for two VASPs out of four, that they control enough assets to fulfill liabilities and obligations against customers, i.e., they meet the capital requirements, while we could not collect enough data for the remaining two.

Then we discuss the data collection-related issues and suggest solutions towards better assessing a VASP solvency. In particular, we remark that any entity in charge of auditing requires proof that a VASP actually controls the funds associated with its on-chain wallets. It is also important that a VASP reports fiat and crypto asset and liability positions, broken down by asset types at a reasonable frequency.

We consider this work to be a starting point for developing more effective strategies to systematically assess the solvency status of virtual asset service providers.

References

Anderson, R., Shumailov, I., Ahmed, M., & Rietmann, A. (2019). Bitcoin redux. *WEIS*.

Aramonte, S., Huang, W., & Schrimpf, A. (2021). Defi risks and the decentralisation illusion. *BIS Quarterly Review*, (pp. 21–36).

Auer, R. (2019). Embedded supervision: how to build regulation into blockchain finance. *Globalization and Monetary Policy Institute Working Paper*, (371).

Auer, R., Farag, M., Lewrick, U., Orazem, L., Zoss, M., et al. (2022). *Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies*. Technical report, Bank for International Settlements.

Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2023). The technology of decentralized finance (defi). *BIS working papers*.

Briola, A., Vidal-Tomás, D., Wang, Y., & Aste, T. (2022). Anatomy of a stablecoin's failure: The terra-luna case. *Finance Research Letters*, (pp. 103358).

Buterin, V. (2022). Having a safe cex: proof of solvency and beyond. Available at: `https://vitalik.ca/general/2022/11/19/proof_of_solvency.html`.

Buterin, V., Illum, J., Nadler, M., Schär, F., & Soleimani, A. (2023). Blockchain privacy and regulatory compliance: Towards a practical equilibrium. *Available at SSRN*.

Cheah, E.-T. & Fry, J. (2015). Speculative bubbles in bitcoin markets? an empirical investigation into the fundamental value of bitcoin. *Economics letters*, 130, 32–36.

Ciaian, P., Rajcaniova, M., & Kancs, d. (2016). The economics of bitcoin price formation. *Applied economics*, 48(19), 1799–1815.

Dagher, G. G., Bünz, B., Bonneau, J., Clark, J., & Boneh, D. (2015). Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 720–731).

Decker, C., Guthrie, J., Seidel, J., & Wattenhofer, R. (2015). Making bitcoin exchanges transparent. In *Computer Security–ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part II 20* (pp. 561–576).: Springer.

Dutta, A. & Vijayakumaran, S. (2019a). Mprove: A proof of reserves protocol for monero exchanges. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 330–339).: IEEE.

Dutta, A. & Vijayakumaran, S. (2019b). Revelio: A mimblewimble proof of reserves protocol. In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 7–11).: IEEE.

EC (2018). *5th anti money laundering Directive - Directive (EU) 2018/843 of the European Parliament and of the Council*. Technical report.

EC (2022). *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and Amending Directive (EU) 2019/1937*. Technical report.

Eichengreen, B., T Nguyen, M., & Viswanath-Natraj, G. (2023). Stablecoin devaluation risk. *WBS Finance Group Research Paper*.

ElBahrawy, A., Alessandretti, L., Kandler, A., Pastor-Satorras, R., & Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. *Royal Society open science*, 4(11), 170623.

FATF (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Technical report, FATF, Paris.

FATF (2022). *Jurisdictions under Increased Monitoring*. Technical report.

FMA (2021). *Federal Act on the Prevention of Money Laundering and Terrorist Financing in Financial Markets*. Technical report.

IMF (2019). *Past IMF Staff Assessments on Offshore Financial Centers (OFCs)*. Technical report.

Kazan, E., Tan, C.-W., & Lim, E. T. (2015). Value creation in cryptocurrency networks: Towards a taxonomy of digital business models for bitcoin companies.

Makarov, I. & Schoar, A. (2021). Blockchain analysis of the bitcoin market. *National Bureau of Economic Research*.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of Bitcoins. *Communications of the ACM*, 59(4), 86–93.

Moore, T., Christin, N., & Szurdi, J. (2018). Revisiting the risks of Bitcoin currency exchange closure. *ACM Transactions on Internet Technology*, 18(4), 50:1–50:18.

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the bitcoin ecosystem. In *2013 APWG eCrime researchers summit* (pp. 1–14).: Ieee.

Murtagh, F. & Contreras, P. (2012). Algorithms for hierarchical clustering: an overview. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 2(1), 86–97.

Saggese, P., Belmonte, A., Dimitri, N., Facchini, A., & Böhme, R. (2023). Arbitrageurs in the bitcoin ecosystem: Evidence from user-level trading patterns in the mt. gox exchange platform. *Journal of Economic Behavior & Organization*, 213, 251–270.

SEC (2023). Security and exchange commission files 13 charges against binance entities and founder changpeng zhao. `https://www.sec.gov/news/press-release/2023-101`.

The Economist (2022). The failure of ftx and sam bankman-fried will leave deep scars. `https://www.economist.com/briefing/2022/11/17/the-failure-of-ftx-and-sam-bankman-fried-will-leave-deep-scars`. Accessed: November 2022.

Urquhart, A. (2016). The inefficiency of bitcoin. *Economics Letters*, 148, 80–82.

Victor, F. (2020). Address clustering heuristics for ethereum. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24* (pp. 617–633).: Springer.

WKO (2020). *Die Wirtschaftskammer Wien: Past IMF Staff Assessments on Offshore Financial Centers (OFCs)*. Technical report.

Wu, L. & Chen, S. (2020). Long memory and efficiency of bitcoin under heavy tails. *Applied Economics*, 52(48), 5298–5309.

Zetzsche, D., Buckley, R., Arner, D., & van Ek, M. (2023). *Remaining regulatory challenges in digital finance and crypto-assets after MiCA*. Technical report.

Appendix A. Supplemental material

In this appendix we report additional information about how many VASPs offer several services or support multiple coins (Figure A.1). Most VASPs ($N = 14$) provide services on cryptoassets of three or more different DLTs; $N = 11$ VASPs provide only one service, and $N = 7$ offer three different services.

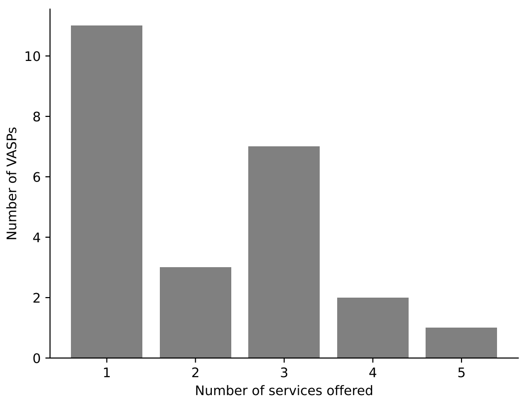
Furthermore, we provide further insights on the address clustering technique utilized and on the data gathering procedure. The address clustering we implement assumes that the addresses utilized as input in a Bitcoin transaction must be controlled by the same entity. If addresses are reused across transactions, then multiple input addresses can be associated as belonging to the same entity. We note that in this study we computed the VASP balances by analyzing the flows at the level of clusters. We also repeated the analysis at the address level, and found minor inconsistencies most likely due to rounding errors.

Next, we report additional information on the addresses we utilized to identify VASPs. The full list of addresses used is reported in Tables A.1 and A.2. As explained in Section 4.1, we first exploited a collection of tagpacks that associate addresses to the entities controlling them.

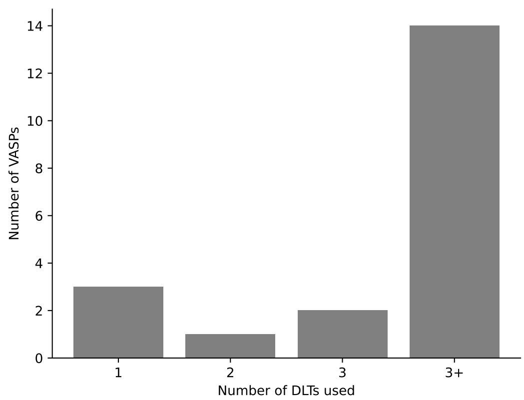
Furthermore, to increase our dataset sample, we conducted manual transactions against the VASPs that were already in our sample. This led to the identification of 9 new addresses and their corresponding clusters, that we highlight in light gray in Tables A.1 and A.2.

We further expanded the dataset by conducting transaction pattern analyses of the new collected addresses. We identified 7 additional addresses that follow specific patterns indicating the redirection of funds from temporary addresses to collector wallets. These are highlighted in Tables A.1 and A.2 in darker gray.

Finally, Table A.3 reports the VASP categorization by their service offering according to their online documentation.



(a)



(b)

Figure A.1: ***The Austrian VASP landscape***. *(a) histogram showing how many services VASPs offer; (b) histogram showing how many DLTs VASPs utilize.*

Table A.1: List of Bitcoin cluster-defining addresses.

Address	Label	Address	Label
372iojpPqRP2e3oh7eUs1VZowS8kDkMrff	VASP A	bc1qagw7nw7na3ev9yln2yeggp2wd26h6lxm25um3v	VASP A
bc1pgwsxt7ww3s2rsa8g0jpjyyvyd30xm4kg3skhm5...	VASP A	3A4p29nPvfFGBa7a1KNFsioRyKwv9GdvBL	VASP A
35TviLjv9zD91Q9N7X3kcqstZdBusTpqNe	VASP A	bc1q3nmcqejgyldax0ekfcj2w5zcjgmf43wwdfcugj...	VASP A
36iUjkZwQAvkz8StPqudfdQnkq57e5tZTL	VASP A	3BqHzZAgqEE8pYz2cYikWrvwW8UZSL4Y6w	VASP A
3AQGNPTTY4D3a5AfG2C3ktQdkBfbJzFaZG	VASP A	13b84xNArAK8T4KbjbqaHDVREVC11CaAqQ	VASP A
bc1qwqgtpvh7u5fcf043y7ze9934jct8g74ducmpat	VASP A	3F8z98fknEknhwVwmfDLo9kwdzrFo5PGZe	VASP A
3Ms6oxUU9vdek3tFS2UxtC6v77aLurfTnV	VASP A	18p9Ftp3m4435tdpZTvoBsm3yjUgkvTF2b	VASP A
3QVRCiqw2HRCf3vnbkiQmNYSHcPnuVy8Lj	VASP A	3AkxoL4gEUvZLjAikYn49J7cLDWkYsZyqy	VASP A
3Djd57FoRZjjT5rJx6WWmibgA2esSSEPLs	VASP A	38p43PUvNEXLZMyHzCddbfznzU44RPokc4	VASP A
3AqPuD4ZdHPjnN79mKNCk46mpMMmyFPgQd	VASP A	bc1q908vpavz7f4aej5aw7d6qku5u3llrcfc42d680	VASP A
3AZfcZ8NqaGfB5PHGCpQ29QXE8TgbmyxGL	VASP A	3BNHfkoeJ5hTAtGviQKGtuHdDnUP4fS67s	VASP A
bc1qufd8s2e7l29mkpnxh29z4zmyhqhz4jh8u62j64	VASP A	bc1qz0klefh90jpnk48krl8kka22z034g9dv9mfwxy	VASP A
bc1qla7dpxf23yqghxvgsnm6e46e4kgvgk3ghwanhs	VASP A	3LLxkyXbymE6gyncUtWCtDm2kMBYnh8Y5H	VASP A
36y5oizZAKNSXEEcvQnHHjBPzgDoyUgH6U	VASP A	3NjTTuWoAimdkF6kU29Wg3TaX9Y41xJk2Q	VASP A
3EwXtQN38N7bczhtssTaQXQ8V1ESzGCWXp	VASP A	36M14LUZ5QdCpPAvRhbyuPrbySCixana7q	VASP A
35WA9LqtgrFtnW99ZjG8SigwsDJfvCFNN6	VASP A	3NeVui16zjEFB5DAkZYnEzFzemwffxdLGC	VASP A
3FJuyixsUGR8aCHaJXotyu5mFTdgQTUGN8	VASP A	365dwi6ePGn5NQwrJPgpkn4AZtY7U1DAzd	VASP A
bc1qlvaaw7qg60g4r34uqvcykcyeprqq3gzunxl959	VASP A	1G2k682CGjbgDt5TA9LPvUUZALVnGRJNbX	VASP A
32oA2zy5g8bsH6ibA84zyTiot57UNn6cZk	VASP A	3ABGvFN2KUmyqCciVqGRWP7qozXC3GJY1t	VASP A
38Hed9w9ipv7chiztoXmVFpE9QoKK4A5e2	VASP A	37sF88thJvtaHKtDxWam1iNE967VXMYmZ4	VASP A
37h3xPkADPXz2Gf13LCbcQGPWSs9VUbijD	VASP A	1hseBvYYoSmrwLRxAiW8mZJ4PuDCk8vC6	VASP A
3BSLDuJ5BniD89ss7AixMAaxzNLxz73tqC	VASP A	bc1qpm8uuck4nd2drmah7pg4wn2ry8svpkzc5g9h2d	VASP A
3P51Su6oAUgKnqHA8RwAB17iXtNh1MqrLN	VASP A	12j9hDEUjjPx9r5fP6S6QwFrDt86pipHY5	VASP A
bc1q90ln97x30cu07k0c6f4sd5d0w304csx7wl65af	VASP A	3BaZvbaJMoLw7xDjk5kuujMCRkebSh35x7	VASP A
3GXL7pb7AQU2PuDUx2FanShaSxfaijSuoq	VASP A	3EX9Bufgb7E5dy63vwSPfBfbvuxz6AEdJ8	VASP A
3NSvc7wp661GKovmtsUowXirVsPZaaXfEA	VASP A	3PGzrQkvYshnDAdQb8mcajcXT69SLAUqNM	VASP A
3NKeW5Zp1C6MTVDvu45FrPwv64wmgwokMx	VASP A	3KbJUSyQxEQi7fgie2U8oEbEMPgzEXPhxb	VASP A
1DQUovque483G1qogond6ar2jekVbBbQoa	VASP A	3H1M9CJaGTmNWiKiGJSdjqvYK4jvgCkWZD	VASP A
3Q3R7ohNcmPAP8cJBxbGHvJ11dtD4AiWA4	VASP A	3R2Gf3pLjh4T45VoJbpXNUErjyu7iNi9Lc	VASP A
3JcHEnvorB1iYjb3PtNGGWZRekE3hrYZg2	VASP A	3LWD798xiNsHEj3tHmseTvMGicTyMw89yH	VASP A
3PZVQhKmXVyeF1u58GTpshWwba6MrVwoxx	VASP A	bc1qyw3t7aapdgfc6nnsq9cjt9snyyzm0h2m5cvz6c	VASP A
1AmicLpEygMr6XbifV3v89HEJE1JAob6MP	VASP A	3CFSNanniaS3TgXvKkDQxSdjaqFiZhYFjo	VASP A
bc1q2fuj4pdlvftes962udrl6rg8hserg5al9mwwq2	VASP A	3GiJn8VRRfuCWLcepv2vpz3SijnWDZbJNV	VASP A
1AXhjxmb84UXUuKMz1kiotrEWkYGHdr2pk	VASP A	3QTejSeVyUEyi1bdcYLBrbaW2Y7PcT1mYC	VASP A
33CcPBjiX8BSoAq1bnSwBykNvDu6D2ikPe	VASP A	1J8p8e8XerfNsT2rHPsT4EGXewcKN4TcZC	VASP A
3PoVeBNfNhyCkAXfY7zXFvevqxvAyjkZHo	VASP A	139JQeoAHTUvHbhZQrumMfvTVjjj4XHWqJ	VASP A
1EnxErtRRpfshfZHCGj2dhVfKqNUvqB6uV	VASP A	349o5hFXzajRqd5keuhc4Vpvk5UnJvKDwe	VASP A
3QDrBALoR558xr7AQ2qbUweLYMdkhTzGNi	VASP A	3EBhkMekkAbZnjZKj278S9Ep5CBopUwJAJ	VASP B
bc1qa2sshk7mf8ln6dcz3yshga4ry6yad40fafks3m	VASP B	bc1q5upx09sj98mkql9uchnjf2fz9zk0e5cp28393n	VASP B
bc1qekd92htscmj9jhnhe4c8uw5acnvgsl6pphzumg	VASP B	36WHTtkZ5jmwNk8ZyEQK7DYyjv99REjiXg	VASP C
3CoiP8UBMLkbqCftfE9VWfpTwFdTk4v8tk	VASP C	3Gc1VcYkVZN7onTxxMkRLqtmokzxpaFHGG	VASP C
bc1qnxx404l623aaejv252htxh39s42te6wu6aa8ay	VASP D	3Ai4XQYJyD3NRToE3PA8odv6SLqGLgCaaC	VASP D
bc1qp7h0wh3hxyax5nxawv36vxvpl7gml6t7dqr2tp	VASP D	3BoECgzNsS5NqNHn5wvtR9xVmyxCFDcGuD	VASP D
33cXNWciLE74bnRjk6Dz2k1fGVSxByewc8	VASP D	bc1qlu2qrxcxzkd2jkgzpj7ldspn8myfraxgwkyg2h	VASP D

Table A.2: List of Ethereum addresses.

Address	Label	Address	Label
0x1eDB8A5d51880c81bA6B4812485c3dC16085fC39	VASP A	0x2754b28227F041a66c46509D5620782BFC4766EF	VASP A
0x74dEc05E5b894b0EfEc69Cdf6316971802A2F9a1	VASP A	0xCC6E3Fd35F034F5baA27b6E74DCB197f084A8721	VASP A
0xF32682d5F99ba4143532618d6f516859a055Ea06	VASP A	0xDd0b0DE8D457b6FC20e8f9E9dd5a38A525EF4258	VASP B
0x0067F95A79c3C404a9d128168DDFDf3cB70c0852	VASP B	0x16076b17bd55a2ebbda011d39dca8916094a0c38	VASP C
0xC3b7336D5A5158215599572012CeDd4403A81629	VASP C		

Table A.3: VASPs categorization by their service offering — VASP-specific observations.

Name	Custody services	Buy/Sell services	Payment processing	Consulting services	Trading platform
VASP-0	N	Y	N	N	N
VASP-1	N	Y	N	N	N
VASP-2	Y	Y	N	N	Y
VASP-3	Y	Y	N	Y	Y
VASP-4	Y	Y	N	Y	N
VASP-5	Y	Y	N	N	N
VASP-6	Y	Y	N	Y	N
VASP-7	Y	Y	N	Y	N
VASP-8	N	Y	N	N	N
VASP-9	Y	Y	N	N	N
VASP-10	N	Y	N	N	N
VASP-11	N	Y	N	N	N
VASP-12	N	Y	N	N	N
VASP-13	Y	Y	N	Y	N
VASP-14	N	N	Y	N	N
VASP-15	Y	Y	N	Y	N
VASP-16	Y	Y	N	N	Y
VASP-17	Y	Y	N	Y	N
VASP-18	N	Y	N	N	N
VASP-19	Y	N	N	N	N
VASP-20	Y	Y	Y	N	N

Index of Working Papers:

January 13, 2021	Maximilian Böck, Martin Feldkircher, Burkhard Raunig	233	A View from Outside: Sovereign CDS Volatility as an Indicator of Economic Uncertainty
May 20, 2021	Burkhard Raunig	234	Economic Policy Uncertainty and Stock Market Volatility: A Causality Check
July 8, 2021	Thomas Breuer, Martin Summer, Branko Uroševic	235	Bank Solvency Stress Tests with Fire Sales
December 14, 2021	Michael Sigmund, Kevin Zimmermann	236	Determinants of Contingent Convertible Bond Coupon Rates of Banks: An Empirical Analysis
February 14, 2022	Elisabeth Beckmann, Christa Hainz, Sarah Reiter	237	Third-Party Loan Guarantees: Measuring Literacy and its Effect on Financial Decisions
February 16, 2022	Markus Knell, Reinhard Koman	238	Pension Entitlements and Net Wealth in Austria
May 9, 2022	Nicolás Albacete, Pirmin Fessler, Peter Lindner	239	The Wealth Distribution and Redistributive Preferences: Evidence from a Randomized Survey Experiment
June 20, 2022	Erwan Gautier, Cristina Conflitti, Riemer P. Faber, Brian Fabo, Ludmila Fadejeva, Valentin Jouvanceau, Jan-Oliver Menz, Teresa Messner, Pavlos Petroulas, Pau Roldan-Blanco, Fabio Rumler, Sergio Santoro, Elisabeth Wieland, Hélène Zimmer	240	New Facts on Consumer Price Rigidity in the Euro Area
June 29, 2022	Svetlana Abramova, Rainer Böhme, Helmut Elsinger, Helmut Stix	241	What can CBDC designers learn from asking potential users? Results from a survey of Austrian residents

July 1, 2022	Marcel Barmeier	242	The new normal: bank lending and negative interest rates in Austria
July 14, 2022	Pavel Ciaian, Andrej Cupak, Pirmin Fessler, d'Artis Kancs	243	Environmental-Social-Governance Preferences and Investments in Crypto-Assets
October 18, 2022	Burkhard Raunig, Michael Sigmund	244	The ECB Single Supervisory Mechanism: Effects on Bank Performance and Capital Requirements
April 5, 2023	Norbert Ernst, Michael Sigmund	245	Are zombie firms really contagious?
May 8, 2023	Richard Sellner, Nico Pintar, Norbert Ernst	246	Resource Misallocation and TFP Gap Development in Austria
September 5, 2023	Katharina Allinger, Fabio Rumler	247	Inflation Expectations in CESEE: The Role of Sentiment and Experiences
October 16, 2023	Pietro Saggese, Esther Segalla, Michael Sigmund, Burkhard Raunig, Felix Zangerl, Bernhard Haslhofer	248	Assessing the Solvency of Virtual Asset Service Providers: Are Current Standards Sufficient?