# Revisiting Transactional Statistics of High-scalability Blockchains

Daniel Perez
Imperial College London

Jiahua Xu
UCL CBT
EPFL

Benjamin Livshits
Imperial College London
UCL CBT
Brave Software

## ABSTRACT

Scalability has been a bottleneck for major blockchains such as Bitcoin and Ethereum. Despite the significantly improved scalability claimed by several high-profile blockchain projects, there has been little effort to understand how their transactional throughput is being used. In this paper, we examine recent network traffic of three major high-scalability blockchains—EOSIO, Tezos and XRP Ledger (XRPL)—over a period of seven months. Our analysis reveals that only a small fraction of the transactions are used for value transfer purposes. In particular, 96% of the transactions on EOSIO were triggered by the airdrop of a currently valueless token; on Tezos, 76% of throughput was used for maintaining consensus; and over 94% of transactions on XRPL carried no economic value. We also identify a persisting airdrop on EOSIO as a DoS attack and detect a two-month-long spam attack on XRPL. The paper explores the different designs of the three blockchains and sheds light on how they could shape user behavior.

## CCS CONCEPTS

• **Information systems** → **Data extraction and integration**.

## KEYWORDS

Blockchain, Transactional throughput, Internet measurements, Data extraction

## 1 INTRODUCTION

As the most widely-used cryptocurrency and the first application of a blockchain system, Bitcoin has been frequently criticized for its slow transactional throughput, making it hard to adopt as a payment method. Indeed, Bitcoin is only able to process around 10 transactions per second, significantly slower than the throughput offered by centralized payment providers such as Visa, which can process over 65,000 transactions per second [55]. Many blockchains have since been designed and developed in order to improve scalability, the most valued of these in terms of market capitalization [12] being EOSIO [8], Tezos [24], and XRP Ledger (XRPL) [62].

Although many of these systems have existed for several years already, to the best of our knowledge, no in-depth evaluation of the actual usage of their transactional throughput has yet been performed, and it is unclear up to what point these blockchains have managed to generate economic activity. The knowledge of both the quantity and the quality of the realized throughput is crucial for the improvement of blockchain design, and ultimately a better utilization of blockchains. In this paper, we analyze transactions of the three blockchains listed above and seek to find out:

RQ1 To what extent has the alleged throughput capacity been achieved in those three blockchains?
RQ2 Can we classify transactions by analyzing their metadata and patterns?
RQ3 Who are the most active transaction initiators and what is the nature of the transaction they conducted?
RQ4 Can we reliably identify DoS and transactional spam attacks by analyzing transaction patterns?

**Contributions.** We contribute to the body of literature on blockchain in the following ways:

(1) We perform the first large-scale detailed analysis of transaction histories of three of the most widely-used high-throughput blockchains: EOSIO, Tezos, and XRPL.
(2) We classify on-chain transactions and measure each category's respective share of the total throughput, in terms of the number of transactions and their economic volume.
(3) We establish a measurement framework for assessing the quality of transactional throughput in blockchain systems.
(4) We expose spamming behaviors that have inflated throughput statistics and caused network congestion.

(5) We highlight the large gap between the alleged throughput capacity and the well-intended transactions being performed on those three blockchains.

Our analysis serves as the first step towards a better understanding in the nature of user activities on high-scalability blockchains. On-chain monitoring tools can be built based on our framework to detect undesired or even malicious behavior.

**Summary of our findings.** Despite the advertised high throughput and the seemingly commensurate transaction volume, a large portion of on-chain traffic, including payment-related transactions, does not result in actual value transfer. The nature and purpose of non-payment-related activities varies significantly across blockchains.

Specifically, we observe that the current throughput is only 34 TPS (transactions per second) for EOSIO, 0.43 TPS for Tezos and 15 TPS for XRPL. We show that 96% of the throughput on EOSIO was used for the airdrop of a valueless token, 76% of transactions on the Tezos blockchain were used to maintain consensus, and that over 94% of transactions on XRPL carried zero monetary value.

## 2 BACKGROUND

In this section, we briefly explain the fundamentals of permissionless blockchains and describe the structure of the three blockchain systems that we evaluate, highlighting their various design aspects.

### 2.1 Blockchain Basics

In its essence, a blockchain is an append-only, decentralized database that is replicated across a number of computer nodes. Most blockchain systems record activities in the form of "transactions". A transaction typically contains information about its sender, its receiver, as well as the action taken, such as the transfer of an asset. Newly created transactions are broadcast across the network where they get validated by the participants. Valid transactions are grouped into data structures called *blocks*, which are appended to the blockchain by referencing the most recent block. Blocks are immutable, and state changes in the blockchain require new blocks to be produced.

Network latency and asynchrony inherent in the distributed nature of blockchains lead to a number of challenges. In particular, a blockchain must be able to reach consensus about the current state when the majority of participating nodes behave honestly. In order to resolve disagreement, a consensus protocol prescribing a set of rules is applied as part of the validation process.

The Proof-of-Work (PoW) consensus, introduced by Bitcoin and currently also implemented by Ethereum, requires the participant to solve a computationally expensive puzzle to create a new block. Although PoW can maintain consistency well, it is by nature very time- and energy-consuming, which limits its throughput. To preserve security while maintaining a sufficient degree of decentralization, scalability is often sacrificed [60]. Indeed, the rate of block creation for both Bitcoin and Ethereum is relatively slow—on average

10 minutes and 14 seconds per block, respectively—and the only way to increase the throughput is to increase the size of a single block, allowing for more transactions per block.

Another issue related to blockchain systems is the need for all participants to replicate the data. Since blockchains are append-only, participants need to ensure that their storage capacity keeps pace with the ever-increasing size of blockchain data. It is therefore crucial for blockchains to be designed in such a way that the storage used increases only moderately with time.

### 2.2 Consensus Mechanisms

In response to the scalability issues related to PoW, many blockchains have developed other mechanisms to ensure consensus, which allow higher rates of block creation.

**Delegated Proof-of-Stake (DPoS) in EOSIO.** EOSIO uses the Delegated Proof-of-Stake (DPoS) protocol which was first introduced in Bitshares [7].

Users of EOSIO, stake EOS tokens to their favored block producers (BPs) and can choose to remove their stake at any time. The 21 BPs with the highest stake are allowed to produce blocks whereas the rest are put on standby. Blocks are produced in rounds of 126 ($6 \times 21$). The order of block production is scheduled prior to each round and must be agreed upon by at least 15 block producers [8].

**Liquid Proof-of-Stake (LPoS) in Tezos.** For its consensus mechanism, Tezos employs another variant of Delegated Proof-of-Stake: the Liquid Proof-of-Stake (LPoS) [49]. Tezos' LPoS differs from EOSIO's DPoS in that with the former, the number of consensus participants—or "delegates"—changes dynamically [24, 49]. This is because any node with a minimum amount of staked assets, arbitrarily defined to be 8,000 XTZ (about 16,000 USD at the time of writing [12]), is allowed to become a delegate, who then has the chance to be selected as either a "baker" or an "endorser". Each block is produced ("baked") by one randomly selected baker, and verified ("endorsed") by 32 randomly selected endorsers [49]. The endorsements are included in the following block.

**XRP Ledger Consensus Protocol (XRP LCP) in XRPL.** XRPL is a distributed payment network created by *Ripple Labs Inc.* in 2012 that uses the XRP ledger consensus protocol [11]. Each user sets up its own unique node list of validators (UNL) that it will listen to during the consensus process. The validators determine which transactions are to be added to the ledger. Consensus is reached if at least 90% of the validators in each ones' UNL overlap. If this condition is not met, the consensus is not assured to converge and forks can arise [11].

### 2.3 Account and Transaction Types

In this section we describe the types of transactions that exist on the three blockchains.

*2.3.1 EOSIO.* EOSIO differentiates between system and regular accounts. The former are built-in accounts created when the blockchain was first instantiated, and are managed by

| | **EOSIO** | | | **Tezos** | | | **XRPL** | | |
|---|---|---|---|---|---|---|---|---|---|
| Category | Action name | # | % | Operation kind | # | % | Transaction type | # | % |
| Peer-to-peer transactions | **Transfer** | 8,479,573,653 | **96.2** | Transaction | 1,941,230 | 21.4 | **Payment** | 100,328,458 | **36.9** |
| | | | | | | | EscrowFinish | 677 | 0.0 |
| Account actions | newaccount | 289,680 | 0.0 | Reveal | 113,915 | 0.0 | TrustSet | 3,339,620 | 1.2 |
| | bidname | 244,248 | 0.0 | Origination | 3,159 | 1.3 | AccountSet | 150,401 | 0.1 |
| | deposit | 243,881 | 0.0 | Activate | 2,659 | 0.0 | SignerListSet | 13,707 | 0.0 |
| | linkauth | 148693 | 0.0 | | | | SetRegularKey | 734 | 0.0 |
| | updateauth | 136,926 | 0.0 | | | | DepositPreauth | 3 | 0.0 |
| Other actions | delegatebw | 684,449 | 0.0 | **Endorsement** | 6,957,612 | **76.6** | **OfferCreate** | 160,451,595 | **59.1** |
| | undelegatebw | 461,320 | 0.0 | Delegation | 56,336 | 0.6 | OfferCancel | 7,259,908 | 2.7 |
| | buyrambytes | 353,695 | 0.0 | Reveal nonce | 9,409 | 0.1 | EscrowCreate | 1,393 | 0.0 |
| | rentcpu | 187,878 | 0.0 | Ballot | 514 | 0.0 | EscrowCancel | 84 | 0.0 |
| | voteproducer | 137,713 | 0.0 | Proposals | 90 | 0.0 | PaymentChannelClaim | 172 | 0.0 |
| | buyram | 89,971 | 0.0 | Double baking evidence | 4 | 0.0 | PaymentChannelCreate | 33 | 0.0 |
| | Others | 332,799,590 | 3.8 | | | | EnableAmendment | 12 | 0.0 |
| Total | | 8,815,351,697 | 100.0 | | 9,084,928 | 100.0 | | 271,546,797 | 100.0 |

**Figure 1: Distribution of action types per blockchain.**

currently active BPs, while the latter can be created by anyone. System accounts are further divided into privileged and unprivileged accounts. Privileged accounts, including `eosio`, `eosio.msig`, and `eosio.wrap`, can bypass authorization checks when executing a transaction [19, 28] (see Section 2.2).

EOSIO system contracts, defined in `eosio.contracts` [21], are held by system accounts. One of the most commonly used system contracts is `eosio.token`, which is designed for creating and transferring user-defined tokens [19]. Regular accounts can freely design and deploy smart contracts.

Each smart contract on EOSIO has a set of actions. Actions included in non-system contracts are entirely user-defined, and users have a high degree of flexibility in terms of structuring and naming the actions. This makes the analysis of actions challenging, as it requires understanding their true functionality on a case-by-case basis. While many actions have a candid name that gives away their functionality (e.g. `payout` from contract `betdicegroup`), some are less expressive (e.g. `m` from user `pptqipaelyog`).

In Figure 1, we show different types of existing actions. Since actions from non-system contracts have arbitrary designs, we only examine actions that belong to system accounts for the moment, as these are already known and easier to classify. We make one exception to this and include the actions of *token* contracts, as they have a standardized interface [32]. Overall, we can see that token transfers account alone for more than 96% of the transactions. The rest of the transactions are mostly user-defined and appear under "Others" in the table, while actions defined in system contracts only account for a very small percentage of the entire traffic volume.

*2.3.2 Tezos.* Tezos has two types of accounts: implicit and originated. Implicit accounts are similar to the type of accounts found in Ethereum, generated from a public-private key pair [59]. These accounts can produce—or "bake"—blocks and receive stakes, but cannot be used as smart contracts. Bakers' accounts must be implicit, to be able to produce

blocks. Originated accounts are created and managed by implicit accounts, but do not have their own private key [39]. They can function as smart contracts, and can delegate voting rights to bakers' implicit accounts [36].

"Transactions" on Tezos are termed "operations." Operations can be roughly classified into three types: consensus related, governance related and manager operations [3]. Consensus-related operations, as the name indicates, ensure that all participating nodes agree on one specific version of data to be recorded on the blockchain. Governance-related operations are used to propose and select a new set of rules for the blockchain. However, these events are very rare and only involve bakers, which is why these operations only represent a low percentage of the total number of transactions. Operations mainly consist of delegations and peer-to-peer payment transactions. As shown in Figure 1, endorsement operations account for a vast majority, 76%, of total operations. Endorsements are performed by bakers, and a block needs a minimum of 32 endorsements for it to be accepted [37].

*2.3.3 XRPL.* XRPL also uses an account-based system to keep track of asset holdings. Accounts are identified by addresses derived from a public and private key pair. There are a handful of "special addresses" that are not derived from a key pair. Those addresses either serve special purposes (e.g. acting as the XRP issuer) or exist purely for legacy reasons. Since a secret key is required to sign transactions, funds sent to any of these special addresses cannot be transferred out and are hence permanently lost [61].

XRPL has a large number of predefined transaction types. We show part of them in Figure 1. The most common transaction types are `OfferCreate`, which is used to create a new order in a decentralized exchange (DEX) on the ledger, and `Payment`, which is used to transfer assets. There are also other types of transactions such as `OfferCancel` used to cancel a created order or `TrustSet` which is used to establish a "trustline" [62] with another account.

## 2.4 Expected Use Cases

In this section, we describe the primary intended use cases of the three blockchains and provide a rationale for the way they are being used, to better understand the dynamics of actual transactions evaluated in Section 4.

**EOSIO.** EOSIO was designed with the goal of high throughput and has a particularity compared to many other blockchains: there are no direct transaction fees. Resources such as CPU, RAM and bandwidth are rented beforehand, and there is no fixed or variable fee per transaction [8]. This makes it a very attractive platform for building decentralized applications with a potentially high number of micro-payments. Many games, especially those with a gambling nature, have been developed using EOSIO as a payment platform. EOSIO is also used for decentralized exchanges, where the absence of fees and the high throughput allow placing orders on-chain, unlike many decentralized exchanges on other platforms where only the settlement is performed on-chain [56].

**Tezos.** Tezos was one of the first blockchains to adopt on-chain governance. This means that participants can vote to dynamically amend the rules of the consensus. A major advantage of this approach is that the blockchain can keep running without the need of hard forks, as often observed for other blockchains [1, 2]. Another characteristic of Tezos is the use of a strongly typed programming language with well-defined semantics [38] for its smart contracts, which makes it easier to provide these for correctness. These properties make Tezos a very attractive blockchain for financial applications, such as the tokenization of assets [9].

**XRPL.** Similar to EOSIO, XRPL supports the issuance, circulation, and exchange of customized tokens. However, in contrast to EOSIO, XRPL uses the IOU ("I owe you") mechanism for payments. Specifically, any account on XRPL can issue an IOU with an arbitrary ticker — be it USD or BTC. Thus, if Alice pays Bob 10 BTC on XRPL, she is effectively sending an IOU of 10 BTC, which literally means "I (Alice) owe you (Bob) 10 BTC". Whether the BTC represents the market value of Bitcoin depends on Alice's ability to redeem her "debt" [65]. This feature contributes to the high throughput on XRPL, as the speed to transfer a specific currency is no more constrained by its original blockchain-related limitations: For example, the transfer of BTC on XRPL is not limited by the block production interval of the actual Bitcoin blockchain (typically 10 minutes to an hour to fully commit a block), and the transfer of USD is not limited to the speed of the automated clearing house (ACH) (around two days [33]).

## 3 METHODOLOGY

In this section, we describe the methodology used to measure the transactional throughput of the selected blockchains.

### 3.1 Definitions

We first introduce important definitions used in the rest the paper.

**Throughput-related definitions.** When quantified, a throughput value is expressed in TPS (transactions per second).

**Alleged Capacity** The theoretical capacity that a blockchain claims to be able to achieve

**Average Throughput** Average throughput recorded on the network throughout the observation period

**Maximum Throughput** Maximum throughput recorded on the network during the observation period

**Blockchain-related definitions.** We unify the terms that we use across the systems analyzed in this work. We sometimes diverge from the definition provided by a particular blockchain for terminological consistency.

**Block** Entity recorded on a blockchain and included as part of the blockchain to *advance* its state. Blocks are named as such on EOSIO and Tezos, the equivalent of which on XRPL is termed a "ledger".

**Transaction** Entity included at the top-level of a block and typically representing an atomic state transition. These are named as such on EOSIO and XRPL but are called "operations" in Tezos.

**Action** Entity included as part of the transaction and describing what the transaction should do. EOSIO and Tezos can have multiple actions per transaction. A single transaction containing multiple actions is only counted towards throughput once. Actions are called as such in EOSIO and are the "contents" of an "operation" on Tezos. XRPL does not feature this concept and each XRPL transaction can be thought of as a single action.

### 3.2 Measurement Framework

We implement a framework to measure throughput on the different blockchains. Our framework allows one to fetch historical data for all of the blockchains analyzed in this work, and to compute several statistics regarding blocks, transactions, actions and users. Transactions and actions can be, where relevant, aggregated by time, type, sender or receivers. Our framework is publicly available[1] and can easily be extended to add not only new statistics but also new blockchains. We provide an extended overview of the framework in Appendix.

### 3.3 Data Collection

We collect historical data on the three blockchains from October 1, 2019 to April 30, 2020. We provide an overview of the characteristics of the data in Figure 2. We note that the numbers of transactions is not the same as in Figure 1 as here we count only a transaction once, while in the previous table we counted all the actions included in a single transaction.

For all three of the blockchains, we first pinpoint the blocks which correspond to the start and end of our measurement period and use our framework to collect all the blocks included in this range. Each time, we use publicly available nodes or data providers to retrieve the necessary data.

---

[1]https://github.com/danhper/blockchain-analyzer

| | Block index | | Count | Count | Storage | Throughput (TPS) | | |
|---|---|---|---|---|---|---|---|---|
| | from | to | of blocks | of transactions | (.gzip, GB) | Alleged | Max | Average |
| **EOSIO** | 82,152,667 | 118,286,375 | 36,133,709 | 631,445,236 | 264 | 4,000 [30] | 136 | 34 |
| **Tezos** | 630,709 | 932,530 | 301,822 | 7,890,133 | 1.4 | 40 [4] | 0.57 | 0.43 |
| **XRPL** | 50,399,027 | 55,152,991 | 4,753,965 | 271,546,797 | 130 | 65,000 [44] | 56 | 15 |

Figure 2: Characterizing the datasets for each blockchain. All measurements are performed from October 1, 2019 to April 30, 2020. Max throughput is the average TPS within a 6-hour interval that has the highest count of transactions. Storage size is computed with data saved as JSON Lines with one block per line and compressed using gzip level 6 of compression.

**EOSIO.** EOSIO nodes provide an RPC API [22] which allows clients to retrieve the content of a single block, through the get_block endpoint [18]. EOSIO also has a list of block producers who usually provide a publicly accessible RPC endpoint. Out of 32 officially advertised endpoints, we shortlist 6 that have a generous rate limit with stable latency and throughput.

We collect data from block 82,152,667 to block 118,286,375, or a total of 36,133,709 blocks containing 631,445,236 transactions, representing more than 260GB of data.

**Tezos.** Similar to EOSIO, Tezos full nodes provide an RPC API and some bakers make it publicly available. We measure the latency and throughput of several nodes and select the one for which we obtained the best results [54]. We obtain 301,822 blocks containing 7,890,133 transactions, for a total size of approximately 1.4 GB of data.

**XRPL.** XRPL has both an RPC API and a websocket API with similar features. Although there are no official public endpoints for XRPL, a high-availability websocket endpoint is provided by the XRP community [58]. We use the ledger method of the Websocket API to retrieve the data in the same way we did with EOSIO and Tezos.

In addition, we use the API provided by the ledger explorer XRP Scan [48] to retrieve account information including username and parent account.[2] Since large XRP users such as exchanges often have multiple accounts, this account information can be used to identify and cluster accounts.

In total, we analyze 4,753,965 blocks covering seven months of data, and containing a total of more than 150 million transactions. The total size of the compressed data is about 130 GB.

## 4 DATA ANALYSIS

In this section, we present summary statistics and high-level illustrations of the transactions contained in the datasets of the three different blockchains.

### 4.1 Transaction Overview

In Figure 3, we decompose the number of actions into different categories. XRPL and Tezos have well-defined action types, and we use the most commonly found ones to classify the throughput. EOSIO does not have pre-defined action types: contract creators can decide on arbitrary action types.

To be able to classify the actions and understand where throughput on EOSIO is coming from, we manually label the top 100 contracts, representing more than 99% of the total throughput, by grouping them into different categories and assign one of the categories to each action.

**EOSIO.** Interestingly, there is a huge spike in the number of token actions from the November 1, 2019 onward. We find that this is due to a new coin called EIDOS [17] giving away tokens. We will describe this more extensively as a case study in Section 5.1. Before this peak, the number of actions on EOSIO was vastly dominated by games, in particular betting games.

**Tezos.** Tezos has a high number of "endorsements"—76%, which are used as part of the consensus protocol, and only a small fraction of the throughput are actual actions. It is worth noting that the number of "endorsements" should be mostly constant regardless of the number of transactions, and that if the number of transactions were to increase enough, the trend would reverse. We can also clearly see that Tezos has very regular spikes, with an interval of approximately two to three days each time. These appear to be payments from bakers to stakers [14],[3] which can arguably be thought to be part of the consensus. We use the TzKT API[4] to find account names and find that roughly 53% of these "Transaction" actions are sent by bakers and 6% of the are sent by the Tezos faucet [51]. Endorsements and actions sent by either bakers or the faucet sums up about 87% of the total number of actions.

**XRPL.** On XRPL, both successful and unsuccessful transactions are recorded. A successfully executed transaction executes the command—such as Payment, OfferCreate, OfferCancel—specified by its initiator, while the only consequence of an unsuccessful transaction is the deduction of transaction fees from the transaction initiator. Across the sample period, roughly one tenth of transactions are unsuccessful (Figure 3c), with the most frequently registered errors being PATH_DRY for Payment (insufficient liquidity, hence "dry", for specified payment path) and tecUNFUNDED_OFFER for OfferCreate (no funds for the currency promised to offer by the offer creator).

Successful transactions primarily consist of Payment (39.6%) and OfferCreate (59.1%) (Figure 1). The number of OfferCreate is generally constant across time, but the
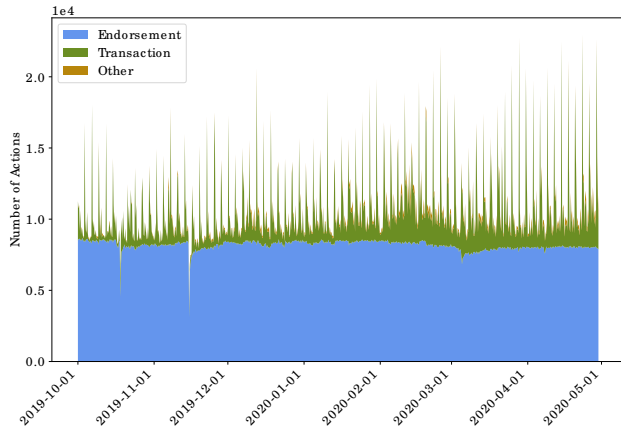
---

[2]A parent account sends initial funds to activate a new account.

[3]https://twitter.com/CitezenB/status/1256147427905716224
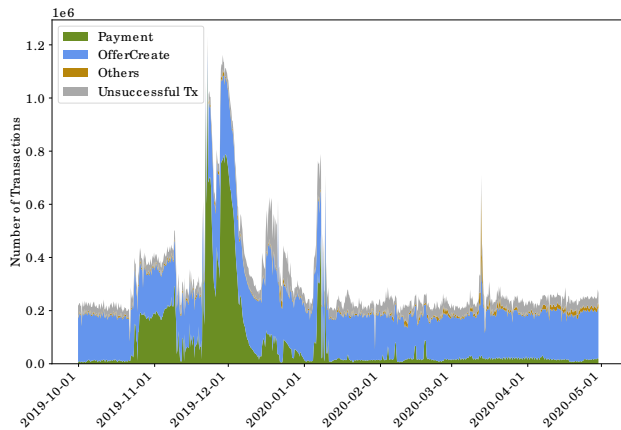[4]https://api.tzkt.io/
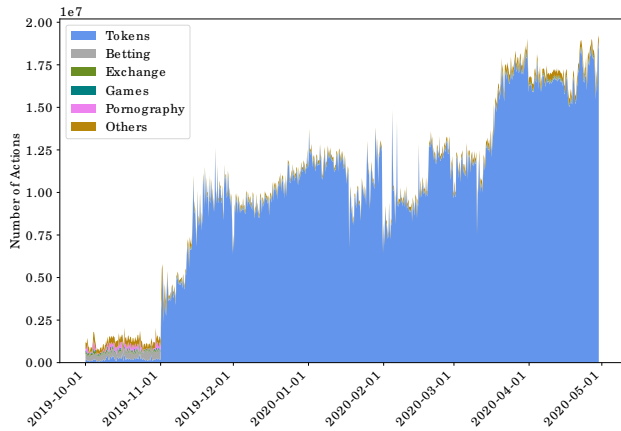
(a) EOSIO throughput over time



(b) Tezos throughput over time



(c) XRPL throughput over time

**Figure 3: On-chain throughput over time, y-axis represents transaction count per 6 hours.**

| Receiver | Description | Tx Count | Actions | |
|---|---|---|---|---|
| | | | Name | % |
| eosio.token | EOS token | 8,430,707,864 | transfer | 100.0% |
| betdicetasks | Gambling game | 32,804,674 | removetask | 66.65% |
| | | | log | 15.71% |
| whaleextrust | Decentralized exchange | 26,102,077 | verifytrade2 | 18.63% |
| | | | verifytrade3 | 17.52% |
| | | | clearing | 16.77% |
| pptqipaelyog | Unknown | 24,109,437 | m | 93.00% |
| pornhashbaby | Pornography website | 23,677,938 | record | 99.86% |

**Figure 4: EOSIO top applications as measured using the number of received transactions.**

number of Payment has a very high variance, with some periods containing virtually no payments and others having significant spikes. In Section 5.3, we reveal why most transactions during these high-volume periods are economically meaningless.

Except for the two spam periods, we observe that OfferCreate is the most common transaction type. Nonetheless, OfferCreate transactions contribute little to the total volume on XRPL.[5] This is because an offer expires if not fulfilled (fully or partially) before the expiry time defined by the offer creator; it can also be cancelled by its creator or superseded by a new offer. In fact, 0.2% of OfferCreate transactions resulted into an actual token exchange deal during our observation period.

## 4.2 Transaction Patterns

To understand better what the major sources of traffic constitute, we analyze the top accounts on EOSIO, Tezos, and XRPL, and find various transaction patterns.

**EOSIO.** In Figure 4, we show EOSIO accounts with the highest number of received actions. We can see that the eosio.token account, which is the account used to handle EOS token transfers, is by far the most used account, and that almost all calls to this account use the transfer action. Although EOS transfers are indeed a central part of the EOSIO ecosystem, more than 99.9% of the transfers shown are exclusively to and from this EIDOS account. The second account is a betting website where all the bets are performed transparently using EOSIO. However, around 80% of the actions—removetask and log—are bookkeeping, and the actual betting-related actions such as betrecord represent a very low percentage of the total number of actions. The third account is a decentralized exchange and is used to exchange different assets available on EOSIO. This exchange will be discussed in Section 5. We could not find information about the fourth account, but it is very actively sending EOS tokens to the EIDOS account. Finally, the last account was a pornography website which used EOSIO as a payment system. This account is still the fifth account with the highest number

---

[5]On May 10, 2020, for example, Ripple reported that the 24-hour XRP ledger trade volume—enabled via OfferCreate transactions—only accounts for 1% of the total ledger volume, while the payment volume—enabled via Payment transactions—accounts for 99%.

| Sender | Sent count | Unique receivers | Avg. # of transactions per receiver |
|---|---|---|---|
| tz1VwmmesDxud2BJEyDKUTV5T5VEP8tGBKGD | 106,477 | 23,649 | 4.50 |
| tz1cNARmnRRrvZgspPr2rSTUWq5xtGTuKuHY | 105,202 | 2,096 | 50.19 |
| tz1Mzpyj3Ebut8oJ38uvzm9eaZQtSTryC3Kx | 93,448 | 93,444 | 1.00 |
| tz1SiPXX4MYGNJNDsRc7n8hkvUqFzg8xqF9m | 57,841 | 19,382 | 2.98 |
| tz1acsihTQWHEnxxNz7EEsBDLMTztoZQE9SW | 42,683 | 1,436 | 29.72 |

**Figure 5: Tezos accounts with the highest number of sent transactions.**

of received actions although the service was discontinued in November 2019 for financial reasons [26].

**Tezos.** As Tezos neither has account names nor actions in the transactions metadata, analyzing the top receivers' accounts is less interesting, as it is very difficult to perform any type of attribution. However, we find interesting patterns from observing the top sending accounts. Most of the top senders in Tezos seem to follow a similar pattern: Sending a small number of transactions (between 5 and 50) to many different accounts. Another important thing to note is that all of these accounts are not contracts but regular accounts, which means that the transactions are automated by an off-chain program. After further investigation, we find that the top address is the Tezos Faucet [51]. The other addresses appear to be bakers' payout addresses and the transactions are payouts to stakers [31], corresponding to the peaks seen in Figure 3b. For completeness, we include the top senders and some statistics about them in Figure 5.

**XRPL.** From October 1, 2019 to April 30, 2020, a total of 195 thousand accounts collectively conducted 272 million transactions, i.e. an average of 1.4 thousand transactions per account during the seven-month observation period.

The distribution of the number of transactions per account is highly skewed. Over one third (71 thousand) of the accounts have transacted only once during the entire observation period, whereas the 35 most active accounts are responsible for half of the total traffic. Figure 6 lists of the top 10 accounts by the number of conducted transactions. With the exception of rKLpjpCoXgLQQYQyj13zgay73rsgmzNH13 and r96HghtYDxvpHNaru1xbCQPcsHZwqiaENE, all these accounts share suspiciously similar patterns:

(1) more than 98% of their transactions are OfferCreate;
(2) they are either descendants of an account from Huobi, a crypto exchange founded in China, or frequently transact with descendants from Huobi;
(3) they have all transacted using CNY;
(4) their payment transactions conspicuously use the same destination tag 104398, a field that—similar to a bank reference number—exchanges and gateways use to specify which client is the beneficiary of the payment [64].

The aforementioned similarities, in particular the last one, signal that those accounts are controlled by the same entity, presumably with a strong connection to Huobi. The frequent placement of offers might come from the massive client base of the entity.

Notably, the sixth most active account, r96HghtYDxvpHNaru1xbCQPcsHZwqiaENE, registered under the username chineseyuan only carried out *one* successful Payment transaction during the observation period, while the rest of the over four million transactions failed with a PATH_DRY error. Recall that failed transactions still occupy on-chain throughput. Therefore, it is evident that chineseyuan spammed the network.

## 4.3 Analysis Summary

Here, we highlight some of the observations about the data described above.

- Transactions on EOSIO can be roughly divided by the category of contracts they belong to. Before the arrival of the EIDOS token, approximately 50% of these are transactions to betting games. The rest was split between token transfers and various forms of entertainment, such as games not involving betting as well as payments to pornography web sites. The launch of EIDOS increased the total number of transactions more than tenfold, resulting in 96% of the transactions being used for token transfers.
- The vast majority (76%) of transactions on Tezos are used by the endorsement operation to maintain consensus. This is due to the fact that blocks typically contain 32 endorsements [49] and the number of transactions on the network is still low. The rest of the throughput is mainly used by transactions to transfer assets between accounts.
- OfferCreate and Payment are the two most popular transaction types on XRPL, accounting for 59.1% and 36.9% of the total throughput, respectively. Between October 1, 2019 and October 8, 2019, before the systematic spamming periods, the fractions of OfferCreate and Payment are 79% and 18%, respectively. Overall, one tenth of the transactions fail.

## 5 CASE STUDIES

In this section, we present several case studies of how the transaction throughput on the three blockchains is used in practice, for both legitimate and less legitimate purposes.

## 5.1 Inutile Transactions on EOSIO

**Exchange Wash-trading.** We investigate WhaleEx, who claims to be the largest decentralized exchange (DEX) on EOSIO in terms of daily active users [57]. As shown in Figure 4, the most frequently-used action of the WhaleEx contract are verifytrade2 and verifytrade3, with a combined total of 9,437,393 calls over the seven months observational period, which corresponds to approximately one action every two seconds. These actions are executed when a buy offer and a sell offer match each other and signals a settled trade.

Firstly, and most obviously, we notice that in more than 75% of the trades, the buyer and the seller are *the same*. This means that no asset is transferred at the end of the action. Furthermore, the transaction fees for both the

| Account | Type | Count | TotalCount | % of total throughput |
|---|---|---|---|---|
| r4AZpDKVoBxVcYUJCWMcqZzyWsHTteC4ZE | OfferCreate<br>Others<br>Payment | 21,790,612<br>291,687<br>132 | 22,082,431 | 8.13% |
| rQ3fNyLjbvcDaPNS4EAJY8aT9zR3uGk17c | OfferCreate<br>Others<br>Payment | 21,716,850<br>140,088<br>46 | 21,856,984 | 8.05% |
| rh3VLyj1GbQjX7eA15BwUagEhSrPHmLkSR | OfferCreate<br>Others<br>Payment | 21,510,597<br>31,295<br>37 | 21,541,929 | 7.93% |
| r4dgY6Mzob3NVq8CFYdEiPnXKboRScsXRu | OfferCreate<br>Others<br>Payment | 21,474,131<br>29,841<br>163 | 21,504,135 | 7.92% |
| rKLpjpCoXgLQQYQyj13zgay73rsgmzNH13 | Payment | 4,493,754 | 4,493,754 | 1.65% |
| r96HghtYDxvpHNaru1xbCQPcsHZwqiaENE | Payment | 4,488,127 | 4,488,127 | 1.65% |
| rBW8YPFaQ8WhHUy3WyKJG3mfnTGUkuw86q | OfferCreate<br>Others | 4,474,481<br>967 | 4,475,448 | 1.65% |
| rDzTZxa7NwD9vmNf5dvTbW4FQDNSRsfPv6 | OfferCreate<br>Others | 4,472,749<br>1,043 | 4,473,792 | 1.65% |
| rV2XRbZtsGwvpRptf3WaNyfgnuBpt64ca | OfferCreate<br>Others<br>Payment | 4,470,525<br>977<br>76 | 4,471,578 | 1.65% |
| rwchA2b36zu2r6CJfEMzPLQ1cmciKFcw9t | OfferCreate<br>Others<br>Payment | 4,470,528<br>1,008<br>15 | 4,471,551 | 1.65% |

**Figure 6: XRPL accounts with the highest number of transactions.**

buyer and the seller are 0, which means that such a transaction is achieving absolutely nothing else than *artificially* increasing the service statistics, i.e. wash-trading.

Further investigation reveals that accounts involved in the trades that are signaled by either `verifytrade2` or `verifytrade3` are highly concentrated: the top 5 accounts, as either a "seller" or a "buyer", are associated with over 78% of the trades. We compute the percentage of such transactions for the top 5 accounts and find that each of these accounts acts simultaneously as both seller and buyer in more than 88% of the transactions they are associated with. This means that the *vast majority* of transactions of the top 5 accounts represent wash-trading.

Next, we analyze the amount of funds that has been moved, i.e. the difference between the total amount of cryptocurrency sent and received by the same account. For the most active account, we find that only one of the 4 currencies has a balance change of over 0.3%. The second most frequently used account has a similar transaction pattern, with only 2 out of the 32 currencies traded showing a balance change larger than 0.6%. The rest of the top accounts all follow a very similar trend, with almost all the traded currencies having almost the same sent and received amounts.

**Boomerang transactions.** As shown in Figure 3a, there was a very sharp increase of activity on EOSIO after November 1, 2019. After investigating, we find that this increase is due to the airdrop of a new coin called `EIDOS` [17].

The token distribution works as follows: Users send any amount of `EOS` to the EIDOS contract address, the EIDOS contract sends the `EOS` amount back to the sender and also sends 0.01% of the `EIDOS` tokens it holds. This creates a "boomerang" transaction for the `EOS` token and a transaction to send the `EIDOS` token. The tokens can then be traded for USDT (Tether) which can in turn be converted to other

currencies. There are no transaction fees on EOSIO and users can execute transactions freely within the limits of their rented CPU capacity. Therefore, this scheme incentivizes users with idle CPU resources on EOSIO to send transactions to this address, creating a large increase in the numbers of transactions.

Soon after the launch of this coin, the price of CPU usage on EOSIO spiked by 10,000% and the network entered a congestion mode. In a normal mode, users can consume more CPU than they staked for, but when the network is in congestion mode, they can only consume the amount staked. Although this is how the network is supposed to behave, it is problematic if it lasts for a non-negligible period of time. For example, `EOS` is used for games where many users make a small number of transactions without staking CPU. When the network enters congestion mode for a long period of time, these users cannot continue to play unless they actively stake `EOS` for CPU. This has caused some services to threaten with their migration to another blockchain [16].

The coin seems to be operated by an entity called Enumivo but there is very scarce information about what service it provides. Given the very hostile tone in communications[6], it is likely that the creator indeed intended to congest the EOSIO network. Furthermore, the entity behind the `EIDOS` token seems to be willing to launch a "sidechain" of EOSIO [46].

**Summary.** One of the major selling points of EOSIO is its absence of transaction fees for most users. Although this clearly provides advantages for users, it can also result in spamming behaviors, as observed in this section. The fee-free transaction environment encourages market manipulation such as the WhaleEx wash-trading; moreover, it has also back-fired with the `EIDOS` token, as the network had to enter

---

[6]https://twitter.com/enumivo/status/1193353931797057536

(a) Proposal period      (b) Exploration period      (c) Promotion period
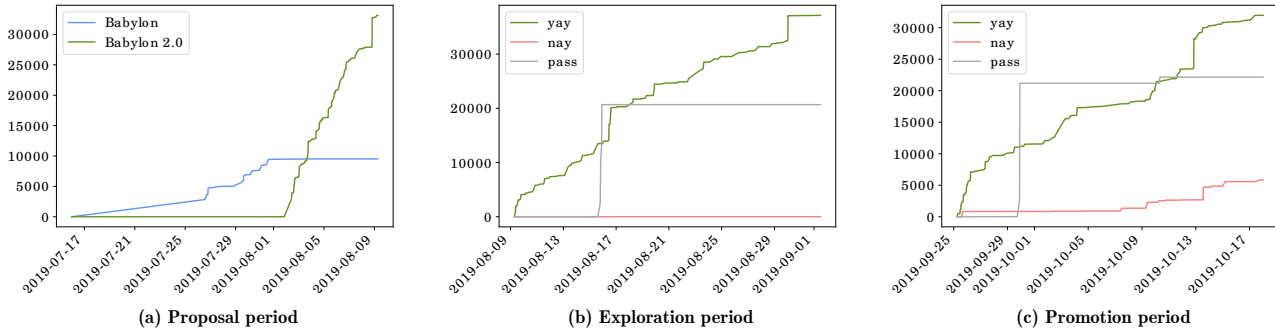
Figure 7: Tezos Babylon on-chain amendment voting process.

congestion mode and users have to stake an amount much higher than transaction fees in the Bitcoin network [16].

## 5.2 Governance Transactions on Tezos

One of the main particularities of Tezos, compared to other blockchains, is its on-chain governance and self-amendment abilities. Given that only *bakers* are allowed to send such transactions and that they can only perform a limited number of actions within a certain time frame, governance-related transactions represent only a very small fraction of the total number of transactions: merely 604 within our observation period. However, given that this type of transaction is rather unique and has, to the best of our knowledge, not been researched before, we analyze how the different phases of the governance process are executed in practice.

**Tezos voting periods.** Tezos voting is divided into four periods, each lasting around 23 days [24]. During the first period, the proposal period, bakers are allowed to propose an amendment in the form of source code to be deployed as the new protocol for Tezos. At the end of this period, the proposal with the highest number of bakers' votes is selected for the next period: The exploration period. During the exploration period, the bakers either choose to approve, refuse or abstain on voting on the proposal. If the quorum and the minimum positive votes—both thresholds are dynamically adjusted based on past participation—is reached, the proposal enters the testing period. During the testing period, the proposal is deployed on a testing network, without affecting the main network. Finally, the last period is the promotion vote period, which works in the same way as the exploration period but if successful, the new protocol is deployed as the new main network.

**Analyzing Tezos Voting.** To investigate the entire voting process in Tezos, we collect extra data associated with a recent amendment called Babylon 2.0 [13], which was proposed on August 2, 2019 and promoted to the main network on October 18, 2019. We show the evolution of the votes during the different voting phases in Figure 7.

During the proposal period, a first proposal, "Babylon", was submitted and slowly accumulated votes. During this phase, the authors of Babylon received feedback from involved parties and released an updated protocol, Babylon 2.0. Votes can be placed on multiple proposals which is why the number of previous votes on Babylon did not decrease. At the end of the vote, the participation was roughly 49%. It is worth noting that, although in practice any baker can propose an amendment to the network, from the creation of the Tezos blockchain up until the time of this writing, only Cryptium Labs and Nomadic Labs, who are both supported by the Tezos Foundation, have made successful proposals.

During the exploration period, participants can vote "yay" to support the proposal, "nay" to reject it, or "pass" to explicitly abstain from voting. No negative votes were cast during this period and the only abstention was from the Tezos Foundation, whose policy is to always abstain to leave the decision to the community. This phase had a participation of over 81%, significantly higher than for the previous round. This can be explained by the fact that explicit abstention counts as participation, while there is no way to explicitly abstain in the proposal phase.

Finally, after the testing period during which the proposal was deployed and tested on a testnet, the promotion period started. The trend was mostly similar to what was observed in the exploration period, but the number of votes against the proposals increased from 0 to 15%, as some bakers encountered trouble during the testing period due to changes in the transaction format that led to breaking components [40].

**Improvement potential on voting mechanism.** There are currently four periods in the Tezos voting system. First, participants can submit proposals, then they decide whether to try the elected proposal on a testing network and finally whether to amend the main network using the proposal. However, at the time of writing, in every exploration period seen, proposals have always received more than 99% approval during the exploration period. With the only exception where more than 99% of rejections were received [50] during the exploration period, the participation during the proposal period was below 1%. This shows that proposals selected by a large enough number of participants are almost unanimously approved in the exploration period. Although the current voting scheme could be useful in the future, we believe this shows that in the current state of the network, the proposal

| Issuer name | Issuer account | Rate |
|---|---|---|
| Bitstamp | rvYAfWj5gh67oV6fW32ZzP3Aw4Eubs59B | 36,050 |
| Gatehub Fifth | rchGBxcD1A1C2tdxF6papQYZ8kjRKMYcL | 35,817 |
| BTC 2 Ripple | rMwjYedjc7qqtKYVLiAccJSmCwih4LnE2q | 409 |
| *not registered* | r3fFaoqaJN1wwN68fsMAt4QkRuXkEjB3W4 | 1 |
| *not registered* | rpJZ5WyotdphojwMLxCr2prhULvG3Voe3X | 0 |

(a) **Rates (in XRP) of BTC IOUs issued by exemplary accounts in demonstration of the wide rate range. Each rate value is the average exchange rate of the issuer-specific BTC IOU tokens. Data retrieved through https://data.ripple.com/v2/exchange_rates/BTC+{issuer_ address}/XRP?date=2020-01-01T00:00:00Z&period=30day [63].**

| Date | Seller account of BTC IOU | Rate |
|---|---|---|
| 2019-12-14 | rHVsygEmrjSjafqFxn6dqJWHCdAPE74Zun | 30,500 |
| 2020-01-09 | rU6m5F9c1eWGKBdLMy1evRwk34HuVc18Wg | 1 |
| 2020-01-09 | rU6m5F9c1eWGKBdLMy1evRwk34HuVc18Wg | 0.1 |

(b) **Rate (in XRP) of BTC IOUs issued by rKRNtZzfrkTwE4ggqXbmfgoy57RBJYS7TS at different time. In all the three exchange transactions, the account that buys the BTC IOU against XRP is rMyronEjVcAdqUvhzx4MaBDwBPSPCrDHYm**

**Figure 8: Rate (in XRP) of BTC IOUs on XRPL.**

and exploration periods could be merged. This would allow a reduction in the time until amendments ship to the main network without compromising the functionality or security of the network.

## 5.3 Zero-value Transactions on XRPL

**Payments with zero-value tokens.** As described in Section 2.4, XRPL offers autonomy in currency issuance. On the flip side, this means that it is easy to generate seemingly high-value, but in effect valueless and useless transactions. Currencies bearing the same ticker issued by different accounts can have drastically differing valuations due to the varying level of trust in their issuers and the redeemability of their IOU tokens, which has in the past caused confusion among less informed users.[7]

In fact, the only currency whose value is recognized outside of XRPL is its native currency XRP, which is also the only currency that cannot be transferred in the form of IOUs. Non-native currencies can be exchanged with each other or to XRP via decentralized exchanges (DEX) on the ledger. Therefore, a reliable way of evaluating a currency by a certain issuer is to look up its exchange rate against XRP. Normally, only IOU tokens issued by featured XRPL gateways are deemed valuable; in contrast, tokens issued by random accounts are most likely to be deemed worthless. For example, the value of BTC IOUs from various issuer accounts could range from 0 to 36,050 XRP (Figure 8a).

The ledger experienced two waves of abnormally high traffic in the form of Payment transactions in late 2019, the first between the end of October and the beginning of November, the second—at a higher level—between the end of November and the beginning of December (Figure 3c). The culprit behind the increased traffic is rpJZ5WyotdphojwMLxCr2prhULvG3Voe3X, an account activated on October 9, 2019 which itself managed to activate 5,020 new accounts within one week with a

[7]https://twitter.com/Lord__of__Crypto/status/965344062084497408
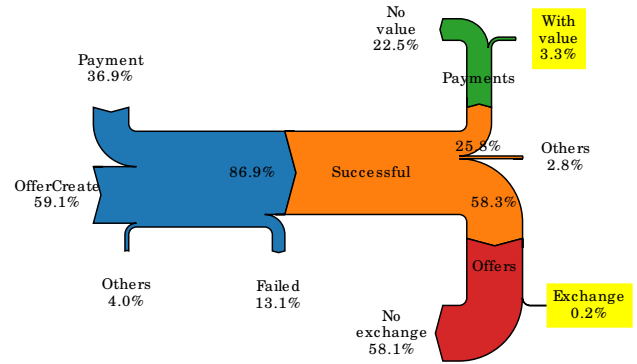


(a) Observation period: October 1, 2019 to April 30, 2020.
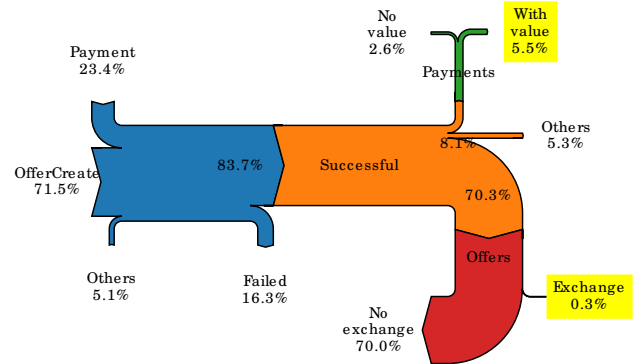


(b) Observation period: February 1, 2020 to April 30, 2020, during which the throughput was not polluted by systematic Payment spams.

**Figure 9: XRPL throughput by transaction type, success and value transferred. Highlighted transactions carry economic value.**

total of 1 million XRP (roughly 250,000 USD), only to have them perform meaningless transactions between each other, wasting money on transaction fees. The behavior triggered a heated debate in the XRP community where a member claimed that the traffic imposed such a burden to their validator that it had to be disconnected [53].

Ripple suspected it to be "an attempt to spam the ledger" with little impact on the network.[8] However, large exchanges such as Binance suffered from temporary XRP withdrawal failures, who cited the XRP network congestion as the cause [5]. It remains something of a mystery how such an expensive form of "spam" benefited its originators.

The payment transactions from the spam did not carry any value, since they involved transferring BTC IOU tokens unacceptable outside of the spammer's network.

To quantify true value-transferring Payment transactions, we retrieve the exchange rate with respect to XRP of all the issuer-specific tokens that were transferred between October 1, 2019 and April 30, 2020. Only 12.8% (3.3%/25.8%) of all successful Payment transactions involve tokens with a positive XRP rate (Figure 9a).

[8]https://twitter.com/nbougalis/status/1198670099160322048

To obtain a picture of throughput usage uncontaminated by systematic spam, we re-examine the transaction data from February 1, 2020 to April 30, 2020. During this period, 67.9% successful `Payment` transactions led to value transfer (Figure 9b). Nevertheless, the value-carrying share of total throughput remains under 6%, since successful `Payment` transactions only account for a small fraction (8.1%) of the overall traffic and the majority (97.9%) of `OfferCreate` transactions eventually becomes void.

In Figure 10, we show the top senders and receivers of value-carrying `Payment` transactions, as well as the most popular currencies being transferred. To cluster accounts, we rely on usernames as the identifier, as one entity can have multiple addresses under a given user name (e.g. `Binance`, `Coinbase`). For accounts with no registered username, we use their parent's username, if available, plus the suffix "descendant" as their identifier.

As one might expect, `XRP` is by far the most used currency on the ledger in terms of payment volume: 125 billion `XRP` for seven months, or 586 million `XRP` per day.

The top 10 senders cover 53% of this volume, while the top 10 receivers are the beneficiaries of 50% of the volume. Payments from Ripple alone account for 7% (9 billion `XRP`) of the `XRP` volume, largely due to transactions associated with the monthly release of one billion `XRP` from escrows. While the `XRP` release itself is captured through `EscrowCreate` transactions, 90% of the released funds were unused and returned to escrows for future release [47] through `Payment` transactions. All other top accounts presented are held either by exchanges, or, in rare cases, by accounts that were opened by an exchange. `Binance` appears to be the most avid `XRP` user, sending 15.2 billion and receiving 14.5 billion `XRP` during the observation period.

The most popular IOU tokens for fiat currencies include `USD`, `EUR` and `CNY` (Figure 10). Specifically, 328 million `USD`, 8 million `EUR` and 19 million `CNY` issued had positive exchange rates against `XRP`. The average on-ledger exchange rates of those three fiat currency tokens, irrespective of their issuers, were 5.4 XRP/USD, 5.5 XRP/EUR and 0.7 XRP/CNY, largely in accordance with the off-ledger exchange rates.[9]

**Fulfilled offers with zero-value tokens.** We found a series of conspicuous payment transactions with the aggregate transfer of 360,222 `BTC IOU`, issued by `rKRNtZzfrkTwE4ggqXbmfgoy57RBJYS7TS`, an account activated by Liquid (liquid.com), from the issuer itself to `rMyronEjVcAdqUvhzx4MaBDwBPSPCrDHYm`, an account activated by uphold (uphold.com). The `BTC IOU` token was exchanged at 30,500 `XRP`, resulting in a valuation of 11 billion `XRP` of those payments. We examine the legitimacy of the exchange rates in the next step.

The issuer is not the only factor behind the value of an IOU token. Even IOU tokens for the same currency from the same issuer can at times exhibit vastly different rates. Figure 8b shows an example where the `BTC IOU` from the same issuer
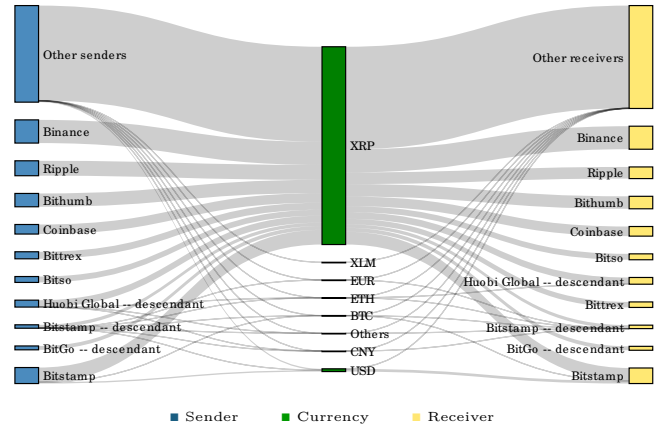


**Figure 10: Value flow on the XRP ledger between October 1, 2019 and April 30, 2020. The bandwidth of each flow represents the magnitude of aggregate value transferred denominated in `XRP`. Only `Payment` transactions are included.**

`rKRNtZzfrkTwE4ggqXbmfgoy57RBJYS7TS` was traded at 30,500 `XRP` in December 2019 but then declined to 0.1 `XRP` within a month.

The three exchange instances in Figure 8a were `OfferCreate` transactions where the initiator intended to sell `BTC ICO` for `XRP`. We discover that all three offers were filled by the same account `rMyronEjVcAdqUvhzx4MaBDwBPSPCrDHYm`, who received the aforementioned `BTC IOU` tokens directly from the issuer's account. Additional evidence on social media reveals that the IOU issuer's account is held by someone named `Myrone Bagalay`.[10] It becomes obvious that the offer taker's address, starting with `rMyronE`, must belong to the same person.

By tracing the transaction history of the concerned accounts, we notice that the two offer creators' accounts received their initial `BTC IOU` tokens through payments from the offer taker. Furthermore, one offer creator's account, `rU6m5F9c1eWGKBdLMy1evRwk34HuVc18Wg`, was activated by the offer taker's account. Now we can safely assume that all the accounts involved are controlled by that `Myrone Bagalay`, who issued `BTC IOU` tokens and traded them at arbitrarily determined rates with himself.

What `Myrone Bagalay` did is completely legitimate within the confines of XRPL. In fact, one of the key features of the ledger is the flexibility to establish a closed economy with a limited number of mutually-trusting users who can exchange self-defined assets that are not necessarily acknowledged outside the system. However, this makes it challenging to gauge the true value transfer on XRPL, since an IOU token's price—which we proxy by its exchange rate against `XRP`—can be easily inflated or deflated.

Additionally, privately-issued IOU tokens that are never exchanged on the ledger, while seemingly worthless, might be valuable to their transactors after all, should they reach

---

[9]https://finance.yahoo.com/

---

[10]See https://youtu.be/gVoyCEPvO30 and https://www.twipu.com/ MyroneBagalay/tweet/1161288087386894341.

an agreement on those tokens' value off the ledger. However, there is no easy way to assess such value, and we leave the analysis of IOUs to future work.

**Summary.** In summary, the throughput on XRPL during our observation period appeared to be fraught with zero-value transactions. We learned that both transaction volume and token value on XRPL are highly manipulable. One must thus fully understand the underlying measurement approach to correctly interpret the resultant statistics.

## 6 DISCUSSION

In this section, we discuss the results from the previous sections and also answer the research questions presented in Section 1 in light of our results.

### 6.1 Interpretation of the Throughput Values

Overall, we observe that the throughput on EOSIO has been volatile since last November, the throughput on Tezos has been very stable over time, and the throughput on XRPL has been stable in general except during the spam episode. A common factor between all blockchains is that the current throughput is vastly lower than the alleged capacity even during their utilization peaks, and is on average several orders of magnitude lower. A similarity between EOSIO and XRPL is that the maximum throughput was reached due to DoS attacks on the network. Indeed, the maximum numbers of transactions on EOSIO is due to the `EIDOS` coin airdrop, while the peak on XRPL was due to the network being spammed with payments. However, while the spam on XRPL appeared to be anecdotal and lasted for roughly two months, the spam attack on EOSIO is persistent and has continued for over six months to date. That the increased throughput has different implications for each network. While on XRPL the consequences of such a spam attack are limited, on EOSIO they forced the network to enter congestion mode, hindering normal usage of the network as transactions become too costly due to the elevated threshold for staking.

Unlike XRPL and EOSIO, Tezos has not seen any spam attack and the level of utilization has been consistent, and relatively low, across time. A majority of the throughput is used for consensus, with most of the spikes in the number of transactions due to baker payments, which are also related to consensus.

### 6.2 Revisiting Research Questions

We now return to the research questions posed in Section 1 and seek to understand better how the different blockchains are used in practice, by attempting to answer them based on the data analysis we perform above.

**RQ1: used throughput capacity.** Although the maximum throughput of all blockchains appears vastly lower than the alleged capacity, the situation is not as simple for EOSIO and XRPL. As previously discussed, EOSIO started to be congested because of an airdrop, preventing regular users to use the blockchain normally. During the attack against

XRPL, there were several reports of the network being congested [5, 53], showing that although the claimed capacity was much higher, the *actual* capacity might have maxed. Nevertheless, it is yet unclear whether the congestion is mainly due to the suboptimal design of blockchain protocols or the physical constraint of participating nodes' infrastructure. On the other hand, Tezos has not yet come close to maximizing its actual capacity.

**RQ2: classifying actions.** We made a generalized categorization of transaction types. Some transaction types are common to all blockchains, such as peer-to-peer transactions and account related transactions, while other types of transactions are inherent to the particularities of the underlying blockchain. While XRPL and Tezos contain easily identifiable action types, making them easy to classify, EOSIO does not have pre-defined action types and classifying actions requires knowledge of the account receiving the action.

**RQ3: identifying active blockchain participants.** EOSIO has named accounts which makes it easy to identify participants. XRPL has optional names, which are registered by the most active players such as exchanges. Tezos endorsements are often created by bakers, who usually publicize their address and are identifiable. However, there is no easy way to identify participants in peer-to-peer transactions and doing so would require using de-anonymization techniques [6, 23].

**RQ4: detecting DoS and spam.** The blockchains analyzed are currently under-utilized and when spam occurs, their utilization level increases significantly, as seen in Figure 3. This makes DoS and spam attacks very easy to detect by simply looking at the transactions, as we saw for EOSIO and XRPL.

### 6.3 Transaction Fee Dilemma

Overall, we have seen that there is a dilemma between having lower transactions fees, which induces spam, or having higher transaction fees, which deters legitimate usage of the network.

One the one side, we have seen that both EOSIO and XRPL have chosen to go with extremely low transaction fees, which in both cases resulted in a very large amount of spam. On the other side of the spectrum, Ethereum, which has transaction fees based on supply and demand [59] has seen a 10-times increase in the fees, mainly because of an increase in the utilization of decentralized finance protocols [25], making it extremely difficult to use for regular users [41].

There has been work on both sides to improve the current situation but, at the time of writing, no significant progress has been made. Despite fee structure changes having been proposed in XRPL [66], concerns are that a fee increase discourages the engagement of legitimate users. In EOSIO, despite the integration of a new rental market for CPU and RAM [20], the current fee structure remains problematic, as the network has now been congested for more than half a year, making it hard to use for regular users. On the Ethereum side of things, changes in the current pricing system to try to reduce the transaction fees have been proposed [10] but are still under discussion.

Overall, for a functional and sustainable blockchain system, it is crucial to find a balanced transaction fee mechanism that can make regular usage of the network affordable while DoS attacks expensive [42].

## 7 RELATED WORK

Existing literature on transactional patterns and graphs on blockchains has been largely focused on Bitcoin.

Ron et al. [45] are among the first to analyze transaction graphs Bitcoin. Using on-chain transaction data with more than 3 million different addresses, the authors find that Mt. Gox was at the time by far the most used exchange, covering over 80% of the exchange-related traffic.

Kondor et al. [29] focus on the wealth distribution in Bitcoin and provided an overview of the evolution of various metrics. They find that the Gini coefficient of the balance distribution has increased quite rapidly and show that the wealth distribution in Bitcoin is converging to a power law.

McGinn et al. [34] focus their work on visualizing Bitcoin transaction patterns. At this point, in 2016, Bitcoin already had more than 300 million addresses, indicating exponential growth over time. The authors propose a visualization which scales well enough to enable pattern searching. Roughly speaking, they present transactions, inputs and outputs as vertices while treating addresses as edges. The authors report that they were able to discover high frequency transactions patterns such as automated laundering operations or denial-of-service attacks.

Ranshous et al. [43] extend previous work by using a directed hypergraph to model Bitcoin transactions. They model the transaction as a bipartite hypergraph where edges are in and out amounts of transactions and the two types of vertices are transactions and addresses. Based on this hypergraph, they identify transaction patterns, such as "short thick band", a pattern where Bitcoins are received from an exchange, held for a while and sent back to an exchange. Finally, they used different features extracted from the hypergraph, such as the amount of Bitcoin received but also how many times the address appeared in a certain pattern, to train a classifier capable of predicting if a particular address belongs to an exchange.

Di Francesco Maesa et al. [15] analyze Bitcoin user graphs to detect unusual behavior. The authors find that discrepancies such as outliers in the in-degree distribution of nodes are often caused by artificial users' behavior. They then introduce the notion of pseudo-spam transactions, which consist of transactions with a single input and multiple outputs where only one has a value higher than a Satoshi, the smallest amount that can be sent in a transaction. They find that approximately 0.5% of the total number of multi-input multi-output transactions followed such a pattern and that these were often chained.

Several other works also exist about the subject and very often try to leverage some machine learning techniques either to cluster or classify Bitcoin addresses. Monamo et al. [35] attempted to detect anomalies on Bitcoin and show that their approach is able to partly cluster some fraudulent activity on the network. Toyoda et al. [52] focus on classifying Ponzi schemes and related high yield investment programs by applying supervised learning using features related to transaction patterns, such as the number of transactions an address is involved in, or its ratio of pay-in to pay-out.

More recently, a study of EOSIO decentralized applications (DApps) has been published [27]. The authors analyze the EOSIO blockchain from another angle: they look at the DApps activities and attempt to detect bots and fraudulent activities. The authors identified thousands of bot accounts as well as real-world attacks, 80 of which have been confirmed by DApp teams.

To the best of our knowledge, this is the first academic work to empirically analyze the transactions of Tezos and XRPL, and the first to compare transactional throughput on these platforms.

## 8 CONCLUSIONS

We investigate transaction patterns and value transfers on the three major high-throughput blockchains: EOSIO, Tezos, and XRPL. Using direct connections with the respective blockchains, we fetch transaction data between October 1, 2019 and April 30, 2020. With EOSIO and XRPL, the majority of the transactions exhibit characteristics resembling DoS attacks: on EOSIO, 95% of the transactions were triggered by the airdrop of a yet valueless token; on XRPL, over 94%—consistently in different observation periods—of the transactions carry no economic value. For Tezos, since transactions per block are largely outnumbered by mandatory endorsements, most of the throughput, 76% to be exact, is occupied for maintaining consensus.

Furthermore, through several case studies, we present prominent cases of how transactional throughput was used on different blockchains. Specifically, we show two cases of spam on EOSIO, on-chain governance related transactions on Tezos, as well as payments and exchange offers with zero-value tokens on XRPL.

The bottom line is: the three blockchains studied in this paper demonstrate the capacity to support high levels of throughput; however, the massive potential of those blockchains has thus far not been fully realized for their intended purposes.

## ACKNOWLEDGMENT

## REFERENCES

[1] 2017. EIP 609: Hardfork Meta: Byzantium. https://eips.ethereum.org/EIPS/eip-609
[2] 2017. EIP 779: Hardfork Meta: DAO Fork. https://eips.ethereum.org/EIPS/eip-779
[3] Amit Panghal. 2019. The Lifecycle of an Operation in Tezos. https://medium.com/tqtezos/lifecycle-of-an-operation-in-tezos-248c51038ec2
[4] Jacob Arluck. 2018. Liquid Proof-of-Stake. https://medium.com/tezos/liquid-proof-of-stake-aec2f7ef1da7

[5] AtoZ Markets. 2019. Binance facing XRP withdrawal issues. https://atozmarkets.com/news/binance-facing-xrp-withdrawal-issues/

[6] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. 2014. Deanonymisation of Clients in Bitcoin P2P Network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale, Arizona, USA) *(CCS '14)*. Association for Computing Machinery, New York, NY, USA, 15–29. https://doi.org/10.1145/2660267.2660379

[7] Bitshares. 2018. Delegated Proof of Stake (DPOS). https://github.com/bitshares/how.bitshares.works/blob/master/docs/technology/dpos.rst

[8] block.one. 2018. EOS.IO Technical White Paper v2. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[9] BTG Pactual and Dalma Capital. 2019. BTG Pactual and Dalma Capital to utilize Tezos Blockchain for Security Token Offerings (STOs). https://www.prnewswire.co.uk/news-releases/btg-pactual-and-dalma-capital-to-utilize-tezos-blockchain-for-security-token-offerings-stos--880726956.html

[10] Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, and Ian Norden. 2019. EIP-1559: Fee market change for ETH 1.0 chain. https://eips.ethereum.org/EIPS/eip-1559

[11] Brad Chase and Ethan Macbrough. 2018. *Analysis of the XRP Ledger Consensus Protocol*. Technical Report. Ripple Labs, Inc. http://arxiv.org/abs/1802.07242

[12] CoinMarketCap. 2020. Tezos (XTZ) price, charts, market cap, and other metrics. https://coinmarketcap.com/currencies/tezos/

[13] Cryptium Labs. 2019. Babylon 2.0 (PsBABY5HQ). https://www.tezosagora.org/proposal/5

[14] Blockwatch Data. 2020. Cryptium Labs Payouts. https://tzstats.com/tz1cNARmnRRrvZgspPr2rSTUWq5xtGTuKuHY

[15] Damiano Di Francesco Maesa, Andrea Marino, and Laura Ricci. 2017. An analysis of the Bitcoin users graph: inferring unusual behaviours. In *Complex Networks & Their Applications V*, Hocine Cherifi, Sabrina Gaito, Walter Quattrociocchi, and Alessandra Sala (Eds.). Springer International Publishing, Cham, 749–760.

[16] EarnBet. 2019. EOS 30 Day Notice.

[17] enumivo. 2019. Get Free EIDOS. https://enumivo.org/get-free-eidos

[18] EOSDocs.io. 2020. API endpoints. https://www.eosdocs.io/resources/apiendpoints/

[19] EOSIO. 2019. About System Contracts. https://eosio.github.io/eosio.contracts/latest/index

[20] EOSIO. 2020. EOSIO Resource Allocation Proposal. https://eos.io/news/eosio-resource-allocation-proposal/

[21] EOSIO. 2020. eosio.contracts. https://github.com/EOSIO/eosio.contracts/blob/master/README.md

[22] EOSIO. 2020. RPC API Guide. https://developers.eos.io/eosio-nodeos/reference#get_account

[23] A Gaihre, S Pandey, and H Liu. 2019. Deanonymizing Cryptocurrency With Graph Learning: The Promises and Challenges. In *2019 IEEE Conference on Communications and Network Security (CNS)*. 1–3. https://doi.org/10.1109/CNS.2019.8802640

[24] L M Goodman. 2014. *Tezos—a self-amending crypto-ledger White paper*. Technical Report.

[25] Lewis Gudgeon, Sam M Werner, Daniel Perez, and William J Knottenbelt. 2020. DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency. *arXiv preprint arXiv:2006.13922* (2020).

[26] HashBaby. 2019. Mark's HBS, from dapp "vulgar rights" to DeFi "industry foundation". https://bit.ly/hashbaby-closing

[27] Yuheng Huang, Haoyu Wang, Lei Wu, Gareth Tyson, Xiapu Luo, Run Zhang, Xuanzhe Liu, Gang Huang, and Xuxian Jiang. 2020. Characterizing EOSIO Blockchain. arXiv:2002.05369 [cs.CR]

[28] Josh Kauffman. 2019. What Are EOSIO System Accounts and What Do They Each Do? https://www.eoscanada.com/en/what-are-eosio-system-accounts-and-what-do-they-each-do

[29] Dániel Kondor, Márton Pósfai, István Csabai, and Gábor Vattay. 2014. Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network. *PLOS ONE* 9, 2 (2014), 1–10. https://doi.org/10.1371/journal.pone.0086197

[30] Melanie Kramer and Michael O'Sullivan. 2019. Could EOSIO be the Foundation of a Blockchain Future. https://bywire.news/articles/could-eosio-be-the-foundation-of-a-blockchain-future

[31] Cryptium Labs. 2020. backerei — Automated reward payment & account management for Tezos bakers. https://github.com/cryptiumlabs/backerei

[32] Obsidian Labs. 2019. eosio.token. https://docs.eosstudio.io/contracts/eosio-token.html

[33] Robert Anthony Love, Lantanya Neale Mauriello, Nesta Valerie Reckord-Yarde, Susan Lynne Robertson, Robert Williams, and Donald E. Nelson. 2013. Value tracking and reporting of automated clearing house transactions. https://patentimages.storage.googleapis.com/03/e3/98/0cfb0fe7ee16e9/US8543477.pdf

[34] Dan McGinn, David Birch, David Akroyd, Miguel Molina-Solana, Yike Guo, and William J Knottenbelt. 2016. Visualizing dynamic bitcoin transaction patterns. *Big data* 4, 2 (2016), 109–119.

[35] P Monamo, V Marivate, and B Twala. 2016. Unsupervised learning for robust Bitcoin fraud detection. In *2016 Information Security for South Africa (ISSA)*. 129–134. https://doi.org/10.1109/ISSA.2016.7802939

[36] Nomadic Labs. 2018. Delegating your coins. https://tezos.gitlab.io/introduction/howtorun.html#delegating-your-coins

[37] Nomadic Labs. 2018. Delegation. http://tezos.gitlab.io/whitedoc/proof_of_stake.html#delegation

[38] Nomadic Labs. 2018. Michelson: the language of Smart Contracts in Tezos. https://tezos.gitlab.io/whitedoc/michelson.html

[39] Nomadic Labs. 2018. Originated accounts and contracts. https://tezos.gitlab.io/introduction/howtouse.html

[40] ObsidianSys. 2019. Summary of Ledger Support for the Babylon Protocol. https://www.reddit.com/r/tezos/comments/dj7g9y/summary_of_ledger_support_for_the_babylon_protocol/

[41] Marcel Pechman. 2020. Record Ethereum Network Use and Gas Fees Pose Risk to DeFi Expansion. https://cointelegraph.com/news/record-ethereum-network-use-and-gas-fees-pose-risk-to-defi-expansion

[42] Daniel Pérez and Benjamin Livshits. 2020. Broken Metre: Attacking Resource Metering in EVM. In *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*. The Internet Society. https://www.ndss-symposium.org/ndss-paper/broken-metre-attacking-resource-metering-in-evm/

[43] Stephen Ranshous, Cliff A Joslyn, Sean Kreyling, Kathleen Nowak, Nagiza F Samatova, Curtis L West, and Samuel Winters. 2017. Exchange Pattern Mining in the Bitcoin Transaction Directed Hypergraph. In *Financial Cryptography and Data Security*, Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y A Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson (Eds.). Springer International Publishing, Cham, 248–263.

[44] Ripple. 2020. Benefits of XRP in Payments. https://ripple.com/xrp/

[45] Dorit Ron and Adi Shamir. 2013. Quantitative Analysis of the Full Bitcoin Transaction Graph. In *Financial Cryptography and Data Security*, Ahmad-Reza Sadeghi (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 6–24.

[46] EIDOS Team. 2019. YAS Network. https://enumivo.org/blog/2019/11/24/yas-network

[47] Team Ripple. 2020. Q4 2019 XRP Markets Report. https://ripple.com/insights/q4-2019-xrp-markets-report/

[48] Scrambled Egg Technologies. 2020. XRP Scan | Ripple XRP ledger explorer. https://xrpscan.com/

[49] Tezos. 2018. Proof-of-stake in Tezos. , 6 pages. https://tezos.gitlab.io/whitedoc/proof_of_stake.html

[50] Tezos Agora. 2020. Tezos Brest A amendment. https://www.tezosagora.org/period/15

[51] Tezos Foundation. 2020. Tezos Foundation's Faucet. https://faucet.tezos.com/

[52] K Toyoda, T Ohtsuki, and P T Mathiopoulos. 2017. Identification of High Yielding Investment Programs in Bitcoin via Transactions Pattern Analysis. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. 1–6. https://doi.org/10.1109/GLOCOM.2017.8254420

[53] tulo. 2019. Spam? suspect BTC payments on XRPL. https://www.xrpchat.com/topic/33284-spam-suspect-btc-payments-on-xrpl/?do=findComment&comment=793048

[54] Tezos Ukraine. 2020. Tezos Ukraine Infrastructure. https://api.tezos.org.ua/

[55] Visa. 2020. Visa Fact Sheet. https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

[56] Will Warren and Amir Bandeali. 2017. 0x: An open protocol for decentralized exchange on the Ethereum blockchain. (2017).

[57] WhaleEx. 2020. WhaleEx - #1 DEX. https://www.whaleex.com/

[58] Wietse Wind. 2020. XRP ledger full history cluster. https://rippled.xrptipbot.com/
[59] Gavin Wood. 2019. *Ethereum: a secure decentralised generalised transaction ledger*. Technical Report. 1–32 pages. https://doi.org/10.1017/CBO9781107415324.004
[60] Junfeng Xie, F. Richard Yu, Tao Huang, Renchao Xie, Jiang Liu, and Yunjie Liu. 2019. A Survey on the Scalability of Blockchain Systems. *IEEE Network* 33, 5 (2019), 166–173. https://doi.org/10.1109/MNET.001.1800290
[61] XRP Ledger. 2019. Accounts. https://xrpl.org/accounts.html#special-addresses
[62] XRP Ledger. 2019. Fast, Efficient Consensus Algorithm. https://xrpl.org/xrp-ledger-overview.html#fast-efficient-consensus-algorithm
[63] XRP Ledger. 2020. Get Exchange Rates. https://xrpl.org/data-api.html#get-exchange-rates
[64] XRP Ledger. 2020. Source and Destination Tags. https://xrpl.org/source-and-destination-tags.html
[65] XRP Ledger. 2020. Trust Lines and Issuing. https://xrpl.org/trust-lines-and-issuing.html
[66] XRP Ledger Project. 2019. Fee Voting. https://xrpl.org/fee-voting.html

# APPENDIX: MEASUREMENT FRAMEWORK

We implement an extensible and reusable measurement framework to facilitate future transactions analysis related research. Our framework currently supports the three blockchains analyzed in this work, Tezos, EOSIO and XRPL but can easily be extended to support other blockchains. The core of the software is implemented in Go and is designed to work well on a single machine with many cores. The framework frontend is provided as a cross-platform static binary command line tool.

While the framework is responsible for the heavy lifting and processing the gigabytes of data, we also provide a companion tool implemented in Python to generate plots and tables from the data generated by the framework.

**Data fetching.** The framework currently allows to fetch data either using RPC over HTTP or websockets. Tezos and EOSIO both use the HTTP adapter to retrieve data while XRPL uses the websocket interface. The data is retrieved from publicly available archive nodes but the framework can be configured to use other nodes if necessary. The retrieved data is stored in a gzipped JSON Lines format where each line corresponds to a block. Blocks are stored in chunk of $n$ blocks per file — where $n$ can be configured — making parallel processing straightforward. It took less than two days to fetch all the data presented in Figure 2.

**Data processing.** The framework provides several processors which can mainly be used to aggregate the data either over time, or over certain properties such as the sender of a transaction. The framework is configured using a single JSON file, containing the configuration for the data to be processed as well as the specification of what type of statistics should be collected from the dataset. We show a sample configuration file in Figure 11. This configuration computes three statistics from block 82,152,667 to block 118,286,375, using the data contained in all the files matching /data/eos_blocks-*.jsonl.gz. The framework will compute the total number of transactions, the number of actions grouped using their receiver over a period of 6 hours, and finally the total number of actions grouped by their name. All the statistics described above

```
{
  "Pattern": "/data/eos_blocks-*.jsonl.gz",
  "StartBlock": 82152667,
  "EndBlock": 118286375,
  "Processors": [{
      "Name": "TransactionsCount",
      "Type": "count-transactions"
    }, {
      "Name": "GroupedActionsOverTime",
      "Type": "group-actions-over-time",
      "Params": {
        "By": "receiver",
        "Duration": "6h"
      }
    }, {
      "Name": "ActionsByName",
      "Type": "group-actions",
      "Params": {
        "By": "name"
      }
    }
  ]
}
```

**Figure 11: Configuration file for our measurement framework**

can be used for all the blockchains but the framework also supports blockchain-specific statistics where needed. New statistics can easily be added to the framework by implementing a common interface.

Our framework was able to analyze the data and output all the statistics required for this paper in less than 4 hours using a powerful 48 core machine.

```
type Blockchain interface {
    FetchData(filepath string,
             start, end uint64) error
    ParseBlock(rawLine []byte) (Block, error)
    EmptyBlock() Block
}

type Block interface {
    Number() uint64
    TransactionsCount() int
    Time() time.Time
    ListActions() []Action
}

type Action interface {
    Sender() string
    Receiver() string
    Name() string
}
```

**Figure 12: Main interfaces of our measurement framework**

**Extending to other blockchains.** The framework has been made as generic as possible to allow integrating other blockchains to perform similar kind of analysis. In particular, the framework contains three main interfaces shown in Figure 12. The `FetchData` method can be implemented by reusing the HTTP or websocket adapters provided by the framework while the `Block` and `Action` interfaces typically involves defining

the schema of the block or action of the blockchain implemented. In our implementation, adding a blockchain takes on average 105 new lines of Go code not including tests.