

# FastPay: High-Performance Byzantine Fault Tolerant Settlement

Mathieu Baudet\*  
mathieubaudet@fb.com  
Facebook Novi

George Danezis  
gdanezis@fb.com  
Facebook Novi

Alberto Sonnino  
asonnino@fb.com  
Facebook Novi

## ABSTRACT

FastPay allows a set of distributed authorities, some of which are Byzantine, to maintain a high-integrity and availability settlement system for pre-funded payments. It can be used to settle payments in a native unit of value (crypto-currency), or as a financial side-infrastructure to support retail payments in fiat currencies. FastPay is based on Byzantine Consistent Broadcast as its core primitive, foregoing the expenses of full atomic commit channels (consensus). The resulting system has low-latency for both confirmation and payment finality. Remarkably, each authority can be sharded across many machines to allow unbounded horizontal scalability. Our experiments demonstrate intra-continental confirmation latency of less than 100ms, making FastPay applicable to point of sale payments. In laboratory environments, we achieve over 80,000 transactions per second with 20 authorities—surpassing the requirements of current retail card payment networks, while significantly increasing their robustness.

## KEYWORDS

distributed system, bft, settlement system, consistent broadcast

### ACM Reference Format:

Mathieu Baudet, George Danezis, and Alberto Sonnino. 2021. FastPay: High-Performance Byzantine Fault Tolerant Settlement. In *Proceedings of ACM Conference (Conference'17)*. ACM, New York, NY, USA, 15 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

## 1 INTRODUCTION

Real-time gross settlement systems (RTGS) [4] constitute the most common approach to financial payments in closed banking networks, that is, between reputable institutions. In contrast, blockchain platforms have proposed a radically different paradigm, allowing account holders to interact directly with an online, yet highly secure, distributed ledger. Blockchain approaches aim to enable new use cases such as personal e-wallets or private transactions, and generally provide ecosystems more favorable to users. However, until now, such open, distributed settlement solutions have come at a high performance cost and questionable scalability compared to traditional, closed RTGS systems.

\*Alphabetical order.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

*Conference'17, July 2017, Washington, DC, USA*

© 2021 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM... \$15.00

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

FastPay is a Byzantine Fault Tolerant (BFT) real-time gross settlement (RTGS) system. It enables authorities to jointly maintain account balances and settle pre-funded retail payments between accounts. It supports extremely low-latency confirmation (sub-second) of eventual transaction finality, appropriate for physical point-of-sale payments. It also provides extremely high capacity, comparable with peak retail card network volumes, while ensuring gross settlement in real-time. FastPay eliminates counterparty and credit risks of net settlement and removes the need for intermediate banks, and complex financial contracts between them, to absorb these risks. FastPay can accommodate arbitrary capacities through efficient sharding architectures at each authority. Unlike any traditional RTGS, and more like permissioned blockchains, FastPay can tolerate up to  $f$  Byzantine failures out of a total of  $3f + 1$  authorities, and retain both safety, liveness, and high-performance.

FastPay can be deployed in a number of settings. First, it may be used as a settlement layer for a native token and crypto-currency, in a standalone fashion. Second, it may be deployed as a side-chain of another crypto-currency, or as a high performance settlement layer on the side of an established RTGS to settle fiat retail payments. In this paper we present this second functionality in detail, since it exercises all features of the system, both payments between FastPay accounts, as well as payments into and out of the system.

**Contributions.** We make the following contributions:

- The FastPay design is novel in that it forgoes full consensus; it leverages the semantics of payments to minimize shared state between accounts and to increase the concurrency of asynchronous operations; and supports sharded authorities.
- We provide proofs of safety and liveness in a Byzantine and fully asynchronous network setting. We show that FastPay keeps all its properties despite the lack of total ordering, or asynchrony of updates to recipient accounts.
- We experimentally demonstrate comparatively very high throughput and low latency, as well as the robustness of the system under conditions of extremely high concurrency and load. We show that performance is maintained even when some (Byzantine) authorities fail.

**Outline.** This paper is organized as follows: Section 2 introduces real-time gross settlement systems, and permissioned blockchains. Section 3 introduces the entities within FastPay, their interactions, and the security properties and threat model. Section 4 details the design of FastPay both as a standalone system, and operated in conjunction with a Primary. Section 5 discusses safety and liveness. Section 6 briefly describes the implementation of the FastPay prototype. Section 7 provides a full performance evaluation of FastPay as we modulate its security parameters and load. Section 8 discusses key open issues such as privacy, governance mechanisms and economics of the platform. Section 9 covers the related work,

both in terms of traditional financial systems and crypto-currencies. Section 10 concludes.

## 2 BACKGROUND

Real-time gross settlement systems (RTGS) [4] are the backbone of modern financial systems. Commercial banks use them to maintain an account with central banks and settle large value payments.

RTGS systems are limited in their capacity<sup>1</sup>, making them unsuitable for settling low-value high-volume retail payments directly. Such retail payments are deferred: banks exchange information bilaterally about pending payments (often through SWIFT [33, 47]), they aggregate and net payments, and only settle net balances through an RTGS, often daily. The often quoted volume figure of around 80,000 transactions per second for retail card networks [26, 48] represents the rate at which ‘promises’ for payments are exchanged between banks, and not settled payments. Traditional RTGS systems are implemented as monolithic centralized services operated by a single authority, and must employ a number of technical and organizational internal controls to ensure they are reliable (through a primary-replica architecture with manual switch over) and correct—namely ensuring availability and integrity. Traditionally only regulated entities have accounts in those systems. This result in a Balkanized global financial system where financial institutions connect to multiple RTGS, directly or indirectly through corresponding banks, to execute international payments.

Blockchain-based technologies, starting with Bitcoin [35] in 2009, provide more open settlement systems often combined with their own digital tokens to represent value. Permissionless blockchains have been criticized for their low performance [18] in terms of capacity and finality times. However, a comparison with established settlement systems leads to a more nuanced assessment. Currently, Ethereum [50] can process 15 transactions per second. The actual average daily load on the EU ECB TARGET2 system is about 10 transactions per second [22] (in 2018) which is a comparable figure (and lower than the peak advertised capacity of 500 transaction per second). However, it falls very short of the advertised transaction rate of 80,000 transaction per second peak for retail payment networks—even though this figure does not represents settled transactions. The stated ambitions of permissionless projects is to be able to settle transactions at this rate on an open and permissionless network, which remains an open research challenge [49].

Permissioned blockchains [5, 7] provide a degree of decentralization—allowing multiple authorities to jointly operate a ledger—at the cost of some off-chain governance to control who maintains the blockchain. The most prominent of such proposals is the Libra network [14], developed by the Libra Association. Other technical efforts include Hyperledger [12], Corda [10] and Tendermint [11]. These systems are based on traditional notions of Byzantine Fault Tolerant state machine replication (or sometimes consensus with crash-failures only), which presupposes an atomic commit channel (often referred as ‘consensus’) that sequences all transactions. Such architectures allow for higher capacities than Bitcoin and Ethereum. LibraBFT, for example, aims for 1,000 transactions per second at peak capacity [1, 21]; this exceeds many RTGS systems but is still

<sup>1</sup>For example, the relatively recent European Central Bank TARGET2 system has a maximum capacity of 500 transactions per second [22].

below the peak volumes for retail payment systems. Regarding transaction finality, a latency of multiple seconds is competitive with RTGS systems but is not suitable for retail payment at physical points of sale.

## 3 OVERVIEW

To illustrate its full capabilities, we describe FastPay as a side chain of a primary RTGS holding the primary records of accounts. We call such a primary ledger *the Primary* for short, and its accounts *the Primary accounts*. The Primary can be instantiated in two ways: (i) as a programmable blockchain, through smart contracts, like Ethereum [50] or Libra [14]. The Primary can also be instantiated (ii) as a traditional monolithic RTGS operated by a central bank. In this case the components interfacing with FastPay are implemented as database transactions within the Primary. In both cases FastPay acts as a side infrastructure to enable pre-funded retail payments. FastPay can also operate with a native asset, without a primary ledger. In this case sub-protocols involving the Primary are superfluous, since all value is held within FastPay accounts and never transferred out or into the system.

### 3.1 Participants

FastPay involves two types of participants: (i) authorities, and (ii) account owners (*users*, for short). All participants generate a key pair consisting of a private signature key and the corresponding public verification key. As a side-chain, FastPay requires a smart contract on the main blockchain, or a software component on an RTGS system that can authorize payments based on the signatures of a threshold of authorities from a *committee* with fixed membership.

By definition, an *honest* authority always follows the FastPay protocol, while a *faulty* (or *Byzantine*) one may deviate arbitrarily. We present the FastPay protocol for  $3f + 1$  equally-trusted authorities, assuming a fixed (but unknown) subset of at most  $f$  Byzantine authorities. In this setting, a *quorum* is defined as any subset of  $2f + 1$  authorities. (As for many BFT protocols, our proofs only use the classical properties of quorums thus apply to all Byzantine quorum systems [34].)

When a protocol message is signed by a quorum of authorities, it is said to be *certified*: we call such a jointly signed message a *certificate*.

### 3.2 Accounts and Actions

A FastPay *account* is identified by its *address*, which we instantiate as the cryptographic hash of its public verification key. The state of a FastPay account is affected by four main high-level actions:

- (1) Receiving funds from a Primary account.
- (2) Transferring funds to a Primary account.
- (3) Receiving funds from a FastPay account.
- (4) Transferring funds to a FastPay account.

FastPay also supports two read-only actions that are necessary to ensure liveness despite faults: reading the state of an account at a FastPay authority, and obtaining a certificate for any action executed by an authority.

### 3.3 Protocol Messages

The FastPay protocol consists of *transactions* on the Primary, denoted with letter  $T$ , and network requests that users send to FastPay authorities, which we call *orders*, and denote with letter  $O$ . Users are responsible for broadcasting their orders to authorities and for processing the corresponding responses. The authorities are passive and *do not communicate directly with each other*.

**Transfer orders.** All transfers initiated by a FastPay account start with a *transfer order*  $O$  including the following fields:

- The sender's FastPay address, written  $\text{sender}(O)$ .
- The recipient, either a FastPay or a Primary address, written  $\text{recipient}(O)$ .
- A non-negative amount to transfer, written  $\text{amount}(O)$ .
- A sequence number  $\text{sequence}(O)$ .
- Optional user-provided data.
- A signature by the sender over the above data.

Authorities respond to valid transfer orders by signing them (see next section for validity checks). A quorum of such signatures is meant to be aggregated into a *transfer certificate*, noted  $C$ .

**Notations.** We write  $O = \text{value}(C)$  for the original transfer order  $O$  certified by  $C$ . For simplicity, we omit the operator value when the meaning is clear, e.g.  $\text{sender}(C) = \text{sender}(\text{value}(C))$ . FastPay addresses are denoted with letters  $x$  and  $y$ . We use  $\alpha$  for authorities and by extension for the shards of authorities.

### 3.4 Security Properties and Threat Model

FastPay guarantees the following security properties:

- **Safety:** No units of value are ever created or destroyed; they are only transferred between accounts.
- **Authenticity:** Only the owner of an account may transfer value out of the account.
- **Availability:** Correct users can always transfer funds from their account.
- **Redeemability:** A transfer to FastPay or Primary is guaranteed to eventually succeed whenever a valid transfer certificate has already been produced.
- **Public Auditability:** There is sufficient public cryptographic evidence for the state of FastPay to be audited for correctness by any party.
- **Worst-case Efficiency:** Byzantine authorities (or users) cannot significantly delay operations from correct users.

The above properties are maintained under a number of security assumptions: (i) there are at most  $f$  Byzantine authorities out of  $3f + 1$  total authorities. (ii) The network is fully asynchronous, and the adversary may arbitrarily delay and reorder messages [20]. However, messages are eventually delivered. (iii) Users may behave arbitrarily but availability only holds for *correct users* (defined in Section 4.5). (iv) The Primary provides safety and liveness (when FastPay is used in conjunction with it). We further discuss the security properties of FastPay in Section 5.

## 4 THE FASTPAY PROTOCOL

FastPay authorities hold and persist the following information.

**Authorities.** The state of an authority  $\alpha$  consists of the following information:

- The authority name, signature and verification keys.
- The committee, represented as a set of authorities and their verification keys.
- A map  $\text{accounts}(\alpha)$  tracking the current account state of each FastPay address  $x$  in use (see below).
- An integer value, noted  $\text{last\_transaction}(\alpha)$ , referring to the last transaction that paid funds into the Primary. This is used by authorities to synchronize FastPay accounts with funds from the Primary (see Section 4.3).

**FastPay accounts.** The state of a FastPay account  $x$  within the authority  $\alpha$  consists of the following:

- The public verification key of  $x$ , used to authenticate spending actions.
- An integer value representing the balance of payment, written  $\text{balance}^x(\alpha)$ .
- An integer value, written  $\text{next\_sequence}^x(\alpha)$ , tracking the expected sequence number for the next spending action to be created. This value starts at 0.
- A field  $\text{pending}^x(\alpha)$  tracking the last transfer order  $O$  signed by  $x$  such that the authority  $\alpha$  considers  $O$  as *pending confirmation*, if any; and absent otherwise.
- A list of certificates, written  $\text{confirmed}^x(\alpha)$ , tracking all the transfer certificates  $C$  that have been *confirmed* by  $\alpha$  and such that  $\text{sender}(C) = x$ . One such certificate is available for each sequence number  $n$  ( $0 \leq n < \text{next\_sequence}^x(\alpha)$ ).
- A list of *synchronization* orders, written  $\text{synchronized}^x(\alpha)$ , tracking transferred funds from the Primary to account  $x$ . (See Section 4.3.)

We also define  $\text{received}^x(\alpha)$  as the list of confirmed certificates for transfers received by  $x$ . Formally,  $\text{received}^x(\alpha) = \{C \text{ s.t. } \exists y. C \in \text{confirmed}^y(\alpha) \text{ and } \text{recipient}(C) = x\}$ .

We assume arbitrary size integers. Although FastPay does not let users overspend, (temporary) negative balances for account states are allowed for technical reasons discussed in Section 5. When present, a pending (signed) transfer order  $O = \text{pending}^x(\alpha)$  effectively locks the sequence number of the account  $x$  and prevents  $\alpha$  from accepting new transfer orders from  $x$  until *confirmation*, that is, until a valid transfer certificate  $C$  such that  $\text{value}(C) = O$  is received. This mechanism can be seen as the ‘Signed Echo Broadcast’ implementation of a Byzantine consistent broadcast on the label (account, next sequence number) [13].

**Storage considerations.** The information contained in the lists of certificates  $\text{confirmed}^x(\alpha)$  and  $\text{received}^x(\alpha)$  and in the synchronization orders  $\text{synchronized}^x(\alpha)$  is self-authenticated—being respectively signed by a quorum of authorities and by the Primary. Remarkably, this means that authorities may safely outsource these lists to an external high-availability data store. Therefore, FastPay authorities only require a constant amount of local storage per account, rather than a linear amount in the number of transactions.

### 4.1 Transferring Funds within FastPay

FastPay operates by implementing a Byzantine consistent broadcast channel per account, specifically using a ‘Signed Echo Broadcast’

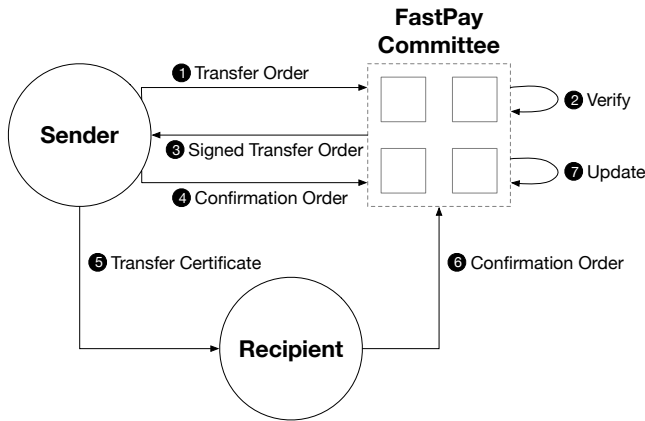


Figure 1: Transfer of funds from FastPay to FastPay.

variant (Algorithm 3.17 in [13]). It operates in two phases and all messages are relayed by the initiating user. Consistent Broadcast ensures *Validity*, *No duplication*, *Integrity*, and *Consistency*. It always terminates when initiated by a correct user. However, if a FastPay user equivocates, current operations may fail, and the funds present on the users account may become inaccessible.

**Transferring funds.** Figure 1 illustrates a transfer of funds within FastPay. To transfers funds to another FastPay account, the sender creates a FastPay transfer order ( $O$ ) with the next sequence number in their account, and signs it. They then send the FastPay transfer order to all authorities. Each authority checks (1) (i) that the signature is valid, (ii) that no previous transfer is pending (or is for the same transfer), (iii) that the amount is positive, (iv) that the sequence number matches the expected next one ( $\text{sequence}(O) = \text{next\_sequence}^x(\alpha)$ ), and (iv) that the balance ( $\text{balance}^x(\alpha)$ ) is sufficient (2). Then, it records the new transfer as pending and sends back a signature on the transfer order (3) which is also stored. The authority algorithm to handle transfer orders, corresponding to step 2, is presented in Figure 2.

The user collects the signatures from a quorum of authorities, and uses them along the FastPay transfer order to form a transfer certificate. The sender provides this transfer certificate to the recipient as proof that the payment will proceed (5). To conclude the transaction, the sender (4) or the recipient (6) broadcast the transfer certificate ( $C$ ) to the authorities (called *confirmation order*)<sup>2</sup>.

Upon reception of a confirmation order for the current sequence number, each authority  $\alpha$  (7) (i) checks that a quorum of signatures was reached, (ii) decreases the balance of the sender, (iii) increments the sequence number ( $\text{next\_sequence}^x(\alpha) + 1$ ) to ensure ‘deliver once’ semantics, and (iv) sets the pending order to None ( $\text{pending}^x(\alpha) = \text{None}$ ). Each authority  $\alpha$  also (v) adds the certificate to the list  $\text{confirmed}^x(\alpha)$ , and (vi) increases the balance of the recipient account asynchronously (*i.e.* without sequencing this write in relation to any specific payments from this account across

authorities). The authority algorithm to handle confirmation orders (as in step 7) is presented in Figure 2.

In Section 5 and Appendix A, we show that the FastPay protocol is safe thanks to the semantics of payments into an account and their commutative properties. FastPay is a significant simplification and deviation from an orthodox application of Guerraroui *et al.* [24], where accounts are single-writer objects and all write actions are mediated by the account owner. FastPay allows payments to be executed after a single consistent broadcast, rather than requiring recipients to sequence payments into their accounts separately. This reduces both latency and the state necessary to prevent replays.

**Payment finality.** Once a transfer certificate *could* be formed, namely  $2f + 1$  authorities signed a transfer order, no other order can be processed for an account until the corresponding confirmation order is submitted. Technically, the payment is final: it cannot be canceled, and will proceed eventually. As a result, showing a transfer certificate to a recipient convinces them that the payment will proceed. We call the showing of a transfer certificate to a recipient a *confirmation*, and then subsequently submitting the confirmation order, to move funds, *settlement*. *Confirmation* requires only a single round trip to a quorum of authorities resulting in very low-latency (see Section 7), and giving the system its name.

**Proxies, gateways and crash recovery.** The protocols as presented involve the sender being on-line and mediating all communications. However, the only action that the sender *must* perform personally is forming a transfer order, requiring their signature. All subsequent operations, including sending the transfer order to the authorities, forming a certificate, and submitting a confirmation order can be securely off-loaded to a proxy trusted only for liveness. Alternatively, a transfer order may be given to a merchant (or payment gateway) that drives the protocol to conclusion. In fact, any party in possession of a signed transfer order may attempt to make a payment progress concurrently. And as long as the sender is correct the protocol will conclude (and if not may only lock the account of the faulty sender). This provides significant deployment and implementation flexibility. A sender client may be implemented in hardware (in a NFC smart card) that only signs transfer orders. These are then provided to a gateway that drives the rest of the protocol. Once the transfer order is signed and handed over to the gateway, the sender may go off-line or crash. Authorities may also attempt to complete the protocol upon receiving a valid transfer order. Finally, the protocol recovers from user crash failures: anyone may request a transfer order that is partially confirmed from any authority, proceed to form a certificate, and submit a confirmation order to complete the protocol.

## 4.2 Sharding authorities

FastPay requires minimal state sharing between accounts, and allows for a very efficient sharding at each authority by account. The consistent broadcast channel is executed on a per-account basis. Therefore, the protocol does not require any state sharing between accounts (and shards) up to the point where a valid confirmation order has to be settled to transfer funds between FastPay accounts. On settlement, the sender account is decremented and the funds are

<sup>2</sup>Aggregating signed transfer orders into a transfer certificate does not requires knowledge of any secret; therefore, anyone (and not only the sender or the recipient) can broadcast the transfer certificate to the authorities to conclude the transaction.

```

fn handle_transfer_order( $\alpha$ ,  $O$ ) -> Result {
  // Check shard and signature.
  ensure!( $\alpha$ .in_shard(sender( $O$ )));
  ensure!( $O$ .has_valid_signature());

  // Obtain sender account.
  match accounts( $\alpha$ ).get(sender( $O$ )) {
    None => bail!(),
    Some(account) => {
      // Check if the same order is already pending.
      if let Some(pending) = account.pending {
        ensure!(pending.transfer ==  $O$ );
        return Ok();
      }
      ensure!(account.next_sequence == sequence( $O$ ));
      ensure!(account.balance >= amount( $O$ ));
      // Sign and store new transfer.
      account.pending = Some( $\alpha$ .sign( $O$ ));
      return Ok();
    }
  }
}

fn handle_confirmation_order( $\alpha$ ,  $C$ )
-> Result<Option<CrossShardUpdate>> {
  // Check shard and certificate.
  ensure!( $\alpha$ .in_shard(sender( $C$ )));
  ensure!( $C$ .is_valid( $\alpha$ .committee));
  let  $O$  = value( $C$ );

  // Obtain sender account.
  let sender_account =
    accounts( $\alpha$ ).get(sender( $O$ ))
    .or_insert(AccountState::new());

  // Ignore old certificates.
  if sender_account.next_sequence > sequence( $O$ ) {
    return Ok(None);
  }

  // Check sequence number and balance.
  ensure!(sender_account.next_sequence == sequence( $O$ ));
  ensure!(sender_account.balance >= amount( $O$ ));

  // Update sender account.
  sender_account.balance -= amount( $O$ );
  sender_account.next_sequence += 1;
  sender_account.pending = None;
  sender_account.confirmed.push( $C$ );

  // Update recipient locally or cross-shard.
  let recipient = match recipient( $O$ ) {
    Address::FastPay(recipient) => recipient,
    Address::Primary(_) => { return Ok(None) }
  };

  // Same shard: read and update the recipient.
  if  $\alpha$ .in_shard(recipient) {
    let recipient_account = accounts( $\alpha$ ).get(recipient)
      .or_insert(AccountState::new());
    recipient_account.balance += amount( $O$ );
    return Ok(None);
  }

  // Other shard: request a cross-shard update.
  let update = CrossShardUpdate {
    shard_id:  $\alpha$ .which_shard(recipient),
    transfer_certificate:  $C$ ,
  };
  Ok(Some(update))
}

```

Figure 2: Authority algorithms for handling transfer and confirmation orders. (The cross-shard update logic is presented in Appendix B.)

deposited into the account of the recipient, requiring interaction between at most two shards (second algorithm of Figure 2).

Paying into an account can be performed asynchronously, and is an operation that cannot fail (if the account does not exist it is created on the spot). Therefore, the shard managing the recipient account only needs to be notified of the confirmed payment through a reliable, deliver once, authenticated, point to point channel (that

can be implemented using a message authentication code, inter-shard sequence number, re-transmission, and acknowledgments) from the sender shard. This is a greatly simplified variant of a two-phase commit protocol coordinated by the sender shard (for details see the Presume Nothing and Last Agent Commit optimizations [31, 43]). Modifying the validity condition of the consistent broadcast to ensure the recipient account exists (or any other precondition on the recipient account) would require a full two-phase commit before an authority signs a transfer order, and can be implemented while still allowing for (slightly less) efficient sharding.

The algorithms in fig. 2 implement sharding. An authority shard checks that the transfer order ( $O$ ) or certificate ( $C$ ) is to be handled by a specific shard and otherwise rejects it without mutating its state. Handling confirmation orders depends on whether a recipient account is on the same shard. If so, the recipient account is updated locally. Otherwise, a *cross shard message* is created for the recipient shard to update the account (see code in the Appendix for this operation). The ability to shard each authority has profound implications: increasing the number of shards at each authority increases the theoretical throughput linearly, while latency remains constant. Our experimental evaluation confirms this experimentally (see Section 7).

### 4.3 Interfacing with the Primary

We describe the protocols required to couple FastPay with the Primary, namely transferring funds from the Primary to a FastPay account, and conversely from a FastPay to a Primary account. We refer throughout to the logic on the Primary as a *smart contract*, and the primary store of information as the *blockchain*. A traditional RTGS would record this state and manage it in conventional ways using databases and stored procedures, rather than a blockchain and smart contracts. We write  $\sigma$  for the state of the ‘blockchain’ at a given time, and  $\text{transactions}(\sigma)$  for the set of FastPay transactions  $T$  already processed by the blockchain.

**Smart contract.** The smart contract mediating interactions with the Primary requires the following data to be persisted in the blockchain:

- The FastPay committee composition: a set of authority names and their verification keys.
- A map of accounts where each FastPay address is mapped to its current Primary state (see below).
- The total balance of funds in the smart contract, written  $\text{total\_balance}(\sigma)$ .
- The transaction index of the last transaction that added funds to the smart contract, written  $\text{last\_transaction}(\sigma)$ .

**Accounts.** The Primary state of a FastPay account  $x$  consists of the set of sequence numbers of transfers already executed from this account to the Primary. This set is called the *redeem log* of  $x$  and written  $\text{redeemed}^x(\sigma)$ .

**Adding funds from the Primary to FastPay.** Figure 3 shows a transfer of funds from the Primary to FastPay. The owner of the FastPay account (or anyone else) starts by sending a payment to the FastPay smart contract using a Primary transaction (1). This

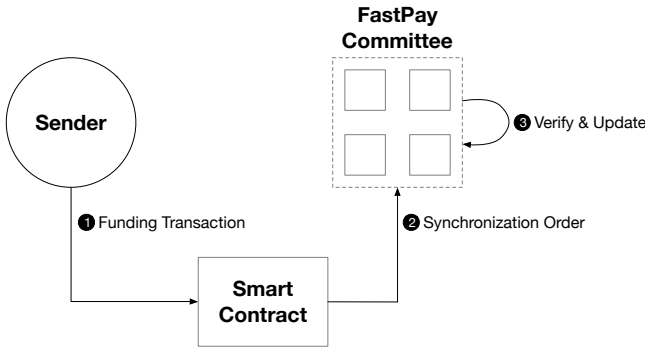


Figure 3: Transfer of funds from the Primary to FastPay.

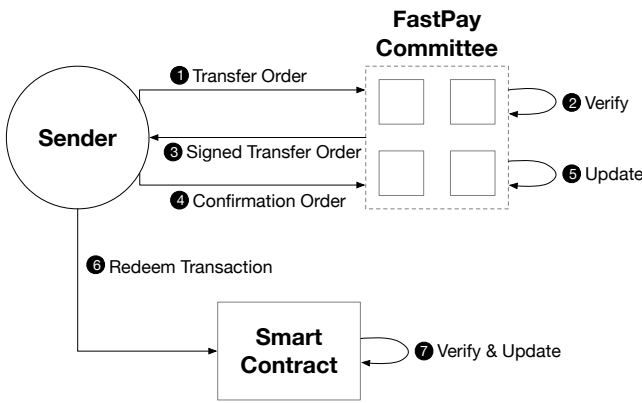


Figure 4: Transfer of funds from FastPay to the Primary.

transaction is called a *funding transaction*, and includes the recipient FastPay address for the funds and the amount of value to transfer.

When the Primary transaction is executed, the FastPay smart contract generates a *Primary event* that instructs authorities of a change in the state of the FastPay smart contract. We assume that each authority runs a full Primary client to authenticate such events. For simplicity, we model such an event as a (*Primary*) *synchronization order* (2). The smart contract ensures this event and the synchronization order contain a unique, always increasing, sequential transaction index.

When receiving a synchronization order, each authority (i) checks that the transaction index follows the previously recorded one, (ii) increments the last transaction index in their global state, (iii) creates a new FastPay account if needed, and (iv) increases the account balance of the target account by the amount of value specified (6). Appendix B presents the authority algorithm for handling funding transactions.

**Transferring funds from FastPay to the Primary.** Figure 4 shows a transfer of funds from FastPay to the Primary. The FastPay sender signs a *Primary transfer order* using their account key and broadcasts it to the authorities (1). This is simply a transfer order with a Primary address as the recipient.

Once a quorum of signatures is reached (2 and 3), the sender creates a certified (Primary) transfer order, also called a *transfer*

*certificate* for short. The sender broadcasts this certificate to the authorities to confirm the transaction (4) and unlock future spending from this account. When an authority receives a confirmation order containing a certificate of transfer (5), it must check (i) that a quorum of signatures was reached, and (ii) that the account sequence number matches the expected one; they (iii) then set the pending order to None, (iv) increment the sequence number, and (v) decrease the account balance.

Finally, the recipient of the transfer should send a redeem transaction to the FastPay smart contract on the Primary blockchain (6). When the FastPay smart contract receives a valid redeem transaction (7), it must (i) check that the sequence number is not in the Primary redeem log of the sender, to prevent reuse; (ii) update this redeem log; (iv) transfer the amount of value specified from the smart contract into the recipient’s Primary account.

#### 4.4 State Recovery and Auditing

For every account  $x$ , each authority  $\alpha$  must make available the pending order  $\text{pending}^x(\alpha)$ , the sequence number  $\text{next\_sequence}^x(\alpha)$ , the synchronization orders  $\text{synchronized}^x(\alpha)$ , and the certificates confirmed so far, indexed by senders (*i.e.*  $\text{confirmed}^x(\alpha)$ ) and receivers ( $\text{received}^x(\alpha)$ ). Sharing these data fulfills two important roles: (i) this lets anyone read the state of any incomplete transfer and drive the protocol all the way to settlement; (ii) it enables auditing authority states and detecting Byzantine faults (*e.g.* incorrect balance checks).

#### 4.5 Correct Users and Client Implementation

A *correct user* owning a FastPay account  $x$  follows the correctness rules below:

- (1) The user sets the sequence number of a new transfer order  $O$  to be the next expected integer after the previous transfer (starting with 0); *i.e.* they sign exactly one transfer order per sequence number;
- (2) They broadcast the new transfer order  $O$  to enough authorities until they (eventually) obtain a certificate  $C$ ;
- (3) They successfully broadcast the certificate  $C$  to a quorum of authorities.

**FastPay Client.** To address the correctness rules above, our reference implementation of a FastPay client holds and persists the following minimal state:

- The address  $x$  and the secret key of the account;
- The FastPay committee;
- The sequence number to be used in the next transfer;
- The transfer order that it signed last, in case it is still pending.

In this setting, the available balance of a user account is not tracked explicitly but rather evaluated (conservatively) from the Primary transactions and the available logs for incoming transfers and outgoing transfers (Section 4.4). Evaluating the balance before starting a transfer is recommended, as signing a transfer order with an excessive amount will block (correct) client implementations from initiating further transfers until the desired amount is available.

## 5 SECURITY ANALYSIS

Let  $\sigma$  denote the current state of the Primary. We define  $\text{funding}^x(\sigma)$  as the sum of all the amounts transferred to a FastPay address  $x$  from the Primary:

$$\text{funding}^x(\sigma) = \sum_{\substack{T \in \text{transactions}(\sigma) \\ \text{recipient}(T) = x}} \text{amount}(T)$$

For simplicity, we write  $\sum_C \text{amount}(C)$  when we mean to sum over certified transfer orders:  $\sum_{O \text{ s.t. } \exists C. O = \text{value}(C)} \text{amount}(O)$ .

The results presented in this section are proven in Appendix A. We start with the main safety invariant of FastPay.

**THEOREM 5.1 (SOLVENCY OF FASTPAY).** *At any time, the sum of the amounts of all existing certified transfers from FastPay to the Primary cannot exceed the funds collected by all transactions on the Primary smart contract:*

$$\sum_{\text{recipient}(C) \in \text{Primary}} \text{amount}(C) \leq \sum_x \text{funding}^x(\sigma)$$

Next, we describe how receivers of valid transfer certificates can finalize transactions and make funds available on their own accounts (Primary and FastPay).

**PROPOSITION 5.2 (REDEEMABILITY OF VALID TRANSFER CERTIFICATES TO PRIMARY).** *A new valid Primary transfer certificate  $C$  can always be redeemed by sending a new redeem transaction  $T$  to the smart contract.*

**PROPOSITION 5.3 (REDEEMABILITY OF VALID TRANSFER CERTIFICATES TO FASTPAY).** *Any user can eventually have a valid FastPay transfer certificate  $C$  confirmed by any honest authority.*

Specifically, in Proposition 5.3, the confirmation order for  $C$  is guaranteed to succeed for every honest authority  $\alpha$ , provided that the user first recovers and transfers to  $\alpha$  all the *missing certificates required by  $\alpha$* , defined as the sequence  $C_k \dots C_{n-1}$  such that  $k = \text{next\_sequence}^x(\alpha)$ ,  $x = \text{sender}(C)$ ,  $n = \text{sequence}(C)$ ,  $\text{sender}(C_i) = x$  ( $k \leq i \leq n-1$ ). The fact that no other certificates need to be confirmed (e.g. to credit the balance of  $\text{sender}(C)$  itself) is closely related to the possibility of (temporary) negative balances for authorities, and justified by the proof of safety in Appendix A.

Note that having a FastPay certificate confirmed by an authority  $\alpha$  only affects  $\alpha$ 's recipient and the sender's balances (i.e. *redeems the certificate*) the first time it is confirmed.

Finally, we state that FastPay funds credited on an account can always be spent. We write  $\text{received}(x)$  for the set of *incoming* transfer certificates  $C$  such that  $\text{recipient}(C) = x$  and  $C$  is known to the owner of the account  $x$ .

**PROPOSITION 5.4 (AVAILABILITY OF TRANSFER CERTIFICATES).** *Let  $x$  be an account owned by a correct user,  $n$  be the next available sequence number after the last signed transfer order (if any, otherwise  $n = 0$ ), and  $O$  be a new transfer order signed by  $x$  with  $\text{sequence}(O) = n$  and  $\text{sender}(O) = x$ .*

*Assume that the owner of  $x$  has secured enough funds for a new order  $O$  based on their knowledge of the chain  $\sigma$ , the history of outgoing*

*transfers, and the set  $\text{received}(x)$ . That is, formally:*

$$\begin{aligned} & \left( \text{amount}(O) + \sum_{\substack{\text{sender}(C) = x \\ \text{sequence}(C) < n}} \text{amount}(C) \right) \\ & \leq \left( \text{funding}^x(\sigma) + \sum_{C \in \text{received}(x)} \text{amount}(C) \right) \end{aligned}$$

*Then, for any honest authority  $\alpha$ , the user will always eventually obtain a valid signature of  $O$  from  $\alpha$  after sending the following orders to  $\alpha$ :*

- (1) *A synchronization order from the Primary based on the known state  $\sigma$ ;*
- (2) *A confirmation order for every  $C \in \text{received}(x)$ , preceded by all the missing certificates required by  $\alpha$  (if any) for the sender of  $C$ ;*
- (3) *Then, the transfer order  $O$ .*

**Worst-case efficiency of FastPay clients.** To initiate a transfer (Proposition 5.4) or receive funds (Proposition 5.3) from a sender account  $x$ , a FastPay client must address a quorum of authorities. During the exchange, each authority  $\alpha$  may require missing certificates  $C_k \dots C_{n-1}$ , where  $k = \text{next\_sequence}^x(\alpha)$  is provided by  $\alpha$ . In an attempt to slow down the client, a Byzantine authority could return  $k = 0$  and/or fail to respond at some point. To address this, a client should query each authority  $\alpha$  in parallel. After retrieving the sequence number  $k$ , the required missing certificates should be downloaded sequentially, in reverse order, then forwarded to  $\alpha$ . Given that FastPay client operations succeed as soon as a quorum of authorities completes their exchanges, this strategy ensures client efficiency despite Byzantine authorities.

## 6 IMPLEMENTATION

We implemented both a FastPay client and a networked multi-core multi-shard FastPay authority in Rust, using Tokio<sup>3</sup> for networking and ed25519-dalek<sup>4</sup> for signatures. For the verification of the multiple signatures composing a certificate we use ed25519 batch verification. To reduce latency we use UDP for FastPay requests and replies, and make the core of FastPay idempotent to tolerate retries in case of packet loss; we also provide an experimental FastPay implementation using exclusively TCP. Currently, data-structures are held in memory rather than persistent storage.

We implement an authority shard as a separate operating system process with its own networking and Tokio reactor core, to validate the low overhead of intra-shard coordination (through message passing rather than shared memory). We experimented with manually pinning processes to physical cores without a noticeable increase in performance through the Linux *taskset* feature. It seems the Linux OS does a good job in distributing processes and keeping them on inactive cores. We also experimented with a single process multi-threaded implementation of FastPay, using a single Tokio reactor for all shards on multi-core machines. However, this led to significantly lower performance, and therefore we opted for using separate processes even on a single machine for each shard. The exact bottleneck justifying this lower performance—whether at the

<sup>3</sup><https://tokio.rs>

<sup>4</sup><https://github.com/dalek-cryptography/ed25519-dalek>

level of Tokio multi-threading or OS resource management—still eludes us.

The implementation of both server and client is less than 4,000 LOC (of which half are for the networking), and a further 1,375 LOC of unit tests. It required about 2.5 months of work for 3 engineers, and a bit over 1,500 git commits. Keeping the core small required constant re-factoring and its simplicity is a significant advantage of the proposed FastPay design. We are open sourcing the Rust implementation, Amazon web services orchestration scripts, benchmarking scripts, and measurements data to enable reproducible results<sup>5</sup>.

## 7 EVALUATION

We evaluate the throughput and latency of our implementation of FastPay through experiments on AWS. We particularly aim to demonstrate that (i) sharding is effective, in that it increases throughput linearly as expected; (ii) latency is not overly affected by the number of authorities or shards, and remains near-constant, even when some authorities fail; and (iii) that the system is robust under extremely high concurrency and transaction loads.

### 7.1 Microbenchmarks

We report on microbenchmarks of the single-CPU core time required to process transfer orders, authority signed partial certificates, and certificates. Table 1 displays the cost of each operation in micro seconds ( $\mu s$ ) assuming 10 authorities (recall  $1\mu s = 10^{-6}s$ ); each measurement is the result of 500 runs on an Apple laptop (MacBook Pro) with a 2.9 GHz Intel Core i9 (6 physical and 12 logical cores), and 32 GB 2400 MHz DDR4 RAM. The first 3 rows respectively indicate the time to create and serialize (i) a transfer order, (ii) a partial certificate signed by a single authority, and (iii) a transfer certificate as part of a confirmation order. The last 3 rows indicate the time to deserialize them and check their validity. The dominant CPU cost involves the deserialization and signature check on certificates ( $236\mu s$ ), which includes the batch verification of the 8 signatures (7 from authorities and 1 from sender). However, deserializing orders ( $58\mu s$ ) and votes ( $60\mu s$ ) is also expensive: it involves 1 signature verification (no batching) and creating 1 signature. These results indicate that a single core shard implementation may only settle just over 4,000 transactions per second—highlighting the importance of sharding to achieve high-throughput.

In terms of networking costs, a transfer order is 146 bytes, and the signed response is 293 bytes. This could be reduced by only responding with a signature (64 bytes) rather than the full signed order, but we chose to echo back the order to simplify client implementations. A full certificate for an order is 819 bytes, and the response—consisting of an update on the state of the FastPay account—is 51 bytes. For deployments using many authorities we can compress certificates by using an aggregate signature scheme (such as BLS [9]). However, verification CPU costs of BLS only make this competitive for committees larger than 50-100 authorities. We note that all FastPay message types fit within the common maximum transmission unit of commodity IP networks, allowing requests and replies to be executed using a single UDP packet (assuming no packets loss and 10 authorities).

<sup>5</sup><https://github.com/novifinancial/fastpay>

| Measure                           | Mean ( $\mu s$ ) | Std. ( $\mu s$ ) |
|-----------------------------------|------------------|------------------|
| Create & Serialize Order          | 27               | 1                |
| Create & Serialize Partial Cert.  | 27               | 2                |
| Create & Serialize Certificate    | 4                | 0                |
| Deserialize & Check Order         | 58               | 1                |
| Deserialize & Check Partial Cert. | 60               | 1                |
| Deserialize & Check Certificate   | 236              | 10               |

**Table 1: Microbenchmark of single core CPU costs of FastPay operations; average and standard deviation of 500 measurements for 10 authorities.**

### 7.2 Throughput

We deploy a FastPay multi-shard authority on Amazon Web Services (Stockholm, eu-north-1 zone), on a m5d.metal instance. This class of instance guarantees 96 virtual CPUs (48 physical cores), on a 2.5 GHz, Intel Xeon Platinum 8175, and 384 GB memory. The operating system is Linux Ubuntu server 18.04, where we increase the network buffer to about 96MB. In all graphs, each measurement is the average of 9 runs, and the error bars represent one standard deviation; all experiments use our UDP implementation. We measure the variation of throughput with the number of shards. Our baseline experiment parameters are: 4 authorities (for confirmation orders), a load of 1M transactions, and applying back-pressure to allow a maximum of 1000 concurrent transactions at the time into the system (*i.e.* the *in-flight* parameter). We then vary these baseline parameters through our experiments to illustrate their impact on performance. We select 4 authorities as baseline for our experiments to make it easier to compare with other systems' evaluations [25].

**Robustness and performance under high concurrency.** Figures 5 and 6 respectively show the variation of the throughput of processing transfer and confirmation orders as we increase the number of shards per authority, from 15 to 85. We measure these by processing 1M transactions, across 4 authorities. Figure 5 shows that the throughput of transfer orders slowly increases with the number of shards. The *in-flight* parameter—the maximum number of transactions that is allowed into the system at any time—influences the throughput by about 10%, and setting it to 1,000 seems optimal for performance. The degree of concurrency in a system depends on the number of concurrent client requests, and we observe that FastPay is stable and performant even under extremely high concurrency peaks of 50,000 concurrent requests. Afterwards, the Operating System UDP network buffers fill up, and the authority network stacks simply drop the requests.

Figure 6 shows that the throughput of confirmation orders initially increases linearly with the number of shards, and then reaches a plateau at around 48 shards. This happens because our experiments are run on machines with 48 physical cores, running at full speed, and 48 logical cores. The *in-flight* parameter of concurrent requests does not influence the throughput much, but setting it too low (*e.g.* at 100) does not saturate our CPUs. These figures show that FastPay can support up to 160,000 transactions per second on 48 shards (about 7x the peak transaction rate of the Visa payments network [48]) while running on commodity computers that cost less than 4,000 USD/month per authority<sup>6</sup>.

<sup>6</sup>AWS reports a price of 5.424 USD/hour for their m5d.metal instances. <https://aws.amazon.com/ec2/pricing/on-demand> (January 2020)



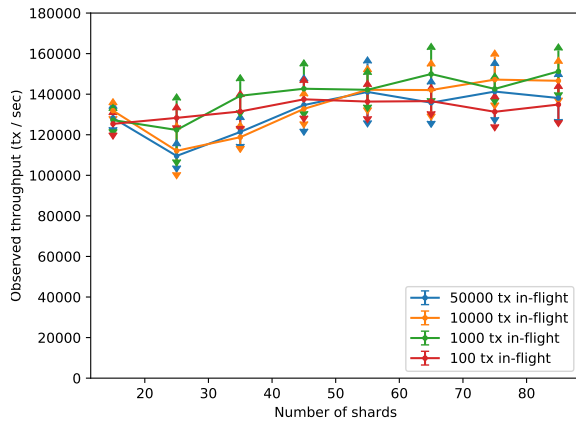


Figure 5: Variation of the throughput of transfer orders with the number of shards, for various levels of concurrency (in-flight parameter). The measurements are run under a total load of 1M transactions.

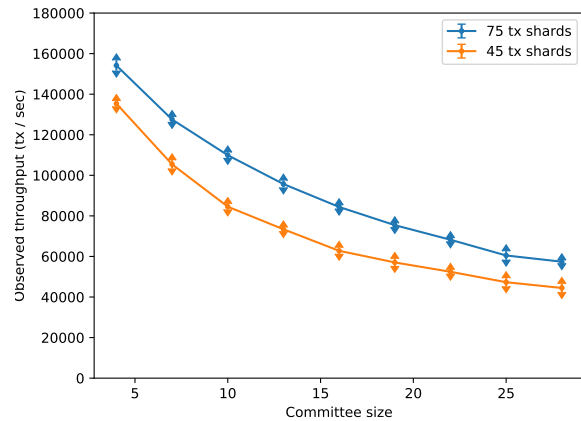


Figure 7: Variation of the throughput of confirmation orders with the number of authorities, for various number of shards. The in-flight parameter is set to 1,000 and the system load is of 1M transactions.

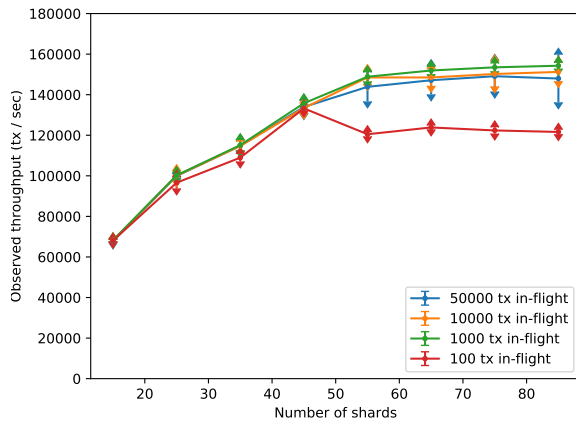


Figure 6: Variation of the throughput of confirmation orders with the number of shards, for various levels of concurrency (in-flight parameter). The certificates are issued by 4 authorities, and the measurements are run under a total load of 1M transactions.

**Robustness and performance under total system load.** Figures 11 and 12 (see Appendix C) show the variation of the throughput of transfer and confirmation orders with the number of shards, for various total system loads—namely the total number of transactions in the test, submitted at the same time. The goal of this experiment is to analyze the system’s performance when experiencing high peaks of utilization. Our results show that the throughput is not affected by the system load. The tests were performed with 4 authorities, and the client concurrency in-flight parameter set to 1,000. These figures illustrate that FastPay can process about 160,000 transactions per second even under a total load of 1.5M transactions, and that the total load does not significantly affect performance. These supplement figures 5 and 6 that illustrate the

concurrent transaction rate (in-flight parameter) also does not influence performance significantly (except when it is too low by under-utilizing the system).

For comparison, in the key experimental work [25], Han *et al.* study a number of permissioned systems under a high load. They show that for all of Hyperledger Fabric (v0.6 with PBFT) [28], Hyperledger Fabric (v1.0 with BFT-Smart) [29], Ripple [16], and R3 Corda v3.2 [41], the successful requests per second *drops to zero* when the transaction rate increases to more than a few thousands transactions per second (notably for Corda only a few hundred). An important exception is Tendermint [11], which maintains a processed transaction rate of about 4,000 to 6,000 transactions per second at a high concurrency rate. These findings were confirmed for Hyperledger Fabric that reportedly starts saturating at a rate of 10,000 transactions per second [36]. In contrast, our results suggest that FastPay stays performant under extremely high rates of concurrent transactions (in-flight parameter) and high work load (total number of transactions processed).

**Influence of the number of authorities.** As discussed in Section 4, we expect that increasing the number of authorities only impacts the throughput of confirmation orders (that need to transfer and check transfer certificates signed by  $2f + 1$  authorities), and not the throughput of transfer orders. Figure 7 confirms that the the throughput of confirmation orders decreases as the number of authorities increases. FastPay can still process about 80,000 transactions per second with 20 authorities (for 75 shards). The measurements are taken with an in-flight concurrency parameter set to 1,000, and under a load of 1M total transactions. We note that for higher number of authorities, using an aggregate signature scheme (e.g. BLS [9]) would be preferable since it would result in constant time verification and near-constant size certificates. However, since we use batch verification of signatures, the break even point may be after 100 authorities in terms of verification time.

### 7.3 Latency

We measure the variation of the client-perceived latency with the number of authorities. We deploy several FastPay multi-shard authorities on Amazon Web Services (all in Stockholm, eu-north-1 zone), each on a m5d.8xlarge instance. This class of instance guarantees 10Gbit network capacity, on a 3.1 GHz, Intel Xeon Platinum 8175 with 32 cores, and 128 GB memory. The operating system is Linux Ubuntu server 16.04. Each instance is configured to run 15 shards. The client is run on an Apple laptop (MacBook Pro) with a 2.9 GHz Intel Core i9 (6 physical and 12 logical cores), and 32 GB 2400 MHz DDR4 RAM; and connected to a reliable WIFI network. We run experiments with the client in two different locations; (i) in the U.K. (geographically close to the authorities, same continent), and (ii) in the U.S. West Coast (geographically far from the authorities, different continent). Each measurement is the average of 300 runs, and the error bars represent one standard deviation; all experiments use our UDP implementation.

We observe that the client-authority WAN latency is low for both transfer and confirmation orders; the latency is under 200ms when the client is in the U.S. West Coast, and about 50ms when the client is in the U.K. Figure 8 illustrates the latency between a client creating and sending a transfer order to all authorities, and receiving sufficient signatures to form a transfer certificate (in our experiment we wait for all authorities to reply to measure the worse case where  $f$  authorities are Byzantine). The latency is virtually constant as we increase the number of authorities, due to the client emitting orders asynchronously to all authorities and waiting for responses in parallel.

Figure 9 illustrates the latency to submit a confirmation order, and wait for all authorities to respond with a success message. It shows latency is virtually constant when increasing the number of authorities. This indicates that the latency is largely dominated by the network (and not by the verification of certificates). However, since even for 10 authorities a FastPay message fits within a network MTU, the variation is very small. Due to our choice of using UDP as a transport there is no connection initiation delay (as for TCP), but we may observe packet loss under very high congestion conditions. Authority commands are idempotent to allow clients to re-transmit to overcome loss without sacrificing safety.

**Performance under failures.** Research literature suggests permissioned blockchains based on (often leader-based) consensus suffer an enormous performance drop when some authorities fail [32]. We measure the effect of authority failure in FastPay and show that latency is not affected when  $f$  or fewer authorities are unavailable.

We run our baseline experimental setup (10 authorities distributed over 10 different AWS instances), when a different number of authorities are not available for  $f = 0 \dots 3$ . We measure the latency experienced by a client on the same continent (Europe), sending a transfer order until it forms a valid transfer certificate. Table 2 summarizes the mean latency and standard deviation for different  $f$ . There is no statistically significant difference in latency,

| $f$ | Latency (ms $\pm$ std) |
|-----|------------------------|
| 0   | 43 $\pm$ 2             |
| 1   | 41 $\pm$ 3             |
| 2   | 44 $\pm$ 4             |
| 3   | 47 $\pm$ 2             |

Table 2: Crash-failure Latency.

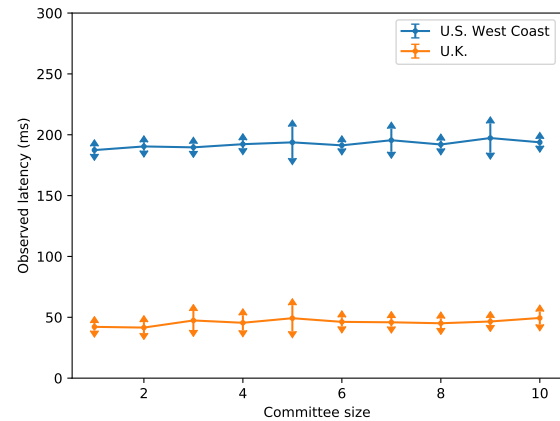


Figure 8: Variation of the latency of transfer orders with the number of authorities, for various locations of the client.

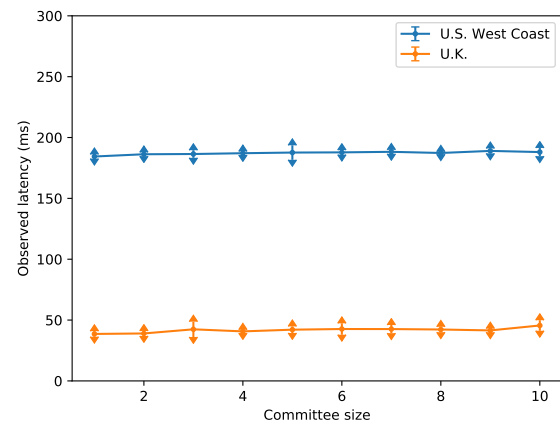


Figure 9: Variation of the latency of confirmation orders with the number of authorities, for various locations of the client.

no matter how many tolerable failures FastPay experiences (up to  $f \leq 3$  for 10 authorities). We also experimented with killing authorities one by one with similar results, up to  $f > 3$  when the system did observably lose liveness as expected. The underlying reason for the steady performance under failures is FastPay's lack of reliance on a leader to drive the protocol.

## 8 LIMITATIONS AND FUTURE WORK

**Threats to validity of experiments.** Our experiments represent the best case performance, for a set number of authorities and shards, as they are performed in laboratory conditions. In particular, real-world transactions may have the same sender account, which would prevent them from being executed in parallel. Further, the throughput evaluation places transaction load on an authority through the local network interface, and therefore does not

take fully into account the operating system networking costs of a full WAN stack. Further, our WAN latency experiments were performed against authorities with very low-load. Finally, the costs of persisting databases to storage are not taken into account when measuring latency and throughput (we leave the implementation of low-latency persistent storage to future work).

**Integrating privacy.** As presented, FastPay exposes information about all transactions, namely the sender-recipient accounts and the amounts transferred, as well as the timings of those transfers. Fully integrating stronger privacy protections is a separate research project. However, we want to highlight that the architecture of FastPay is highly compatible with threshold issuance selective disclosure credential designs, such as Coconut [46]. In those schemes a threshold of authorities can jointly sign a credential that the user can subsequently randomize and present to execute a payment. Implementing hidden balances, like MinbleWinble [37] and combining them with credentials should be possible—but beyond the scope of the present work.

**Checkpointing, authority, and key rotation.** The important enabler for the good performance of FastPay, but also an important limitation, is the fact that authorities do not need to reach consensus on the state of their databases. We demonstrate that payments are secure in this context, but various system maintenance operations are harder to implement. For example, checkpointing the state of all accounts in the systems, to compress the list of stored certificates would be beneficial, but cannot be straightforwardly implemented without consensus. Similarly, it would be beneficial for authorities to be able to rotate in and out of the committee, as well as to update their cryptographic signature keys. Due to the lack of tight synchronization between authorities there is no natural point that guarantees they all update their committees at the same logical time. Further, our proofs of liveness under asynchrony presume that transfer orders and certificates that were once valid, will always be valid. Integrating such governance features into FastPay will require careful design to safely leverage either some timing (synchrony) assumptions or use a more capable (but maybe lower performance) consensus layer, such as one facilitated by the Primary.

**Economics and fees.** Some cost to insert transactions into a system (like fees in Bitcoin), allows for sound accounting and prevents Denial of Service attacks by clients over-using an open system. The horizontal scalability of FastPay alleviates somehow the need to integrate such a scheme, since issues of capacity can be resolved by increasing its capacity through more shards (as well as deploying network level defenses). However, if there was a need to implement fees for using FastPay we would not recommend using micro-payments associated with each payment like in Bitcoin. We would rather recommend allowing a client to deposit some payment into a service account with all authorities, and then allow them to deduct locally some of this fee for any services rendered (namely any signed transfer order or confirmation order processed). In practical terms, the variable costs of processing transactions in FastPay is low. There is no artificial shortage due to lack of scalability, and a flat periodic fee on either senders or recipients might be sufficient to support operations (rather than a charge per transaction).

## 9 RELATED WORKS

ABC [45] is an asynchronous payment system which can be sharded similarly to FastPay to achieve arbitrary throughput. ABC proposes a relaxed notion of consensus where termination is only guaranteed if the sender of the transaction is honest, and similarly to FastPay dishonest users may lock their own account. FastPay and ABC share similar features but are designed for different purposes. FastPay can be deployed as a RTGS or a (permissioned) side-infrastructure, and heavily focuses on implementation and evaluation; ABC is a permissionless standalone system providing great details on how to run it as an open system based on proof-of-stake [5], but provides no implementation or evaluation.

Other systems similar to FastPay are Astro [17] and Brick [2], which were both developed concurrently to FastPay. Astro relies on *Byzantine reliable broadcast* [13] which adds *totality* [13] to Byzantine consistent broadcast. This allows Astro to guarantee availability even to incorrect users (while FastPay only guarantees it for correct users, see Section 3.4) at the cost of one extra broadcast step among the authorities. Astro is designed to be a standalone system and does not natively integrate into a Primary infrastructure, and does not offer security proofs. As FastPay, Brick uses Byzantine consistent broadcast as underlying primitive and positions itself as a payment channel. As such, Brick offers details on how to efficiently open and close channels, provides proofs of fraud in case authorities misbehave, and presents detailed incentive mechanisms to keep authorities honest. However, it does not present an implementation or evaluation (it only presents a quick latency benchmark), and only works with two users. In contrast, FastPay focuses on high performance, robustness, and scalability; it provides a scalable architecture and is specifically designed to handle high transaction volumes, from a high number of users.

We now compare FastPay with traditional payment systems and some relevant crypto-currencies.

**Traditional payment systems.** In the context of traditional payment systems FastPay is a real-time gross settlement system (RTGS) [4, 6]—payments are executed in close to real-time, there is no netting between participants, and the transfer of funds is final upon the full payment protocol terminating. All payments are pre-funded so there is no need to keep track of credit or liquidity, which makes the design vastly simpler.

FastPay, from an assurance and performance perspective is significantly superior to deployed RTGS systems: it (i) implements a fully Byzantine fault tolerant architecture (established systems rely on master-slave configurations to only recover from few crash failures), (ii) has higher throughput (as compared, for example with the TARGET2 [22] European Central Bank RTGS systems that has a target throughput of 500 tx/sec), and (iii) has faster finality (as compared to TARGET2 providing finality of a few seconds). Since FastPay allows for fast gross settlement, participants are not exposed to credit risk, as in the case of retail payment systems such as VISA and Mastercard (that use daily netting, and have complex financial arrangements to mitigate credit risk in case of bank default). Furthermore, it does achieve both throughput and latency, comparable to those systems combined—about 80,000 tx/sec at peak times, when adding up the throughput of Visa and Mastercard together [26, 48].

On the downside, FastPay lacks certain features of mature RTGS systems: in particular it does not support Delivery-on-Payment transactions that atomically swap securities when payment is provided, or Payment-versus-Payment, that atomically swap amounts in different currencies to minimize the risk of foreign exchange transactions. These require atomic operations across accounts controlled by different users, and would therefore require extending FastPay to support them (namely operations with consensus number of 2 per Herlihy [27]), which we leave for future work.

**Crypto-currencies.** FastPay provides high assurance in the context of Byzantine failures within its infrastructure. In that respect it is comparable with systems encountered in the space of permissioned blockchains and crypto-currencies, as well as their ecosystem of payment channels. FastPay is permissioned in that the set of authorities managing the system is closed—in fact we do not even propose a way to rotate those authorities and leave this to future work. Qualitatively, FastPay differs from other permissioned (or permissionless) crypto-currencies in a number of ways: it is secure under full network asynchrony (since it does not require or rely on atomic broadcast channels or consensus, but only consistent broadcast)—leading to higher performance. This direction was explored in the past in relation to central bank crypto-currency systems [19] and high performance permissionless systems [42]. It was recently put on a formal footing by Guerraroui *et al.* [24]. Our work extends this theory to allow increased concurrency, correctness under sharding, and rigorous interfacing with external settlement mechanisms. FastPay achieves auditability through a set of certificates signed by authorities rather than a sequential log of actions (blockchain), which would require authorities to reach agreement on a common sequence.

Quantitatively, compared with other permissioned systems FastPay is extremely performant. HyperLedger Fabric [12] running with 10 nodes achieves about 1,000 transactions per second and a latency of about 10 seconds [36]; and Libra [14] and Corda [10, 40] achieve similar performance. JP Morgan developed a digital coin built from the Ethereum codebase, which can achieve about 1,500 transactions per second with four nodes, and imposing a block time of 1 second [3]. Tendermint [11] reportedly achieves 10,000 transactions per second with 4 nodes, with a few seconds latency [30]. However, as we discussed in Section 7, many of those systems see their performance degrading dramatically under heavy load—whereas FastPay performs as expected.

FastPay can be used as a side chain of any crypto-currency with reasonable finality guarantees, and sufficient programmability. As compared to bilateral payment channels it is superior in that it allows users to pay anyone in the system without locking liquidity into the bilateral channel, and is fully asynchronous. However, FastPay does rely on an assumption of threshold non-Byzantine authorities for safety and liveness, whereas payment channel designs only rely on network synchrony for safety and liveness (safety may be lost under conditions of asynchrony). As compared to traditional payment channel networks (such as the lighting network [38]) FastPay is simpler and does not require complex path finding algorithms [23, 38, 39, 44].

## 10 CONCLUSION

FastPay is a settlement layer based on consistent broadcast channels, rather than full consensus. The FastPay design leverages the nature of payments to allow for asynchronous payments into accounts, and optional interactions with an external Primary to build a practical system, while providing proofs of both safety and liveness; it also proposes and evaluates a design for sharded implementation of authorities to horizontally scale and match any throughput need.

The performance and robustness of FastPay is beyond and above the state of the art, and validates that moving away from both centralized solutions and full consensus to manage pre-funded retail payments has significant advantages. Authorities can jointly process tens of thousands of transactions per second (we observed a peak of 160,000 tx/sec) using merely commodity hardware and lean software. A payment confirmation latency of less than 200ms between continents make FastPay practical for point of sale payments—where goods and services need to be delivered fast and in person. Pretty much instant settlement enables retail payments to be freed from intermediaries, such as banks payment networks, since they eliminate any credit risk inherent in deferred netted end-of-day payments, that underpin today most national Fast Payment systems [8]. Further, FastPay can tolerate up to one-third of authorities crashing or even becoming Byzantine without losing either safety or liveness (or performance). This is in sharp contrast with existing centralized settlement layers operating on specialized mainframes with a primary / backup crash fail strategy (and no documented technical strategy to handle Byzantine operators). Surprisingly, it is also in contrast with permissioned blockchains, which have not achieved similar levels of performance and robustness yet, due to the complexity of engineering and scaling full Byzantine Fault-Tolerant consensus protocols.

## ACKNOWLEDGMENTS

This work is funded by Novi, a Facebook subsidiary. The authors would like to thank Dahlia Malkhi for her constant feedback on this project, and Kostas Chalkias for feedback on late manuscript. We also thank the Novi Research and Engineering teams for valuable feedback.

## REFERENCES

- [1] Alex Prut. 2020 (accessed January 29, 2020). *Libra Quick Introduction*. <https://medium.com/@alexprut/libra-quick-introduction-6ce2c51d703c>
- [2] Georgia Avarikioti, Eleftherios Kokoris Kogias, and Roger Wattenhofer. 2019. Brick: Asynchronous state channels. *arXiv preprint arXiv:1905.11360* (2019).
- [3] Arati Baliga, I Subhod, Pandurang Kama, and Siddhartha Chatterjee. 2018. Performance evaluation of the quorum blockchain platform. *arXiv preprint arXiv:1809.03421* (2018).
- [4] Bank for International Settlements. 2005 (accessed January 20, 2020). *New developments in large-value payment systems*. <https://www.bis.org/cpmi/publ/d67.pdf>
- [5] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. 2019. SoK: Consensus in the age of blockchains. In *Proceedings of the ACM Conference on Advances in Financial Technologies*. 183–198.
- [6] Morten L. Bech and Bart Hobijn. 2006. Technology diffusion within central banking: the case of real-time gross settlement. *FRB of New York Staff Report* (2006).
- [7] Blockchain Council. 2019 (accessed January 29, 2020). *Permissioned and permissionless blockchains: a comprehensive guide*. <https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide>
- [8] Stephanie Bolt, David Emery, Paul Harrigan, et al. 2014. Fast retail payment systems. *RBA Bulletin, December* (2014), 43–51.

- [9] Dan Boneh, Ben Lynn, and Hovav Shacham. 2001. Short signatures from the Weil pairing. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 514–532.
- [10] Richard Gendal Brown, James Carlyle, Ian Grigg, and Mike Hearn. 2016. Corda: an introduction. *R3 CEV, August 1* (2016), 15.
- [11] Ethan Buchman. 2016. *Tendermint: Byzantine fault tolerance in the age of blockchains*.
- [12] Christian Cachin. 2016. Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers*, Vol. 310. 4.
- [13] Christian Cachin, Rachid Guerraoui, and Luis Rodrigues. 2011. *Introduction to reliable and secure distributed programming*. Springer Science & Business Media.
- [14] Calibra. 2019 (accessed January 17, 2020). *The Libra Blockchain*. <https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf>
- [15] Miguel Castro, Barbara Liskov, et al. 1999. Practical Byzantine fault tolerance. In *OSDI*, Vol. 99. 173–186.
- [16] Ryan Chard. 2018 (accessed January 20, 2020). *Ripple Documentation*. <https://buildmedia.readthedocs.org/media/pdf/ripple/latest/ripple.pdf>
- [17] Daniel Collins, Rachid Guerraoui, Jovan Komatovic, Matteo Monti, Athanasios Xygkis, Matej Pavlovic, Petr Kuznetsov, Yvonne-Anne Pignolet, Dragos-Adrian Seredinschi, and Andrei Tonkikh. 2020. Online Payments by Merely Broadcasting Messages (Extended Version). *arXiv preprint arXiv:2004.13184* (2020).
- [18] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, et al. 2016. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*. Springer, 106–125.
- [19] George Danezis and Sarah Meiklejohn. 2015. Centrally banked cryptocurrencies. *arXiv preprint arXiv:1505.06895* (2015).
- [20] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. 1988. Consensus in the presence of partial synchrony. *Journal of the ACM (JACM)* 35, 2 (1988), 288–323.
- [21] Elizabeth Lopatto. 2019 (accessed January 29, 2020). *Libra, Explained. Move fast and bank things*. <https://www.theverge.com/2019/6/26/18716326/facebook-libra-cryptocurrency-blockchain-irs-starbucks>
- [22] European Central Bank. 2018 (accessed January 20, 2020). *Single Shared Platform User Detailed Functional Specifications Core Services 1st Book (Version 12.01)*. [https://www.ecb.europa.eu/paym/target/target2/profuse/nov\\_2018/shared/pdf/T2\\_UDFS\\_book\\_1\\_v12.01.pdf](https://www.ecb.europa.eu/paym/target/target2/profuse/nov_2018/shared/pdf/T2_UDFS_book_1_v12.01.pdf)
- [23] CYRIL Grunspan and Ricardo Pérez-Marco. 2018. Ant routing algorithm for the Lightning Network. *arXiv preprint arXiv:1807.00151* (2018).
- [24] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovič, and Dragos-Adrian Seredinschi. 2019. The Consensus Number of a Cryptocurrency. In *Symposium on Principles of Distributed Computing (PODC)*.
- [25] Runchao Han, Gary Shapiro, Vincent Gramoli, and Xiwei Xu. 2019. On the performance of distributed ledgers for internet of things. *Internet of Things* (2019), 100087.
- [26] Susan Herbst-Murphy. 2013 (accessed January 20, 2020). *Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts*. <https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2013/D-2013-October-Clearing-Settlement.pdf>
- [27] Maurice Herlihy. 1991. Wait-free synchronization. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 13, 1 (1991), 124–149.
- [28] Hyperledger. 2017 (accessed January 20, 2020). *Hyperledger Fabric V0.6*. <https://readthedocs.org/projects/fabricdocs/downloads/pdf/origin-v0.6>
- [29] Hyperledger. 2020 (accessed January 20, 2020). *Hyperledger Fabric V1.0*. <https://readthedocs.org/projects/hyperledger-fabric/downloads/pdf/master>
- [30] Oumma El Khazzani. 2019 (accessed January 17, 2020). *Creating the future of Blockchain – Thorchain Update 002*. <https://www.swishlabs.com/blog/creating-the-future-of-blockchain-thorchain-update-002>
- [31] Butler W. Lampson and David B. Lomet. 1993. A New Presumed Commit Optimization for Two Phase Commit. In *VLDB*. Morgan Kaufmann, 630–640.
- [32] Hyejeong Lee, Jeff Seibert, Md. Endadul Hoque, Charles Edwin Killian, and Cristina Nita-Rotaru. 2014. Turret: A Platform for Automated Attack Finding in Unmodified Distributed System Implementations. In *ICDCS*. IEEE Computer Society, 660–669.
- [33] Stephen Lindsay. 2015. ISO 20022 and real-time domestic payments. *Journal of Payments Strategy & Systems* 9, 1 (2015), 22–29.
- [34] Dahlia Malkhi and Michael Reiter. 1998. Byzantine quorum systems. *Distributed computing* 11, 4 (1998), 203–213.
- [35] Satoshi Nakamoto. 2019. *Bitcoin: A peer-to-peer electronic cash system*. Technical Report. Manubot.
- [36] Qassim Nasir, Ilham A Qasse, Manar Abu Talib, and Ali Bou Nassif. 2018. Performance analysis of hyperledger fabric platforms. *Security and Communication Networks* 2018 (2018).
- [37] Andrew Poelstra. 2016. Mumblewimble.
- [38] Joseph Poon and Thaddeus Dryja. 2015. The bitcoin lightning network. *Scalable o-chain instant payments* (2015).
- [39] Pavel Prihodko, Slava Zhigulin, Mykola Sahnó, Aleksei Ostrovskiy, and Olaoluwa Osuntokun. 2016. Flare: An approach to routing in lightning network. *White Paper* (2016).
- [40] R3. 2018 (accessed January 17, 2020). *Sizing and Performance*. <https://docs.corda.r3.com/sizing-and-performance.html>
- [41] R3. 2018 (accessed January 20, 2020). *R3 Corda (Release Notes)*. <https://docs.corda.net/releases/release-V3.2/release-notes.html>
- [42] Team Rocket. 2018. Snowflake to avalanche: A novel metastable consensus protocol family for cryptocurrencies.
- [43] George Samaras, Kathryn Britton, Andrew Citron, and C. Mohan. 1995. Two-Phase Commit Optimizations in a Commercial Distributed Environment. *Distributed and Parallel Databases* 3, 4 (1995), 325–360.
- [44] Vibhaalakshmi Sivaraman, Shaileshh Bojja Venkatakrishnan, Mohammad Alizadeh, Giulia Fanti, and Pramod Viswanath. 2018. Routing cryptocurrency with the spider network. *arXiv preprint arXiv:1809.05088* (2018).
- [45] Jakub Sliwinski and Roger Wattenhofer. 2019. ABC: Asynchronous Blockchain without Consensus. *arXiv preprint arXiv:1909.10926*.
- [46] Alberto Sonnino, Mustafa Al-Bassam, Shehar Bano, Sarah Meiklejohn, and George Danezis. 2018. Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers. *arXiv preprint arXiv:1802.07344* (2018).
- [47] Swift. 2020 (accessed February 04, 2020). *SWIFT The global provider of secure financial messaging services*. <https://www.swift.com/>
- [48] Visa. 2020 (accessed January 20, 2020). *Visa acceptance for retailers*. <https://usa.visa.com/run-your-business/small-business-tools/retail.html>
- [49] Marko Vukolić. 2015. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International workshop on open problems in network security*. Springer, 112–125.
- [50] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151 (2014), 1–32.

## A PROOFS OF SECURITY

We now prove the results presented in Section 5.

### A.1 Additional Notations

We define  $\text{funding}^x(\alpha)$  as the sum of all the amounts received from the Primary by a FastPay address  $x$ , as seen at a given time by an authority  $\alpha$ :

$$\text{funding}^x(\alpha) = \sum_{S \in \text{synchronized}^x(\alpha)} \text{amount}(S)$$

### A.2 Safety

LEMMA A.1 (TRANSFER CERTIFICATE UNIQUENESS). *If*

$$\begin{cases} \text{sender}(C) = \text{sender}(C'), \text{ and} \\ \text{sequence}(C) = \text{sequence}(C') \end{cases}$$

*then*  $C$  and  $C'$  *certify the same transfer order:*

$$\text{value}(C) = \text{value}(C')$$

PROOF. Both certificates  $C$  and  $C'$  are signed by a quorum of authorities. By construction, any two quorums intersect on at least one honest authority. Let  $\alpha$  be an honest authority in both quorums.  $\alpha$  signs at most one transfer order per sequence number, thus  $C$  and  $C'$  certify the same transfer order.  $\square$

LEMMA A.2 (FASTPAY INVARIANT). *For every honest authority  $\alpha$ , for every account  $x$ , it holds that*

$$\begin{aligned} & \left( \text{balance}^x(\alpha) + \sum_{C \in \text{confirmed}^x(\alpha)} \text{amount}(C) \right) \\ & \leq \left( \text{funding}^x(\alpha) + \sum_{C \in \text{received}^x(\alpha)} \text{amount}(C) \right) \end{aligned}$$

*Besides, if  $n = \text{next\_sequence}^x(\alpha)$ , we have that  $\text{confirmed}^x(\alpha) = \{C_0 \dots C_{n-1}\}$  for some certificates  $C_k$  such that  $\text{sequence}(C_k) = k$  and  $\text{sender}(C_k) = x$ .*

PROOF. By construction of the FastPay authorities (Figure 2 and Figure 10): Whenever a confirmed certificate  $C$  is added to  $\text{confirmed}^x(\alpha)$ ,  $\text{balance}^x(\alpha)$  is decreased by  $\text{amount}(C)$ , and the value  $\text{next\_sequence}^x(\alpha)$  is incremented into  $\text{sequence}(C) + 1$ . Any new synchronization order equally increases  $\text{balance}^x(\alpha)$  and  $\text{funding}^x(\alpha)$ . Whenever a confirmed certificate  $C$  is added to  $\text{received}^x(\alpha)$ , eventually  $\text{balance}^x(\alpha)$  is increased once by  $\text{amount}(C)$ . (This may take time due to cross-shard updates.)  $\square$

LEMMA A.3 (PRIMARY INVARIANT). *The total balance of all FastPay accounts on Primary is such that*

$$\text{total\_balance}(\sigma) = \left( \sum_x \text{funding}^x(\sigma) - \sum_{C \in \text{redeemed}(\sigma)} \text{amount}(C) \right)$$

PROOF. By construction of the smart contract handling funding and redeeming transactions (Section 4.3): whenever a funding transaction  $T$  is executed by the smart contract, both  $\text{funding}^x(\sigma)$  and  $\text{total\_balance}(\sigma)$  increase by  $\text{amount}(T)$ .

Conversely,  $\text{total\_balance}(\sigma)$  decreases by  $\text{amount}(C)$  whenever a Primary transfer certificate  $C$  is redeemed on-chain and added to  $\text{redeemed}(\sigma)$ .  $\square$

LEMMA A.4 (FUNDING LOG SYNCHRONIZATION). *For every honest authority  $\alpha$  and every account  $x$ , it holds that*

$$\text{funding}^x(\alpha) \leq \text{funding}^x(\sigma)$$

PROOF. By definition of the synchronization with the Primary (Section 4.3), and by security of the Primary and its client, we note that  $\text{funding}^x(\alpha)$  only increases after a funding transaction has already increased  $\text{funding}^x(\sigma)$  by the same amount.  $\square$

LEMMA A.5 (BALANCE CHECK). *For every honest authority  $\alpha$ , when an order  $O = \text{pending}^x(\alpha)$  is pending, we have*

$$\text{amount}(O) \leq \text{balance}^x(\alpha)$$

PROOF. By construction of the FastPay authorities (Figure 2), if  $O = \text{pending}^x(\alpha)$ , then  $O$  was successfully processed by  $\alpha$  as a new transfer order from account  $x$ . At the time of the request,  $\text{amount}(O)$  did not exceed the current balance  $B$ . Since  $O$  is still pending, in the meantime, no other transfer certificates from account  $x$  have been confirmed by  $\alpha$ . (A confirmation would reset the field pending and prevent  $O$  from being pending again due to increasing sequence numbers.) Therefore, the balance did not decrease, and  $\text{balance}^x(\alpha) \geq B \geq \text{amount}(O)$ .  $\square$

PROPOSITION A.6 (ACCOUNT SAFETY). *For every account  $x$ , at any given time, we have that*

$$\sum_{\text{sender}(C)=x} \text{amount}(C) \leq \text{funding}^x(\sigma) + \sum_{\text{recipient}(C)=x} \text{amount}(C)$$

PROOF. Let  $n$  be the highest sequence number of a transfer certificate  $C_n$  from  $x$ . Let  $\alpha$  an honest authority whose signature is included in the certificate. At the time of the signature, we

had  $\text{value}(C_n) = \text{pending}^x(\alpha)$ . Therefore, by Lemma A.2 and Lemma A.5, we have

$$\begin{aligned} & \left( \text{amount}(C_n) + \sum_{C \in \text{confirmed}^x(\alpha)} \text{amount}(C) \right) \\ & \leq \left( \text{funding}^x(\alpha) + \sum_{C \in \text{received}^x(\alpha)} \text{amount}(C) \right) \end{aligned}$$

Given that  $n$  is the highest sequence number, by Lemma A.1 and Lemma A.2, the left-hand term exactly covers the certified transfer orders from  $x$  and is equal to  $\sum_{\text{sender}(C)=x} \text{amount}(C)$ .

Given that amounts are non-negative, for every honest node  $\alpha$ , we have

$$\sum_{C \in \text{received}^x(\alpha)} \text{amount}(C) \leq \sum_{\text{recipient}(C)=x} \text{amount}(C)$$

Finally,  $\text{funding}^x(\alpha) \leq \text{funding}^x(\sigma)$  by Lemma A.4.  $\square$

PROOF OF THEOREM 5.1 (SOLVENCY). By applying Proposition A.6 on every account and summing, we obtain:

$$\begin{aligned} \sum_x \text{funding}^x(\sigma) & \geq \\ & \left( \sum_C \text{amount}(C) - \sum_{\text{recipient}(C) \in \text{FastPay}} \text{amount}(C) \right) \\ & = \sum_{\text{recipient}(C) \in \text{Primary}} \text{amount}(C) \end{aligned}$$

$\square$

### A.3 Liveness

PROOF OF PROPOSITION 5.2 (REDEEMING TO PRIMARY). We have seen in Theorem 5.1 that the smart contract always has enough funding for all certified Primary transfer orders. The definition of  $\text{redeemed}(\sigma)$  (Section 4.3) thus ensures that any new certified Primary transfer order can be redeemed exactly once.  $\square$

PROOF OF PROPOSITION 5.3 (REDEEMING TO FASTPAY). If a certificate  $C$  exists for account  $x$  and sequence number  $n$ , this means at least  $f + 1$  honest authorities contributed signatures to the transfer order  $O = \text{value}(C)$ . By construction of FastPay, these authorities have received (Figure 2) and will keep available (Section 4.4) all the previous confirmation orders  $C_0 \dots C_{n-1}$  with  $\text{sender}(C_k) = x$ ,  $\text{sequence}(C_k) = k$ . Therefore, any client can retrieve them and eventually bring any other honest authority up to date with  $C$ .  $\square$

PROOF OF PROPOSITION 5.4 (AVAILABILITY OF CERTIFICATES). Let  $B \geq \text{amount}(O)$  be the value defined as follows at the time of the creation of the new transfer order  $O$ :

$$\begin{aligned} B = & \left( \text{funding}^x(\sigma) - \sum_{\substack{\text{sender}(C)=x \\ \text{sequence}(C) < n}} \text{amount}(C) \right. \\ & \left. + \sum_{C \in \text{received}(x)} \text{amount}(C) \right) \end{aligned}$$

By a case analysis similar to the proof of Lemma A.2, provided that the owner of  $x$  is communicating the information described in Proposition 5.4 to the authority  $\alpha$ , it will hold eventually that  $\text{balance}^x(\alpha) \geq B \geq \text{amount}(O)$  and  $\text{next\_sequence}^x(\alpha) = n$ . We deduce that eventually  $\alpha$  will accept the transfer order  $O$  and make the value of its signed (pending) order available.  $\square$

```

fn handle_cross_shard_commit( $\alpha$ , C) -> Result {
  let O = value(C);
  let recipient = match recipient(O) {
    Address::FastPay(recipient) => recipient,
    Address::Primary(_) => { bail!(); };
  };
  ensure!( $\alpha$ .in_shard(recipient));
  let recipient_account = accounts( $\alpha$ ).get(recipient)
    .or_insert(AccountState::new());
  recipient_account.balance += amount(O);
  Ok()
}

fn handle_primary_synchronization_order( $\alpha$ , S) -> Result {
  // Update recipient(S) assuming that S comes from
  // a trusted source (e.g. Primary client).
  let recipient = recipient(S);
  ensure!( $\alpha$ .in_shard(recipient));

  if transaction_index(S) <= last_transaction( $\alpha$ ) {
    // Ignore old synchronization orders.
    return Ok();
  }
  ensure!(transaction_index(S) == last_transaction( $\alpha$ ) + 1);

  last_transaction( $\alpha$ ) += 1;
  let recipient_account = accounts( $\alpha$ ).get(recipient)
    .or_insert(AccountState::new());
  recipient_account.balance += amount(S);
  recipient_account.synchronized.push(S);
  Ok()
}

```

Figure 10: Authority algorithms for cross-shard updates and (Primary) synchronization orders.

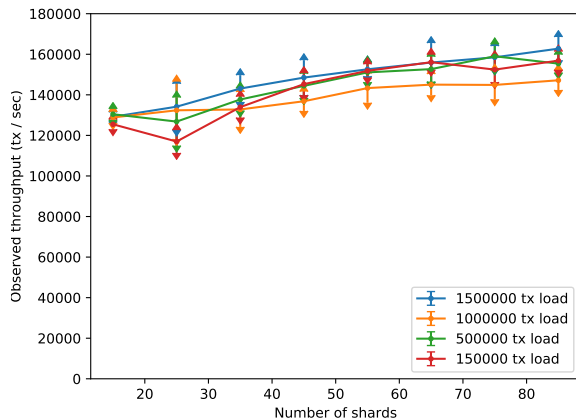


Figure 11: Variation of the throughput of transfer orders with the number of shards, for various loads. The in-flight parameter is set to 1,000.

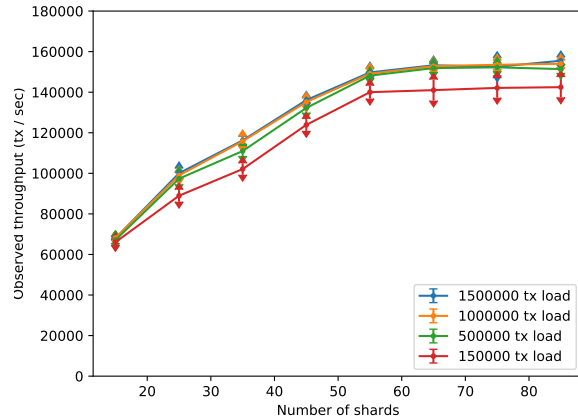


Figure 12: Variation of the throughput of confirmation orders with the number of shards, for various loads. The certificates are issued by 4 authorities, and the in-flight parameter is set to 1,000.

#### A.4 Performance under Byzantine Failures

The FastPay protocol does not rely on any designated leader (like PBFT [15]) to make progress or create proposals; FastPay authorities do not directly communicate with each other, and their actions are symmetric. Clients create certificates by gathering the first  $2f + 1$  responses to a valid transfer order, and no action of a Byzantine authority may delay the creation of a certificate. A Byzantine authority may not even present a signature on a different order as a response to confuse a correct client, since it would have to be signed by the correct payer. Subsequently, a correct client submits the confirmation order to all authorities. Again, Byzantine authorities cannot in any way delay honest authorities from processing the payment locally in their databases, and enabling a subsequent payment for the sending account.

Byzantine clients may attempt denial of service attacks by over-using the system, and for example creating a very large number of receiving accounts (this could be disincentivized by charging some fee for an account creation). However, an attempt to equivocate by sending two transfer orders for a single sequence number could either result in their own account being locked (no single transfer order can achieve  $2f + 1$  signatures to form a certificate and move to the next sequence number), or one of them succeeding—neither of which degrade performance. Transfer orders with insufficient funds or incorrect sequence numbers are simply rejected, which does not significantly affect performance (if anything they do not result in confirmation orders that are more costly to process than transfer orders, see Section 7).

## B CODE LISTINGS FOR CORE OPERATIONS

Algorithms for the core authority operations are simplified directly from the Rust implementation. We omit explicit typing, details of error messages returned, de-referencing, and managing variable ownership. The macro *ensure*, returns with an error unless the condition is fulfilled, and *bail* always returns with an error.

## C ADDITIONAL FIGURES

Figures 11 and 12 show the increase of throughput of transfer and confirmation orders with the number of shards, for various total system loads. They complement Section 7.2 by showing that the throughput is not affected by the system load.