Sui Lutris: A Blockchain Combining Broadcast and Consensus

Sam Blackshear
Mysten Labs

Andrey Chursin
Mysten Labs

George Danezis
Mysten Labs &
University College London

Anastasios Kichidis
Mysten Labs

Lefteris Kokoris-Kogias
Mysten Labs &
IST Austria

Xun Li
Mysten Labs

Mark Logan
Mysten Labs

Ashok Menon
Mysten Labs

Todd Nowacki
Mysten Labs

Alberto Sonnino
Mysten Labs &
University College London

Brandon Williams
Mysten Labs

Lu Zhang
Mysten Labs

Abstract

Sui Lutris is the first production-grade smart-contract platform that leverages consensusless agreement to achieve sub-second finality. Unlike prior work, Sui Lutris integrates seamlessly consensusless agreement with a high-throughput consensus protocol to not compromise expressiveness or throughput and is able to run perpetually without restarts. This feat is especially delicate during reconfiguration events, where the system needs to preserve the safety of the consensusless path without compromising the long-term liveness of potentially misconfigured clients. Sui Lutris combined with the Move programming language enables safe execution of smart-contracts that expose objects as a first-class resource.

1 Introduction

Traditional blockchains totally order transactions across replicated miners or validators to mitigate "double-spending" attacks, i.e., a user trying to use the same coin in two different transactions. It is well known that total ordering requires consensus. In recent years, however, systems based on consistent [4] and reliable [20] broadcasts have been proposed instead. These rely on objects (e.g., a coin) being controlled by a single authorization path (e.g., a single signer or a multi-sig mechanism), responsible for the liveness of transactions. This concept has been used to design asynchronous, and lightweight alternatives to traditional blockchains for decentralized payments [4, 5, 13]. We call these systems *consensus-less* as they do not require full consensus of atomic broadcast channels. Yet, so far they have not been used in a production blockchain.

On the one hand, consensus-based protocols allow for general-purpose smart contracts. But come at the cost of using more complex consensus protocols with higher latency. On the other hand, consensus-less protocols are simpler to implement and have low latency. But typically support a restricted set of operations, and deploying them in a dynamic environment is challenging as they do not readily support state checkpoints and validator reconfiguration. Supporting these functions is vital for the health of a long-lived production system.

We present Sui Lutris, a system that combines the consensus-less and consensus-based approaches to provide the best of both worlds when processing transactions in a replicated Byzantine setting. Sui Lutris uses a consistent broadcast protocol between validators to ensure the safety of common operations on assets owned by a single owner, ensuring lower latency as compared to consensus. It only relies on consensus for the safety of complex smart contracts operating on shared-ownership objects, as well as to support network maintenance operations such as defining checkpoints and reconfiguration. It is maintained by a permissionless set of validators that play the same role as miners in other blockchains.

Sui Lutris has been designed for and adopted as the core system behind the Sui blockchain. As of May 2, 2023, its latest testnet is operated by 97 geo-distributed heterogeneous validators and processes over 251 million certificates a day over 775 epoch changes using the Sui Lutris protocols. It stores over 810 million objects defined by over 86,000 Move packages. For this reason we present in the paper details that go beyond merely illustrating core components.

Challenges. Designing Sui Lutris requires tackling 3 key issues: Firstly, a high-throughput system such as Sui Lutris requires a checkpoint protocol in order to archive parts of its history and reduce the memory footprint and bootstrap cost of new participants. Checkpointing however is not as simple as in classic blockchains since we do not have total ordering guarantees for all transactions. Instead, Sui Lutris proposes an after-the-fact checkpointing protocol that eventually generates a cannonical sequence of transactions and certificates, without delaying execution and transaction finality.

Secondly, consensus-less protocols typically provide low latency at the cost of usability. A misconfigured client (e.g., underestimating the gas fee or crash-recovering) risks deadlocking its account. We consider this an unacceptable compromise for production systems. We develop Sui Lutris such that client bugs only affect the liveness of a single epoch, and provide rigorous proofs to support it.

Finally, the last challenge to solve is the dynamic participation of validators in a permissionless system. The lack of total ordering makes the solution non-trivial as different validators may stop processing transactions at different points compromising the liveness of the system. Additional challenges stem from the non-starvation needs of misconfigured clients coupled with ensuring that final transactions are never reverted across reconfiguration events.

Contributions. This paper makes the following contributions:

- We present Sui Lutris, a smart-contract system that forgoes consensus for single-writer operations and only relies on consensus for multi-writer operations, combining the two modes securely.
- As part of Sui Lutris we propose checkpointing transactions into a sequence after execution for large categories of transactions, reducing the need for agreement and therefore latency.
- As part of Sui Lutris we show how to perform reconfiguration safely and with minimal downtime.

2 Overview

Sui Lutris uses a hybrid approach to processing blockchain transactions: it ensures low latency for single-owner assets (assets that are immutable or owned directly or indirectly by a single address, see below) by forgoing the need for consensus. This has low-latency and allows for significant amounts of parallelism during transaction validation. Finality for such transactions is achieved without any assumption on the network which can be fully asynchronous.

Yet, single-owner assets are not expressive enough to implement all types of smart-contracts – since some transactions must process assets belonging to different parties. For this purpose we couple Sui Lutris with a consensus protocol. This hybrid architecture is both a curse and a blessing: two different processing paths creates the threat for inconsistencies and safety concerns; but, the consensus component allows us to implement checkpointing and reconfiguration, which previous consensus-less systems lack.

In this section we define the problem Sui Lutris addresses, the threat model considered, the security properties maintained, as well as a high-level overview of the core algorithm.

2.1 Threat Model

We assume a message-passing system with a set of n validators per epoch and a computationally bound adversary that controls the network and can statically corrupt up to $f < n/3$ validators within any epoch. We say that validators corrupted by the adversary are *Byzantine* or *faulty* and the rest are *honest* or *correct*. To capture real-world networks we assume asynchronous *eventually reliable* communication links among honest validators. That is, there is no bound on message delays and there is a finite but unknown number of messages that can be lost. Informally, Sui Lutris exposes to all participants a *key-value* object store abstraction that can be used to read and write objects.

Consensus Protocol. Sui Lutris uses a consensus protocol as a black box that takes some valid inputs, and outputs a total ordering. It makes no additional synchrony assumptions, and thus inherits the synchrony assumptions of the underlying consensus protocol. In our implementation we specifically use the Bullshark protocol [18] by default. It is secure in the partially synchronous network model [15], which stipulates that after some unknown global stabilization time all messages are delivered within a bounded delay. It could be configured to run the Tusk protocol [14], making Sui Lutris asynchronous.

2.2 System Model

Objects. Sui Lutris validators replicate the state represented as set of objects. Each object has a type associated with a Move language module that defines operations that are valid state transitions for the type. Each object may be read-only, owned or shared:

- *Read-only objects* cannot be mutated or deleted within an epoch, and can be used in transactions concurrently and by all users. Move packages describing immutable smart contract logic and types, for example, are read-only.
- *Owned objects* have an owner field. The owner can be set to an address representing a public key. In that case, a transaction is authorized to use the object, and mutate it, if it is signed by that address. A transaction is signed by a single address, and therefore can use objects owned by that address. However, a single transaction cannot use objects owned by multiple addresses. The owner of an object (called a child object) can also be another object (called the parent object). In that case the child object may only be used if the root object (the first one in a tree of possibly many parents) is part of the transaction, and the transaction is authorized to use the parent. This facility is used by contracts to construct dynamic collections and other complex data structures.
- *Shared objects* are mutable, and do not have a specific owner. They can instead be included in transactions by anyone and they perform their own authorization logic as part of the smart contract. Such objects, by virtue of having to support multiple writers while ensuring safety and liveness, require a full agreement protocol to be used safely.

Both owned and shared objects are associated with a version number. The tuple $(\mathsf{ObjID}, \mathsf{Version})$ is called an ObjKey and takes a single value, thus it can be seen as the equivalent of a Bitcoin UTXO [24] that should not be equivocated.

Transactions. A transaction is a signed command specifying a number of input objects (read-only, owned or shared), a version number per object, an entry function into a Move smart contract, and a set of parameters. If valid, it consumes the mutable input objects, and constructs a set of output objects at a fresh version – which can be the same objects at a later version or new objects.

2.3 Core Properties

Sui Lutris achieves the standard security properties of blockchain systems relating to validity, safety and liveness:

- **Validity**: State transitions at correct validators are in accordance to the authorization rules relating to objects, as well as the VM logic constraining valid state transitions on objects of defined types. This property is unconditional with respect to the number of correct validators in the network.
- **Safety**: If two transactions t and t' are executed on correct validators, in the same or different epochs, and take as input the same ObjKey, then $t = t'$. This property holds in full asynchrony subject to a maximum threshold of Byzantine nodes in the system.
- **Liveness**: All valid transactions sent by correct clients will eventually be processed up to a final status, and their effects will persist across epoch boundaries. All ObjKey that have not been

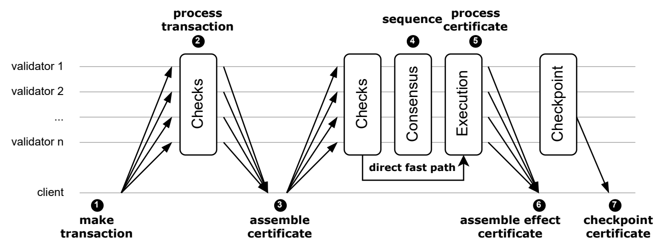

Figure 1: Overview of Sui Lutris and transaction life cycle. The Byzantine agreement protocol is only executed for transactions containing shared objects, and is not necessary for transactions involving only single-owner objects.

used as inputs to a committed transaction will eventually be available to be used by a correct client as part of a valid transaction. This property holds in the partial synchrony model, due to our use of Bullshark [18] consensus (and would hold in asynchrony when using Tusk [14]).

Liveness encompasses censorship resistance. It also only holds for a correct client that may not equivocate by sending conflicting transactions for the same owned object version.

Additionally, Sui Lutris uses a novel data model that explicitly encodes dependency information to allow efficient processing of transactions, meaning that any two transactions touching a causally independent set of input objects can be executed in parallel. For transactions taking as input owned objects Sui Lutris is particularly efficient as they can be executed in two round-trips latency, while for transactions operating on shared objects, Sui Lutris is designed to minimize the critical locking region.

2.4 Core Protocol Overview

We give a high-level overview of Sui Lutris and its transaction life cycle. Section 3 provides extensive pseudocode and detailed description for each action taken by the Sui Lutris validators.

Figure 1 illustrates the high-level interactions between a client and Sui Lutris validators to commit a transaction. A user with a private key creates and signs a *user transaction* to either mutate objects they own (case 1), or a mix of objects they own (at least one is gas) and shared objects (case 2). This is the only time user signature keys are needed; the remaining process may be performed by the user or a gateway on behalf of the user (❶). The transaction is sent to each Sui Lutris validator, which checks it for validity, locks all input owned objects using their ObjKey, signs it and returns the *signed transaction* to the client (❷). Algorithm 1 of Section 3.4 describes in details this step. It is critical to see that since an ObjKey is locked for a specific transaction, no double-spend can happen. As we discuss later, however, there is a chance of liveness loss if the client equivocates. This check is also used to prevent attacking consensus with spam transactions which is easy to do in Bullshark [18] as it orders bytes which could be duplicate transactions.

The client collects the responses from a quorum ($2f + 1$) of validators to form a *transaction certificate* (❸). This design pattern unburdens validators from gossiping signatures and aggregating certificates, which is now the responsibility of the client/gateway. Once the certificate is assembled, it is sent back to all validators, who respond once they check its validity (a quorum of responses at this point ensures *transaction finality*, see below). If the transaction involves exclusively read-only and owned objects the transaction certificate can be processed immediately and executed (illustrated as the *direct fast path* in the diagram).

All certificates are forwarded to a *Byzantine agreement protocol* operated by the Sui Lutris validators (❹). When step (❹) terminates consensus outputs a total order of certificates, and validators check the certificate and execute those containing shared objects. The execution result is a summary of how the transaction affects the state and is used to construct a *signed effects* response (❺). Algorithm 4 of Section 3.4 describes in details this step. Once a quorum of validators has executed the certificate its effects are final (in the sense of *settlement finality*, see below). Clients can collect a quorum of validator responses and create an *effects certificate* and use it as proof of the finality of the transactions effects (❻). Subsequently, checkpoints are formed for every consensus commit (❼), which are also used to drive the reconfiguration protocols (not shown, see Section 5.1 and Section 5.3).

The goal of the above protocol is to ensure that execution for transactions involving read-only and owned objects requires only reliable broadcast and a single certificate to proceed, costing a minimal $O(n)$ communication and computation complexity and no validator to validator communication. Smart contract developers can therefore design their types and their operations to optimize transfers and other operations on objects of a single user to have real-time latency. At the same time, Sui Lutris provides the flexibility of using shared objects as well, through the classic Byzantine agreement path, and enables developers to implement logic that needs to be accessed by multiple users.

Transaction finality. The BIS [25] defines finality as the property of being "irrevocable and unconditional". We make a distinction between transaction finality, after which a transaction processing is final, and settlement finality, after which the effects of a transaction are final and may be used in subsequent transactions in the system. In Sui Lutris, unlike other blockchains, both types of finality occur before checkpoints are formed. In all cases a transaction becomes final when a quorum of validators accept its transaction certificate for processing, even before such a certificate is sequenced by consensus or executed. After this no conflicting transaction can occur, the transaction may not be revoked, and it will be eventually executed and persist across epochs. However, the result of execution is only known a-priori for owned object transaction, and for shared object transactions it is known only after execution. Transaction finality is achieved within two network round trips.

Settlement finality, occurs upon execution on $2f + 1$ validators, when an effects certificate could be formed (even through it is not known by any single party). For owned object transactions this occurs upon $2f + 1$ correct validators executing the certificate without the delay of consensus; for shared object transactions this happens upon $2f + 1$ correct validators executing them just after the certificate has been sequenced. In both cases, settlement finality is not delayed by the process of sealing the transaction within a checkpoint, and thus, has lower latency than checkpoint creation.

3 The Sui Lutris System

We present the Sui Lutris core protocol by providing algorithms and specifying the checks performed by validators at each step.

3.1 Objects Operations

Sui Lutris validators rely on a set of objects to represent the current and historical state of the replicated system. An *Object* (Obj) stores user smart contracts and data within Sui Lutris. Transactions can affect objects which can be Created, Mutated, Wrapped, Unwrapped and Deleted. We discuss wrapping objects in Section 4.

Calling *key*(Obj) returns the *key* (ObjKey) of the object, namely a tuple (ObjID, Version). ObjID is cryptographically derived so that finding collisions is infeasible. Versions monotonically increase with each transaction processing the object, and are determined via Lamport timestamps [22]. Calls to *version*(Obj) and *initial*(Obj) return the current and initial version of the object respectively.

The *owner*(Obj) is either the owner's public key that may use this object, or the ObjID of another *parent* object, in which case this is a *child* object. *owned*(Obj) returns whether the object has an owner, or whether it is read-only or a shared object (see below).

3.2 Protocol Messages

Sui Lutris validators and users run the core protocol described in Section 2.4 by exchanging the following messages.

Transactions. A *transaction* (Tx) is a structure representing a state transition for one or more objects. They support a few self-explanatory access operations, such as to get its digest *digest*(Tx), and different types of input objects *inputs*(Tx) (object reference), *read_only_inputs*(Tx), *shared_inputs*(Tx) (object ID and initial version), and *payment*(Tx) (the reference to the gas object to pay fees).

A Transaction may be checked for validity given a set of input objects, or can be executed to compute output objects:

- *valid*(Tx, [Obj]) returns true if the transaction is valid, given the requested input objects provided. This verifies that the transactions is authorized to act on the input objects, as well as sufficient gas being available to cover the costs of its execution. Transaction validity, as returned by *valid*(Tx, [Obj]) can be determined statically without executing the Move contract.
- *exec*(Tx, $[\text{Obj}_o]$, $[\text{Obj}_s]$) executes using the MoveVM [6] and returns a structure Effects representing its effects along with the output objects $[\text{Obj}_{out}]$. The output objects are the new objects Created, Mutated, Wrapped, Unwrapped and Deleted by the transaction. When objects are created, updated, or unwrapped their version number is the Lamport timestamp of the transaction. $[\text{Obj}_o]$ and $[\text{Obj}_s]$ respectively represent the owned and shared input objects. A valid transaction execution is infallible, and has deterministic output.

A transaction is indexed by the TxDigest over the raw data of the transaction, which may also be used to authenticate its full contents. All valid transactions[1]. have at least one owned input, namely the objects used to pay for gas.

Certificates. A *transaction certificate* (TxCert) on a transaction contains the transaction itself, the signature of the user authorizing the use of the input objects, and the identifiers and signatures from a quorum of $2f + 1$ validators or more. For simplicity we assume that every operation defined over a transaction is also defined over a certificate. For instance, "*digest*(Tx)" is equivalent to "*digest*(TxCert)".

[1]Except the special hard-coded genesis and other system transactions.

A certificate may not be unique, and the same logical certificate may be signed by a different quorum of validators or even have different authorization paths (e.g., a 2-out-of-3 multisig). However, two different valid certificates on the same transaction should be treated as representing semantically the same certificate. The identifiers of signers are included in the certificate to identify validators ready to process the certificate, or that may be used to download past information required to process the certificate. Additionally, the signatures are aggregated (e.g., using BLS [7]), compressing the quorum of signers to a single signature.

Transaction effects. A *transaction effects* (Effects) structure summarizes the outcome of a transaction execution. Its digest and authenticator is computed by *digest*(Effects). It supports operations to access its data such as *transaction*(Effects) (returns the transaction digest) and *dependencies*(Effects) (the digest of all transactions to create input objects). The *contents*(Effects) returns a summary of the execution: Status reports the outcome of the smart contract execution. The lists Created, Mutated, Wrapped, Unwrapped and Deleted, list the object references that underwent the respective operations. Finally, Events lists the events emitted by the execution.

Partial certificate. A *partial certificate* (TxSign) contains the same information, but signatures from a set of validators representing stake lower than the required quorum, usually a single one. We call *signed transaction* a partial certificate signed by a one validator.

Effect certificates. Similarly, an *effects certificate* (EffCert) on an effects structure contains the effects structure itself, and signatures from validators[2] that represent a quorum for the epoch in which the transaction is valid. The same caveats, about non-uniqueness and identity apply as for transaction certificates. A partial effects certificate, usually containing a single validator signature and the effects structure is denoted as EffSign.

3.3 Data Structures

Each validator maintains a set of persistent tables abstracted as key-value maps, with the usual contains, get, and set operations.

Reliable broadcast on owned objects uses the *owned lock map* (OwnedLock[ObjKey] $\rightarrow$ TxSignOption) which records the first valid transaction Tx seen and signed by the validator for an owned object's ObjKey, or None if the ObjKey exists but no valid transaction using it as an input has been seen. The *certificate map* (Ct[TxDigest] $\rightarrow$ (TxCert, EffSign)) records all full certificates TxCert, including Tx, processed by the validator, along with their signed effects EffSign.

To manage the execution of shared object transactions, the *shared lock map* (SharedLock[(TxDigest, ObjID)] $\rightarrow$ Version) records the version number of ObjID assigned to a transaction TxDigest. The *next shared lock map* (NextSharedLock[ObjID] $\rightarrow$ Version) records the next available version (we discuss their use in Section 3.4).

The *object map* (ObjDB[ObjKey] $\rightarrow$ Obj) records all objects Obj created by executed certificates within Ct by object key, and also allows lookups for the latest known object version. This store can

[2]Note that if the signature algorithm permits it, validator signatures can be compressed, but always using signature aggregation because tracking who signed is important for gas profit distribution and other network health measurements.

be completely derived by re-executing all certificates in Ct. Only the latest version is necessary to process new transactions, and older versions are only maintained to facilitate parallel execution, reconfiguration, reads and audits.

Only the lock maps (OwnedLock, SharedLock, NextSharedLock) require strong key self-consistency, namely a read on a key should always return whether a value or None is present for a key that exists, and such a check should be atomic with an update that sets a lock to a non-None value. This is a weaker property than strong consistency across keys and allows for efficient sharding of the store for scaling. To ensure this property, they are only updated by a single task (see Section 3.4). The other stores may be eventually consistent without affecting safety. Section 5.2 shows how to initialize and securely reset stores upon epoch changes.

3.4 Validator Core Operation

Sui Lutris validators process transactions and certificates as described in Section 2.4. Transactions are submitted to the validator core for processing by users, while certificates can either be submitted by users or by the consensus engine.

Process Transaction. Algorithm 1 shows how Sui Lutris processes transactions; that is, step ❷ of Figure 1 (see Section 2.4). The function LoadObjects (Line 3) simply loads the specified object(s) from the ObjDB store; LoadLatestVersionObjects (Line 4) loads the the latest version of the specified object(s) from the ObjDB store; and AcquireLocks (Line 14) acquires a mutex for every owned-object transaction input. Upon receiving a transaction Tx a validator calls ProcessTx to perform a number of checks:

(1) It ensures all object references *inputs*(Tx) and the gas object reference in *payment*(Tx) exist in the ObjDB store and loads them into [Obj]. For owned objects both the ID and version should be available; for read-only or shared objects the object ID should exist, and for shared objects, the initial version specified in the input must match the initial version of the shared object returned by *initial*(·). This check implicitly ensures that all owned objects have the expected version number specified in the transaction since the call to LoadObjects (Line 3) loads the pair ObjKey = (ObjID, Version) from the ObjDB store; the ObjDB store holds a single entry (the latest version) per object.
(2) It checks *valid*(Tx, [Obj]) is true. This step ensures the authentication information in the transaction allows access to the owned objects. That is, (i) the signer of the transaction must be the owner of all the input objects owned by an address input; (ii) the parent object of any included child object owned by another object should be an input to the transaction; and (iii) sufficient gas can be made available in the gas object to cover the minimum cost of executing the transaction.
(3) It ensures it can acquire a lock for every owned-object transaction input; otherwise, it returns an error. Acquiring a lock ensures that no other task can concurrently perform the next step of the algorithm on the same input objects.
(4) It checks that OwnedLock[ObjKey] for all owned *inputs*(Tx) objects exist, and it is either None or set to *the same* Tx, and atomically sets it to TxSign. In other words, for each owned input version in the transactions: (i) a key for this object *exists* in OwnedLock and (ii) no other transaction Tx′ ≠ Tx has been assigned as a value for this object version in OwnedLock, i.e. Tx is the first valid transaction seen using this input object. This is a key validity check to implement *Byzantine consistent broadcast* [8] and ensure safety.

Algorithm 1 Process transaction

```
    // Executed upon receiving a transaction from a user.
    // Many tasks can call this function.
 1: procedure ProcessTx(Tx)
 2:     // Check 1.1: Ensure all objects exist.
 3:     [$Obj_o$] = LoadObjects(inputs(Tx))
 4:     [$Obj_r$] = LoadLatestVersionObjects(read_only_inputs(Tx))
 5:     for (ObjID, InitialVersion) ∈ shared_inputs(Tx) do
 6:         $Obj_s$ = LoadLatestVersionObjects(ObjID)
 7:         if initial($Obj_s$) ≠ InitialVersion then
 8:             return Error
 9:
10:     // Check 1.2: Check the transaction's validity (see Section 3.2).
11:     if !valid(Tx, [$Obj_o$]) then return Error
12:
13:     // Check 1.3: Try to acquire a mutex over inputs(Tx)
14:     guard = AcquireLocks(Tx)        ▷ Error if cannot acquire all locks
15:
16:     // Check 1.4: Lock all owned-objects.
17:     TxSign = sign(Tx)
18:     for ObjKey ∈ inputs(Tx) do
19:         if OwnedLock[ObjKey] == None then
20:             OwnedLock[ObjKey] = TxSign
21:         else if OwnedLock[ObjKey] ≠ TxSign then
22:             return Error
23:
24:     return TxSign
```

Transaction processing ends if any of the checks fail and an error is returned. If all checks are successful then the validator returns a signature on the transaction, i.e., a partial certificate TxSign. Processing a transaction is idempotent upon success, and always returns a partial certificate (TxSign) within the same epoch. Any party may collate a transaction and signatures (TxSign) from a set of validators forming a quorum for epoch e, to form a transaction certificate TxCert. It is critical that this step happens for all transactions as it acts as a spam protection for order-execute consensus engines. In the original Bullshark [18] work it is trivial to drop the throughput to zero by a single malicious client sending corrupted transactions or duplicates. Sui Lutris prevents such attacks thanks to the stronger coupling with the state that allows only transactions with gas to make it to consensus.

Many tasks can call ProcessTx concurrently (or in parallel). Sui Lutris only acquires mutexes on the minimum amount of data: the owned-objects transaction inputs (Algorithm 1 Line 14).

Process user certificates. Algorithm 4 shows how Sui Lutris processes certificates; that is, step ❺ of Figure 1 (see Section 2.4). Algorithms 2 and 3 provide non-trivial support functions. Every certificate input to a function of Algorithm 4 is first checked to ensure it is signed by $2f + 1$ validators. Upon receiving a certificate TxCert a validator calls ProcessCert to perform a number of checks:

Algorithm 2 Storage support (generic)

```
    // Check whether the certificate as already been executed.
1:  procedure AlreadyExecuted(TxCert)
2:      TxDigest = $digest$(TxCert)
3:      (_, EffSign) = Ct[TxDigest]
4:      if EffSign then return EffSign
        return None

    // All operations inside this function are atomic.
    // Note that all owned and shared objects have the same version $v$.
5:  procedure AtomicPersist(TxCert, EffSign, [$Obj_{out}$])
6:      TxDigest = $digest$(TxCert)
7:      Ct[TxDigest] = (TxCert, EffSign)
8:      for Obj $\in$ $Obj_{out}$ do
9:          ObjKey = $key$(Obj)
10:         ObjDB[ObjKey] = Obj
11:         if $owned$(Obj) then
12:             OwnedLock[ObjKey] = None
```

Algorithm 3 Storage support (shared objects)

```
    // Assign locks to the shared objects referenced by TxCert.
1:  procedure WriteSharedLocks(TxCert, $v$)
2:      TxDigest = $digest$(TxCert)
3:      for (ObjID, InitialVersion) $\in$ $shared\_inputs$(TxCert) do
4:          Version = NextSharedLock[ObjID] || InitialVersion
5:          SharedLock[(TxDigest, ObjID)] = Version
6:          NextSharedLock[ObjID] = $v + 1$            ▷ Lamport timestamp

    // Check whether all shared objects referenced by TxCertare locked.
7:  procedure SharedLocksExist(TxCert)
8:      TxDigest = $digest$(TxCert)
9:      for ObjID $\in$ $shared\_inputs$(TxCert) do
10:         if !SharedLock[(TxDigest, ObjID)] then
11:             return false                            ▷ lock not found
12:     return true

    // Ensure that TxCert is the next certificate scheduled for execution.
13: procedure CheckSharedLocks(TxCert)
14:     TxDigest = $digest$(TxCert)
15:     for ObjID $\in$ $shared\_inputs$(TxCert) do
16:         Obj = ObjDB[ObjID]
17:         Version = $version$(Obj)
18:         if SharedLock[(TxDigest, ObjID)] $\neq$ Version then
19:             return false
20:     return true
```

Algorithm 4 Process certificate

```
Require: Input certificate (TxCert) is signed by a quorum

    // Executed upon receiving a certificate from a user.
    // Many tasks can call this function.
1:  procedure ProcessCert(TxCert)
2:      // Check 4.1: Ensure the TxCert is for the current epoch Epoch.
3:      if $epoch$(TxCert) $\neq$ Epoch then return Error
4:
5:      // Check 4.2: Load objects from store, return error if missing object.
6:      [$Obj_o$] = LoadObjects($inputs$(TxCert))
7:      [$Obj_s$] = LoadObjects($shared\_inputs$(TxCert))
8:
9:      // Check 4.3: Check the objects locks.
10:     if !SharedLocksExist(TxCert) then
11:         ForwardToConsensus(TxCert)     ▷ Sequence the certificates
12:         return
13:     if !CheckSharedLocks(TxCert) then return Error
14:
15:     // Execute the certificate.
16:     (EffSign, [$Obj_{out}$]) = $exec$(TxCert, [$Obj_o$], [$Obj_s$])
17:     AtomicPersist(TxCert, EffSign, [$Obj_{out}$])
18:     return EffSign

    // Executed upon receiving a certificate from consensus.
    // This function must be called by a single task.
19: procedure AssignSharedLocks(TxCert)
20:     // Ensure shared locks are assigned only once.
21:     if SharedLocksExist(TxCert) then
22:         return
23:
24:     // Extract the highest objects version.
25:     $v_o = 1$
26:     for (ObjID, Version) $\in$ $inputs$(TxCert) do
27:         $v_o = \max(v_o, \text{Version})$
28:     $v_s = 1$
29:     for (ObjID, InitialVersion) $\in$ $shared\_inputs$(TxCert) do
30:         Version = NextSharedLock[ObjID] || InitialVersion
31:         $v_s = \max(v_s, \text{Version})$
32:     $v_{max} = \max(v_o, v_s)$                  ▷ Lamport timestamp
33:
34:     // Lock all shared objects to $v_{max}$.
35:     WriteSharedLocks(TxCert, $v_{max}$)
```

(1) It ensures $epoch$(TxCert) is the current epoch. This is a property of the quorum of signatures forming the certificate.
(2) It loads the owned objects (Line 6) and shared objects (Line 7). Success in loading these objects ensures the validator already processed all past certificates concerning the loaded objects. If any object is missing, the validator aborts and returns an error. When loading shared objects, the function LoadObjects returns the shared object with the highest version number.
(3) If the certificate contains shared objects, it ensures the certificate has already been sequenced by the consensus engine; otherwise, it forwards the certificate to consensus (Line 11). Finally, it checks the shared locks to ensure the current certificate TxCert is the next certificate scheduled for execution.

If all checks succeed, the transaction can be executed. The validator then atomically persists the execution results to storage (function AtomicPersist of Algorithm 2). It inserts the new (or mutated) objects in the ObjDB store and sets the version number of all owned and shared objects to the highest version number amongst all objects in the transaction plus 1 (Lamport timestamp); that is, the new version is $v = 1 + \max_{o \in [Obj_o] \cup [Obj_s]} version(o)$. The validator also persists the certificate along with the effects resulting from its execution; and updates the owned-object lock store to unblock future transactions using these objects. If transaction execution fails, Sui Lutris unlocks any owned objects used as input of the transaction. That is, it sets OwnedLock[ObjKey] = None, $\forall$ObjKey $\in$ $inputs$(Tx). Unlocking owned objects is essential to allow future transactions to re-use them. Gas payment is deduced from the payment objects whether the execution succeeds or fails.

Process consensus certificates. Upon receiving a certificate output from consensus, the validator calls AssignSharedLocks (Algorithm 4) to lock the transaction's shared-objects to a version number. This can be done without executing the transactions, only by inspecting and updating the transaction as well as the SharedLock and NextSharedLock tables. When an entry for a shared object does not exist in the tables it is assigned the initial version number given in the transaction input[3]. Otherwise, it is given the value in the NextSharedLock table. The NextSharedLock is updated with the Lamport timestamp [22] of the transaction: the highest version of all input objects used (owned, read-only, and shared) plus one. AssignSharedLocks must be only called by a single task. After successfully calling AssignSharedLocks, the validator can call (again) ProcessCert to execute the certificate.

Shared objects may be included in a transaction explicitly only for reads (we omit this special case from the algorithms for clarity). In that case the transaction is assigned in SharedLock the version in the NextSharedLock table for the shared object. However, the version of the object in NextSharedLock is not increased, and upon transaction execution the shared object is not mutated. In order to preserve safety of dynamic accesses we make sure that within a Bullshark commit (level of concurrency) all read-only transactions on shared objects are executed on the initial version V and only after writes are allowed to execute and mutate the object. This facility allows multiple transactions executing in parallel to use the same shared object for reads. For example, it is used to update a clock object with the current system time upon each commit that transactions may read concurrently.

Additional checks. Algorithms 1 and 4 only describe the core validator operations. In practice, validators perform a number of extra checks to early reject duplicate messages. For instance, validators can easily check whether a certificate has already been executed by calling AlreadyExecuted (Algorithm 2). Such check is useful to improve performance and prevent obvious DoS attacks but is not strictly needed for security (it does not guarantee idempotent validators replies on its own since both ProcessTx and ProcessCert can be called concurrently by multiple tasks).

Protecting Users from Bugs. Equivocation of an ObjKey is considered malicious in prior work and permanently locks the Obj forever. However, equivocation is often the result of a misconfigured wallet due to poor synchronization between gateways or poor gas predictions leading to re-submissions. As we discuss in Section 5.2 in Sui Lutris we only lose liveness until the end of the epoch (at most 24 hours). In the new epoch the user can try again to access the same ObjKey with a fresh, hopefully correct, transaction.

4 Programming with Objects

Although objects give the developers a way to expose dependencies and parallelism, we need to develop a few object-oriented processes to make it work seamlessly with low programming overhead.

[3]At the beginning of a new epoch, the most recent version from the objects table is used to support bootstrapping validators

Sui Lutris relies on the correct implementation of the MoveVM [6] and its semantics to guarantee a number of properties:

- The type checker ensures an object may only be wrapped into another object if the wrapped object is an input of the transaction, or itself indirectly a child of an input object in the transaction.
- The type checker ensures that an input object may only become a child of another object if the new parent object is an input of the transaction, or indirectly a child of an input to the transaction.

These checks ensure that wrapped and child objects will always have a version number that is not larger than the object that wraps them, the top-level object that wraps their parent, or their parent if it is already top-level. In turn, this ensures that when unwrapped or a child object becomes a top-level object again the Lamport timestamp corresponding to its new version number will be greater than any version number it was assigned before. Lamport timestamps [22] allow Sui Lutris to efficiently delete and re-create objects without opening itself to replay attacks through version number re-use. In a nutshell, re-created objects always have a higher version number.

Object Wrapping/Unwrapping. Sui Lutris allows an executed transaction to *wrap* an input object into another object that is output. The wrapped object then 'disappears' from the system tables as it is in-lined within the data of the object that wraps it. The Move type system that bounds all executions ensures that the type of a wrapped object does not change; and that it is not cloned with the same object ID. Eventually, the wrapped object can be *unwrapped* by a transaction taking the object that wraps it as an input. Once unwrapped the object is again included and tracked in the system tables under a version that is the Lamport timestamp of the transaction that unwrapped it. This ensures that the version is greater than any previous version, preventing replay attacks on the consistent broadcast protocol.

Parent-child object relations. An owned object (called a *child*) may be owned by another object (called the *parent*). Parent object may be shared objects or owned objects, and the latter may themselves be children of other parents, forming a chain of parent-child relations. A transaction is authorized to use a child object if the ultimate parent, ie. the object in the parent-child chain that is either shared or owned by an address, is included in the transaction as an input. Assigning an owned object to a parent requires both the child and the parent to be included or authorized in the inputs of the transaction that performs the assignment. This ensures that all operations on a child (including assignment) result in the full chain of parent–child relationships being updated as part of the transaction output, and assigned the Lamport timestamp of the transaction.

Notably, children may be used as inputs to transactions implicitly without specifying them in the transactions inputs. A Move call may load a child object by object ID, and the owned objects table (which is consistent) is used to determine the correct version of the loaded child object to use. Since the transaction executing has a lock on the parent it also has implicitly a lock on all direct or indirect children removing any ambiguity about the correct version to use. The full chain of a dynamically loaded child is treated as if it was an input to the transaction and version numbers of all objects on the chain updated in the output. This ensures that when the child object is assigned to an address (stops being a child) it will always have a fresh version.

Objects Deletion. Any type of Sui Lutris object (read-only, owned, or shared) can be either created by a transaction containing only owned objects or by a transaction containing a mix of owned and shared objects. As a result, owned objects can be created by transactions sequenced by the consensus engine, and shared objects can be created by transactions forgoing consensus. This creates a challenge when deleting shared objects that are created without consensus, as the creation transaction might be replayed causing a double-spend. To resolve this issue we rely on remembering deleted objects through tombstones. We achieve this by marking deleted objects with the version number zero upon successfull execution of the certificate (i.e., when calling *exec*(TxCert) in Algorithm 4). Remember the second transactions validity check of Section 3.4 prevents transactions from using objects with version zero as inputs. Thus setting the version of an object to zero is effectively a tombstone. Since this could create infinite memory needs we also rely on the fact that certificates are valid only while the epoch is ongoing and clear all tombstones upon epoch change.

5 Long-Term Stability

Beyond Sui Lutris's basic protocols, this section outlines protocols required to ensure its long-term stability, namely to produce checkpoints and enable reconfiguration.

Unlike prior blockchains, Sui Lutris executes before creating blocks, to minimize latency. However, it makes it more complex for external parties to obtain proofs of transaction execution, perform complete audits, or even systematically replicate the state of the chain. To facilitate these functions, we introduce checkpoints.

Further, to tolerate mistakes we need to safely unlock objects that were mistakenly locked through client double spending bugs. The validator set, and validator voting power, also need to evolve over time, to support permissionless delegated proof of stake. These functions are supported in the epoch-change and reconfiguration process. It persists all final transactions and their effects across epochs; enables client to unlock objects involved in partial locked transactions; and is a secure means for validators to enter or exit the system without affecting its liveness and performance. The period between reconfiguration is a rare time of perfect synchrony and consistency across all validators, when software upgrades can be performed and global incentives and rewards can be distributed.

5.1 Checkpoints

Sui Lutris validators emit a sequence of certified *checkpoints* each containing an agreed-upon sequence of transactions, the authorization path of the transactions, and a commitment to their effects. These form a hash-chain, which is the closest Sui Lutris has to the blocks of a traditional blockchain. Checkpoints are used for multiple purposes: they are gossiped from validators to full nodes to update them about the state of the chain; they are used by validators to perform synchronization in case they fall behind in execution; as well as to bring new validators up to speed with the state at the start of each epoch. Checkpoints, packaged along with the transactions and effects structures they contain are also the canonical historical record of execution used for audit.

Checkpoints are created asynchronously and/or in parallel with execution and attaining finality. However, a key safety property holds due to our reconfiguration protocol design. Namely, if a transaction is final within an epoch then it will be present in a checkpoint within the epoch, and will persist across epochs. And conversely, if a transaction is present within an epoch its effects are final. The checkpoint creation process guarantees these invariants.

Checkpoint creation. Upon receiving a valid certificate a correct validator records it and commits to including it in a checkpoint before the end of the epoch. A validator schedules all certificates for sequencing using the consensus engine. For owned transactions this does not block execution, which can continue before the transaction is sequenced; in the case of shared object transactions execution resumes once the transaction certificate has been sequenced and the shared object locks are determined (see Section 2.4). A correct validator will not proceed to end an epoch before all valid certificates it received are sequenced into checkpoints (either as a result of itself or others inserting them into the consensus engine).

Periodically, using a deterministic rule, validators pick a consensus commit to use as a checkpoint (our current implementation checkpoints each and every commit separately). The new checkpoint contains all transactions present in the commits since the last checkpoint and any additional transaction required for the execution to be causally complete. If a transaction's certificate exists more than once, the first occurrence is taken as the canonical one and the accompanied user signature is included in the checkpoint for audit purposes. Note that due to asynchrony and failures, the certificates sequenced may not be in causal order, or may contain 'gaps', i.e., missing transactions dependencies. Checkpoint creation waits for all transactions necessary for the checkpoint to be causally complete to be within a commit, sorts them in a canonical topological order, and includes them in the checkpoint.

Each correct validator uses the same sequence of commits to form the checkpoint, and therefore will yield and sign the same checkpoint. The checkpoint header and validator signature of each validator can then be sequenced and the first $2f + 1$ form the canonical certificate for the new checkpoint. Note that due to the need to fill causal gaps in execution using subsequent commits, a checkpoint for a commit may only be constructed after a future commit.

Properties and uses. Eventually, the complete set of transactions will be sent to be checkpointed, and the entire causal history will be in the checkpoint history. Informally, since a final transaction is executed by $2f + 1$ nodes, $f + 1$ correct nodes will try to sequence it until they succeed. As we discuss in the next section $2f + 1$ validators need to consent to close the epoch and by quorum intersection at least one of them will delay until a transaction that is final is in the checkpoint. Causally preceding transactions must have been executed and be final, thus they will eventually be sequenced leading to a complete causal history being checkpointed. All these processes may happen eventually without blocking earlier transaction or settlement finality.

Checkpoints are used as part of reconfiguration, but are also used as a simpler synchronization mechanism between validators, as well as full nodes. Since correct validators eventually include all certificates into consensus, this ensures that all correct validators will eventually see and execute all transactions without the need for complex state synchronization protocols. Full nodes, in turn, may download the sequence of checkpoints to ensure they have a complete replica of the state of the system. In peer-to-peer synchronization full nodes can use the sequence number of the checkpoint as a reference when requesting blocks of information from other peers in sequence or in parallel.

5.2 Committee Reconfiguration

Reconfiguration occurs between epochs when the current committee is replaced by a new committee. Other changes requiring global coordination, such as software updates and parameter updates, also take effect between epochs. Immutable objects, such as system parameters or software packages, may be mutated in that period.

The goal of the reconfiguration protocol is to preserve safety of transactions between epochs, while allowing for liveness recovery of equivocated transactions. To this end, we require that if a transaction Tx was committed during epoch e or before, no conflicting transaction can be committed after epoch e. This is trivial to ensure when running only a consensus protocol since a reconfiguration event logged on-chain clearly separates transactions committed in epoch e from transactions committed in epoch $e + 1$. However, in Sui Lutris solutions are not as straightforward. More specifically, Sui Lutris requires a final transaction at epoch e to have its effects reflected in all subsequent epochs.

The main challenge for Sui Lutris reconfiguration at each validator is the race between committing transactions and constructing checkpoints, that are running potentially asynchronously to each other. If a checkpoint snapshots the end-state of epoch e at time T and is only committed at time $T + 1$, we cannot set that checkpoint as the initial state of epoch $e + 1$. If we did, all transactions happening during the last timestamp are at risk of being unsafe when validators drop their OwnedLock to allow for liveness recovery of equivocated transactions. This is not an issue for the consensus path of Sui Lutris since we can define as end state the checkpoint at time T plus all transactions ordered before it is committed at $T + 1$. That end state is well-defined thanks to the total ordering property of consensus. Unfortunately, it is not easy to establish a set of committed transactions on the consensus-less path.

Remember that the consensus-less path works in two phases, first a transaction locks the single-owner object and produces a certificate. Then this certificate is sent as proof to the validators who reply with a signed-effects certificate (execution). The safety risk during a reconfiguration is that a transaction is executed during the transition phase without the checkpoint recording it. However, Sui Lutris splits reconfiguration into multiple steps instead of doing it atomically. As part of the last step, we pause the consensus-less path. This allows us to show that if a transaction had executed before the reconfiguration message then there is no safety risk because we can guarantee that at least one honest party will persist the execution in the state. We enforce this by introducing an *End-of-Epoch* message that the committee members of the current epoch send when they have seen all the certificates they executed in the consensus output sequence. The new committee takes over completely only after $2f + 1$ such End-of-Epoch messages are ordered. As a result, Sui Lutris manages to preserve safety without needing to block for long periods.

Algorithm 5 Reconfiguration Contract

```
    // Smart contract state
    T                                  ▷ Minimum stake to become a validator
    S                   ▷ Last sequence number before starting epoch change
    total_old_stake = GenesisStake         ▷ Total stake of the old committee
    total_new_stake = 0                    ▷ Total stake of the new committee
    old_keys = GenesisKeys      ▷ Identifiers of the old committee members
    new_keys = {}               ▷ Identifiers of the new committee members
    epoch_edge = 0        ▷ Sequence number of the last epoch's checkpoint
    state = Register                     ▷ Current state of the smart contract
    stake = 0                   ▷ Variable counting the accumulated stake

    // Step 1: Users register to become the next validators.
 1: function Register(sender)
 2:     if state ≠ Register then return
 3:     if sender.stake ≥ T then
 4:         new_keys = new_keys ∪ sender
 5:         total_new_stake += sender.stake

    // Step 2: New validators signal they are ready to take over.
 6: function Ready(sender)
 7:     seq = GetLatestCheckpointSeq()
 8:     if state = Register and seq ≥ S then
 9:         state = Ready
10:     if state ≠ Ready then return
11:     if sender ∈ new_keys then
12:         stake += sender.stake
13:     if stake ≥ 2 * total_new_stake/3 + 1 then
14:         state = End-of-Epoch
15:         stake = 0
16:         PauseTxLocking          ▷ Old validators stop signing messages

    // Step 3: Old validators signal the epoch can safely finish.
17: function End-of-Epoch(sender)
18:     if state ≠ End-of-Epoch then return
19:     if sender ∈ old_keys then
20:         stake += sender.stake
21:     if stake ≥ 2 * total_old_stake/3 + 1 then
22:         state = Handover
23:         stake = 0
24:         epoch_edge = GetLatestCheckpointSeq()

    // Step 4: The new validators take over.
25: function Handover(sender)
26:     if state ≠ Handover then return
27:     seq = GetLatestCheckpointSeq()
28:     if seq ≥ epoch_edge + 1 then
29:         old_keys = new_keys
30:         total_old_stake = total_new_stake
31:         state = Register
32:         new_keys = {}, total_old_stake = 0, epoch_edge = 0
33:         Shutdown                    ▷ Old validators can shutdown
```

5.3 The Sui Lutris Reconfiguration Protocol

The Sui Lutris reconfiguration logic is coded as the smart contract shown in Algorithm 5. Once a quorum of stake for epoch e votes to end the epoch, authorities exchange information to commit to a checkpoint, determine the next committee, and change the epoch. More specifically, reconfiguration happens in four steps, (i) *stake recalculation*, (ii) *ready new committee*, (iii) *End-of-Epoch*, and (iv) *Handover*. Each step is handled by the interaction of the new and old committee members with the smart contract functions. This is key for the correctness of the protocol.

The smart contract is parametrized with (i) the total number of checkpoints before initiating the epoch change protocol S and (ii) the minimum amount of stake T required to become a validator. The function GetLatestCheckpointSeq (Line 24) simply loads the latest checkpoint sequence number known by the validator.

Step 1: Registration of new validators. Users wishing to become validators in the next epoch submit a transaction to the reconfiguration contract calling the Register function. This function establishes the static stake distribution for the next epoch.[4] The smart contract accepts registrations until the S$^{\text{th}}$ checkpoint is created.

Step 2: Ready new committee. Before taking over committee operations, future validators run a full node to download the required state to become a validator. At the bare minimum, they ensure their following stores are up-to-date: NextSharedLock, Ct, and ObjDB (see Section 3.3). Once a validator for the new epoch is ready to start validating they call the Ready function to signal they have successfully synchronized the required state. This function can only be called towards the end of the epoch, after the creation of S checkpoints (Line 8). The cutoff period for the epoch is when a quorum of new validators is ready. At this point, the old committee stops locking objects (Line 16), i.e., executing Algorithm 1.

Step 3: End of Epoch. When the new committee is ready the old committee only runs consensus and their only job is to make sure all the transactions they executed are sequenced by the consensus engines (so that they are part of the next checkpoint). To this end, they stop accepting certificates from clients and instead make sure that all the certificates they have executed are sequenced by the consensus engine. They then call the End-of-Epoch function. This means that any transactions submitted by clients for this epoch are discarded with an end-of-epoch message and need to be resent with an updated epoch number.

Step 4: Handover. After $2f + 1$ old validators call the End-of-Epoch function, the system enters the handover phase. After an extra checkpoint (Line 28) anyone can call the function Handover that effectively terminates the epoch. At this stage, the state of the smart contract is reset and the old validators can shut down (Line 33). If a validator also participates in the new epoch, it must perform the following operations before entering the next epoch:

- It drops the OwnedLock and SharedLock stores (see Section 3.3).
- It rolls-back execution of any transaction that did not appear in any checkpoint so far. As we discussed this is safe as these transaction were not final.

[4]As this part is contained within one epoch the only risk is that some validators are censored. Fortunately, Bullshark [18] (the consensus protocol used by Sui Lutris) provides sufficient chain quality to allow honest validators to lock their stake.

The protocol design decouples all the essential steps needed for a secure reconfiguration. This decoupling allows for the necessary logic of defining the new committee, providing the new committee sufficient time to bootstrap from the actual hand-over, and preserving the safety of consensusless transactions across epochs. As a result service interruption is minimized.

6 Security Proofs of Sui Lutris

Sui Lutris satisfies validity, safety, and liveness as informally described in Section 2.3. These properties hold against any polynomial-time constrained adversary and for every epoch (and across epochs) as long as the following assumptions hold:

- **BFT:** Every quorum of $3f + 1$ validators contains at most f Byzantine validators. Correct validators of previous epochs never leak their signing keys (this assumption can be relaxed using techniques like Winkle [2]).
- **Network:** The network is partially synchronous [15]. Sui Lutris operates in the partial synchrony model only due to our use of Bullshark [18] as consensus protocol (it would operate in asynchrony if we used Tusk [14] instead).

Under these assumptions, Section 6.1 shows that the state of correct validators is only produced by executing valid transactions; Section 6.2 shows that at the starting of every epoch all correct validators have the same state; and Section 6.3 shows that the state eventually progresses and new correct transactions can be processed. When referring to a 'valid' transaction in the sections below, we mean a transaction that successfully passes check (1.2) defined of Algorithm 1 (Section 2.4).

6.1 Validity

We show that correct Sui Lutris validators only execute valid transactions. Validity holds unconditionally of the network assumption. The protocol described in Section 2.4 ensures validity as long as the BFT assumption holds. However our implementation ensures validity unconditionally because correct validators re-run all checks of Algorithm 1 upon processing a certificate. Should the BFT assumption break, they would thus early-reject certificates over invalid transactions before even starting to process it.

Lemma 6.1 (Valid Certificates). *All certified transactions are valid with respect to the authorization rules relating to owned objects (defined in Section 2.2).*

Proof. Certificates are signed by at least $2f + 1$ validators, out of which at least $f + 1$ are correct. Correct validators only sign a transaction after performing check (2) of Algorithm 1 (ensuring that the transaction is valid with respect to the authorization rules relating to owned objects). As a result, no invalid transaction will ever be signed by a correct validator, and will thus never be certified. □

Theorem 6.2 (Sui Lutris Validity). *State transitions at correct validators are in accordance with (i) the authorization rules relating to owned objects (defined in Section 2.2), and (ii) the Move smart contract logic constraining valid state transitions on object of defined types.*

Proof. State transitions at correct validators only happen if a valid certificate TxCert in Algorithm 4 exists and is processed. Point (i) is thus directly proven by the application of Lemma 6.1, and based on the fact that ownership checks are part of the preconditions for correct validators to sign a transaction. Point (ii) is proven by noting that correct validators only apply a state transition (Line 17 of Algorithm 4) after calling *exec*(TxCert) at Line 16 of Algorithm 4. This function only produces $[\mathsf{Obj}_{out}]$ by calling the Move smart contract logic constraining valid state transitions on object of defined types. □

6.2 Safety

We prove the safety of the Sui Lutris protocol. That is, we show that at the start of every epoch, all correct validators have the same state. We prove safety using three main ingredients: (i) correct validators execute the same set of transactions, (ii) correct validators execute those transactions in the same order whenever (partial) order matters, and (iii) the execution of those transactions causes the same state transition across all correct validators.

Execution set. We start by showing that all correct validators eventually execute the same set of transactions.

Lemma 6.3 (Owned-Object Execution Set). *No correct validators have executed a different set of owned object transactions by the end of epoch e.*

Proof. Correct validators assemble checkpoints through observing the sequence of transaction certificates committed in consensus (Section 5.3). By the agreement properties of the consensus protocol, all correct validators obtain the same sequence of certificates. They then use those ordered certificates to construct the same checkpoints since creating checkpoints is a deterministic process given the certificate sequence input. Correct validators execute all transactions within the checkpoints they assemble. Additionally, at the end of every epoch validators revert the execution of any owned-object transaction not included in a checkpoint (see Section 5.1), hence only owned-object transactions included in a checkpoint persist. Reverting these transactions is safe as only transactions included in a checkpoint are final (see Theorem 6.14). □

Lemma 6.4 (Shared-Object Execution Set). *No correct validators have executed a different set of shared object transactions by the end of epoch e.*

Proof. Correct validators execute all shared object transactions sequenced by the consensus protocol before the last checkpoint of epoch e (see Section 5.2). By the agreement property of the consensus protocol, all correct validators obtain the same sequence and thus execute the same set of shared-object transactions. □

Execution order. We now show that correct validators execute conflicting transactions in the same order.

Lemma 6.5 (BCB Consistency). *No two conflicting transactions, namely transactions sharing the same owned inputs objects, object version, and epoch, are certified.*

Proof. The proof of this lemma directly follows from the consistency property of Byzantine consistent broadcast (BCB) over the label $(e, \mathsf{ObjID}, \mathsf{Version})$. Let's assume two conflicting transactions Tx_A and Tx_B taking as input the same owned object Obj with version Version are certified during the same epoch e. Then $f + 1$ correct validators performed check (1.4) of Algorithm 1 and produced TxSign_A and $f + 1$ correct validators did the same and produced TxSign_B. A correct validator performing check (1.4) cannot successfully process both (conflicting) Tx_A and Tx_B; indeed it will return an error at Line 21. As a result, a set of $f + 1$ correct validators produced TxSign_A but not TxSign_B, and a distinct set of $f + 1$ correct validators produced TxSign_B but not TxSign_A. Hence there should be $f + 1 + f + 1 = 2f + 2$ correct validators additionally to the f byzantine. However $N = 3f + 1 < 3f + 2$ hence a contradiction. □

Lemma 6.5 operates over the label $(e, \mathsf{ObjID}, \mathsf{Version})$ rather than only $(\mathsf{ObjID}, \mathsf{Version})$ because of check (1.4) of Algorithm 1. This check relies on the integrity of the store OwnedLock, that is dropped upon epoch change (Section 5.3). This is however not a problem because certificates carry their epoch number and are only valid for a single epoch (see check (4.1) of Algorithm 4).

Lemma 6.6 (Shared-Locks Consistency). *The shared lock store SharedLock of correct validators are never conflicting; that is, the shared lock store of correct validators are either identical or a subset of each other.*

Proof. Let's assume two correct validators update their store SharedLock by assigning different version numbers to a shared object Obj of a certificate TxCert. Correct validators only assign a version number to Obj after sequencing TxCert through consensus (Section 3.4). They then call AssignSharedLocks (Algorithm 4) and Line 35 of Algorithm 4 assigns a version number to Obj. The function AssignSharedLocks is deterministic and thus the version number assigned to Obj depends only on the consensus output sequence. As a result, two correct validators assign a different version to Obj only if they receive a different consensus output sequence. However, by the agreement property of the consensus protocol all correct validators received the same output sequence, hence a contradiction. □

Lemma 6.7 (Owned Objects Sequential Execution). *If two certificates TxCert and TxCert′ both take as input the same owned object* Obj *(and no shared objects), all correct validators execute TxCert and TxCert′ in the same order.*

Proof. Let's assume two correct validators v and v' execute in different orders TxCert and TxCert′ taking the same input object Obj. That is, v executes TxCert then TxCert′, and v' executes TxCert′ then TxCert. We argue this lemma by contradiction of Lemma 6.5. Check (4.2) of Algorithm 4 ensures that a correct validator only executes certificates by following the sequence of monotonically increasing version numbers (i.e., Lamport timestamps Line 32 of Algorithm 4). As a result, since v executes TxCert before TxCert′, it follows that *version*(Obj) of TxCert is strictly lower than *version*(Obj) of TxCert′. Similarly, since v' executes TxCert′ before TxCert it follows that *version*(Obj) of TxCert′ is strictly lower than *version*(Obj) of TxCert. This implies that both TxCert and TxCert take as input Obj with the same version number. We finally note that correct validators only execute certificates valid for the current epoch (check (4.1) of Algorithm 4), thus TxCert and TxCert′ share the same epoch number. As a result, TxCert and TxCert share the input Obj for the same version and epoch number and are thus conflicting. This is a direct contradiction of Lemma 6.5. □

LEMMA 6.8 (SHARED OBJECTS SEQUENTIAL EXECUTION). *If two certificates TxCert and TxCert′ both take as input the same shared object* Obj*, all correct validators execute TxCert and TxCert′ in the same order.*

PROOF. Let's assume two correct validators v and v' execute in different orders TxCert and TxCert′ taking the same input shared object Obj. That is, v executes TxCert then TxCert′, and v' executes TxCert′ then TxCert. We note TxDigest = *digest*(TxCert), TxDigest′ = *digest*(TxCert′), and call ObjID the identifier of Obj. We argue this lemma by contradiction of Lemma 6.6. First we note that Lamport timestamps (see Line 32 of Algorithm 4) ensure correct validators always assign strictly increasing version numbers to shared objects. Since v executes TxCert before TxCert′, its SharedLock store holds the following two entries:

$$\begin{aligned} \mathsf{SharedLock}[(\mathsf{TxDigest}, \mathsf{ObjID})] &= \mathsf{Version} \\ \mathsf{SharedLock}[(\mathsf{TxDigest}', \mathsf{ObjID})] &= \mathsf{Version}' \end{aligned}$$

with Version < Version′. Similarly, since v' executes TxCert′ before TxCert, its SharedLock store holds the following two entries:

$$\begin{aligned} \mathsf{SharedLock}[(\mathsf{TxDigest}', \mathsf{ObjID})] &= \mathsf{Version}' \\ \mathsf{SharedLock}[(\mathsf{TxDigest}, \mathsf{ObjID})] &= \mathsf{Version} \end{aligned}$$

with Version′ < Version. This however means that the stores of v and v' conflict, which is a direct contradiction of Lemma 6.6. □

State transitions. We finally show that correct validators executing the same sequence of certified transitions end up in the same state.

LEMMA 6.9 (OBJECTS IDENTIFIERS UNIQUENESS). *No polynomial-time constrained adversary can create two objects with the same identifier ObjID without two successful invocations of exec(TxCert) over the same certificate TxCert.*

PROOF. We argue this lemma by the construction of the object identifier ObjID. Section 3.1 derives each objects identifier ObjID by hashing the digest *digest*(TxCert) of the certificate creating the object along with an index unique to each input object of TxCert. The adversary thus needs to find a hash collision to generate the same ObjID twice through the invocation of *exec*(TxCert) and *exec*(TxCert′), where TxCert ≠ TxCert′. □

LEMMA 6.10 (GAS OBJECT CREATION). *Every object o is created by a transaction Tx taking as input a gas object o_g.*

PROOF. Let's assume a transaction Tx creates an object o without taking as input a gas object o_g. Transaction Tx can only create o after a certificate TxCert over Tx is executed (Line 16 of Algorithm 4). Creating TxCert requires the signature of $2f+1$ validators. However, correct validators do not participate in the creation of TxCert as Tx does not satisfy check (1.2) of Algorithm 1 (verifying that Tx includes a gas object o_g for payment). As a result, TxCert is signed by $2f + 1 > f$ byzantine validators, hence a contradiction. □

LEMMA 6.11 (OBJECTS CREATION). *No sequence of valid transactions, by a polynomial-time constrained adversary, may re-create an object with the same identifier ObjID as an object that has already been created in the system.*

PROOF. We argue this property by induction on the serialized application of valid certificates, and for each certificate by application of check (4.2) of Algorithm 4 (ensuring that a certificate is executed after all its dependencies). Assuming a history of $n-1$ certificates for which this property holds we consider certificate n. For certificate n noted TxCert, we sequence all its dependencies and follow the data flow of the creation of new objects by the Move VM starting with the oldest dependency. For two objects to have the same ObjID there need to be two successful invocations of *exec*(TxCert) with the same certificate TxCert (Lemma 6.9). However, this leads to a contradiction: once the first certificate is successfully checked by the Move VM and executed, the input objects' sequence numbers are incremented, and the second invocation becomes ineffective (i.e., it does not mutate the state). Thus, as long as the certificates have at least one input – which is ensured by the presence of a gas object (Lemma 6.10) – the theorem holds unless the adversary can produce a hash collision. The inductive base case involves assuming that no initial (genesis) objects start with the same identifier – which we can ensure axiomatically. Gas objects (like any other object) have as ancestors a genesis object. □

LEMMA 6.12 (DETERMINISTIC EXECUTION). *Every correct validator executing the same set of certificates makes the same state transitions.*

PROOF. Every certificate TxCert in the sequence is executed calling the function PROCESSCERT of Algorithm 4. The function *exec*(TxCert) (Line 16) calls the Move VM to produce the set of the newly created or mutated objects $[\mathsf{Obj}_{out}]$. The determinism of the Move VM and the correctness of its type checker ensures that every correct validators calling *exec*(TxCert) with the same input TxCert produces the same $[\mathsf{Obj}_{out}]$. ATOMICPERSIST (Line 17) then persists the state transition atomically (preventing crash-recoveries from corrupting the state). Finally, Lemma 6.11 ensures that persisting the objects $[\mathsf{Obj}_{out}]$ does not overwrite any existing object in the ObjDB store. □

SUI LUTRIS safety. We now prove the safety of SUI LUTRIS using the previous lemmas.

THEOREM 6.13 (SUI LUTRIS SAFETY). *At the starting of every epoch, all correct validators have the same state.*

PROOF. We argue this property by induction. Assuming a history of $n - 1$ epochs for which this property holds we consider epoch n. Lemma 6.3 and Lemma 6.4 prove that all correct validators will execute the same set of transactions by the start of epoch $n + 1$. Then Lemma 6.7 and Lemma 6.8 show that correct validators can only execute those transactions in the same order (whenever order matter). Finally, Lemma 6.12 shows that the execution of those transactions causes the same state transition across all correct validators. As a result, every correct validator will have the same state at the start of epoch $n + 1$. The inductive base case is argued by construction: all correct validators start in the same state during the first epoch (i.e., genesis). □

Client-perceived safety. Clients consider a transaction Tx final if there exists an effect certificate EffCert over Tx. We thus show that the existence of EffCert implies that Tx is never reverted (Lemma 6.21 shows that Tx will eventually be executed). Thus all final transactions will be in a checkpoint within the epoch.

Theorem 6.14 (Client-Perceived Safety). *If there exists an effect certificate EffCert over a transaction Tx, the execution of Tx is never reverted.*

Proof. Let's assume there exists an effect certificate EffCert over a transaction Tx and that the execution of Tx is reverted. The execution of Tx is reverted if and only if Tx is not included in a checkpoint by the end of the epoch. However, correct validators only sign EffCert after including Tx in the list of certificates to be sequenced and eventually observed into a checkpoint c. By the liveness property of consensus within an epoch, a correct validator will eventually be able to sequence the certificate as long as the epoch is ongoing. The epoch ending before the certificate being sequenced and included in a checkpoint implies that a set of $f + 1$ correct validators signed EffCert and did not see it included in a checkpoint within the epoch, and a disjoint set of $f + 1$ correct validators did not sign EffCert and participated in the reconfiguration protocol to to move to the next epoch. This implies a total of $f+1+f+1+f = 3f+2 > 3f+1$ validators, hence a contradiction. □

Theorem 6.15 (No Conflicts). *No two conflicting effect certificates exist. That is, two different effect certificates sharing the same input objects and object version.*

Proof. Let's assume two conflicting effect certificates EffCert and EffCert′ exist. We distinguish two (exhaustive) cases, (i) EffCert and EffCert′ share an input owned object with the same version number, and (ii) EffCert and EffCert′ share an input shared object with the same version number. Case (i) implies there must exist two conflicting certificates TxCert and TxCert (remember effect certificate are created by signing certificates). This is however a direct contradiction of Lemma 6.5. Case (ii) implies that the $f+1$ correct validators who signed EffCert persisted SharedLock[(TxDigest, ObjID)] = Version, and the $f + 1$ correct validators who signed EffCert′ persisted SharedLock[(TxDigest, ObjID′)] = Version. Since Lemma 6.6 ensures the shared lock store of correct validators do not conflict, the set of $f + 1$ correct validators who signed TxCert is disjoint from the set of $f + 1$ correct validators who signed TxCert′. As a result, there must be a total of $f + 1 + f + 1 + f = 3f + 2 > 3f + 1$ validators, hence a contradiction. □

6.3 Liveness

We prove the liveness of the Sui Lutris protocol. We start by showing that correct users can always obtain a certificate over their valid transactions, even across epochs.

Lemma 6.16 (Dependencies Availability). *Given a certificate TxCert a correct user can always retrieve all the dependencies (i.e. parents) of TxCert.*

Proof. We argue this property by induction on the serialized retrieval of the direct parent certificates. Assuming a history of $n+1$ certificate dependencies for which this property holds, we consider certificate n noted TxCert. TxCert is signed by $2f + 1$ validators, out of which at least $f + 1$ are correct. Correct validators only sign a transaction after ensuring they hold all its input objects (check (1.1) of Algorithm 1). This mean that $f + 1$ correct validators have executed (and persisted) certificate $n - 1$ that created the inputs of TxCert. A correct user can thus query any of those $f + 1$ correct validator for certificate $n - 1$. The inductive base case involves assuming that the first dependency of every certificate is a fixed genesis (which we can ensure axiomatically). □

Lemma 6.17 (Certificate Creation). *After GST, a correct user can obtain a certificate TxCert over a valid transaction Tx.*

Proof. A correct validator always signs a transaction Tx if it passes all 4 checks of Algorithm 1. Lemma 6.16 proves that a correct user can always ensure check (1.1) passes by providing all the transaction's dependencies the validator missed. Correct transactions always pass check (1.2). Check (1.3) always passes for the first copy of Tx received by the validator (at any given time). Finally correct users do not equivocate. Thus Tx is the first and only transaction referencing its owned object, and always passes check (1.4). As a result, if Tx is disseminated to $2f + 1$ correct validators by a correct user, they will eventually all return a signature TxSign to the user. The user then aggregates those TxSign into a certificate TxCert over Tx. After GST, those actions happen within the same epoch. □

Lemma 6.18 (Certificate Renewal). *A correct user holding a certificate over transaction Tx for an old epoch e that did not finalize in e, can get a new certificate over Tx for the current epoch e'.*

Proof. After GST, correct user holding a certificate over transaction Tx for an old epoch e can re-submit Tx to $2f+1$ correct validators to a obtain a new certificate for the current epoch e'. Indeed, correct validators sign Tx if it passes all 4 checks of Algorithm 1 like in Lemma 6.17. If the validator did not already execute Tx, the correct user can ensure check (1.1) passes by providing all the transaction's dependencies the validator missed (Lemma 6.16). Check (1.2) and (1.3) will pass exactly as described in Lemma 6.17. Finally, check (1.4) passes since correct users do not attempt equivocation during epoch e' and correct validators drop the store OwnedLock upon epoch change (and thus OwnedLock[ObjKey] == None, for every input of Tx). As a result, if Tx is disseminated to $2f + 1$ correct validators by a correct user, they will eventually all return a signature TxSign to the user. The user then aggregates those TxSign into a certificate TxCert over Tx. After GST, those actions happen within the same epoch. □

The existence of a certificate implies that every owned object used as input of a certified transaction is locked for a particular version number. We now prove that all the shared objects of the certificate are also eventually locked for a version number.

Lemma 6.19 (Shared Locks Availability). *A correct user can always ensure that all correct validators eventually assign shared locks to all shared objects of a valid transaction Tx.*

Proof. Lemma 6.17 shows that a correct user can always assemble a certificate TxCert over a valid transaction Tx. The correct user can then forward the TxCert to a honest validator who submits it to the consensus engine. By the liveness property of the consensus protocol TxCert is eventually sequenced by all correct validators. When TxCert is sequenced, correct validators call AssignSharedLocks (Algorithm 4). Line 35 of Algorithm 4 then assigns locks to all shared objects of TxCert. □

We finally show that the existence of a certificate ensures the transactions of a correct user are eventually included in a checkpoint, and thus eventually executed.

Lemma 6.20 (Effect Certificates Availability). *After GST, a correct user can always ensure an effect certificate EffCert over transaction Tx will eventually exist if a certificate TxCert over Tx exist.*

Proof. A correct validator always signs an effect EffSign if it passes all 3 checks of function ProcessCert of Algorithm 4. A correct user can always ensure that check (4.1) passes by either providing the validator with the certificate TxCert during the same epoch of its creation or by re-creating a certificate for the current epoch (Lemma 6.18). A correct user can always ensure check (4.2) passes by providing all the certificate's dependencies the validator missed (Lemma 6.16). Lemma 6.19 ensures that a correct user can always make correct validators assign shared locks to all shared objects of a certificate TxCert, thus validating the first part of check (4.3) Line 10. It can then ensure the second part of check (4.3) Line 13 succeeds by providing the validator with all dependencies it missed. As a result, a correct user can collect at least $2f + 1$ effects EffSign over Tx and assemble them into an effect certificate EffCert. After GST, those actions happen within the same epoch. □

Lemma 6.21 (Checkpoint Inclusion). *If an effect certificate over transaction Tx exists within an epoch, Tx will be included in a checkpoint within the same epoch.*

Proof. If an effect certificate EffCert exists, at least $f + 1$ correct validators executed its corresponding transaction Tx. When correct validators execute a transaction they include it in the list of certificates to sequence and checkpoint (Section 5.1). Since $f + 1$ correct validators are also needed to close the epoch, and a correct validator will not do so until it experiences all listed certificates being sequenced, and by the liveness of consensus within an epoch, it follows that eventually the certificate will be sequenced (similar to Theorem 6.14). Since all certificates on which a certificate depends must also have been executed (in case of owned objects) or sequenced and executed (in case of shared objects) before an honest validator executes the transaction and signs it, it follows that if an EffCert exists then an EffCert for all dependencies will also exist and also be eventually sequenced. Since the certificate and all its causal dependencies will eventually be sequenced within the epoch, they will be included in checkpoint within the epoch. □

Lemma 6.22 (Checkpoint Execution). *All correct validators eventually execute all transactions included in all checkpoints.*

Proof. Correct validators assemble checkpoints out of certificates sequenced by consensus. By the liveness property of the consensus protocol, all correct validators can eventually sequence all the certificates they are executed (or observe others do so) and assemble them into checkpoints. We conclude the proof by noting that correct validators execute all transactions within all checkpoints they assemble. □

Theorem 6.23 (Sui Lutris Liveness). *After GST, a correct user can always ensure its transaction Tx will eventually be finalized. That is, all correct validators execute it and never revert it.*

Proof. Lemma 6.17 ensures that a correct user can eventually obtain a certificate TxCert over their valid transaction Tx. Lemma 6.20 then ensures the user can get an effect certificate EffCert using TxCert. Lemma 6.21 shows that the existence of EffCert implies the transaction is eventually included in the a checkpoint. Finally Lemma 6.22 shows that all transactions included in all checkpoints are executed. To conclude the proof we note that the execution of transactions included in checkpoints are never reverted (Section 5.3). □

Theorem 6.24 (Client-Perceived Starvation Freedom). *Let's assume two correct validators respectively set $OwnedLock[ObjKey] = sign(Tx_1)$ and $OwnedLock[ObjKey] = sign(Tx_2)$ (with $Tx_1 \neq Tx_2$) during epoch e. A correct user can eventually obtain an effect certificate over transaction Tx' accessing ObjKey at epoch $e' > e$.*

Proof. All owned objects locked by transactions at epoch e are freed upon entering epoch $e + 1$ (see Section 5.2); that is, correct validators drop all OwnedLock$[\cdot]$ upon epoch change. Correct validators thus sign a correct transaction Tx′ accessing ObjKey at epoch $e' > e$ submitted by correct clients (who do not equivocate). Lemma 6.17 then ensures the client eventually obtains a certificate over Tx′ and Lemma 6.20 ensures the client eventually obtains an effect certificate over Tx′. □

7 Related Work

At a systems level Sui Lutris is an evolution of the FastPay [4] low-latency settlement system, extended to operate on arbitrary objects through user-defined smart contracts, and with a delegated proof-of-stake committee [3]. The Sui Lutris owned object path is based on Byzantine consistent broadcast [8]. Previous works suggested using this weaker primitives to build payment systems [12, 19, 20] but lack an integration with a consensus path making it both impractical to run for a long-time (no garbage-collection or reconfiguration) and of limited functionality (only payments) and usability (client-side bugs result in loss of funds).

The consensus we use, and benchmark against, is Narwhal-Bullshark [14, 18] in a variant without asynchronous fallback, due to their reported and observed high performance. We use a modified version of Move that exposes objects as programmable entities as execution engine; our design is nevertheless modular [11] and can interface with any total-ordering protocol [10, 16, 21, 23] or deterministic execution engine [17, 28] seamlessly.

ABC [27] and CoD [26] propose a relaxed notion of consensus where termination is only guaranteed for honest senders; Sui Lutris and ABC share similar features as they are both designed to operate as a permissionless standalone system based on proof-of-stake [3]. ABC however provides no implementation or evaluation and is limited to payments systems. Other systems similar to Sui Lutris are Astro [13] and Brick [1]. Astro relies on a eager implementation of *Byzantine reliable broadcast* [9] which achieves *totality* [9] without relying on an external synchronizer at the cost of higher communication in the common case. Astro is designed as a standalone payment system but does not handle checkpointing and reconfiguration.

8 Conclusion

Sui Lutris is the first smart-contract platform that forgoes consensus for single-writer operations and only relies on consensus for multi-writer operations, combining the two modes securely. Sui Lutris describes systems aspects to achieve long-term stability and production-readiness that are typically overlooked by research prototypes. It proposes checkpointing transactions into a sequence after execution (for large categories of transactions) to reduce the need for agreement and latency, and shows how to safely reconfigure the system with minimal downtime.

Acknowledgments

This work is funded by Mysten Labs. We thank the Mysten Labs Engineering teams for valuable feedback broadly, and specifically Dmitri Perelman, Todd Fiala, Francois Garillot, Laura Makdah, Mingwei Tian, Andrew Schran, Sadhan Sood and William Smith for bringing up a lot of practical challenges while building a blockchain based on Sui Lutris.

Alonso de Gortari oversaw the crypto economics of the blockchain, and Emma Zhong, Ade Adepoju, Tim Zakia and Dario Russi designed the staking and gas mechanisms. Adam Welc designed several Move tools and provided great feedback on the manuscript. We also extend our thanks to Patrick Kuo, Ge Gao, Chris Li, and Arun Koshy for their work on the Sui SDK, clients, and RPC layer; Kostas Chalkias, Jonas Lindstrøm, and Joy Wang for overseeing the cryptographic aspect of Sui Lutris.

References

[1] Georgia Avarikioti, Eleftherios Kokoris Kogias, and Roger Wattenhofer. 2019. Brick: Asynchronous state channels. *arXiv preprint arXiv:1905.11360* (2019).

[2] Sarah Azouvi, George Danezis, and Valeria Nikolaenko. 2020. Winkle: foiling long-range attacks in proof-of-stake systems. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 189–201.

[3] 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.

[4] Mathieu Baudet, George Danezis, and Alberto Sonnino. 2020. FastPay: High-Performance Byzantine Fault Tolerant Settlement. In *AFT '20: 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, October 21-23, 2020*. ACM, 163–177.

[5] Mathieu Baudet, Alberto Sonnino, Mahimna Kelkar, and George Danezis. 2022. Zef: Low-latency, Scalable, Private Payments. *arXiv preprint arXiv:2201.05671* (2022).

[6] Sam Blackshear, Evan Cheng, David L Dill, Victor Gao, Ben Maurer, Todd Nowacki, Alistair Pott, Shaz Qadeer, Dario Russi Rain, Stephane Sezer, et al. 2019. Move: A language with programmable resources. *Libra Assoc* (2019).

[7] Dan Boneh, Ben Lynn, and Hovav Shacham. 2001. Short Signatures from the Weil Pairing. In *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings (Lecture Notes in Computer Science, Vol. 2248)*, Colin Boyd (Ed.). Springer, 514–532.

[8] Christian Cachin, Rachid Guerraoui, and Luís Rodrigues. 2011. *Introduction to reliable and secure distributed programming*. Springer Science & Business Media.

[9] Christian Cachin, Rachid Guerraoui, and Luís Rodrigues. 2011. *Introduction to reliable and secure distributed programming*. Springer Science & Business Media.

[10] Miguel Castro, Barbara Liskov, et al. 1999. Practical byzantine fault tolerance. In *OsDI*, Vol. 99. 173–186.

[11] Shir Cohen, Guy Goren, Lefteris Kokoris-Kogias, Alberto Sonnino, and Alexander Spiegelman. 2022. Proof of Availability & Retrieval in a Modular Blockchain Architecture. *Cryptology ePrint Archive* (2022).

[12] Daniel Collins, Rachid Guerraoui, Jovan Komatovic, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, Yvonne-Anne Pignolet, Dragos-Adrian Seredinschi, Andrei Tonkikh, and Athanasios Xygkis. 2020. Online Payments by Merely Broadcasting Messages. In *50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2020, Valencia, Spain, June 29 - July 2, 2020*. IEEE, 26–38.

[13] Daniel Collins, Rachid Guerraoui, Jovan Komatovic, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, Yvonne-Anne Pignolet, Dragos-Adrian Seredinschi, Andrei Tonkikh, and Athanasios Xygkis. 2020. Online payments by merely broadcasting messages. In *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 26–38.

[14] George Danezis, Eleftherios Kokoris-Kogias, Alberto Sonnino, and Alexander Spiegelman. 2021. Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus. *CoRR* abs/2105.11827 (2021).

[15] 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.

[16] Rati Gelashvili, Lefteris Kokoris-Kogias, Alberto Sonnino, Alexander Spiegelman, and Zhuolun Xiang. 2022. Jolteon and ditto: Network-adaptive efficient consensus with asynchronous fallback. In *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*. Springer, 296–315.

[17] Rati Gelashvili, Alexander Spiegelman, Zhuolun Xiang, George Danezis, Zekun Li, Dahlia Malkhi, Yu Xia, and Runtian Zhou. 2023. Block-stm: Scaling blockchain execution by turning ordering curse to a performance blessing. In *Proceedings of the 28th ACM SIGPLAN Annual Symposium on Principles and Practice of Parallel Programming*. 232–244.

[18] Neil Giridharan, Lefteris Kokoris-Kogias, Alberto Sonnino, and Alexander Spiegelman. 2022. Bullshark: Dag bft protocols made practical. *arXiv preprint arXiv:2201.05677* (2022).

[19] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, and Dragos-Adrian Seredinschi. 2018. AT2: Asynchronous Trustworthy Transfers. *CoRR* abs/1812.10844 (2018).

[20] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, and Dragos-Adrian Seredinschi. 2019. The Consensus Number of a Cryptocurrency. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, PODC 2019, Toronto, ON, Canada, July 29 - August 2, 2019*, Peter Robinson and Faith Ellen (Eds.). ACM, 307–316.

[21] Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. 2018. Omniledger: A secure, scale-out, decentralized ledger via sharding. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 583–598.

[22] Leslie Lamport. 2019. Time, clocks, and the ordering of events in a distributed system. In *Concurrency: the Works of Leslie Lamport*. 179–196.

[23] Dahlia Malkhi and Kartik Nayak. 2023. HotStuff-2: Optimal Two-Phase Responsive BFT. *Cryptology ePrint Archive* (2023).

[24] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review* (2008), 21260.

[25] Committee on Payment and Settlement Systems. 2003. A glossary of terms used in payments and settlement systems. Bank for International Settlement (BIS) Report.

[26] Jakub Sliwinski, Yann Vonlanthen, and Roger Wattenhofer. 2022. Consensus on demand. In *Stabilization, Safety, and Security of Distributed Systems: 24th International Symposium, SSS 2022, Clermont-Ferrand, France, November 15–17, 2022, Proceedings*. Springer, 299–313.

[27] Jakub Sliwinski and Roger Wattenhofer. 2019. ABC: Asynchronous Blockchain without Consensus. arXiv preprint arXiv:1909.10926.

[28] Weijia Zhang and Tej Anand. 2022. Ethereum Architecture and Overview. In *Blockchain and Ethereum Smart Contract Solution Development: Dapp Programming with Solidity*. Springer, 209–244.