Atomic cross-chain exchanges of shared assets

Krishnasuri Naraynam
IBM Research, India
knaraya3@in.ibm.com

Dhinakaran Vinayagamurthy
IBM Research, India
dvinya1@in.ibm.com

Venkatraman Ramakrishna
IBM Research, India
vramakr2@in.ibm.com

Sandeep Nishad
IBM Research, India
sandeep.nishad1@ibm.com

ABSTRACT
A core enabler for blockchain or DLT interoperability is the ability to atomically exchange assets held by mutually untrusting owners on different ledgers. This atomic swap problem has been well-studied, with the Hash Time Locked Contract (HTLC) emerging as a canonical solution. HTLC ensures atomicity of exchange, albeit with caveats for node failure and timeliness of claims. But a bigger limitation of HTLC is that it only applies to a model consisting of two adversarial parties having sole ownership of a single asset in each ledger. Realistic extensions of the model in which assets may be jointly owned by multiple parties, all of whose consents are required for exchanges, or where multiple assets must be exchanged for one, are susceptible to collusion attacks and hence cannot be handled by HTLC. In this paper, we generalize the model of asset exchange across DLT networks and present a taxonomy of use cases, describe the threat model, and propose MPHTLC, an augmented HTLC protocol for atomic multi-owner-and-asset exchanges. We analyze the correctness, safety, and application scope of MPHTLC. As proof-of-concept, we show how MPHTLC primitives can be implemented in networks built on Hyperledger Fabric and Corda, and how MPHTLC can be implemented in the Hyperledger Labs Weaver framework by augmenting its existing HTLC protocol.

CCS CONCEPTS
- Computing methodologies → Distributed computing methodologies; - Software and its engineering → Software creation and management; - Networks → Network protocols.

KEYWORDS
blockchain, distributed ledger technology, fair exchange, HTLC, shared assets, co-ownership, atomicity, interoperability

1 INTRODUCTION
The existence of diverse blockchain and distributed ledger technologies (DLTs) and networks, especially permissioned ones, has spurred research [4, 8], development [3, 33], and standardization [21, 27] efforts in interoperability. If networks cannot interoperate, their business processes (contracts) cannot interlink and their assets get trapped in silos, preventing them from scaling up and decreasing their relevance in the overall blockchain economy [3, 27]. A key interoperation enabler is the atomic swap [39], or the ability to exchange assets in two different ledgers/networks (we will use these terms interchangeably for systems that manage shared assets using blockchain or DLT) between a pair of owners atomically; i.e., the exchange happens or both ledgers revert to their original states. This problem has gained increased salience with the emergence of Decentralized Finance (DeFi) [20] and Central Bank Digital Currencies (CBDCs) [46]. But, as we will see, the state-of-the-art, and existing models and solutions, are inadequate for complex exchanges involving multiple owners and assets, which require new solutions.

The canonical atomic swap can be understood through an example. Alice and Bob possess accounts in both the Bitcoin and Ethereum Main networks. They come to an (off-chain) agreement whereby Alice will give Bob 10 BTC in exchange for, say, 12 ETH. The expected outcome of this exchange/swap is that a transfer of 10 BTC from Alice to Bob is confirmed on the Bitcoin network while simultaneously a transfer of 12 ETH from Bob to Alice is confirmed on the Ethereum Mainnet. Both transfers occur or neither does, ideally without requiring a trusted mediator or complex cross-network synchronization (e.g., linking clocks, coordinating block confirmation frequencies). A similar example can be conceived between two permissioned networks, built on, e.g., Hyperledger Fabric and Corda, using tokens designed for those DLT platforms [1, 2]. Delivery-vs-payment (DvP), a common DeFi use case, offers additional motivation. Consider a DLT network where different commercial banks possess retail accounts of a Central Bank Digital Currency (CBDC) and another DLT network where banks allow investors to trade securities (e.g. bonds). The transfer of a bond on the latter must simultaneously accompany a CBDC payment on the former [22].

From these examples, we can extrapolate a general model of exchanging an asset $M$, owned by party $X$ in ledger $L_1$, for asset $N$, owned by party $Y$ in ledger $L_2$ (Figure 1). The canonical solution to complete such atomic swaps is the Hash Time Locked Contract (HTLC) [35]. This describes both a contract that supports the locking and claiming of an asset within a fixed time duration and a protocol (see Figure 2), whose "happy path" is as follows:

- $X$ hashes secret $s$ to produce $H = \text{Hash}(s)$
This protocol works because (i) both X and Y have visibility into both ledgers, be they in public or permissioned networks, (ii) X’s secret is revealed to Y only after both assets are locked, (iii) the secret is revealed in public within a transaction for any claimers to use, (iv) Y has sufficient time to make a claim after X does so by revealing s; if Y locks immediately after X does, X has up to T/2 to make its claim, leaving Y at least T/2 before the expiration of X’s lock, and (v) only X and Y will be able to claim assets as designated recipients. To support HTLC, a DLT platform must enable asset locking (or enforce any general constraint) for a fixed time duration.

Can HTLC be generalized for atomic exchanges of more than two assets and joint ownership (or co-ownership) of assets by multiple parties? In one extension to the basic model, we can add party W to the mix so that X and W co-own M in L₁ (Figure 3), with the desired outcome of X and W co-owning N in L₂ and Y owning M in L₁. E.g., M is a title to property owned jointly by two parties, who are willing to sell it to a third party in exchange for money being transferred to a joint account held by them. In another extension, W owns a third asset R in L₁, and the desired outcome is that Y acquires M and R in L₁ in exchange for transferring N in L₂ jointly to X and W (Figure 4). E.g., M and R are separate titles to two co-located properties that are sold together to a third party in exchange for money being transferred to the owners’ joint account. Though these scenarios seem superficially similar to the base case, application of the basic HTLC protocol in either is susceptible to attack whereby X can cheat W by colluding with Y so that W loses ownership of its asset while both X and Y gain something, as we will see in Section 2. Addressing such flaws and creating a generalized HTLC solution for generalized asset exchanges is the goal of this paper, whose contributions can be summarized as follows:

- A generalized model of asset exchanges across DLT networks with a taxonomy of use cases exhaustively covering all atomic cross-network transaction possibilities. We present an associated threat model, call out desired safety properties, and identify the shortcomings of HTLC with respect to these properties.
- An augmented HTLC protocol MPHTLC, using multi-party computation (MPC), for atomic multi-party-and-asset exchanges that is proven secure in this model.
- An implementation of this protocol in the open-source Hyperledger Labs Weaver framework to facilitate generic atomic multi-party-and-asset exchanges between distributed applications built on Hyperledger Fabric and Corda networks. We also perform a simple evaluation to show that MPHTLC is practically usable.

In Section 2, we generalize the asset exchange (or atomic swap) problem, and model the scenarios and resulting threats exhaustively. Our solution for the general model that handles these threats is described in Section 3 and its efficacy is analyzed in Section 4. Practical design considerations, and suggestive implementations on two prominent DLT platforms, are discussed in Section 5. After covering related work in Section 6, we conclude with suggestions for future work in Section 7.

2 GENERALIZING ASSET EXCHANGES

In this section, we will comprehensively analyze and categorize the modes of asset exchanges that a group of parties can carry out across two distributed ledgers. We will scope the problem space, define basic and complex transaction types, and present a formal generalized asset exchange (GAE) model. Then we will show that conventional HTLC when applied to this model is prone to attacks, and identify remedies which lead to our solution.

2.1 Asset Co-Ownership

Before describing the model, we will define what we mean by co-ownership of an asset and state the properties expected from a DLT to manage such co-ownership. Conventionally, ownership of an asset in a blockchain or smart contract system implies sole authority to change the state of that asset, lock (freeze) its state until certain conditions are met, or transfer it to another owner. The state of an asset is subject to change according to rules defined in scripts (e.g., Bitcoin [12]) or contracts (e.g., Ethereum [15], Hyperledger Fabric [5]). DLT systems are expected to ensure, through consensus mechanisms and well-vetted scripts/contracts, that only rightful owners can lock assets, change their properties, or transfer them.

We define co-ownership as the ability of a ledger or smart contract system to enforce similar integrity rules on assets where the
owner is a collective rather than a single entity. Any state update or transfer or lock must require the consent of some or all members of the collective (i.e., co-owners). A typical way to enforce this is multitsig, or multiple signatures, [14, 43], where the contract requires a quorum of signatures on a transaction to update ledger state. Our minimal expectation from a smart contract system is its ability to enforce multiple or unanimous consent on asset modifications, i.e., allow an asset to be governed by multiple users.
2.2 Basic Transaction Types

Let us analyze cross-ledger exchange transactions (or simply cross-ledger exchanges), i.e., transactions that involve multiple asset ownership changes in two ledgers possibly with atomicity requirements. Figures 1, 3, and 4, illustrate examples. We can identify and categorize patterns within cross-ledger exchanges; elements of these categories vary only in the number of co-owners and in the numbers of assets involved in the transactions. We will prove that these patterns exhaustively cover all permutations where arbitrary numbers of assets with arbitrary co-owner sets are to be exchanged across two ledgers. To start with, we can identify certain fundamental operations on which cross-ledger exchanges are built:

- Creation of an asset with assignment of one or more co-owners
- Destruction of an asset with every co-owner losing ownership
- Changes to the co-ownership set of an asset: add co-owner(s), remove co-owner(s), or both simultaneously

Since exchange scenarios take the existence of the assets in question for granted, we can disregard the first two operations and focus on co-ownership changes. As described earlier, addition or removal of co-owners requires existing co-owners’ consents, typically using signatures, though the precise consent criteria can vary with ledger or contract without changing the semantics of ownership change. (For example, if an asset has more than one co-owner, the replacement of one of the co-owners may or may not require consent of the other co-owners.) Therefore, without loss of generality, we will assume in this paper that consent from co-owners is required for any addition or removal of an asset’s co-owners in the context of an atomic exchange. Now we can list the cross-ledger exchanges that are built on these fundamental operations:

- **Unconnected Local Transfers (ULTs):** A pair of asset transfers in two ledgers where neither the initial nor the final owner of one asset matches the initial or final owner of the other asset (as illustrated in Figure 5a). In effect, these transfers are not interdependent and can be executed simply as smart contract invocations localized to the respective ledgers. None of the involved parties have an atomicity requirement.

- **Cross-Ledger Replacements (CLRs):** A pair of transfers where the initial owner of one asset is the same as the final owner of the other (as illustrated in Figure 5b).

- **Cross-Ledger Swaps (CLSs):** A pair of transfers where the initial owner of one asset is the same as the final owner of the other and vice versa (as illustrated in Figure 5c and also earlier in Figure 1).

A CLR can be viewed as a ULT pair with more constraints, where $X \equiv W$, i.e., $X$ and $W$ are combined into a single logical entity. From $X$’s perspective (though not from $Y$’s or $Z$’s), the two transactions must happen atomically. Similarly, a CLS can be viewed as a CLR with more constraints, where $Y \equiv Z$, and both $X$ and $Y$ desire atomicity. As we can see, more constraints create more atomicity requirements. Even though ULTs have no atomicity requirements, it is necessary to list them here for completion. A general cross-ledger exchange (defined later in this section) will be built on a combination and extrapolation of all these basic types, with some subset of parties desiring atomicity.

Our classification covers the possibility of ULT participants \{X, Y, Z, W\} desiring atomicity for their pair of transfers. Using HTLC, the first locker (say X) can share the secret through an off-chain communication channel with the first claimer (say W). To the ledger/contract, this effectively combines X and W into a single logical entity, and the resulting scenario becomes congruent to a CLR. Further, if the second locker (Z) and second claimer (Y) are the same logical (or real-world) entity, the scenario morphs into a CLS. Hence, enforcing atomicity on a pair of ULTs (the most general transfer pair in a 2-ledger system) must correspond to a CLR or a CLS pattern, proving that our categorization of basic transaction types is exhaustive. Without an atomicity requirement, a ULT pair can simply be enforced through a pair of smart contract invocations in the respective ledgers in any sequence, while a CLS can be enforced using HTLC. A CLR can also be enforced using HTLC if the shared entity ($X$ in Figure 5b) locks $M$ first and then claims $N$ from $Z$ by revealing its secret. Also, CLRs can be augmented by adding multiple co-owners in place of $X$ or by adding multiple asset owners in $L_1$, that would jointly claim $N$ in $L_2$ (as with the CLS augmentations in Figures 3 and 4). Hence, we can treat CLRs and CLSs as similar exchange problems requiring similar solutions.

2.3 Complex Cross-Ledger Transactions

We can build arbitrarily complex transactions using the basic transactions as building blocks simply by:

- Adding more co-owners to each asset (Figure 3)
- Involving more assets in the exchange (Figure 4)

In general, a complex transaction involves a set of arbitrary co-ownership transfers of an arbitrary set of assets within two ledgers, some of which require cross-network atomicity guarantees. We claim that this can be expressed as a union of ULTs, CLRs, and CLSs where each asset has one or more co-owners (let us call the generalized multi-co-owner variants as gULT, gCLR and gCLS respectively). We assume that the contracts reflect the intents of the group of parties involved in the exchanges; i.e., some transactions require atomicity and others do not. We can assume, without loss of generality, that all transactions in an exchange scenario require atomicity and that the users have already excluded those that do not. Also, for any asset that is being replaced or swapped, we assume that all co-owners of those assets are actively involved in the cross-network transaction, even if some of those co-owners’ roles are purely limited to one ledger. A ledger/contract can always exclude such co-owners from cross-network transactions, by allowing them to just endorse (sign) a local transfer, which the ledger can process concurrently with a complex atomic cross-ledger transaction. Our model and solution will manage just the complex cross-ledger transaction, which existing ledgers are not equipped for.

For example, let us augment the CLR model in Figure 5b to add an initial co-owner $W$ for asset $M$ in ledger $L_1$, so that $X$ and $W$ together transfer $M$ to $Y$. But in ledger $L_2$, $W$ still does not take part in any transaction. We can represent this as follows:

- $L_1 : M : \{X, W\} \rightarrow \{Y\}$
- $L_2 : N : \{Z\} \rightarrow \{X\}$

From $W$’s perspective, the first transaction is a ULT. Hence this transaction pair is a combination of a ULT and a CLR. W just needs to endorse X’s locking of M in Y’s favor by signing the transaction. But the final outcome requires atomic commitments; hence we can merge this ULT into the CLR and require W and X to lock M
We encounter the exact same possibilities and outcome if we augment a CLS (Figure 5c) as follows:

- \(L_1 : M : \{X, W\} \rightarrow \{Y\}\)
- \(L_2 : N : \{Y\} \rightarrow \{X\}\)

\(W\) plays an ancillary role by simply doing a ULT to \(Y\), but that ULT can be merged with the CLS, making \(W\) an active participant in the swap. Merging ULTs into atomic transactions preserves the final outcome (i.e., co-ownership changes remains the same), while making analysis and solution-building easier. Therefore, we can assume merging as default without our model losing any power.

Here is a scenario that shows how a complex transaction is a composition of basic transactions. This is illustrated in Figure 6 (symbols will be explained later.) The following are the asset transfers (or asset ownership changes) occurring in the two ledgers:

- \(L_1 : \text{Currency} : \{X, Y\} \rightarrow \{W, Y, Z\}\)
- \(L_1 : \text{Security} : \{T, U\} \rightarrow \{V\}\)
- \(L_1 : \text{Diamond} : \{Z\} \rightarrow \{V\}\)
- \(L_2 : \text{Car} : \{T\} \rightarrow \{T, U, W\}\)
- \(L_2 : \text{House} : \{Z\} \rightarrow \{T, X, Y\}\)

By inspection, we can deconstruct this set of transactions:

- \(L_1 : \text{Currency} : \{X, Y\} \rightarrow \{W, Y, Z\}\) and \(L_2 : \text{House} : \{Z\} \rightarrow \{T, X, Y\}\) together comprise a gCLS from the perspective of \(\{X, Y\}\) as one group of co-owners and \(\{Z\}\) as another. \(W\) and \(T\) are simply claimants and don’t play an active role in the swap, but their endorsements (i.e., digital signatures on the transfer transactions) are needed to finalize the transactions; hence, their roles can be merged into the CLS as a whole. (Note: excluding \(W\) and \(T\) still leaves multiple co-owners \((\{X, Y, Z\}\)) for the two assets being swapped, so this scenario is a complex swap according to our model. As we will see in Section 2.6, such an exchange cannot be handled as a simple swap using classic HTLC.)
- \(L_1 : \text{Security} : \{T, U\} \rightarrow \{V\}\) and \(L_2 : \text{Car} : \{T\} \rightarrow \{T, U, W\}\) together comprise a gCLR from \(U\)’s perspective. \(T\) simply gives or shares its co-ownership and \(V\) and \(W\) simply take co-ownerships, but their roles can be merged into the gCLR as a whole. It is up to the users whether or not to complete this gCLR independent of the above gCLS, but if they so intend, it can be enforced atomically with the gCLS, in effect merging the two exchanges into a single atomic exchange. This is the default assumption our solution will make when presented with a set of transactions (see Section 3).
- \(L_1 : \text{Diamond} : \{Z\} \rightarrow \{V\}\) is a ULT as it is unconnected to the other transactions in the set. But, if the users so intend, this can be completed atomically with the other transactions, and that is the default assumption our solution will make when presented with a set of transactions (see Section 3).

2.4 Generalized Asset Exchange Model

We now formally model the problem of atomically changing co-ownership configurations of assets in two independent ledgers, where the co-owners across all assets belong to a common limited size group of parties.

**Definition 2.1 (generalized asset exchange: \(GAE\)).** This is a tuple \((L_1, L_2, P, \mathcal{A}_1, \mathcal{A}_2, \text{IO}_1, \text{IO}_2, \mathcal{AE}_1, \mathcal{AE}_2, \text{FO}_1, \text{FO}_2)\) where:

- \(L_1\) and \(L_2\) are two distinct ledgers
- \(P\) is a common set of parties with accounts in both \(L_1\) and \(L_2\)
- \(\mathcal{A}_1\) is a set of assets on \(L_1\)
- \(\mathcal{A}_2\) is a set of assets on \(L_2\)
- \(\text{IO}_1\) is the initial asset ownership function in \(L_1\), defined as \(\text{IO}_1 : \mathcal{A}_1 \rightarrow 2^P - \{\emptyset\}\)
• IO₂ is the initial asset ownership function in \( L_2 \), defined as \( IO₂ : \mathcal{A}_2 \rightarrow 2^P - \{\varnothing\} \).

• \( \mathcal{A}_{E₁} \) is a set of assets in \( L_1 \) to be exchanged, where \( \mathcal{A}_{E₁} \subseteq \mathcal{A}_1 \).

• \( \mathcal{A}_{E₂} \) is a set of assets in \( L_2 \) to be exchanged, where \( \mathcal{A}_{E₂} \subseteq \mathcal{A}_2 \).

• \( FO₁ \) is the initial asset ownership function in \( L₁ \) after the exchange, defined as \( FO₁ : \mathcal{A}_1 \rightarrow 2^P - \{\varnothing\} \), where:
  - \( \forall a \in \mathcal{A}_1 - \mathcal{A}_{E₁}, FO₁(a) = IO₁(a) \), and
  - \( \forall a \in \mathcal{A}_{E₁}, FO₁(a) = IO₁(a) \land FO₂(a) \neq IO₁(a) \).

• \( FO₂ \) is the final asset ownership function in \( L₂ \) after the exchange, defined as \( FO₂ : \mathcal{A}_2 \rightarrow 2^P - \{\varnothing\} \), where:
  - \( \forall a \in \mathcal{A}_2 - \mathcal{A}_{E₂}, FO₂(a) = IO₂(a) \), and
  - \( \forall a \in \mathcal{A}_{E₂}, FO₂(a) = IO₂(a) \land FO₂(a) \neq IO₂(a) \).

In plain language, \( \mathcal{GAE} \) represents the transfer of co-ownerships of one set of assets in one ledger in exchange for the transfer of co-ownerships of another set of assets in the other ledger, atomically. The standard atomic swap assumption of common parties across ledgers is represented by \( P \). Initial co-ownership of assets are represented by the definitions of \( IO₁ \) and \( IO₂ \) where each asset maps to a non-empty subset of \( P \). The definitions of \( FO₁ \) and \( FO₂ \) indicate that (i) the final co-owners of each asset being transferred are drawn from the full set of parties regardless of their initial ownership statuses, (ii) assets are not expelled from the ledger, and (iii) an asset’s final co-ownership is different from its initial co-ownership. The function mappings remain unchanged for assets outside the swap lists \( \mathcal{A}_{E₁} \) and \( \mathcal{A}_{E₂} \). The range for each co-ownership function is the power set of \( P \), excluding the null set, indicating that each asset can have one or more co-owners drawn from \( P \). The null set is excluded because we wish to avoid handling assets in \( \mathcal{GAE} \) that are created from scratch or destroyed in the course of a cross-ledger exchange. We limit our scenarios to assets exchanging hands because the incentive and trust models we consider in this paper only apply to those scenarios.

The example in Figure 6 illustrates this definition and the tuple elements. From the definition, we can define partitions of the co-owners in order to reason about the exhaustiveness of the definition and the threat models they present, as follows for \( i \in \{2\} \):

• \( G_i \) is the asset co-ownership giver function in \( L_i \), defined as \( G_i : \mathcal{A}_{E_i} \rightarrow 2^P - \{\varnothing\} \), where \( G_i(a) = IO_i(a) - FO_i(a) \).

• \( K_i \) is the asset co-ownership keeper (sharer) function in \( L_i \), defined as \( K_i : \mathcal{A}_{E_i} \rightarrow 2^P - \{\varnothing\} \), where \( K_i(a) = IO_i(a) \land FO_i(a) \).

• \( T_i \) is the asset co-ownership taker function in \( L_i \), defined as \( T_i : \mathcal{A}_{E_i} \rightarrow 2^P - \{\varnothing\} \), where \( T_i(a) = FO_i(a) - IO_i(a) \).

(Note: as we mentioned earlier, the null set is excluded from the giver, keeper, and taker function ranges because we do not consider unattached assets that are created or destroyed in a \( \mathcal{GAE} \) instance.)

As should be clear from these definitions, \( \forall a \in \mathcal{A}_{E₁} \), we have that \( G₁(a) \cup K₁(a) \cap T₁(a) = IO₁(a) - FO₁(a) \) and \( \forall a \in \mathcal{A}_{E₂}, G₂(a) \cup K₂(a) \cup T₂(a) = IO₂(a) \cup FO₂(a) \).

Let us express cross-network transactions in \( \mathcal{GAE} \) parlance, starting with the basic types discussed in Section 2.2. Table 1 shows the givers, keepers, and takers, of the transactions illustrated in Figure 5, each transaction involving the exchange of assets \( M \) and \( N \). We can spot a few conditional cases from these tables:

• In the ULT pair, \( (G₁(M) \cup K₁(M)) \cap T₂(N) = \varnothing \) and \( (G₂(N) \cup K₂(N)) \cap T₁(M) = \varnothing \).

| Ledger | Asset/Transfer | G | K | T |
|--------|----------------|---|---|---|
| ULT    | \( L₁ \)       | \{X\} → \{Y\} | \{Y\} | \{Y\} |
|        | \( L₂ \)       | \{Z\} → \{W\} | \{W\} | \{W\} |
| CLR    | \( L₁ \)       | \{X\} → \{Y\} | \{Y\} | \{Y\} |
|        | \( L₂ \)       | \{Z\} → \{X\} | \{X\} | \{X\} |
| CLS    | \( L₁ \)       | \{X\} → \{Y\} | \{Y\} | \{Y\} |
|        | \( L₂ \)       | \{Y\} → \{X\} | \{X\} | \{X\} |

Table 1: Co-Ownership Sets

| Ledger | Asset/Transfer | G | K | T |
|--------|----------------|---|---|---|
| \( L₁ \) | \( \text{Currency} : \{X,Y\} \rightarrow \{W,Y,Z\} \) | \{X\} | \{Y\} | \{W,Z\} |
|        | \( \text{Security} : \{T,U\} \rightarrow \{V\} \) | \{T,U\} | \{V\} | \{V\} |
|        | \( \text{Diamond} : \{Z\} \rightarrow \{V\} \) | \{Z\} | \{V\} | \{V\} |
| \( L₂ \) | \( \text{Car} : \{T\} \rightarrow \{T,U,W\} \) | \{T\} | \{T,U,W\} | \{T\} |
|        | \( \text{House} : \{Z\} \rightarrow \{T,X,Y\} \) | \{Z\} | \{T,X,Y\} | \{T,X,Y\} |

Table 2: CLS Co-Ownership Sets

• In the CLR, \( (G₁(M) \cup K₁(M)) \cap T₂(N) \neq \varnothing \) and \( (G₂(N) \cup K₂(N)) \cap T₁(M) = \varnothing \).

• In the CLS, \( (G₁(M) \cup K₁(M)) \cap T₂(N) \neq \varnothing \) and \( (G₂(N) \cup K₂(N)) \cap T₁(M) \neq \varnothing \).

We can therefore distinguish ULTs, CLRs, and CLSs using these conditions. Table 2 shows the co-ownership sets corresponding to the complex transaction of Figure 6. The above conditionals hold for the CLS transaction (Currency for House), the CLR transaction (Security for Car), and the ULT transaction (Diamond) are deconstructed earlier. If we merge all transactions in the two ledgers respectively and take the unions of the G, K, and T sets, we end up with the conditional above that corresponds to a CLS.

Now, with multiple assets and co-owners, consider the following sets of parties:

\[
S_{12} = \left( \bigcup_{a \in \mathcal{A}_{E₁}} G₁(a) \cup \bigcup_{a \in \mathcal{A}_{E₁}} K₁(a) \right) \cap \bigcup_{a \in \mathcal{A}_{E₂}} T₂(a)
\]

\[
S_{21} = \left( \bigcup_{a \in \mathcal{A}_{E₂}} G₂(a) \cup \bigcup_{a \in \mathcal{A}_{E₂}} K₂(a) \right) \cap \bigcup_{a \in \mathcal{A}_{E₁}} T₁(a)
\]

We can thus extrapolate the conditionals to complex transactions with multiple assets and co-owners. \( \mathcal{GAE} \) is a combination of:

• only gULTs if both \( S_{12} \) and \( S_{21} \) are empty.

• only gCLRs and gULTs if only one of \( S_{12} \) and \( S_{21} \) are empty.

• all gCLs, gCLRs, and gULTs if neither of \( S_{12} \) and \( S_{21} \) is empty.

In plain language, if no giver or keeper gets anything in return for a transfer in another ledger, then the transactions are local and unconnected. If only a single group of co-owners get compensated, the transactions will only involve cross-ledger replacements. And if there are two sets of co-owners get compensated by each other, the transactions must involve cross-ledger swaps. Using the above test, we can verify that the examples in Figures 3 and 4 map to gCLs and that the complex transaction in Figure 6 contains gCLSs.

\( \mathcal{GAE} \) therefore exhaustively covers all basic and complex transaction types as we have defined them. It also covers all possible
cross-ledger exchanges in which atomicity is required. The above conditionals also tell us how to determine the combinations of basic transaction types within a $GAE$ instance.

### 2.5 Threat model and Properties

**Threat model:** Let us identify the factors that pose threats to the integrity of a $GAE$ instance. We assume that all participants in $P$ are rational, and that they can arbitrarily deviate from a specified exchange protocol, collude with other participants, and attempt to maximize the value that they gain through the protocol. We also assume collective integrity of a network maintaining a shared ledger, i.e., rogue miners or block creators cannot override honest network members to finalize fraudulent or spam transactions.

**Properties:** We desire the atomicity property from a protocol that accomplishes $GAE$. Atomicity ensures for each party that follows the protocol that the assets it co-owns or would co-own either all move to the desired final state or all remain in the original state, even if other parties deviate from the protocol.

**Definition 2.2 (Atomicity in $GAE$).** For every participant $P \in P$, let $AE_{1,P} = \{a | P \in \{I0_1(a) \cup FO_1(a)\}\}$ and let $AE_{2,P} = \{a | P \in \{I0_2(a) \cup FO_2(a)\}\}$. A protocol for $GAE$ is atomic if exactly one of the following holds:

1. For all $a_1 \in AE_{1,P}$, the owners of $a_1$ at the end of the protocol are according to $FO_1(a_1)$ and for all $a_2 \in AE_{2,P}$, the owners of $a_2$ at the end of the protocol are according to $FO_2(a_2)$.
2. For all $a_1 \in AE_{1,P}$, the owners of $a_1$ at the end of the protocol are according to $I0_1(a_1)$ and for all $a_2 \in AE_{2,P}$, the owners of $a_2$ at the end of the protocol are according to $I0_2(a_2)$.

### 2.6 HTLC limitations

Let us categorize $GAE$ instances from single-asset-per-ledger and single-co-owner-per-ledger to multiples of these, and separately analyze the threats they face. In the basic CLR and CLS cases, and also in a case where a party keeps its co-ownership rather than gives it to another (see below), the conventional HTLC as described in Section 1 can be used without it being susceptible to attack.

- $L_1 : M : \{X\} \rightarrow \{X, Y\}$
- $L_2 : N : \{Y\} \rightarrow \{X\}$

Now we will analyze all the permutations of $GAE$ involving multiple co-owners and multiple assets in each ledger in below cases. Because HTLC is known to enforce atomicity for singly-owned assets, we will try to apply it to these scenarios to determine whether it satisfies the properties listed earlier.

1. **Multiple co-owners locking a single asset in one ledger and claiming a single asset in another ledger:** This is the scenario in Figure 3 and which we can represent as follows:

   - $L_1 : M : \{X, W\} \rightarrow \{Y\}$
   - $L_2 : N : \{Y\} \rightarrow \{X, W\}$

   Conventional HTLC can be applied in two different ways: (i) $X$ and $W$ agree offline on a secret; either of them locks $M$ with its hash and signatures (i.e., consents) of both $X$ and $W$, following which $Y$ locks $N$ with the same hash; either $X$ or $W$ claims $N$ (on behalf of both parties), and then $Y$ claims $M$. (ii) $X$ and $W$ independently lock $M$ in either sequence using two different secrets (the contract deems $M$ to be locked only when both $X$ and $W$ have submitted their respective transactions), following which $Y$ locks $N$ with both the hashes; $X$ and $W$ submit claims to $N$ (by revealing their respective secrets in any order), following which $Y$ claims $M$ using both the revealed secrets.

**Threats/Attacks:** Both approaches are vulnerable to collusion between $Y$ and one of $X$ and $W$ to cheat the other: (i) after $M$ is locked, either of its co-owners (let’s say $W$) may strike a deal with $Y$ to give $M$ away (using the same hash lock) and $Y$ in turn will lock $N$ only for that party (in this case, $W$) rather than jointly to $X$ and $W$; $W$ may also provide some other incentive to $Y$ to encourage it to collude against $X$; since $X$ has already locked away its co-ownership of $M$ using a secret that $W$ also possesses, it is left at a disadvantage (ii) if $X$ submits its claim in $L_2$ first by revealing its secret, $W$ may avoid revealing its secret and submitting a claim, following which $Y$ may allow its earlier lock to lapse and instead lock $N$ again in favor of $W$; having revealed its secret, $X$ is now at a disadvantage as $Y$ can claim its share of $M$ but $W$ now will get all of $N$ instead of having to co-own it with $X$. In this protocol, the party that acts first (i.e., submits a claim) stands at a disadvantage as its co-owner may collude with its counterparty(ies) to rob it of its rightful share of an asset.
Incidentally, if $Y$ locks $N$ first, these attacks will not be possible, but if $Y$ is replaced with multiple co-owners, then these threats will still apply regardless of the lock sequence.

(2) **Co-owners locking multiple assets in one ledger and claiming a single asset in another ledger:** This is the scenario in Figure 4:

- $L_1 : M : \{X\} \rightarrow \{Y\}$
- $L_1 : R : \{W\} \rightarrow \{Y\}$
- $L_2 : N : \{Y\} \rightarrow \{X, W\}$

Conventional HTLC can be applied in the same two ways as in case (1) and suffers from the same collusion possibilities. The only difference is that $Y$ gains two assets instead of one if it colludes with either $X$ or $W$. If $Y$ were to lock $N$ first, it could simply lock in favor of either $X$ or $W$ (whoever the colluding party is). This procedure does not present any interesting features, because $Y$ has the power of unilateral action regardless of how the other parties behave. The same threat possibilities apply if $Y$ is replaced with multiple co-owners.

(3) **Multiple co-owners locking a single asset in one ledger and claiming multiple assets in another ledger:**

- $L_1 : M : \{X, W\} \rightarrow \{Y\}$
- $L_2 : N : \{Y\} \rightarrow \{X\}$
- $L_2 : P : \{Y\} \rightarrow \{W\}$

If conventional HTLC is applied with $M$ being locked first, it will suffer from the same threats as in cases (1) and (2). But if $Y$ were to lock both $R$ and $N$ in $L_2$ first, then conventional HTLC will work without posing any new threats.

If $Y$ is replaced with multiple co-owners, say $(Y, Z)$, the attacks described in case (1) will be possible (either $Y$ or $Z$ colluding with $X$ and $W$).

(4) **Co-owners locking multiple assets in one ledger and claiming multiple assets in another ledger:**

- $L_1 : M : \{X\} \rightarrow \{Y\}$
- $L_1 : R : \{W\} \rightarrow \{Y\}$
- $L_2 : N : \{Y\} \rightarrow \{X\}$
- $L_2 : P : \{Y\} \rightarrow \{W\}$

If conventional HTLC is applied with $M$ and $R$ being locked first as in case (2), it will face the same threats. If $Y$ were to lock $N$ and $P$ first, it could simply lock one of those assets in favor of either $X$ or $W$ (whoever the colluding party is). On the other hand, if $Y$ locked both its assets first and then waited for both $X$ and $W$ to lock theirs, then HTLC will fulfill the exchange. But if $Y$ were replaced with multiple co-owners, the same threat possibilities apply as in case (1).

By induction, the above breakup of cases and the threats identified can be extrapolated to a generic $G \mathcal{AE}$ instance. The threat faced by conventional HTLC when applied to $G \mathcal{AE}$ is that there is no mechanism to enforce a joint lock and claim over more than one asset by more than one co-owner. We must therefore (i) ensure that parties can jointly lock one or more assets without revealing the secret to any of them in clear, and (ii) ensure that parties jointly locking one or more assets for transfer in one ledger cannot unilaterally make claims in the other ledger. We will address these challenges by creating primitives for these operations and providing an augmented HTLC protocol in the next section.

3 **SOLUTION: MULTI-PARTY HASH TIME LOCKED CONTRACT (MPHTLC)**

We present an augmented form of HTLC, called MPHTLC, to solve $G \mathcal{AE}$. The basic capabilities required of a ledger (or a smart contract system over it) are that it supports hash and time locks on assets. Therefore, any ledger that is capable of implementing conventional HTLC [35] will also be able to implement MPHTLC. We also make the practical assumption that both participating ledgers have known (or predictable) upper and lower bounds for transaction, or block, confirmation times. As a consequence, we can safely assume that no adversary in our threat model can arbitrarily speed up or slow down either of the ledgers. This ensures predictability and a priori selection of asset time lock durations, preventing the counter-parties from racing each other or denying each other adequate time to mount their claims. In addition, we will utilize secure multi-party computation (MPC) protocols [17, 25, 47], to enforce the ability to jointly lock and claim assets, which we identified as a key requirement to handle the threats.

3.1 **MPHTLC protocol**

In a $G \mathcal{AE}$ instance, let us define $O_1$ as the set of initial co-owners of assets $\mathcal{AE}_1$ in $L_1$ (givers and keepers, as defined in Section 2) as

$$O_1 = \bigcup_{a \in \mathcal{AE}_1} IO_1(a) = \bigcup_{a \in \mathcal{AE}_1} G_1(a) \cup \bigcup_{a \in \mathcal{AE}_1} K_1(a)$$

Let the cardinality of $O_1$, or $|O_1|$, be $n$. Here are the protocol steps:

1. Let $x_1, x_2, \ldots, x_n$ be the secrets chosen by the $n$ parties of $O_1$ respectively in $L_1$. They compute a hash $H = F_1(x_1, x_2, \ldots, x_n)$ where $F_1$ is an MPC protocol (see Section 3.2) among the $n$ parties. Note: no information about the secrets $x_1, x_2, \ldots, x_n$ is revealed during the computation other than the output $H$ itself.

2. Each asset $a \in \mathcal{AE}_1$ is locked by one of its initial co-owners ($a \in IO_1(a)$) using hash $H$ in $L_1$ with expiration duration $T$ in favor of the parties in $FO_1(a)$. All initial co-owners of $a$ in $IO_1(a)$ are required to sign the lock transaction before it is submitted to the chain. It is up to the ledger/contract to determine if each asset is to be locked using a separate transaction or if all assets are to be locked together in a single transaction. The contract(s) validate the signatures from all the co-owners of each asset and if valid, locks the assets pending either the supply of the secret pre-image corresponding to $H$ or the passing of $T$ time units.

3. Each asset $a \in \mathcal{AE}_2$ is locked by one of its initial co-owners ($a \in IO_2(a)$) after verifying that all the locks in Step (2) have been committed in favor of the expected final owners with appropriate time locks in $L_1$. The locks in $L_2$ are created using same hash $H$ from $L_1$ with an expiration duration $T/2$ in favor of the parties in $FO_2(a)$, pending either the supply of the secret pre-image corresponding to $H$ or the passing of $T/2$ time units. All initial co-owners of $a$ in $IO_2(a)$ are required to sign the lock transaction before it is submitted to the chain. Note that hash $H$ can be obtained from $L_1$, because $IO_2(a) \subseteq \mathcal{P}$ and all members of $\mathcal{P}$ have read access to both ledgers.
(4) The \( n \) parties of \( O_1 \) in \( L_1 \) first verify that all the locks in steps (2) and (3) have been committed in favor of the expected final owners with appropriate time locks in \( L_1 \) and \( L_2 \) respectively. If these checks are successful, the \( n \) parties compute \( x = F_2(x_1, x_2, \ldots, x_n) \) such that \( \text{Hash}(x) = H \), using their respective secrets chosen in step 1 as inputs. Here, \( F_2 \) is an MPC protocol (described in section 3.2) between the \( n \) parties.

(5) Every asset \( a \in \mathcal{AE}_2 \) can now be claimed by its final owners \( \text{FO}_2(a) \) in \( L_2 \) if the secret \( x \) is revealed before time duration \( T/2 \) elapses. If the transfer of \( a \) is part of a gCLS or a gCLR, i.e., if the intersection of \( O_1 \) and \( \text{FO}_2(a) \) is not \( \emptyset \), there will be at least one party with an incentive to reveal the secret. If the intersection is \( \emptyset \), then the transfer of \( a \) is a gULT with respect to the transfers in \( L_1 \); as described in section 2.2, this will require an off-chain sharing of the secret among parties if and only if this gULT must be conducted atomically with transfers in \( L_1 \). All assets in \( \mathcal{AE}_2 \) get transferred to the final co-owners as defined by the \( \text{FO}_2 \) function once any party reveals \( x \) in \( L_2 \) within \( T/2 \). At this stage, the revelation of the secret benefits all claiming parties equally, and gives no advantage to a subset. If nobody supplies \( x \) in \( L_2 \) within \( T/2 \), the co-owners remain as defined by \( \text{IO}_2 \). All transfers occur or no transfer occurs, thereby satisfying the cross-ledger atomicity property. Lastly, depending on how the assets were locked, the claim should be submitted via a single transaction for all locked assets or using one transaction per locked asset.

(6) Every asset \( a \in \mathcal{AE}_1 \) can now be claimed by its final owners \( \text{FO}_1(a) \) in \( L_1 \) by supplying the secret \( x \) within duration \( T \). \( x \) is already public in \( L_2 \) and therefore known to every party in \( \mathcal{P} \). Every asset in \( \mathcal{AE}_1 \) gets transferred to its final co-owners as defined by \( \text{FO}_1 \) once any party reveals \( x \) in \( L_1 \) within \( T \). If nobody supplies \( x \) in \( L_1 \) (which would be irrational on their part), then the co-owners remain as defined by \( \text{IO}_1 \).

Timing Considerations: If each asset has a separate lock and claim transaction, there is a potential hazard that must be managed as follows. In step 5, there may be an asset \( a \in \mathcal{AE}_2 \) whose owners don’t overlap with \( O_1 \), i.e., \( \text{IO}_2(a) \cap O_1 = \emptyset \). These claimers are dependent on some party in \( O_1 \) revealing \( x \). But if parties in \( O_1 \) compute MPC \( F_2 \) to reveal \( x \) close to the timeout \( T/2 \), these non-overlapping claimers may lose the chance to claim their assets. Therefore, the time locks on such assets should have extra tolerance. And because we can determine these assets a priori, by inspecting the \( \mathcal{G} \cap \mathcal{AE} \) tuple, the contracts can enforce this. A suggestive guideline would be to use \( T/4 \) as the timeout for every asset in \( L_2 \) that has at least one claimant belonging to \( O_1 \), and \( T/2 \) for the other assets in \( L_2 \). The timeout for every asset in \( L_1 \) remains \( T \) as \( x \), once revealed in \( L_2 \), is immediately available for claiming in \( L_1 \).

3.2 Selection of the MPC functions \( F_1 \) and \( F_2 \)

The \( n \) parties output \( H = \text{Hash}(g(x_1, x_2, \ldots, x_n)) \) by participating in an MPC protocol \( F_1 \) with \((x_1, x_2, \ldots, x_n)\) as their respective inputs, where \( g \) can be any function with the following properties:

(1) The output of \( g \) contains sufficient entropy for input from each party, such that inputs of any \( n - 1 \) parties cannot be used to guess the output with non-negligible probability.

(2) The output of function \( g \) need not hide information about the inputs \( x_1, x_2, \ldots, x_n \). This is what differentiates \( g \) from, say, a secret sharing protocol.

(3) The one-wayness of \( H \) ought to be retained when hashing \( g(x_1, x_2, \ldots, x_n) \) instead of \( x_1, x_2, \ldots, x_n \). Note: the security of HTLC assumes one-wayness of \( H \) on randomly chosen inputs.

In our instantiation of MPHTLC, \( g \) is an identity function which outputs \( x_1, x_2, \ldots, x_n \), but any \( g \) satisfying the above properties can be used. Any maliciously secure MPC protocol with fairness can be used for \( F_1 \), where the malicious security protects against participants arbitrarily deviating from the protocol and the fairness property guarantees that either all the parties get the output or none of them do. The fairness property ensures that the same output hash is obtained by all the parties in \( O_1 \) and is a valid hash according to the inputs \( x_1, x_2, \ldots, x_n \). Note again that no information is revealed about the secrets \( x_1, x_2, \ldots, x_n \) during the computation of \( \text{Hash}(g(x_1, x_2, \ldots, x_n)) = H \), other than the final output \( H \). The above mentioned properties of \( g \) do not affect the confidentiality provided by the MPC protocol.

The MPC protocol \( F_2 \) among the \( n \) parties of \( O_1 \) in \( L_1 \) (used during the claim phase) involves computing \( x = g(x_1, x_2, \ldots, x_n) \) using their respective inputs \( x_1, x_2, \ldots, x_n \) chosen in step 1. Note that \( \text{Hash}(x) = H \). We use an MPC protocol with fairness and hence either all the parties in \( O_1 \) obtain \( x \) or none of them do.

A discussion on Fair MPC protocols. Fairness in MPC is extensively studied in the cryptography literature, and there are different possibilities of instantiating a fair MPC based on the requirements of MPHTLC. It is possible to achieve fairness with just point-to-point secure communication between each pair of individual parties if less than one-third of the parties are malicious [10, 25], and with the use of a broadcast network to protect up to \( \lceil n/2 \rceil - 1 \) parties being malicious [25, 37]. If the goal is to protect against a majority of the parties being malicious, it is proven that the standard definition of fairness is impossible to achieve this without additional assumptions [19], and this impossibility holds even in the presence of a trusted hardware without trusted clocks [36]. There are different relaxed definitions of fairness proposed in the literature that protect against a dishonest majority of parties [6, 13, 24, 26]. But if a use of MPHTLC demands the standard definition of fairness against a dishonest majority of parties, there are protocols that use public blockchains, financial penalties and sometimes additionally trusted hardware like Intel SGX (to make the protocol more efficient) to enable this [7, 11, 18, 31, 36].

The fairness property is sufficient if all the assets are locked in a single transaction. But in the variant that assets are locked separately across multiple transactions, there is an additional hazard that we need to address. Fairness ensures that either all the parties get the output or none of them do, but it does not specify any time bound on when the parties get the output if they do. There could exist fair MPC protocols where one of the parties delays the output “release” to whenever they want to. This is a concern when the assets are individually locked since a party can delay the output release to just before the timeout \( T/2 \), and hence, due to network delays, there will invariably be some parties at a disadvantage. Though all the parties will get the output, some of them might
3.3 Instantiations

We now instantiate the MPHTLC protocol for a couple of scenarios, that also provides an intuition on how MPHTLC avoids the attacks identified as possible with conventional HTLC in Section 2.6. Across all the cases, we discovered that collusion attacks are possible when

- multiple co-owners must lock an asset first before making a joint claim for an asset in another ledger, as described in case (1) in Section 2.6 (also see Figure 3)
- co-owners of different assets must lock their respective assets first before making a joint claim for an asset in another ledger, as described in case (2) in Section 2.6 (also see Figure 4)

MPHTLC applied to case (1) goes as follows (also see Figure 7).

1. Let \( s_1 \) and \( s_2 \) be the secrets chosen by \( X \) and \( W \) respectively. They compute a hash \( H = H_1(s_1, s_2) \) where \( H_1 \) is an MPC protocol instance agreed by both of them.
2. Party \( X \) locks the asset \( M \) using \( H \) in \( L_1 \) till time \( T \) with the signature of the party \( W \) for party \( Y \), or vice versa.
3. Party \( Y \) locks the asset \( N \) using \( H \) in \( L_2 \) till time \( T/2 \) for both the parties \( X \) and \( W \).
4. Parties \( X \) and \( W \) in \( L_1 \) compute \( s = F_2(s_1, s_2) \) using their respective secrets chosen in Step 1 above where \( F_2 \) is another MPC protocol instance chosen by them such that \( \text{Hash}(s) = H \).
5. Party \( X \) (or \( W \)) submits a claim on asset \( N \) in \( L_2 \) by revealing the secret \( s \) before time \( T/2 \) elapses.
6. Party \( Y \) submits a claim on assets \( M \) and \( X \) in \( L_1 \) by using the secret \( s \) obtained from ledger \( L_2 \) before time \( T \) elapses.

This protocol avoids the two hazards identified in Section 2.5, at lock time and at claim time, as follows:

- Neither \( X \) nor \( W \) knows the secret at the end of Step 2, and hence neither can collude with \( Y \) to get the latter to lock \( N \) only in favor of one of them. If \( Y \) chooses not to execute Step 3, the protocol will end with no change in either ledger’s state.
- There is exactly one secret, which is only revealed in Step 4, so \( X \) nor \( W \) will be left at a disadvantage. If either of them reveals \( s \) in that step, both will collectively co-own \( N \). If neither reveals \( s \), the protocol will end with no change in either ledger’s state.

MPHTLC applied to case (2) goes as follows.

1. Let \( s_1 \) and \( s_2 \) be the secrets chosen by \( X \) and \( W \) respectively. They compute a hash \( H = H_1(s_1, s_2) \) where \( H_1 \) is an MPC protocol instance agreed by both of them.
2. Party \( X \) locks asset \( M \) using \( H \) in \( L_1 \) for time \( T \) for party \( Y \).
3. Similarly, \( W \) locks asset \( R \) using \( H \) in \( L_1 \) for time \( T \) for \( Y \).
4. Party \( Y \) locks asset \( N \) using \( H \) in \( L_2 \) for time \( T/2 \) for both the parties \( X \) and \( W \).
5. Parties \( X \) and \( W \) in \( L_1 \) compute \( s = F_2(s_1, s_2) \) using their respective secrets chosen in Step 1 above where \( F_2 \) is another MPC protocol instance chosen by them such that \( \text{Hash}(s) = H \).
6. Party \( X \) (or \( W \)) submits a claim on asset \( N \) in \( L_2 \) by revealing the secret \( s \) before time \( T/2 \) elapses.

This protocol avoids the same two hazards in the same ways as discussed for the previous use case.

4 ANALYSIS

We now prove the atomicity property of our MPHTLC protocol in our threat model that all parties are rational and the adversarial parties can arbitrarily deviate from the protocol.

We state some basic assumptions before we prove atomicity:

- At least one party in \( O_1 \) has incentive to claim a locked asset in \( L_2 \).
- For each asset locked in \( L_1 \), there exists at least one party in \( P \) has an incentive to claim it.
- The time lock duration can be determined by the parties based on the environmental considerations to ensure that the claimers are left with sufficient time.
- The completion time of the fair MPC protocol is predictable.

CLAIM 1. MPHTLC is atomic according to Definition 2.2.

Proof. We will start by arguing atomicity for the variant of MPHTLC where there is a single transaction in \( L_1 \) (respectively \( L_2 \)) which locks all the assets in \( \mathcal{AE}_1 \) (respectively \( \mathcal{AE}_2 \)). The honest parties (that follow the protocol) in \( O_1 \) proceed with the MPC protocol only if the contracts are appropriate in \( L_1 \) and \( L_2 \), and if they proceed, the fairness property of the MPC protocol ensures that all or none of the parties in \( O_1 \) obtain the pre-image. If none of them obtain the pre-image, then all assets in \( \mathcal{AE}_2 \) and later the ones in \( \mathcal{AE}_1 \) revert to their initial owners. And if all the parties obtain the pre-image, since at least one of them has the incentive to do the claim in \( L_2 \), the assets in \( \mathcal{AE}_2 \) would go to the final owners according to \( FO_2 \). And on seeing the pre-image used, a party that has an incentive to claim a locked asset in \( L_1 \) (we assumed there exists at least one) does so. The protocol allows sufficient time for this party to succeed with the claim in \( L_1 \), and hence the assets in \( \mathcal{AE}_1 \) would also go their final owners as prescribed by \( FO_1 \).

In the variant where each asset is locked and claimed via separate transactions, the extra time available for parties not in \( O_1 \) facilitates their asset claims even if no party in \( O_1 \) submits a claim in \( L_2 \) until very close to their timeout. The rest of the argument follows, with the help of our assumption that there exists at least one party in \( P \) to have the incentive to claim each locked asset in \( L_1 \). □

CLAIM 2. MPHTLC results in a Nash equilibrium for parties engaged in a set of asset swaps (gCLSs).
We provide an informal proof of this claim using a high-level game-theoretic argument, based on a proof in Belotti et al. [9] that conventional HTLC results in Nash equilibrium. We limit $G_{AE}$ scenarios under consideration to those involving only gCLSs (i.e., all parties are involved in a set of swaps across 2 ledgers, like the scenarios in Figures 3 and 4). We argue that if none of the target co-owners of an asset $a$ (i.e., $FO_2(a)$) bother to claim it in Step 5 (after completing Step 4 and revealing the secret), then it is guaranteed that at least one or more of these co-owners always get cheated by one or more other co-owners, who can collude with current co-owners of $a$ (i.e., $IO_2(a)$) in $L_2$. (This is the hazard we identified in Section 2.6 and avoided in MPHTLC.)

We informally prove our argument with reference to the $gCLS$ illustrated in Figure 3, where multiple co-owners of a single asset in one ledger are attempting to swap another single asset in the other ledger with a single owner. Let us follow the MPHTLC protocol applied to this scenario (see Section 3.3). Let’s assume the protocol has proceeded as expected until the end of Step 4. Now, if neither $X$ nor $W$ bothers to claim $N$ in $L_2$ before time $T/2$ elapses, $Y$’s lock expires. Now, one of the co-owners of $M$ (say $W$) can collude with $Y$ to obtain $N$ all for itself (excluding $X$) via a hash lock using the same $H$. Then it proceeds to reveal secret $s$, and claims $N$. $Y$ in turn can claim $M$ in $L_1$ using $s$ before $T$ elapses.

But note that this fraud on the part of $W$ requires it to race $X$ to collude with $Y$, and there is no guarantee that it will win. The loser of this race stands to lose all of $N$ instead of a co-ownership of $N$, which it was guaranteed to get had it followed protocol (i.e., Step 5). Therefore, it is in the interest of both $W$ and $X$ to reveal the secret in Step 4 rather than let $T/2$ elapse without claiming $N$. As we assumed that all parties in a $G_{AE}$ are rational, none of them would pick the alternate strategy described above. Speaking generally, at least one member of $O_1$ is guaranteed to reveal the secret within $T/2$. Hence, following the MPHTLC protocol results in the best outcome for the parties involved (an equilibrium), and there is no incentive for parties to deviate from it.

5 IMPLEMENTATION

Any DLT that can support HTLC can also support MPHTLC through simple changes in the core logic of the locking and claiming modules (DLT’s smart contract). For a DLT to support MPHTLC (or plain HTLC), it needs to support the locking (or freezing) of state for a finite period time (a time lock).

A typical DLT application model has 2 layers: the Contracts layer has business logic in contracts which run on peers and update state through consensus, whereas the Applications layer consists of client applications which invoke transactions on contracts. Any asset exchange protocol (HTLC or MPHTLC) requires implementation in both layers to protect asset integrity against Byzantine failures; just an Applications layer implementation without decentralized trust (consensus) guarantees cannot protect asset integrity. Core MPHTLC capabilities of locking, claiming, and signature verifications can be built as smart contracts while client layer apps can submit lock and claim transaction requests to these contracts.

We will show how an existing atomic swap capability built on HTLC can be augmented to support MPHTLC between permissioned DLTs like Hyperledger Fabric and Corda. From several interoperability framework candidates (Polkadot [44], Cosmos [32], Cactus [33], and Weaver [3]), we picked Hyperledger Labs Weaver [3], which supports HTLC and does not require changes to Fabric or Corda. (Note: our protocol can be implemented on a permissionless network too, as long as the network supports conventional HTLC.)

For Fabric, Weaver supports HTLC through: (i) a special chaincode (contract) called the Interop Chaincode that contains hash-time locks, and asset claim operations, and (ii) client library (API/SDK) to trigger lock and claim transactions from the Applications layer (see Figure 8). Time locks are enforced in contract logic by comparing the timestamp presented in a claim transaction to a peer’s local time; the assumption is that peers’ local times are approximately in sync and therefore a consensus on expiration can be reached. Any asset management application’s chaincode needs to be modified only to trigger locks and claims by invoking the Interop Chaincode. The client application can then submit asset lock and claim.
instructions to its chaincode using the Weaver API and libraries, and expose hashes and secrets after revelation via API functions.

We implemented our protocol by creating a fork\(^1\) of open source Weaver repository. To support MPHTLC in Fabric, we implemented the capabilities described in Section 3.1 directly in the Weaver Interop Chaincode and client SDK. Application developers will need to change very little (just additional API calls in both layers) apart from enforcing the properties of asset co-ownerships.

In Corda, CorDapps deployed on network nodes scope business logic in the Contracts layer and flows (in the Applications layer). To support HTLC, Weaver offers a special Interop CorDapp that contains features similar to those described earlier for Fabric (locks, claims, and time lock enforcement). Any CorDapp that manages assets must, as in the Fabric case, be augmented to exercise the Interop CorDapp (contract features and client libraries). To support MPHTLC in Corda using Weaver, we modified the Interop CorDapp to create a flow so that multiple co-owners (instead of a single one) in a GAE instance sign the lock transactions (Steps 2 and 3 in Section 3.1), while multiple co-owners (instead of a single one) sign the claims (Steps 5 and 6 in Section 3.1). As an aside, multiple co-owners can reclaim/unlock an asset if it is unclaimed before timeout. CorDapp developers need only insert calls to these bulk lock/claim/unlock functions in their code.

Experimental Evaluation: We evaluated our Weaver implementation of GAE by creating a sample application for co-owned assets in both Corda and Fabric. We ran our experiments on a Virtual Machine with 8-cores of Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz, 16GB RAM, and 64-bit Ubuntu 18.04 as the OS. Table 3 reports the latency for locking an asset, querying a locked asset state, claim, and unlock. Latency is computed as the time taken by the respective API (SDK) calls to complete execution. 2nd (Fabric 2P) and 3rd (Corda 2P) columns in Table 3 report latencies for asset exchange operations for two parties co-owning one shared asset before and after the asset exchange. We also observe that the time required for the API execution is proportional to the number of parties involved in each of these transactions (lock/claim/unlock) since we need to collect the consent from all these parties. We expect the time to run the MPC tasks \(F_1\) and \(F_2\) will be about a second and a few milliseconds respectively (by extrapolating the results in [17]). MPC overhead will increase the overall operational latency of MPHTLC, but not by a significant amount. With increase in number of participants, we expect that the runtime operation of \(F_1\) and \(F_2\) will increase, but only by a fraction of one second as suggested by Choudhuri et al. [17].

| Operation | Fabric 2P (s) | Corda 2P(s) |
|-----------|--------------|-------------|
| Locks     | 2.124        | 7.486       |
| Queries   | 0.019        | 0.366       |
| Claims    | 2.121        | 5.898       |
| Unlocks   | 2.128        | 5.892       |

6 RELATED WORK

Atomic cross-chain swaps between a pair of mutually distrusting parties without using trusted intermediaries a well-studied problem [35]. The model and solution have been extended to multiple parties in multiple distinct ledgers [29, 30]. Efforts have been made to add robustness to crash faults and address vulnerabilities in HTLC-like solutions [46, 48]. But all of these works assume single-owned assets and a single pair of assets across a bilateral link; none of these works consider co-ownerships or multiple assets on a ledger like we do. Therefore, none of the proposed solutions can directly work for our setting, nor can the graph model in [29] be directly extended to model our scenarios. However, the three attributes of a cross-chain atomic swap protocol defined by Herlihy in [29] in terms of the guarantees that one such protocol offers are also applicable to our proposed MPHTLC protocol. There also exist several HTLC implementations ([23, 38, 41]), but none support scenarios involving co-owned assets.

Some of these works address threats that are orthogonal to the threats we address. E.g., in [46], Xue and Herlihy handle sore loser (or lockup gifting attacks [28]) in n-party swaps, where one party decides to halt participation midway, leaving the other party’s locked funds unclaimed for a long duration. Our contribution, distinct from theirs, is to extrapolate the basic two-party HTLC model to handle multiple assets and co-owners and provide a solution that ensures atomicity and asset integrity. MPHTLC is susceptible to sore loser attacks too, but Xue and Herlihy’s technique for single-owned assets (associating premiums to escrows and paying these premiums to counterparties upon refunding) [46] will be equally effective for MPHTLC. Analysis and implementation of MPHTLC handling sore loser attacks is beyond the scope of this paper though. As an aside, this also allows us to sidestep the question of external market prices of assets impacting the exchange protocol.

In literature, we find other game-theoretic analyses of HTLC-based cross-chain atomic swaps [9, 45] as well as DLT-agnostic and cryptocurrency-agnostic techniques for universal atomic swaps using transaction signature verification [42]. But none of these works analyze atomic swaps involving assets co-owned by a group of mutually distrusting parties, as we do. Uniquely, our work prevents co-owners of an asset swapping it for another asset without the consent of all the co-owners of that asset.

\(^1\)github.com/mphtlc/weaver-dlt-interoperability

Figure 8: Fabric Network and Decentralized App Architecture

AFT '22, September 19–21, 2022, Cambridge, MA, USA
7 CONCLUSION AND FUTURE WORK

Cross-chain atomic swaps and the HTLC protocol have been studied in recent years. In this paper, we have presented a general asset exchange model (GAE) whereby assets can be co-owned and multiple assets can be simultaneously exchanged. We have shown that HTLC cannot be applied directly to fulfill GAE exchanges because of potential for collusion and fraud. We have presented a solution, MPHTLC (Multi-Party Hash Time Locked Contract), for GAE, and analyzed its correctness and atomicity properties. We have demonstrated how the protocol can be easily implemented in the Weaver interoperability framework. We intend to demonstrate the practical worth of MPHTLC in DeFi scenarios by implementing our solution contracts on a permissionless network like Ethereum. Lastly, our conjecture is that MPHTLC can be extrapolated to multiple ledgers, and we will investigate this in future work. Please refer to [34] for a full length version of this paper.

REFERENCES

[1] 2019. Introduction to Token SDK in Corda. https://www.corda.net/blog/introduction-to-token-sdk-in-corda/ Published on 16-Jul-2019.
[2] 2021. Hyperledger Fabric Token SDK. https://labs.hyperledger.org/labs/fabric-token-sdk.html Accessed on 15-Dec-2021.
[3] 2019. Introduction to Token SDK in Corda. https://www.corda.net/blog/introduction-to-token-sdk-in-corda/ Published on 16-Jul-2019.
[4] Enryss Abbe, Dushyant Behl, Chander Govindarajan, Yining Hu, Dilesh Karunanmoorthy, Petr Novotný, Vinayaka Pandit, Venkatraman Ramakrishna, and Christian Vecchiola. 2019. Enabling Enterprise Blockchain Interoperability with Trusted Data Transfer (Industry Track). In Middleware. ACM, 29–35.
[5] Elin Androulaki, Artem Rager, Varta Bortnikov, Christian Cachin, Konstantinos Christidis, Angelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas. 2016. Fair and Robust Multi-party Computation Using a Global Transaction Ledger. In EUROCRYPT II. 357–374.
[6] Testo 1982. Protocols for Secure Computations (Extended Abstract). In STOC. ACM, 30:1–30:15.
[7] 2021. Weaver: DLT Interoperability (Hyperledger Labs). https://github.com/hyperledger-labs/weaver-dlt-interoperability Accessed on 16-Aug-2022.
[8] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2022. Elliptic Curve Digital Signature Algorithms (ECDSA) for Digital Signatures. (Extended Abstract). In EUROCRYPT. 591–606.
[9] Carsten Baum, Bernardo David, and Rafael Dowlesi. 2020. Insured MPC: Efficient Secure Computation with Financial Penalties. In FC. 404–420.
[10] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2022. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. ACM Comput. Surv. 54, 8 (2022), 166:1–166:41. doi:10.1145/3471140
[11] Marimma Belotti, Stefano Moretti, Maria Florina Butucaru, and Stefano Secchi. 2020. Game Theoretical Analysis of Cross-Chain Swaps. In (ICBCD). 30:1–30:15.
[12] Michael Bent-Or, Shafi Goldwasser, and Avi Wigderson. 1988. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract). In STOC. 1–10.
[13] Idolo Bentov and Ittai Kaminer. 2014. How to Use Bitcoin to Design Fair Protocols. In CRYPTO II. 421–439.
[14] Bitcoin. 2021. Bitcoin Script. https://en.bitcoin.it/wiki/Script Accessed on 10-Dec-2021.
[15] Manuel Blum. 1983. How to Exchange (Secret) Keys. ACM Trans. Comput. Syst. 1, 2 (1983), 173–193.
[16] Wietse Bronkema. 2020. Multi Signature. https://medium.com/mycrypto/introduction-to-multisig-contracts-33d5b25134b2 Published on 16-Jan-2020.
[17] Vitalik Buterin. 2015. Ethereum Whitepaper. https://ethereuim.org/en/ whitepaper/ Accessed on 10-Dec-2021.
[18] Banque de France. 2021. Experiment on the use of Central Bank Digital Currency (CBDC). https://www.banque-france.fr/en/communication-de-presse/experiment-use-central-bank-digital-currency-cbdc.
[19] Decred. 2017. Decred-compatible cross-chain atomic swapping. https://github.com/decred/atomicswap.
[20] Jiahua Xu, Damien Ackerer, and Alevtina Dubovitskaya. 2021. A Game-Theoretic Analysis of Cross-Chain Atomic Swaps with HTLCs. In (ICDCS).
[21] Ms Emily Dawson. 2016. ISO/TC 307: Blockchain and distributed ledger technologies. https://www.iso.org/committee/6266604.html.
[22] Andrey Sergeenkov. 2021. A Beginner's Guide to Atomic Swaps. https://www.whitepaper.cryptocurrency.com/document/582/cosmos-whitepaper Published on 15-Dec-2021.