LedgerHedger: Gas Reservation for Smart-Contract Security

Itay Tsabary
itaytsabary@gmail.com
Technion and IC3, Israel

Alex Manuskin
alex@manuskin.org
Israel

Ittay Eyal
ittay@technion.ac.il
Technion and IC3, Israel

ABSTRACT

Smart-contract ledger platforms, like Ethereum, rate-limit their workload with incentives. Users issue orders, called *transactions*, with assigned fees, and system operators, called *miners*, confirm them and receive the fees. The combination of limited throughput and varying demand results in a volatile fee market, where underpaying transactions are not confirmed. However, the security of prominent smart contracts, securing billions of dollars, critically relies on their transactions being confirmed in specific, future time frames. Despite theoretical and practical active efforts, guaranteeing timely confirmation remained an open problem.

We present LedgerHedger, a two-party mechanism for assuring that a transaction will be confirmed in a target time frame. As the name implies, LedgerHedger employs hedging: An issuing party pays for a transaction in advance; the other party commits to bearing its required fee, even if it rises above the paid amount.

Unlike regulated markets, there are no external enforcers, and the committing party can technically break her commitment. Due to the amounts at stake, relying on her altruism does not suffice. Therefore, LedgerHedger uses a combination of collateral deposits, giving rise to a game. The contract requires the issuer to deposit her payment and the committing party to deposit a collateral. During the target time frame, the latter should confirm the issuer's transaction if it exists, but is also capable of withdrawing the payment and the collateral if not.

For a wide range of parameter values there is a subgame perfect equilibrium where both parties are incentivized to act as desired. We implement LedgerHedger and deploy it on an Ethereum test network, showing its efficacy and minor overhead.

CCS CONCEPTS

• Security and privacy → Distributed systems security; **Security protocols**; **Economics of security and privacy**.

KEYWORDS

Blockchains; Cryptocurrency; Smart Contracts; Hedging; Gas Price

1 INTRODUCTION

Decentralized smart-contract platforms like Ethereum [21, 155], Solana [157], Avalanche [122, 123] and Binance Smart Chain [15] have reached market caps of hundreds of billions of dollars [32]. These systems facilitate *transactions* of virtual *cryptocurrency tokens* among their users. They run *smart contracts* – stateful programs that users can interact with using the transactions. For a transaction to take effect it needs to be *confirmed* by one of the system operators, called *miners*; those place the transaction in a ledger called a *blockchain*.

The blockchain has a limited transaction throughput [38, 40, 155]. Therefore, transaction *issuers* assign *fees* to their transactions, paid to the confirming miner. Miners prioritize transactions by their fees, ignoring those that offer lower amounts. Due to the varying demand [37, 57, 69, 100, 130, 132, 146], the required confirmation fee at a future time frame is unknown and volatile [4, 74], e.g., doubles itself within day.

This unpredictability is not just an inconvenience, but a security concern. Many smart-contract applications, valued in billions of dollars [33, 34], rely on their transactions being confirmed in a timely manner (§2). These include *optimistic* and *zero-knowledge rollups* [11, 22, 61, 73, 78, 83, 93, 107, 134, 149], *off-chain channels* [41, 46, 47, 65, 95, 96, 114, 116], *atomic swaps* [72, 88, 97, 145, 156, 162], *vaults* [19, 94, 99, 158], and *contingent payments* [9, 20, 23, 58, 91]. For any of the above applications, price surges can result with either safety or liveness violations, despite previous progress in addressing the issue [10, 84, 87, 92, 126].

We present LedgerHedger, a blockchain reservation smart contract, conducted between a *Buyer* (transaction issuer) and a *Seller* (naturally, but not necessarily, a miner). *Buyer* and *Seller* agree on a predetermined fee for a future time frame, guaranteeing a future transaction inclusion despite the fee market volatility.

To reason about LedgerHedger, we use a model (§3) with an append-only log of transactions called the blockchain. Miners batch transactions in *blocks*, and append the blocks to the blockchain; this confirms the added transactions. Transactions consume system resources, measured in *gas*. Each block has a *gas-price*, a tokens-per-gas-unit metric indicating the required transaction fee for confirmation based on a transaction's gas consumption.

We consider two system participants: a *Seller* with gas allocation at a specific, future time frame, and a *Buyer*, interested in having a transaction confirmed within that time frame. We use a common price fluctuation model for the stochastic future *gas-price*, which we validate using historical Ethereum data.

The LedgerHedger mechanism (§4) employs hedging. In regulated markets, hedging contracts are enforced by external measures, e.g., courts. In a decentralized cryptocurrency system, only the miners, but not users, decide on transaction confirmation, making them the sole enforcers of any contract. Faced with clear incentives as potential contract participants, the inherent power asymmetry invalidates solutions that rely on parties' altruistic behavior [104].

LedgerHedger overcomes this by incentivizing honest behavior of both parties, despite their disparate capabilities. For that, *Seller* deposits a collateral as part of the contract initiation [6, 45, 140], which is later returned only if she abides by the contract. LedgerHedger also protects *Seller*, ensuring she is paid even if *Buyer* misbehaves. Nonetheless, it is *Seller*'s best response to have *Buyer*'s transaction confirmed if it is available.

The contract operates in two phases. In the first, *setup* phase, *Buyer* initiates the contract, setting its parameters, and then *Seller* accepts it. Note that *Buyer* does not commit to a transaction yet. In the second, *exec* phase, *Buyer* publishes her transaction, and *Seller* has it confirmed through the contract.

We analyze the incentives of *Buyer* and *Seller* as a game with two phases (§5). In the first phase, *Buyer* and *Seller* choose whether to engage in a LedgerHedger contract or to wait without hedging. Then, when the target interval arrives, if there exists a contract, *Buyer* and *Seller* can interact with it; otherwise, they can publish or confirm transactions at the market *gas-price*.

The players' *strategies*, along with the stochastic market *gas-price*, determine the number of tokens each player has at the game conclusion. *Buyer* and *Seller* are *risk averse* [27, 28, 35, 75], that is, their utilities are concave functions of their token holdings.

We analyze the game using the *subgame-perfect-equilibrium (SPE)* solution concept (§6), suitable for its dynamic, turn-based nature. A SPE comprises a strategy of *Buyer* and a strategy of *Seller* such that both cannot increase their utility by deviating at any stage of the game. We show that engaging in the contract and fulfilling it is a SPE for a wide range of practical parameters.

We conclude the analysis by showing that LedgerHedger is applicable for a *Seller* that is a miner, regardless if block generators are chosen probabilistically, as in Ethereum, or deterministically, as in planned Central Bank Digital Currencies (CBDCs) [2, 60] (§7). Specifically, for probabilistic systems, we show that for practical LedgerHedger parameter values, a mining *Seller* creates a block with overwhelming probability. We also show how a non-mining *Seller* can use the transaction-fee mechanism to facilitate the required actions of LedgerHedger.

We demonstrate LedgerHedger's efficacy by implementing it as an Ethereum smart contract and deploying it on a test network (§8). LedgerHedger's overhead is low – three orders of magnitude lower than the hedged gas for prevalent use cases.

In summary, our contributions are: (1) a *gas-price* fluctuation model, verified with Ethereum measurements; (2) LedgerHedger, the first mechanism for addressing the prevalent requirement of timely blockchain confirmation; (3) an analysis showing LedgerHedger's security and applicability for a wide range of parameters; and (4) an open-source implementation for Ethereum, deployed on a test network.

2 RELATED WORK

We are not aware of previous work that guarantees future transaction confirmation in a timely manner, despite this being a security requirement of prominent cryptocurrency applications. We review several of these applications (e.g., roll-ups) in Appendix A.

Recently, Lotem et al. [87] suggested extending Ethereum's contract capabilities to allow applications to monitor the blockchain congestion level. The applications can then extend their timeouts in case of congestion. This mechanism replaces safety with liveness violations – the timeout does not expire, but the application cannot progress to its post-timeout state. In contrast, LedgerHedger assures confirmation at the desired interval, and is directly applicable to Ethereum and similar blockchains.

Infura's any.sender [92] service gets issuers' transactions confirmed at competitive fees using estimation and dynamic fee update. Unlike LedgerHedger, it does not address long-term reservation and its necessary mechanisms.

Several projects suggest mitigating *gas-price* changes using so-called *gas-tokens*. These are tokens, managed by designated smart contracts, whose value follows the *gas-price*. To protect against *gas-price* rising (falling), one buys (sells) gas-tokens, and later sells (buys) them. A future transaction issuer can acquire gas-tokens beforehand, and sell them to fund the transaction fees at the desired inclusion time.

The first type of gas tokens [1, 18, 102] was implemented by abusing Ethereum's *gas refund mechanism*, where several operations had negative gas costs. The principle was to deliberately expend gas on storing arbitrary data when the *gas-price* is low, and later, when the *gas-price* rises, delete that data for a gas refund. This method was inefficient, as only about a third of the spent gas is refunded. Moreover, the August 2021 Ethereum upgrade [55] broke this mechanism by changing the refund policy [13, 147]. In contrast, LedgerHedger does not rely on Ethereum's internal implementation, and hence applies to a wide range of systems. Moreover, its overhead is three orders of magnitude less than the hedged amount for practical parameter values.

Another approach for implementing gas tokens is pegging them to the gas value, e.g., *uGAS* [42]. uGAS tokens have month-granularity expiration dates, and their expiration value is set according to an *oracle* [142] – another contract that, by external measures, feeds the median gas price of all Ethereum transactions. Users can deposit and release cryptocurrency to mint and destroy uGAS tokens, respectively. The required cryptocurrency amount, deposit duration and withdrawal availability all depend on a set of variables such as the oracle-reported price and the token availability in the managing contract. Moreover, user deposits may be confiscated in a so-called *liquidation* if their deposit value falls below a certain threshold. Protocols of this kind are susceptible various attacks and manipulations [39, 119, 120, 151, 160, 161], in particular to taking advantage of the oracle [3, 49, 68, 110, 112, 118, 127, 128, 136, 137, 150, 159]. Furthermore, setting the oracle measured time period is nontrivial – short periods make it easy to manipulate, but long periods result with the reported value being inaccurate. In contrast, LedgerHedger does not rely on oracles, and is conducted solely among the two interacting parties, removing the ability to affect its state through the aforementioned manipulations. LedgerHedger also enables arbitrary choice of the target time frame.

The August 2021 [55] update to the Ethereum network applied *Ethereum Improvement Proposal (EIP)* 1559 [126], changing the transaction fee mechanism. EIP1559, along with other work [86, 89, 113, 141, 143, 153], attempts to ease transaction issuers estimation of the required fee solely for the next block; they do not apply (or claim to apply) to further blocks.

Aside from benign price fluctuations, previous work shows the fee market is susceptible to *congestion attacks* [70, 98, 100]. These create multiple transactions that artificially increase the market price, congesting the network, resulting with the time-sensitive transactions being delayed.

LedgerHedger can withstand these attacks or benign market spikes of any magnitude by including a sufficiently-high *Seller* collateral, incentivizing *Seller* to abide by the contract. This guarantees transaction issuers even far-future confirmations at predetermined prices. We emphasize LedgerHedger is functional regardless of the EIP1559 changes.

3 MODEL

To reason about blockchain reservation, we first describe a general model for an underlying blockchain-based cryptocurrency (§3.1). We then present the setup for a future transaction inclusion deal (§3.2) and the stochastic value of fees (§3.3).

3.1 Cryptocurrency System

The blockchain system tracks internal cryptocurrency *tokens* that its *users* can *transact*. To apply their transactions, users broadcast them across a peer-to-peer network. A subset of users, called *miners*, batch transactions in data structures called *blocks*.

Miners add blocks to a global data structure, called the *blockchain*, forming an append-only list of blocks. Blocks have indexes matching their append order, and we denote the i'th block by b_i. A transaction is *confirmed* when it is included in the blockchain.

We follow the common assumption [21, 45, 47, 72, 88, 96, 103, 115, 126, 139, 140] that all miners create blocks according to the above description, and all published transactions and all created blocks are instantaneously available to all system users and miners.

The *system state* is the association of tokens to *smart contracts*, predicates that need to be satisfied in order to transact their associated tokens. Parties infer the state by sequentially parsing the blockchain. Only transactions that satisfy the contract predicates can be confirmed, and we disregard transactions that do not.

The smart-contract predicates can verify that the transaction is digitally signed, for an *existentially unforgeable under chosen message attacks (EU-CMA)* [8, 45, 63, 76, 140] digital signature algorithm; that the transaction is included in a block numbered higher or lower than a parameter; that the transaction transfers a number of tokens; or a combination of the above. We say a user *owns* tokens if she is the only user that is able to satisfy the contract predicate.

Transactions are measured by their *gas* requirement – an internal measure of transaction resource consumption. Each operation in a transaction requires a certain amount of gas, and the total transaction gas is the sum of all operations' gas. When considering a transaction *tx*'s gas requirement, denoted by g_{tx}, we consider it with respect to the system state when it is confirmed.

Each block has a bound on the total gas of its transactions. Transactions may offer tokens as a fee for the including miner. This fee is set by the transaction issuer, determining a non-negative tokens-per-gas ratio, which we denote by π_{tx} for transaction *tx*. Therefore, π_{tx} is a rational number. When confirmed, transaction *tx* pays $g_{tx} \cdot \pi_{tx}$ tokens to the miner that included it in a block.

Miners choose which transactions to include in a block based on their offered π_{tx} values. We refer to the minimal required value to be included in a block by *gas-price*. For simplicity, we assume there are always sufficiently many transactions that offer *gas-price* to exactly fill a block [24, 139], and that any transaction offering at least *gas-price* is confirmed.

3.2 Future Transaction Setup

Consider two system participants, *Buyer* and *Seller*, with the following interests: *Buyer* requires g_{alloc} gas allocated to a transaction of her choice in future blocks; *Seller* has a gas allocation of g_{alloc} in such a suitable block, which she can sell for tokens.

We denote the transaction that *Buyer* wants to be included by $tx_{payload}$, and the relevant block interval for its inclusion by $[b_{start}, b_{end}]$. Note that the content of $tx_{payload}$ is not necessarily known up to b_{start}. We also denote the block interval in which *Buyer* wishes to assure the future allocation by $[b_{init}, b_{acc}]$ such that $init \leq acc < start \leq end$.

3.3 Gas Price

To reason about hedging, one requires a prediction of the commodity future price. We assume the future *gas-price* is drawn from some price distribution. We assume both *Buyer* and *Seller* have perfect knowledge of this distribution.

Previous work [86, 89, 113, 141, 143, 153] provides *gas-price* predictions, but focuses exclusively on prediction for the *next* block. We are not aware of work modeling the *gas-price* for a further future (e.g., a week ahead), hence we assume it follows the prevalent *random-walk price model* [17, 54, 80, 121]. According to this model, the *gas-price* follows a Gaussian random walk, where in each block it changes according to a random sample from a normal distribution $N\left(\mu, \sigma^2\right)$. It follows [111, 148] that the future *gas-price* change after n blocks is also drawn from a normal distribution with parameters $N\left(n \cdot \mu, n \cdot \sigma^2\right)$.

For simplicity, we assume the random walk is without a *drift*, meaning $\mu = 0$. We also assume that σ^2 is small [51], so in the short term the *gas-price* has a low variance.

We validate this model using the Kolmogorov–Smirnov [90] test on historical Ethereum gas prices over a month (Appendix B).

We slightly enhance the price model to neglect rare events. Specifically, the *gas-price* cannot be negative, as that would imply the miner pays users to transact, instead of the obvious option of leaving blocks empty; excessively high *gas-price* is also impossible, as that removes any incentive to transact and renders the system unusable.

In summary, denote by $\mathcal{F}$ the *gas-price* distribution in the target interval. $\mathcal{F}$ is a *truncated* normal distribution [135]; its mean value is the *gas-price* for block b_{init}; its lower tail is truncated such that the *gas-price* is non-negative, and we truncate the upper tail symmetrically with respect to the mean. Denote the *probability density function (PDF)* of $\mathcal{F}$ by $\mathcal{F}_{\text{pdf}}$.

Denote the *gas-price* for block b_{init} by π_{setup}. We assume that $[b_{init}, b_{acc}]$ is relatively short, and make the simplifying assumption that the *gas-price* for this entire interval is π_{setup}. Similarly, we assume that $[b_{start}, b_{end}]$ is relatively short, and denote the *gas-price* for this interval by $\pi_{exec} \sim \mathcal{F}$.

4 LEDGER-HEDGER

We present LedgerHedger, our construction enabling a *Buyer* and a *Seller* to hedge future block gas for a predetermined *gas-price*. We begin by detailing LedgerHedger's design (§4.1), and follow by formalizing its security guarantees (§4.2).

4.1 Ledger-Hedger Design

LedgerHedger operates in two phases, *setup* and *exec*, representing its setup and execution in the block intervals of interest, presented in Figure 1. Throughout the following functions, the contract verifies identities using the EU-CMA digital signature algorithm.

In the *setup* phase, *Buyer* initiates a LedgerHedger instance using a transaction. The initiation sets the contract parameters, including the block ranges in which interactions can be made with

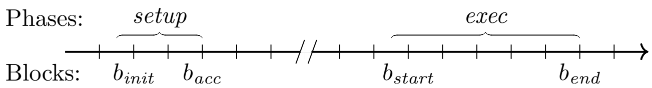


Figure 1: LedgerHedger interaction block ranges.

the contract instance, the required gas for the future transaction, and a required collateral to be deposited by *Seller*. She also deposits the token payment for the future transaction confirmation.

Following its initiation, the contract starts an *acceptance block countdown*, during which a *Seller* can accept it using a transaction. Additionally, accepting the contract requires *Seller* to deposit tokens as a collateral matching the collateral parameter. The collateral is returned conditioned on *Seller* further interacting with the contract. Either if *Seller* accepted the contract, or if the acceptance countdown is completed, the contract accepts no further interactions until the *exec* phase.

Towards or even during the *exec* phase, *Buyer* can publish $tx_{payload}$. This allows *Seller* to *apply* it, executing $tx_{payload}$, and getting the payment and collateral tokens from the contract. This is the main functionality of LedgerHedger – enabling *Seller* to execute a transaction provided by *Buyer*.

Alternatively, *Seller* can *exhaust* the contract, consuming the hedged gas on null operations, and then receiving its tokens. The motivation for this functionality is to enable *Seller* to claim the tokens, regardless if *Buyer* provides a transaction or not; this protects *Seller* from a faulty or malicious *Buyer*. However, the naive solution of letting *Seller* report *Buyer* as faulty is not sufficient: It allows a *Seller* to falsely accuse a correct *Buyer*, getting the contract tokens without providing the confirmation service. By making *Seller* waste equivalent gas, we remove her incentive to do so.

If *Seller* has not accepted the contract, then *Buyer* can *recoup* the contract tokens using a transaction.

LedgerHedger comprises these functions, which we now describe in detail and present in Alg. 1.

Initiate. *Buyer* initiates the contract through the invocation of the *Initiate* function (lines 1–6), setting the contract parameters. These include *acc*, the block number by which *Seller* is required to accept the contract; *start* and *end*, the range in block numbers during which block *Seller* is required to confirm the transaction; g_{alloc}, a positive number of gas units *Buyer* wishes to use; *col*, the non-negative token collateral required by *Seller*; and, ε, an additional non-negative number of tokens that will be transferred to *Seller* for confirming the provided *Buyer* transaction. For simplicity we consider the block confirming the initiation transaction is b_{init}.

The contract verifies the provided parameters are valid according to the above specification, specifically, that the block numbers are ascending, that the gas parameter is positive, and that the token parameters are non-negative (lines 2– 3).

After this verification, the contract derives the offered *payment*: the additional ε tokens are subtracted from the sent tokens *sentTokens*. This is the number of tokens that will be paid to *Seller* for either executing a transaction or exhausting the contract. This implies the contract's offered *gas-price* is $\pi_{contract} = \frac{payment}{g_{alloc}}$ (line 4). It also stores the public identifier of *Buyer* as PK_{Buyer} (line 5). Finally, the contract sets its status variable *status* to initiated (line 6), indicating the contract has been initiated, but no further transactions have interacted with it. We denote the gas consumption of the *Initiate* function by g_{init}.

Accept. Once the contract is initiated, a *Seller* can accept it through the invocation of the *Accept* function (lines 6–12). This enables only a single *Seller* to accept the contract, and only before the timeout set by *Buyer* expires. It also requires *Seller* to deposit the requested collateral.

For that, this function first verifies that this invocation is no later than b_{acc} (line 8), that the contract has been initiated, but not further interacted with (line 9), and that the sent tokens collateral suffices (line 10).

The contract then stores *Seller* public identifier as PK_{Seller} (line 11), and updates its status variable *status* to accepted, indicating the contract has been accepted (line 12). We denote the gas consumption of the *Accept* function by g_{accept}.

The previous *Initiate* and *Accept* functions facilitate the initiation and acceptance of LedgerHedger. The following three functions detail its conclusion.

Recoup. The *Recoup* function (lines 12–18) enables *Buyer* to withdraw her deposited tokens from LedgerHedger if no *Seller* accepts it prior to b_{acc}.

For that, it first verifies the invocation is within $[b_{start}, b_{end}]$ (line 14), that the contract is initiated, but no *Seller* had accepted it (line 15), and that the invocation is by *Buyer* (line 15). We discuss earlier recouping in Appendix C.

Then, the contract marks its status completed (line 17), and sends *Buyer* her deposited $payment + \varepsilon$ tokens (line 18). We denote the gas consumption of the *Recoup* function by g_{done}.

Apply. The *Apply* function (lines 18–26) implements the main functionally of LedgerHedger: *Seller* executing a transaction tx_{provided} provided by *Buyer*, and receiving the agreed-upon payment for doing so.

This function takes as an input a transaction tx_{provided}, and first verifies tx_{provided} was issued by *Buyer* (line 20). Then, it verifies the invocation is within $[b_{start}, b_{end}]$ (line 21), that *Seller* had previously accepted (line 22), and that the invocation is by *Seller* (line 23).

The contract then executes the operations of tx_{provided} as a subroutine (line 24), marks its status completed (line 32), and sends $payment + \varepsilon + col$ tokens to *Seller* (line 33).

Considering all operations except the execution of tx_{provided}, the *Apply* function performs similar operations to those of *Recoup*. We therefore consider its gas consumption, aside from execution of tx_{provided}, is also g_{done}.

Exhaust. The *Exhaust* function (lines 26–33) allows *Seller* to get $payment+col$ tokens for expending g_{alloc} gas during the required block interval. Its goal is to protect *Seller* from a spiteful *Buyer*, specifically from the case where *Buyer* does not publish a tx_{provided} transaction, or publishes ones that consume more than g_{alloc} gas.

When *Exhaust* is invoked, the contract first verifies the invocation is within $[b_{start}, b_{end}]$ (line 28), that *Seller* had previously accepted (line 29), and that the invocation is by *Seller* (line 30).

The contract then performs null operations consuming g_{alloc} gas (line 31), marks its status completed (line 32), and sends *Seller* $payment + col$ tokens (line 33).

Algorithm 1: LedgerHedger

Parameter : *acc, start, end*, block number operation ranges
Parameter : g_{alloc}, required gas
Parameter : *col*, the required collateral by *Seller*
Parameter : *payment*, payment for execution
Parameter : ε, additional payment for *successful* execution.
Global Variable : *current*, current block number
Variable : $status \leftarrow \bot$, contract status variable
Variable : $PK_{Seller} \leftarrow \bot$, public identifier of *Seller*
Variable : $PK_{Buyer} \leftarrow \bot$, public identifier of *Buyer*

Function `Initiate`(*txIssuer, sentTokens*; *acc, start, end*, g_{alloc}, *col*, ε):
  Assert: $current \leq acc < start \leq end$
  Assert: $g_{alloc} > 0$, $col \geq 0$, $\varepsilon \geq 0$, $sentTokens \geq \varepsilon$
  Set *acc, start, end*, g_{alloc}, *col* from inputs, $payment \leftarrow sentTokens - \varepsilon$
  $PK_{Buyer} \leftarrow txIssuer$
  $status \leftarrow$ initiated

Function `Accept`(*txIssuer, sentTokens*):
  Assert: $current \leq acc$
  Assert: $status = initiated$
  Assert: $sentTokens \geq col$
  $PK_{Seller} \leftarrow txIssuer$
  $status \leftarrow$ accepted

Function `Recoup`(*txIssuer, sentTokens*):
  Assert: $start \leq current \leq end$
  Assert: $status = initiated$
  Assert: $PK_{Buyer} = txIssuer$
  $status \leftarrow$ completed
  Send $payment + \varepsilon$ to PK_{Buyer}

Function `Apply`(*txIssuer, sentTokens*; $tx_{provided}$):
  Assert: $tx_{provided}$ *was issued by* PK_{Buyer}
  Assert: $start \leq current \leq end$
  Assert: $status = accepted$
  Assert: $PK_{Seller} = txIssuer$
  Execute the operations of tx_{provided}
  $status \leftarrow$ completed
  Send $payment + \varepsilon + col$ to PK_{Seller}

Function `Exhaust`(*txIssuer, sentTokens*):
  Assert: $start \leq current \leq end$
  Assert: $status = accepted$
  Assert: $PK_{Seller} = txIssuer$
  Perform null operations summing to g_{alloc} gas
  $status \leftarrow$ completed
  Send $payment + col$ to PK_{Seller}

Note that executing *Exhaust* results with the remaining ε being forever locked in the contract.

Similarly, the operations of *Exhaust*, aside from the exhaustion, resemble those of *Recoup*. Therefore its gas cost, aside from the exhaustion, is also g_{done}.

4.2 Possible Ledger-Hedger Interactions

Following immediately from the functions of LedgerHedger (Alg. 1) and the EU-CMA digital signature algorithm, we get the following properties, which define all possible interactions of the participants with the contract:

Contract parameters are immutable. The contract parameters are set only once by *Buyer* at its initiation and are immutable.

These parameters are set before π_{exec} is drawn. Moreover, *Buyer* must transfer $payment + \varepsilon$ tokens to the contract at its initiation.

Single Seller accepting. Only a single *Seller* can accept the contract, only after it is initiated, and only before b_{acc}. That means *Seller* can accept the contract only after its parameters are set, and only after *Buyer* has already transferred $payment + \varepsilon$ tokens to it. *Seller* can accept the contract only before π_{exec} is known, and only by transferring *col* tokens.

Contract token extraction. Extracting the contract tokens requires successfully invoking either *Recoup*, *Apply* or *Exhaust*, which all require to be invoked during $[b_{start}, b_{end}]$.

Buyer extracting tokens. Only *Buyer* can successfully invoke *Recoup*, only during $[b_{start}, b_{end}]$, and only if *Seller* had not accepted the contract.

Seller extracting tokens. Only *Seller* that accepted the contract can successfully invoke *Apply* or *Exhaust*, but not both. For either function, a successful invocation can be made only during $[b_{start}, b_{end}]$, and only if *Seller* had accepted the contract before b_{start} (specifically, before b_{acc} which precedes b_{start}).

Additionally, *Seller* can only successfully invoke *Apply* by providing a transaction $tx_{payload}$ published by *Buyer*.

5 GAME DEFINITION

The need of *Buyer* to confirm a future transaction, *Seller* having a future gas allocation, and the existence of LedgerHedger contract, all give rise to a game played by *Buyer* and *Seller*. The game, denoted by Γ, begins when the blockchain is at the block preceding b_{init}, and progresses with the players taking *actions*.

We present the possible *game states* and *actions* (§5.1), consider player *strategies* (§5.2) and their resultant player *utilities* (§5.3).

5.1 States and Actions

The game takes places during two *phases*. The first phase, denoted by φ_{setup}, describes the creation of blocks b_{init} to b_{acc}. The second phase, denoted by φ_{exec}, describes the creation of blocks b_{start} to b_{end}.

The *game state* comprises the player tokens, the contracts they possibly engage with, their published transactions, the current phase, and the *gas-price*. Figure 2 summarizes the game progress.

Broadly speaking, *Buyer* and *Seller* can set a LedgerHedger contract at the game start for φ_{exec}, and then execute it. Alternatively, *Buyer* and *Seller* can wait for φ_{exec}, and then *Buyer* can publish $tx_{payload}$ as any other transaction for confirmation, and *Seller* can use her gas allocation to confirm any transaction.

We ignore nonsensical, obviously dominated or unrelated actions [152] such as either party sharing her private key, *Seller* not using her gas allocation, or either player publishing unrelated transactions. We assume both parties initially have sufficiently many tokens to support the following actions.

The value of π_{setup} is known to *Buyer* and *Seller* at the game beginning. However, the value of π_{exec} is drawn by *Nature* from $\mathcal{F}$ just before φ_{exec} starts. After the players publish and confirm transactions for φ_{exec} the game is concluded.

The game starts in state *InitLH* (in φ_{setup}), where *Buyer* can choose to initiate a LedgerHedger instance (action a_{init}), and choose its parameters. She incurs the initiation cost $g_{init} \cdot \pi_{setup}$, deposits the payment $payment + \varepsilon$, and the game transitions to state *AcceptLH*. Alternatively, she can choose to refrain from initiating (action a_{wait}), incurring no costs, and the game transitions to game state *NoLH*.

Game state *NoLH* (in φ_{exec}) takes place after *Nature* draws $\pi_{exec} \sim \mathcal{F}$. In this state, *Buyer* can pay the *gas-price* π_{exec} to have $tx_{payload}$ confirmed (action a_{pubTx}), incurring the fee cost $g_{alloc} \cdot \pi_{exec}$, but have $tx_{payload}$ confirmed. Alternatively, she

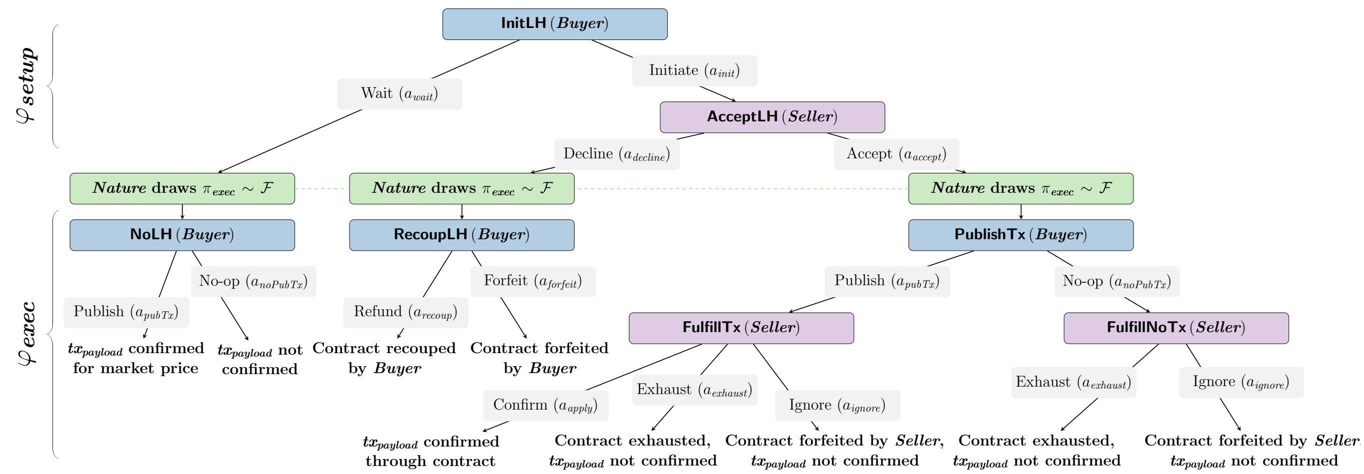


Figure 2: Γ game states, actions, and conclusion.

can do nothing, incurring no costs, but receiving no reward. *Seller* sells her g_{alloc} gas for the *gas-price* π_{exec}, earning $g_{alloc} \cdot \pi_{exec}$.

In game state *AcceptLH* (φ_{setup}) *Seller* chooses whether to accept the LedgerHedger instance (action a_{accept}). To accept, *Seller* publishes a transaction that invokes the *Accept* function, deposits the *col* collateral tokens, and incurs a cost of $g_{accept} \cdot \pi_{setup}$. The game then transitions to state *PublishTx*. Alternatively, she can decline by simply ignoring it ($a_{decline}$), leading to *RecoupLH*.

Game state *RecoupLH* is in φ_{exec}, after *Nature* draws $\pi_{exec} \sim \mathcal{F}$. *Buyer* can choose to withdraw her deposited $payment + \varepsilon$ tokens from the declined LedgerHedger instance (action a_{recoup}), incurring the withdrawal transaction fee cost $g_{done} \cdot \pi_{exec}$. If not, she can simply ignore it (action $a_{forfeit}$), forfeiting the $payment + \varepsilon$ tokens. As in *NoLH*, *Buyer* can also publish $tx_{payload}$, and *Seller* can also confirm other transactions; the former costs *Buyer* $g_{alloc} \cdot \pi_{exec}$ tokens, but has $tx_{payload}$ confirmed, and the latter rewards *Seller* with $g_{alloc} \cdot \pi_{exec}$.

Game state *PublishTx* is in φ_{exec}, after *Nature* draws $\pi_{exec} \sim \mathcal{F}$. Here *Buyer* can publish transactions for *Seller* to confirm using the contract's *Apply* function . These transactions do need not to further incentivize a miner to confirm them, hence offer no fee. However, *Buyer* can publish multiple transactions for *Seller* to choose from, and *Seller* is clearly incentivized to consider only the transaction requiring the least gas. So, we consider the following two cases. First, *Buyer* chooses not to publish a transaction at all (action $a_{noPubTx}$), incurring no costs, leading to *FulfillNoTx*. Alternatively, *Buyer* publishes $tx_{payload}$ (action a_{pubTx}), leading to the *FulfillTx* state.

In game states *FulfillNoTx* and *FulfillTx* (φ_{exec}) *Seller* can choose to invoke the contract's *Exhaust* function (action $a_{exhaust}$). This transfers $payment + col$ tokens to *Seller*, but requires g_{alloc} for the null operations and g_{done} gas for the remaining operations (verification, token transfer, etc.). Note this action exceeds the g_{alloc} quota of *Seller*, requiring *Seller* to pay fees for g_{done}, resulting in an incurred cost of $g_{done} \cdot \pi_{exec}$. Action $a_{exhaust}$ results with $tx_{payload}$ not confirmed, so *Buyer* can have it included by paying the *gas-price*.

Alternatively, *Seller* can choose to ignore the contract (action a_{ignore}), receiving no tokens but incurring no additional costs. Action a_{ignore} results with *Seller* not using her gas, which she can sell for the *gas-price* of π_{exec}. It also results with $tx_{payload}$ not being confirmed through the contract, so *Buyer* can pay the current *gas-price* π_{exec} to have it confirmed.

Finally, in *FulfillTx*, *Seller* can choose to invoke the contract's *Apply* function, using the published transaction $tx_{payload}$. This rewards *Seller* with $payment + \varepsilon + col$ tokens, but requires $g_{pub} + g_{done}$ gas, resulting in an incurred cost of $\left(g_{alloc} - \left(g_{pub} + g_{done}\right)\right) \cdot \pi_{exec}$.

Note 1. *We assume that Seller verifies the execution of $tx_{payload}$ and is content with its results (as in, e.g., [25, 64, 67]). Namely, Seller verifies $tx_{payload}$ does not terminate the contract nor transfer away its funds.*

Note 2. *LedgerHedger works whether Seller is a miner or not: If she is a miner she can use some of her block's gas to confirm $tx_{payload}$ and get the contract tokens, forfeiting other transactions that pay the market price (cost of loss-of-opportunity); if she is not, she can confirm $tx_{payload}$ and get the contract tokens by publishing a transaction that pays the gas-price to a miner (cost of the transaction fee). In both cases, the cost is $(g_{alloc} + g_{done}) \cdot \pi_{exec}$, and the remainder of the game-theoretic analysis is identical.*

As in the *NoLH* and the *RecoupLH* states, if $tx_{payload}$ is not confirmed by *Seller* as part of the contract (i.e., if *Seller* plays $a_{exhaust}$ or a_{ignore}), then *Buyer* can pay to have $tx_{payload}$ included at market price, resulting with $tx_{payload}$ confirmed and a cost of $g_{alloc} \cdot \pi_{exec}$. Any of these actions concludes the game.

5.2 Strategy

Each player has a *strategy*, mapping each game state to an action. The action space for *Buyer* comprises which transactions to publish and when to do so. For *Seller*, it comprises which transactions to publish, when to publish them, and which transactions to confirm using her allotted gas.

We denote by $\bar{s}$ a *strategy profile*, comprising the strategies of *Buyer* and *Seller*.

We denote $\bar{s}\,(state) = a$ if the player's strategy in the profile $\bar{s}$ dictates playing action a in game state *state*. We say a player *follows* strategy profile $\bar{s}$ if at each game state she chooses to play her strategy's mapped action.

5.3 Wealth and Utility

The game concludes with each player having some number of tokens – their resultant *wealth*. We model the exogenous motivation of *Buyer* from having a transaction $tx_{payload}$ that consumes at least g_{alloc} gas confirmed during φ_{exec} as her receiving tokens from doing so, denoting their number by w^{exo}. We capture the player's happiness from having wealth using a *utility* function.

We denote the initially available tokens of *Buyer* and *Seller* by w^{init}_{Buyer} and w^{init}_{Seller}, respectively.

Each player's resultant wealth therefore depends on these values, their paid and received transaction fees, and the values of π_{setup} and π_{exec}.

A player's utility $U : W \to \mathbb{R}$ is a function describing happiness from having W tokens at the game conclusion, including the exogenous motivation w^{exo} for *Buyer*.

We assume both *Seller* and *Buyer* are *risk averse* [5, 30, 44, 82, 85, 117], that is, they value the certainty of their resultant wealth. This implies that they might not prefer to maximize their expected wealth. For example, a risk-averse player might prefer getting 4 tokens with probability 1 over getting 10 token with probability 0.5, despite the latter higher expected value of 5. Risk aversion justifies actions like individuals purchasing insurance [31, 109], or airlines hedging oil prices [36, 71]. Risk and *ambiguity* [48, 138] aversion also capture that players do not have perfect knowledge of $\mathcal{F}$.

The common practice [5, 28, 117] to model risk aversion is using a utility function $U(W)$ with the following two properties: (1) $U(W)$ is strictly increasing in W, meaning a player is strictly happier with having more tokens, and (2) $U(W)$ is concave, where higher curvature implies a stronger risk aversion tendency. Hereinafter, we consider utility functions that meet this definition.

6 ANALYSIS

The goal of our analysis goal is twofold – find contract parameters for which *Buyer* initiates and *Seller* accepts, and, given an initiated and accepted contract, find conditions for *Seller* to confirm the transaction of *Buyer*.

We first specify the solution concept (§6.1): We consider *subgame perfect equilibrium (SPE)*, capturing the dynamic, turn-based nature of the game. We then express the equilibrium strategy as a function of the distribution, the utility functions, and the contract parameters, and prove there are scenarios where engaging and fulfilling the contract is SPE (§6.2):

Theorem 1. *There exists utility functions, a distribution $\mathcal{F}$, and contract gas and token parameters such that: Buyer is incentivized to initiate the contract; Seller is incentivized to accept the initiated contract; Buyer is incentivized to publish $tx_{payload}$ such that $g_{pub} = g_{alloc}$; and, Seller is incentivized to fulfill the contract by confirming $tx_{payload}$.*

Finally, we analyze LedgerHedger using parameters from an operational system, while considering plausible distributions and utility functions, showing its efficacy and applicability in a variety of settings (§6.3).

6.1 Solution Concept

The sequential nature of Γ lends itself to the definition of *subgames*, each capturing the possible extensions starting from a specific state.

We denote by Γ^{player}_{state} the subgame starting at state *state* where *player* $\in \{Buyer, Seller\}$ is to take an action. The game begins with the initial subgame $\Gamma^{Buyer}_{InitLH} = \Gamma$.

We can therefore define the wealth and utility of each player starting in a subgame as follows. Let *Buyer* and *Seller* follow a strategy profile $\bar{s}$ in subgame Γ^{player}_{state}, and let *Nature* draw *gasprice* π_{exec}. We denote the resultant wealth of *Buyer* and of *Seller* by $W_{Buyer}(\pi_{exec}, state, \bar{s})$ and by $W_{Seller}(\pi_{exec}, state, \bar{s})$, respectively. We denote the utility of *Buyer* by $U_{Buyer}\left(W_{Buyer}(\pi_{exec}, state, \bar{s})\right)$ and of *Seller* by $U_{Seller}(W_{Seller}(\pi_{exec}, state, \bar{s}))$, or simply $U_{Buyer}(state, \bar{s})$ and $U_{Seller}(state, \bar{s})$ for succinctness.

We denote the expected utility of *Buyer* and *Seller* when they follow strategy profile $\bar{s}$ starting in Γ^{player}_{state}, over the distribution $\mathcal{F}$, by $\mathbb{E}\left[U_{Buyer}(state, \bar{s})\right]$ and by $\mathbb{E}\left[U_{Seller}(state, \bar{s})\right]$, respectively.

We focus on rational *Buyer* and *Seller* that strive to maximize their expected utility. We assume the players' utility functions, their utility-maximizing tendencies, and the game state are all common knowledge. So, the defined game is of *perfect information* [108, 131].

We are interested in a strategy profile that is a *subgame perfect equilibrium (SPE)* [14, 26, 59, 101, 124, 129, 144, 152]. Intuitively, this means that at any stage of the game both players are content with the action defined in the strategy profile. Formally, SPE is a strategy profile where no player can increase her utility by deviating in any subgame, considering the other player's reaction to such deviation, i.e., Nash equilibrium at every subgame.

We are interested in finding conditions in which the SPE, denoted by $\bar{s}_{\text{spe}}$, results with *Buyer* initiating the contract, *Seller* accepting it, *Buyer* publishing $tx_{payload}$ with $g_{pub} = g_{alloc}$, and *Seller* confirming it.

The common method for finding $\bar{s}_{\text{spe}}$ is using *backward induction* [7, 14, 79, 125], applicable in perfect information and finite games. The analysis begins at the subgames comprising only the last action (e.g., subgames $\Gamma^{Seller}_{FulfillNoTx}$ and $\Gamma^{Seller}_{FulfillTx}$), where the SPE is found by directly comparing the utility from the different possible actions. Then, considering the last player chooses that utility-maximizing action, the second to last subgames are analyzed (e.g., subgame $\Gamma^{Buyer}_{PublishTx}$). This process is repeated recursively until the initial subgame $\left(\Gamma^{Buyer}_{InitLH} = \Gamma\right)$ is analyzed. We move forward to finding $\bar{s}_{\text{spe}}$ in Γ.

6.2 SPE Expressions

We start by expressing the SPE for an initiated and accepted contract (§6.2.1), and then address the initiation (§6.2.2) and acceptance (§6.2.3).

6.2.1 Fulfilling an Initiated and Accepted Contract. The subgame describing possible interactions with the initiated and accepted contract is $\Gamma^{Buyer}_{PublishTx}$, which is played after *Nature* had already drawn π_{exec}. Therefore, any choice of action in $\Gamma^{Buyer}_{PublishTx}$ and its the subsequent subgames results with deterministic wealth for both *Buyer* and *Seller*.

It follows that maximizing the expected utility (by choosing preferable actions) is the same as maximizing the utility. Additionally, since utility functions are monotonic, maximizing the utility is equivalent to maximizing wealth.

Following this observation, we compare the resultant wealth of each action in $\Gamma^{Buyer}_{PublishTx}$ and its the subsequent subgames, presenting a condition on π_{exec}, by which the $\bar{s}_{\text{spe}}$ action is decided.

Throughout the analysis, we assume $\varepsilon = 1$, that is, a single token (we consider different ε values in Appendix C).

Towards the upcoming resultant wealth analysis, recall that in the subgames preceding $\Gamma^{Buyer}_{PublishTx}$, *Buyer* already incurred a cost of $g_{init} \cdot \pi_{setup} + payment + \varepsilon$ for initiating the contract, and *Seller* incurred a cost of $g_{accept} \cdot \pi_{setup} + col$ for accepting the contract.

The available actions in $\Gamma^{Buyer}_{PublishTx}$ are a_{pubTx}, leading to $\Gamma^{Seller}_{FulfillTx}$, or $a_{noPubTx}$, leading to $\Gamma^{Seller}_{FulfillNoTx}$. We begin by considering these two subgames, and present their analysis summary in Table 1.

Subgame $\Gamma^{Seller}_{FulfillNoTx}$. In the $\Gamma^{Seller}_{FulfillNoTx}$ subgame *Seller* plays either $a_{exhaust}$ or a_{ignore}.

Playing $a_{exhaust}$ results with *Seller* exhausting the contract's gas, rewarding *Seller* with $payment + col$ at the incurred cost of $g_{done} \cdot \pi_{exec}$. Alternatively, playing a_{ignore} results with *Seller* forfeiting the contract tokens, but selling her gas for the *gas-price*, that is, a reward of $g_{alloc} \cdot \pi_{exec}$.

It follows $a_{exhaust}$ is preferred over a_{ignore} if

$$payment + col - g_{done} \cdot \pi_{exec} > g_{alloc} \cdot \pi_{exec} \ ,$$

and the resultant wealth of *Seller* in this subgame is therefore

$$\begin{aligned} W_{Seller}\left(\pi_{exec}, FulfillNoTx, \bar{s}_{\text{spe}}\right) &= w^{init}_{Seller} - g_{accept} \cdot \pi_{setup} \\ &+ \max\left(payment - g_{done} \cdot \pi_{exec}, g_{alloc} \cdot \pi_{exec} - col\right) \ . \end{aligned} \tag{1}$$

Regardless of the action *Seller* chooses, *Buyer* can pay the *gas-price* π_{exec} for her transaction inclusion. The cost for that is $g_{alloc} \cdot \pi_{exec}$ with a reward of w^{exo}. This is profitable as long as $w^{exo} > g_{alloc} \cdot \pi_{exec}$, resulting with

$$\begin{aligned} W_{Buyer}\left(\pi_{exec}, FulfillNoTx, \bar{s}_{\text{spe}}\right) &= w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} \\ &- payment - \varepsilon + \max\left(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0\right) \end{aligned} \ . \tag{2}$$

Subgame $\Gamma^{Seller}_{FulfillTx}$. In the $\Gamma^{Seller}_{FulfillTx}$ subgame *Seller* plays either a_{apply}, $a_{exhaust}$ or a_{ignore}.

Playing either $a_{exhaust}$ or a_{ignore} results with the same wealth as playing them in $\Gamma^{Seller}_{FulfillNoTx}$. However, playing a_{apply} includes the published $tx_{payload}$ transaction with its gas requirement g_{pub}, resulting with a reward of $payment + \varepsilon + col$. However, it also results with a cost of $g_{done} \cdot \pi_{exec}$, and an additional $\left(g_{alloc} - g_{pub}\right) \cdot \pi_{exec}$; note the latter is negative if $g_{alloc} < g_{pub}$, that is, if $tx_{payload}$ exceeds the agreed quota g_{alloc}, or positive if $tx_{payload}$ under-utilizes it.

Comparing a_{apply} and $a_{exhaust}$, we get a_{apply} is preferred if $\varepsilon > \left(g_{pub} - g_{alloc}\right) \cdot \pi_{exec}$. As $\varepsilon = 1$, $\pi_{exec} > 0$, and $\left(g_{pub} - g_{alloc}\right) \cdot \pi_{exec}$ is a number of tokens (i.e., an integer), this inequality holds if $g_{pub} \leq g_{alloc}$.

Similarly, comparing a_{apply} and a_{ignore} results with the former yielding more tokens if $\pi_{exec} < \frac{payment+col+\varepsilon}{g_{pub}+g_{done}}$.

The resultant wealth of *Seller* in this subgame is therefore

$$\begin{aligned} W_{Seller}\left(\pi_{exec}, FulfillTx, \bar{s}_{\text{spe}}\right) &= w^{init}_{Seller} - g_{accept} \cdot \pi_{setup} \\ &+ \max\Big(payment - g_{done} \cdot \pi_{exec}, g_{alloc} \cdot \pi_{exec} - col, \\ &payment + \varepsilon - \left(g_{done} + g_{alloc} - g_{pub}\right) \cdot \pi_{exec}\Big) \end{aligned} \ . \tag{3}$$

If *Seller* chooses not to confirm $tx_{payload}$, then *Buyer* can pay the *gas-price* π_{exec} for her transaction inclusion. The cost for that is $g_{alloc} \cdot \pi_{exec}$ with a reward of w^{exo}. This is preferred as long as $w^{exo} > g_{alloc} \cdot \pi_{exec}$, resulting with

$$W_{Buyer}\left(\pi_{exec}, FulfillTx, \bar{s}_{\text{spe}}\right) = w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon + \begin{cases} w^{exo}, & \pi_{exec} < \frac{payment+col+\varepsilon}{g_{pub}+g_{done}} \text{ and } g_{pub} \leq g_{alloc} \\ \max\left(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0\right), & \text{otherwise} \end{cases} \ . \tag{4}$$

We are now ready to consider the $\Gamma^{Buyer}_{PublishTx}$ subgame.

Subgame $\Gamma^{Buyer}_{PublishTx}$. In this subgame *Buyer* chooses whether to publish $tx_{payload}$, and with what gas requirement g_{pub}. We present the following lemma, providing an upper bound for *gas-price* π_{exec} such that *Buyer* is strictly incentivized to publish $tx_{payload}$ with $g_{pub} = g_{alloc}$:

Lemma 1. *If* $\pi_{exec} < \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}}$ *then* $\bar{s}_{spe}\left(PublishTx\right) = a_{pubTx}$, *satisfying* $g_{pub} = g_{alloc}$.

Intuitively, *Buyer* publishing a transaction with gas consumption $g_{pub} > g_{alloc}$ disincentivizes *Seller* to confirm it. But, by definition, the transaction of *Buyer* yields no value to her if $g_{pub} < g_{alloc}$, resulting with the optimal gas consumption being $g_{pub} = g_{alloc}$. Additionally, meeting the π_{exec} bound results with *Seller* confirming the published transaction, incentivizing *Buyer* to publish it to begin with. We bring the full proof in Appendix D.

Following Lemma 1, if the *gas-price* satisfies $\pi_{exec} < \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}}$ then *Seller* confirms $tx_{payload}$, and we get the resultant wealth of the $\Gamma^{Seller}_{FulfillTx}$ subgame (see Eq. 3 and Eq. 4).

However, if *gas-price* exceeds $\pi_{exec} > \frac{payment+col+\varepsilon}{g_{pub}+g_{done}}$ then *Seller* does not confirm $tx_{payload}$. In that case, *Seller* chooses between exhausting or ignoring the contract, and the resultant wealth is that of the $\Gamma^{Seller}_{FulfillNoTx}$ subgame (see Eq. 1 and Eq. 2).

Therefore, we get

$$W_{Seller}\left(\pi_{exec}, PublishTx, \bar{s}_{\text{spe}}\right) = \begin{cases} W_{Seller}\left(\pi_{exec}, FulfillTx, \bar{s}_{\text{spe}}\right), & \pi_{exec} < \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}} \\ W_{Seller}\left(\pi_{exec}, FulfillNoTx, \bar{s}_{\text{spe}}\right), & \pi_{exec} > \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}} \end{cases} \tag{5}$$

and

$$W_{Buyer}\left(\pi_{exec}, PublishTx, \bar{s}_{\text{spe}}\right) = \begin{cases} W_{Buyer}\left(\pi_{exec}, FulfillTx, \bar{s}_{\text{spe}}\right), & \pi_{exec} < \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}} \\ W_{Buyer}\left(\pi_{exec}, FulfillNoTx, \bar{s}_{\text{spe}}\right), & \pi_{exec} > \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}} \end{cases} \ . \tag{6}$$

In conclusion, Lemma 1 presents the required conditions for the SPE to include the publication and confirmation of $tx_{payload}$. We now proceed to express the conditions for initiation and acceptance.

Table 1: $\Gamma^{Seller}_{FulfillNoTx}$ and $\Gamma^{Seller}_{FulfillTx}$ subgame summaries.

Subgame	Condition	$\bar{s}_{\text{spe}}$ Action	W_{Buyer}	W_{Seller}
$\Gamma^{Seller}_{FulfillNoTx}$	$\pi_{exec} < \frac{payment+col}{g_{alloc}+g_{done}}$	$a_{exhaust}$	$w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon +$ $\max\left(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0\right)$ (Eq. 2)	$w^{init}_{Seller} - g_{accept} \cdot \pi_{setup} + payment - g_{done} \cdot \pi_{exec}$ (Eq. 1)
	$\pi_{exec} > \frac{payment+col}{g_{alloc}+g_{done}}$	a_{ignore}	$w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon +$ $\max\left(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0\right)$ (Eq. 2)	$w^{init}_{Seller} - g_{accept} \cdot \pi_{setup} + g_{alloc} \cdot \pi_{exec} - col$ (Eq. 1)
$\Gamma^{Seller}_{FulfillTx}$	$\pi_{exec} < \frac{payment+col+\varepsilon}{g_{pub}+g_{done}}$ $g_{pub} \leq g_{alloc}$	a_{apply}	$w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon +$ w^{exo} (Eq. 4)	$w^{init}_{Seller} - g_{accept} \cdot \pi_{setup} + payment + \varepsilon$ $- \left(g_{done} + g_{alloc} - g_{pub}\right) \cdot \pi_{exec}$ (Eq. 3)
	$\pi_{exec} < \frac{payment+col}{g_{alloc}+g_{done}}$ $g_{pub} > g_{alloc}$	$a_{exhaust}$	$w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon$ $+ \max\left(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0\right)$ (Eq. 4)	$w^{init}_{Seller} - g_{accept} \cdot \pi_{setup} + payment$ $- g_{done} \cdot \pi_{exec}$ (Eq. 3)
	$\pi_{exec} > \frac{payment+col}{g_{alloc}+g_{done}}$ $\pi_{exec} > \frac{payment+col+\varepsilon}{g_{pub}+g_{done}}$	a_{ignore}	$w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon$ $+ \max\left(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0\right)$ (Eq. 4)	$w^{init}_{Seller} - g_{accept} \cdot \pi_{setup} + g_{alloc} \cdot \pi_{exec} - col$ (Eq. 3)

6.2.2 Seller Accepting. We start with analyzing the contract acceptance, that is, with subgame $\Gamma^{Seller}_{AcceptLH}$. In this subgame, *Seller* can play a_{accept}, leading to subgame $\Gamma^{Buyer}_{PublishTx}$, discussed in Lemma 1. She can also play $a_{decline}$, leading to subgame $\Gamma^{Buyer}_{RecoupLH}$, which we analyze below.

Subgame $\Gamma^{Buyer}_{RecoupLH}$. In the $\Gamma^{Buyer}_{RecoupLH}$ subgame *Buyer* plays either a_{recoup} or $a_{forfeit}$.

Playing a_{recoup} results with *Buyer* getting $payment + \varepsilon$ and spending $g_{done} \cdot \pi_{exec}$ tokens. Alternatively, she can play $a_{forfeit}$, not getting or spending any tokens. She can also publish $tx_{payload}$ for $w^{exo} - g_{alloc} \cdot \pi_{exec}$. Either way, *Seller* gets $g_{alloc} \cdot \pi_{exec}$ for her gas allocation.

It follows a_{recoup} is preferred over $a_{forfeit}$ if $payment + \varepsilon > g_{done} \cdot \pi_{exec}$. The resultant wealth of *Seller* is

$$W_{Seller}\left(\pi_{exec}, RecoupLH, \bar{s}_{\text{spe}}\right) = w^{init}_{Seller} + g_{alloc} \cdot \pi_{exec} \ , \tag{7}$$

and of *Buyer* is

$$\begin{aligned} W_{Buyer}\left(\pi_{exec}, RecoupLH, \bar{s}_{\text{spe}}\right) &= w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} \\ &+ \max\left(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0\right) + \max\left(-g_{done} \cdot \pi_{exec}, -payment - \varepsilon\right) \ . \end{aligned} \tag{8}$$

We are now ready to analyze the $\Gamma^{Seller}_{AcceptLH}$ subgame.

Subgame $\Gamma^{Seller}_{AcceptLH}$. Recall this is played in φ_{setup}, before π_{exec} is drawn, so *Seller* chooses the action that maximizes her expected utility.

She can either play a_{accept}, resulting with

$$\begin{aligned} &\mathbb{E}\left[U_{Seller}\left(PublishTx, \bar{s}_{\text{spe}}\right)\right] = \\ &\int_{-\infty}^{\infty} U_{Seller}\left(PublishTx, \bar{s}_{\text{spe}}\right) \cdot \mathcal{F}_{\text{pdf}}\left(\pi_{exec}\right) d\pi_{exec} \ , \end{aligned} \tag{9}$$

or play $a_{decline}$, resulting with

$$\begin{aligned} &\mathbb{E}\left[U_{Seller}\left(RecoupLH, \bar{s}_{\text{spe}}\right)\right] = \\ &\int_{-\infty}^{\infty} U_{Seller}\left(RecoupLH, \bar{s}_{\text{spe}}\right) \cdot \mathcal{F}_{\text{pdf}}\left(\pi_{exec}\right) d\pi_{exec} \ . \end{aligned} \tag{10}$$

Let us denote the *expected utility difference (EUD)* of *Seller* by

$$EUD_{Seller} = \mathbb{E}\left[U_{Seller}\left(PublishTx, \bar{s}_{\text{spe}}\right)\right] - \mathbb{E}\left[U_{Seller}\left(RecoupLH, \bar{s}_{\text{spe}}\right)\right] \ .$$

The following corollary therefore details the condition for *Seller* to accept the contract:

Corollary 1. *In* $\Gamma^{Seller}_{AcceptLH}$*, if* $EUD_{Seller} > 0$ *then* $\bar{s}_{spe}\left(AcceptLH\right) = a_{accept}$*, and if* $EUD_{Seller} < 0$ *then* $\bar{s}_{spe}\left(AcceptLH\right) = a_{decline}$*.*

Corollary 1 presents the contract acceptance condition, as discussed in Theorem 1. It also allows us to draft the expected utility of *Buyer* in $\Gamma^{Seller}_{AcceptLH}$ in the following equation:

$$\begin{aligned} &\mathbb{E}\left[U_{Buyer}\left(AcceptLH, \bar{s}_{\text{spe}}\right)\right] = \\ &\begin{cases} \mathbb{E}\left[U_{Buyer}\left(PublishTx, \bar{s}_{\text{spe}}\right)\right], & EUD_{Seller} > 0 \\ \mathbb{E}\left[U_{Buyer}\left(RecoupLH, \bar{s}_{\text{spe}}\right)\right], & EUD_{Seller} < 0 \end{cases} . \end{aligned} \tag{11}$$

6.2.3 Buyer Initiating. It remains to consider the conditions for contract initiation being SPE for *Buyer*. The subgame describing this decision is Γ^{Buyer}_{InitLH}, where *Buyer* decides whether to initiate the contract (a_{init}), leading to $\Gamma^{Seller}_{AcceptLH}$, or to not initiate ($a_{wait}$), leading to Γ^{Buyer}_{NoLH}.

Subgame Γ^{Buyer}_{InitLH} is also before *Nature* draws π_{exec}, so we compare the actions' expected utilities. Eq. 11 gives $\mathbb{E}\left[U_{Buyer}\left(AcceptLH, \bar{s}_{\text{spe}}\right)\right]$, the expected utility from playing a_{init}.

We now find $\mathbb{E}\left[U_{Buyer}\left(NoLH, \bar{s}_{\text{spe}}\right)\right]$, the expected utility from playing a_{wait}. For that, we first analyze the Γ^{Buyer}_{NoLH} subgame.

Subgame Γ^{Buyer}_{NoLH}. In the Γ^{Buyer}_{NoLH} subgame *Buyer* can pay $g_{alloc} \cdot \pi_{exec}$ to have $tx_{payload}$ confirmed, receiving w^{exo} tokens. We get

$$W_{Buyer}\left(\pi_{exec}, NoLH, \bar{s}_{\text{spe}}\right) = w^{init}_{Buyer} + \max\left(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0\right)$$

and

$$\begin{aligned} &\mathbb{E}\left[U_{Buyer}\left(NoLH, \bar{s}_{\text{spe}}\right)\right] = \\ &\int_{-\infty}^{\infty} U_{Buyer}\left(NoLH, \bar{s}_{\text{spe}}\right) \cdot \mathcal{F}_{\text{pdf}}\left(\pi_{exec}\right) d\pi_{exec} \ . \end{aligned} \tag{12}$$

We are finally ready to address the full game $\Gamma = \Gamma^{Buyer}_{InitLH}$.

Subgame Γ^{Buyer}_{InitLH}. Given $\mathbb{E}\left[U_{Buyer}\left(NoLH, \bar{s}_{\text{spe}}\right)\right]$ (Eq. 12) and $\mathbb{E}\left[U_{Buyer}\left(AcceptLH, \bar{s}_{\text{spe}}\right)\right]$ (Eq. 11), we denote the expected utility difference of *Buyer* by

$$EUD_{Buyer} = \mathbb{E}\left[U_{Buyer}\left(AcceptLH, \bar{s}_{\text{spe}}\right)\right] - \mathbb{E}\left[U_{Buyer}\left(NoLH, \bar{s}_{\text{spe}}\right)\right] \ .$$

The following corollary presents the condition for *Buyer* initiating the contract:

Corollary 2. *If* $EUD_{Buyer} > 0$ *then* $\bar{s}_{spe}\left(\Gamma^{Buyer}_{InitLH}\right) = a_{init}$*.*

Corollary 2 shows the contract initiation condition, thus concluding the conditions for the SPE to be as detailed in Theorem 1.

It is now easy to see the correctness of Theorem 1. Take any distribution $\mathcal{F}$. By Lemma 1, setting *col* sufficiently high deterministically assures (or assures with high probability for an unbounded distribution) that if LedgerHedger is initiated and accepted, then *Buyer* publishes an adequate $tx_{payload}$ and *Seller* confirms it.

Corollary 1 and Corollary 2 both present conditions for the contract initiation and acceptance – conditions on preferring a predetermined payment over one that changes according to the drawn π_{exec}. Sufficiently risk-averse participants result with both of them preferring a predetermined contract over the drawn price uncertainty.

Next, we consider Theorem 1 in practical settings. Specifically, we show that engaging in LedgerHedger is beneficial in a wide range of practical parameters, relevant to operational systems.

6.3 Efficacy

To show the efficacy of LedgerHedger, we first review relevant contract parameters, *gas-price* distributions, and utility functions (§6.3.1). We then show how to set the contract parameters to assure its fulfillment (§6.3.2), and conclude by describing concrete ranges where both parties benefit from the contract (§6.3.3).

6.3.1 Contract Parameters, Distributions, Utility Functions.

Contract parameters. We set $g_{alloc} = 5e6\ (5 \cdot 10^6)$ as a representative example of a ZK roll-up proof gas requirement [53, 105], and arbitrarily choose $w^{exo} = w^{init}_{Buyer} = w^{init}_{Seller} = 1e9$. Considering our implementation gas requirements (presented in §8), we fix the contract function gas requirements at $g_{init} = 0.1e6, g_{accept} = 75e3$ and $g_{done} = 20e3$. We still consider $\varepsilon = 1$, and derive the desired values of *payment* and *col* throughout this section.

Distribution $\mathcal{F}$. The resultant players' wealth depends on their strategies and on the *gas-price* value π_{exec}, which is drawn from $\mathcal{F}$. Therefore, towards our analysis, we need to instantiate $\mathcal{F}$.

Inspired by Ethereum current *gas-price* [52], we set the *gas-price* at initiation to $\pi_{setup} = 100$. For the distribution $\mathcal{F}$, we consider normal distributions with a mean value of π_{setup}, and truncate them symmetrically at 0 and 200. We consider three different distributions, denoted $\forall i \in [1,3] : \mathcal{F}_i$, differing in their variance $\sigma_i^2 = 10^{i+1}$.

Utility functions. Agent risk aversion is modeled through the concavity of its utility function. However, the optimal strategy is not affected by affine transformations of the utility function [12, 133], so simply measuring the curvature fails to capture this preference.

Instead, the risk preference of a utility function $U(W)$ is typically measured using its *Arrow-Pratt Relative Risk Aversion (RRA)* [5, 117], $RRA = -\frac{W \cdot U''(W)}{U'(W)}$, where $U'(W)$ and $U''(W)$ are the first and second derivatives of $U(W)$, respectively.

For our instantiation we use a few common options for utility functions [30, 44, 82]: Linear utility $U(W) = W$ with $RRA = 0$, exhibiting risk-neutrality; Sqrt utility $U(W) = \sqrt{W}$ with $RRA = 0.5$, exhibiting mild risk-aversion; and, Log utility $U(W) = \log(W)$ with $RRA = 1$, exhibiting higher risk-aversion.

6.3.2 Contract Fulfillment.

With the contract parameters, distributions, and utility functions set, we are first interested in finding the *payment* and *col* parameters for *Seller* to confirm $tx_{payload}$.

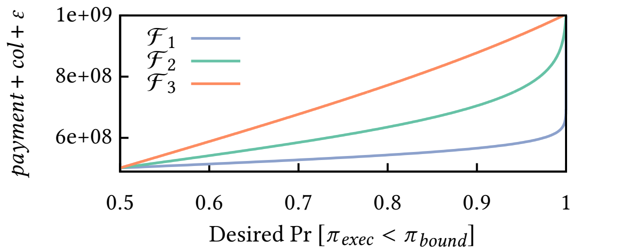


Figure 3: Required contract funds $payment + col + \varepsilon$ to achieve desired fulfillment probability Pr $[\pi_{exec} < \pi_{bound}]$.

By Lemma 1, this occurs when $\pi_{exec} < \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}}$. Let us denote $\pi_{bound} = \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}}$, hence we are interested in finding when $\pi_{exec} < \pi_{bound}$.

Recall $\pi_{exec} \sim \mathcal{F}$, so the condition holds only with some probability. This is not a predicament specific to LedgerHedger but to hedging in general – in extreme cases one party might be better off violating the contract, as the incurred punishment is smaller than the cost of abiding by the contract. However, setting a sufficient incentive can achieve any desired probability. For bounded probabilities, we can achieve deterministic success.

The probability that $\pi_{exec} < \pi_{bound}$ is given by the distribution's *cumulative distribution function (CDF)* at π_{bound}. Figure 3 shows the required $payment + col + \varepsilon$ value to achieve Pr $[\pi_{exec} < \pi_{bound}]$.

Figure 3 illustrates that increasing *payment* and *col* results with higher fulfillment probability, as they increase the incentive for *Seller* to fulfill the contract.

Additionally, Figure 3 shows the effect of the distribution variance on meeting the π_{bound} bound. As expected, the more variant distributions have heavier right tails, requiring more funds to achieve the same success probability.

If there exists an upper bound on the distribution value, like in the truncated normal distribution, simply setting $payment + \varepsilon + col$ such that π_{bound} exceeds that upper bound assures success deterministically. In case of an unbounded distribution, the failure probability is negligible in $payment+\varepsilon+col$ according to the Chernoff bound [29].

As such, hereinafter, we consider *payment* and *col* values such that Pr $[\pi_{exec} < \pi_{bound}] = 1$, and move to consider the contract initiation and acceptance.

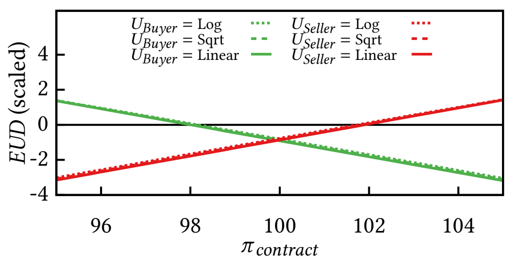
6.3.3 Initiation and Acceptance.

Let us begin by considering the effect of the *payment* and the *col* parameters. *Buyer* pays *payment* tokens to *Seller* for g_{alloc} gas. Too high *payment* values disincentivize *Buyer* from initiating the contract, as she can buy g_{alloc} for the *gas-price* instead. Too low *payment* values disincentivize *Seller* from accepting the contract, as she can instead sell g_{alloc} for *gas-price*.

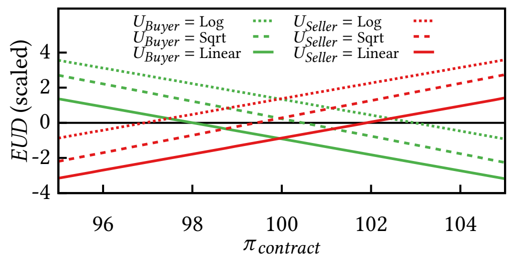
The *col* tokens are used to incentivize *Seller* to abide by an accepted contract, as she loses them otherwise.

We now analyze the contract initiation and acceptance for concrete values of *payment* and *col*, for a specific $\mathcal{F}$, and assuming *Buyer* and *Seller* each have a utility function Utility $\in$ {Linear, Sqrt, Log}.

Recall that Corollary 2 shows that *Buyer* initiates the contract if $EUD_{Buyer} > 0$. Similarly, Corollary 1 shows that *Seller* accepts the contract if $EUD_{Seller} > 0$.



(a) Distribution $\mathcal{F}_1$



(b) Distribution $\mathcal{F}_3$

Figure 4: Normalized expected utility difference.

We arbitrarily set $col = 1e9$ to satisfy $\Pr[\pi_{exec} < \pi_{bound}] = 1$ (lower values suffice as well, as we need $payment + col > 1e9$), and numerically calculate EUD_{Buyer} and EUD_{Seller} for the various distributions and utility functions, as a function of $\pi_{contract} = \frac{payment}{g_{alloc}}$.

Figure 4 presents these values, scaled for comparison, for the various utility functions, and for the lowest-variance distribution $\mathcal{F}_1$ (Figure 4a) and for highest-variant distribution $\mathcal{F}_3$ (Figure 4b).

As expected, the higher the agreed price $\pi_{contract}$ is, engaging in a contract becomes less profitable for *Buyer* and more for *Seller*, since the utility functions are strictly increasing. That is, *Buyer* agrees to initiate up to a maximal price, and *Seller* agrees to accept for no less than a minimal price. We denote these by $\pi^{\max}_{Buyer}$ and by $\pi^{\min}_{Seller}$, respectively, and refer to these as the *required* prices.

Determining the $\pi_{contract}$ that *Buyer* and *Seller* agree upon is a matter of negotiation, outside the scope of this work. We focus on finding conditions for such a price to exist, i.e., for $\pi^{\max}_{Buyer} > \pi^{\min}_{Seller}$.

Figure 4 shows that utility functions with higher RRA are more amenable to engage in the contract. Specifically, it shows that $\pi^{\max}_{Buyer}$ is the highest in case of a logarithmic utility function Log ($RRA = 1$), followed by the price in case of a square root utility function Sqrt ($RRA = 0.5$), and then by the price in case of a linear utility function Linear ($RRA = 0$). This is expected – higher RRA means higher preference for certainty, which is achieved through engaging in the contract.

Symmetrically, it shows that $\pi^{\min}_{Seller}$ is the lowest with a logarithmic utility function, and highest with a linear utility function.

Lastly, Figure 4 highlights how the distribution $\mathcal{F}$ affects the existence of a $\pi_{contract}$ such that $\pi^{\max}_{Buyer} > \pi^{\min}_{Seller}$. For $\mathcal{F}_1$ (Figure 4a), there is no $\pi_{contract}$ where for any combination of utility function for *Buyer* and *Seller* both utility differences are positive, i.e., $\pi^{\max}_{Buyer} < \pi^{\min}_{Seller}$. However, for $\mathcal{F}_3$ (Figure 4b), there is a range of $\pi_{contract}$ values where $\pi^{\max}_{Buyer} > \pi^{\min}_{Seller}$ for some utility function combinations.

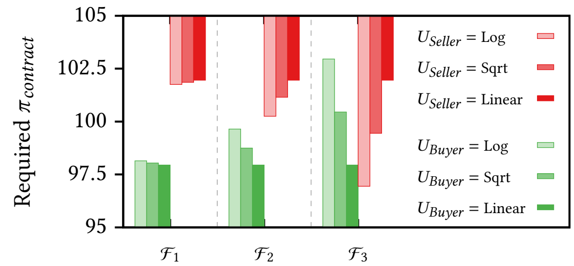


Figure 5: $\pi_{contract}$ for initiation and acceptance.

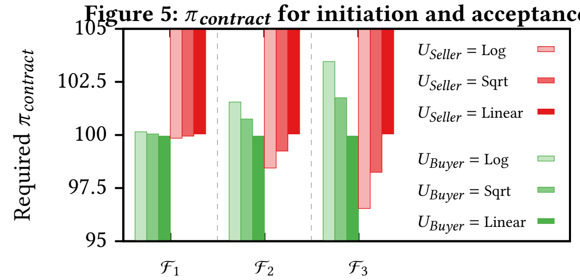


Figure 6: $\pi_{contract}$ for initiation and acceptance without friction.

The difference is due to the different variance values of the distributions. Intuitively, a distribution with higher variance offers less certainty about π_{exec}, making the contract-induced certainty more appealing for risk averse ($RRA > 0$) participants.

To further emphasize the distribution effect, Figure 5 presents the required prices for the various utility functions and distributions. It shows the distributions with lower variance values $\mathcal{F}_1$ and $\mathcal{F}_2$ both result with $\pi^{\max}_{Buyer} < \pi^{\min}_{Seller}$, i.e., no contract.

However, for a high variance value, there exist combinations of U_{Buyer} and U_{Seller} that result with $\pi^{\max}_{Buyer} > \pi^{\min}_{Seller}$. For example, the above is satisfied for $\mathcal{F}_3$ when U_{Buyer} is Log and U_{Seller} is Linear, or vice versa. This implies that the parties engage in a contract even if one of them is risk neutral.

Figure 5 also shows that the required prices are fixed for the linear utility function, for both *Buyer* and *Seller*, for any considered $\mathcal{F}$. Broadly speaking, this holds due to $\Pr[\pi_{exec} < \pi_{bound}] = 1$, the linearity of the utility function, and the fact all considered distributions have the same mean value. We bring a thorough explanation in Appendix E.

Finally, as a theoretical exercise, we consider the cost of *friction* [77] – the inherent costs of g_{init}, g_{accept} and g_{done} that *Buyer* and *Seller* incur. The reason this experiment might be of interest is due to further optimizations in LedgerHedger that result with even lower overheads.

We set $g_{init} = g_{accept} = g_{done} = 0$ and find the required prices for the various utility functions and distributions, brought in Figure 6.

As expected, reducing the friction results with both *Buyer* and *Seller* being more amenable to initiate and accept the contract. Specifically, this relaxation facilitates the contract creation even for $\mathcal{F}_1$ and $\mathcal{F}_2$.

7 GAS ALLOCATION ASSURANCES

As mentioned (§3.2), we consider *Seller* to have a gas allocation of g_{alloc} in the required block interval. This modeling trivially fits ledger systems where the system validators (miners) are chosen in advance, such as planned Central Bank Digital Currencies (CBDCs) [2, 60].

We now show this modeling also applies to systems where miners are chosen probabilistically. We begin by first considering practical parameters, showing that *Seller* manages to create a block with overwhelming probability. Conservatively, consider a short interval of a one hour (cf., Optimistic roll-ups like Optimism [107] and Arbitrum [78] that use week-long intervals). For Ethereum, in one hour interval there are about 240 blocks, and the probability that a 10% miner would fail to create any block in that interval is $(1 - 0.1)^{240} \approx 10^{-11}$. A 5% miner would reach the same probability in about two hours. These values mean failing to find a single block is expected to occur only once in a few million years. We emphasize that in a probabilistic system we do not expect a miner to reserve all her expected future blocks, i.e., miners will retain margins of their reservations.

Finally, we emphasize that a *Seller* does not need to create a block by herself to begin with, as she can have the $tx_{payload}$ confirmed (the action denoted by a_{apply}) by paying the required *gas-price*, regardless of her block-creation capabilities and regardless of random events occurring or not. Moreover, all of *Seller*'s possible interactions with LedgerHedger do not require *Seller* creating a block by herself, and therefore can all be performed even by non-mining entities. It immediately follows that any mining or non-mining *Seller* can simply use the aforementioned transaction-fee mechanism to fulfill the contract as required.

8 IMPLEMENTATION

To demonstrate the practicality of LedgerHedger, we implement it as an Ethereum smart contract, and deploy it on a test network.

Ethereum smart contracts are written in the Solidity smart contract programming language [50]; we bring the code in Appendix G.

Design. Our implementation follows the *smart contract wallet (SCW)* [43, 56, 92] design pattern. This design enables customizing the retrieval of the contract tokens, which, for LedgerHedger, is done only through the *Apply*, *Exhaust*, and *Recoup* functions.

Additionally, this design enables decoupling the transaction *issuer* (i.e., the party that pays the transaction fees) from the transaction *signer* (the party that creates the transaction). This, in turn, enables having one party, *Seller*, use her gas allocation (or pay the transaction fees) to confirm a transaction by the other party *Buyer*, using so-called *meta transactions* [66].

We implemented LedgerHedger to be reusable for *Buyer*, that is, it is deployed once, and then can be used to create new instances over and over again. This amortizes the deployment gas requirements, which are higher than other operations [155].

Function Implementations. The implementation of *Initiate*, *Accept* and *Recoup* is straightforward, based on Alg. 1.

In the *Exhaust* function, the only novel element is the gas exhaustion through null operations. We implement this by looping sufficiently many times to ensure the exhausted gas matches its target. Our implementation results in a difference between the target g_{alloc} and actual consumed gas of up to 120 gas units – 4 orders of magnitude lower than practical values of g_{alloc}.

Finally, the contract pinnacle, the *Apply* function, is implemented using the aforementioned meta-transaction mechanism. It accepts a meta transaction, issued by *Seller*, verifies it is signed by *Buyer*, and then executes it. The signature verification is performed using a prevalent Ethereum cryptographic library [106]. Note this requires *Buyer* to create her transaction $tx_{payload}$ in a format fitting this design.

EIP1559 Compatibility. Recall the payment for $tx_{payload}$ confirmed by LedgerHedger is *payment*, and it does not need to pay an additional fee. In principle, we could have had $tx_{payload}$ offer no fee, and let *Seller* confirm it as an ordinary transaction. However, Ethereum's EIP1559 [55, 126] requires that all transactions in a block pay a minimal, *base fee*. Our implementation is compatible with EIP1559 since $tx_{payload}$ is a meta transaction, and the transaction by *Seller* that invokes the *Apply* is the one that pays the required base fee.

Deployment and Gas Costs. We deploy LedgerHedger on the Ethereum Goerli test network [62], and invoke all its functions. We bring the transaction identifiers in Appendix F.

We initiate the contract using the *Initiate* function three times, and conclude it differently after each initiation.

The first initiation consumed $g_{init} = 117e3$ gas. We then concluded the contract using the *Recoup* function, consuming $g_{done} = 57.3e3$ gas.

The second initiation consumed $g_{init} = 37.4e3$ gas, followed by an invocation of the *Accept*, consuming $g_{accept} = 50e3$ gas, and then an invocation of *Exhaust*, consuming $g_{alloc} + g_{done} = 3.021e6$ gas. Using a local profiler, we found that $g_{done} = 21e3$, aligned with this experiment's chosen $g_{alloc} = 3e6$ value.

Finally, we initiated the contract for the third time, consuming $g_{init} = 37.4e3$ gas, again invoked *Accept* for $g_{accept} = 50e3$ gas. Then, we invoked the *Apply* function on an arbitrary meta-transaction that we created, consuming $g_{pub} + g_{done} = 2.668e6$ gas. Again, using a local profiler, we find that $g_{done} = 12e3$.

Note that the first initiation required $2.5X$ gas compared to the second and third initiations. This discrepancy is due to Ethereum operations consuming gas as a function of their state changes, e.g., setting a value to an unassigned variable is more gas-consuming than assigning a value to an already-assigned one. The first initiation higher costs can therefore be considered as part of the deployment.

To conclude, our LedgerHedger implementation incurs an (amortized) overhead of $g_{init} = 37.4e3$ gas on *Buyer*, and $g_{accept} + g_{done} = 62e3$ gas on *Seller* in the desired execution. These are 3 orders of magnitude lower than a representative example of an applicable hedging use-case of $g_{alloc} = 10e6$ gas [53].

Appendix C reviews possible modifications of interest, concerning user experience and overheads. These include enabling *Buyer* to withdraw the tokens earlier in case *Seller* is unresponsive, and reducing function overheads by using constant, predefined parameters.

9 CONCLUSION

We introduce LedgerHedger, a blockchain smart contract for confirming a future transaction of *Buyer* for a predetermined fee by *Seller*. We analyze fee variability and prove that fulfilling the contract is SPE for a wide range of practical parameters. We implement LedgerHedger as a smart contract for Ethereum, deploy it, and show its efficacy and low gas overhead compared to common gas requirements.

LedgerHedger is directly applicable to secure smart contracts executed over Ethereum and similar systems, resolving the prevalent issue of unjustified reliance on fee stability.

REFERENCES

[1] 1inch Network. 2020. 1inch Introduces Chi Gastoken. https://blog.1inch.io/1inch-introduces-chi-gastoken-d0bd5bb0f92b

[2] Sarah Allen, Srđjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, et al. 2020. *Design choices for central bank digital currency: Policy and technical considerations*. Technical Report. National Bureau of Economic Research.

[3] Chainsight Analytica. 2021. MEV attack – Just-in-Time Liquidity. https://twitter.com/ChainsightA/status/1457958811243778052

[4] Dune Analytics. 2022. Average gas price per day for the last 30 days. https://dune.xyz/queries/7898/15742 Accessed: 2022-01-13.

[5] Kenneth J Arrow. 1971. The theory of risk aversion. *Essays in the theory of risk-bearing* (1971), 90–120.

[6] Aditya Asgaonkar and Bhaskar Krishnamachari. 2019. Solving the buyer and seller's dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator. In *IEEE ICBC*.

[7] Robert J Aumann. 1995. Backward induction and common knowledge of rationality. *Games and Economic Behavior* (1995).

[8] Christian Badertscher, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. 2017. Bitcoin as a transaction ledger: A composable treatment. In *Annual International Cryptology Conference*.

[9] Wacław Banasik, Stefan Dziembowski, and Daniel Malinowski. 2016. Efficient zero-knowledge contingent payments in cryptocurrencies without scripts. In *European Symposium on Research in Computer Security*.

[10] Soumya Basu, David Easley, Maureen O'Hara, and G Sirer. 2020. StableFees: A Predictable Fee Market for Cryptocurrencies. *Work. Pap.* (2020).

[11] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. 2018. Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptol. ePrint Arch.* 2018 (2018), 46.

[12] Jonathan Benchimol. 2014. Risk aversion in the Eurozone. *Research in Economics* 68, 1 (2014), 39–56.

[13] Jeff Benson. 2021. Ethereum London Hard Fork to Make Some Tokens Worthless. https://decrypt.co/77345/ethereum-london-hard-fork-make-some-tokens-worthless

[14] B Douglas Bernheim. 1984. Rationalizable strategic behavior. *Econometrica: Journal of the Econometric Society* (1984).

[15] Binance. 2020. Binance Smart Chain. https://github.com/binance-chain/whitepaper/blob/master/WHITEPAPER.md

[16] Blockchair. 2021. *Blockchain explorer, analytics and web services*. blockchair.com

[17] Chakriya Bowman, Aasim M Husain, et al. 2004. *Forecasting commodity prices: Futures versus judgment*. March.

[18] Lorenz Breidenbach, Phil Daian, and Florian Tramer. 2018. Gas Token. https://gastoken.io/

[19] Bryan Bishop. [n. d.]. Bitcoin vaults with anti-theft recovery/clawback mechanisms. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2019-August/017231.html

[20] Sergiu Bursuc and Steve Kremer. 2019. Contingent payments on a public ledger: models and reductions for automated verification. In *European Symposium on Research in Computer Security*.

[21] Vitalik Buterin. 2013. A Next Generation Smart Contract & Decentralized Application Platform. https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf/

[22] Vitalik Buterin. 2019. The dawn of hybrid layer 2 protocols. Available online.

[23] Matteo Campanelli, Rosario Gennaro, Steven Goldfeder, and Luca Nizzardo. 2017. Zero-knowledge contingent payments revisited: Attacks and payments for services. In *Proceedings of the 2017 ACM CCS*.

[24] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, and Arvind Narayanan. 2016. On the Instability of Bitcoin Without the Block Reward. In *Proceedings of the 2016 ACM CCS*.

[25] Ethan Cecchetti, Siqiu Yao, Haobin Ni, and Andrew C Myers. 2021. Compositional security for reentrant applications. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1249–1267.

[26] J Cerny. 2014. *Playing general imperfect-information games using game-theoretic algorithms*. Ph. D. Dissertation. PhD thesis, Czech Technical University.

[27] Panagiotis Chatzigiannis, Foteini Baldimtsi, Igor Griva, and Jiasun Li. 2019. Diversification across mining pools: Optimal mining strategies under pow. *arXiv preprint arXiv:1905.04624* (2019).

[28] Xi Chen, Christos Papadimitriou, and Tim Roughgarden. 2019. An Axiomatic Approach to Block Rewards. In *Proceedings of ACM AFT*.

[29] Herman Chernoff et al. 1952. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics* (1952).

[30] Pierre-André Chiappori and Monica Paiella. 2011. Relative risk aversion is constant: Evidence from panel data. *Journal of the European Economic Association* 9, 6 (2011), 1021–1052.

[31] Charles J Cicchetti and Jeffrey A Dubin. 1994. A microeconometric analysis of risk aversion and the decision to self-insure. *Journal of political Economy* 102, 1 (1994), 169–186.

[32] coinmarketcap.com. 2022. *Cryptocurrency Market Capitalizations*. https://coinmarketcap.com/ Accessed: 2022-01-10.

[33] coinmarketcap.com. 2022. *Hermez Market Cap*. https://coinmarketcap.com/currencies/hermez-network/ Accessed: 2022-01-10.

[34] coinmarketcap.com. 2022. *Loopring Market Cap*. https://coinmarketcap.com/currencies/loopring/ Accessed: 2022-01-10.

[35] Lin William Cong, Zhiguo He, and Jiasun Li. 2021. Decentralized mining in centralized pools. *The Review of Financial Studies* 34, 3 (2021), 1191–1235.

[36] Thomas Conlon, John Cotter, and Ramazan Gençay. 2016. Commodity futures hedging, risk aversion and the hedging horizon. *The European Journal of Finance* 22, 15 (2016), 1534–1560.

[37] ConsenSys. 2018. *The Inside Story of the CryptoKitties Congestion Crisis*. https://media.consensys.net/the-inside-story-of-the-cryptokitties-congestion-crisis-499b35d119cc

[38] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, et al. 2016. On scaling decentralized blockchains. In *International conference on financial cryptography and data security*. Springer, 106–125.

[39] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. [n. d.]. Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In *2020 IEEE S&P*.

[40] Christian Decker and Roger Wattenhofer. 2013. Information Propagation in the Bitcoin Network. In *IEEE P2P*. Trento, Italy.

[41] Christian Decker and Roger Wattenhofer. 2015. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In *Stabilization, Safety, and Security of Distributed Systems - 17th International Symposium*.

[42] Degenerative. 2021. uGAS Token. https://docs.degenerative.finance/synthetics/ugas

[43] Monika di Angelo and Gernot Salzer. 2020. Wallet Contracts on Ethereum–Identification, Types, Usage, and Profiles. *arXiv preprint arXiv:2001.06909* (2020).

[44] James S Dyer and Rakesh K Sarin. 1982. Relative risk aversion. *Management science* 28, 8 (1982), 875–886.

[45] Stefan Dziembowski, Lisa Eckey, and Sebastian Faust. 2018. Fairswap: How to fairly exchange digital goods. In *ACM CCS*.

[46] Stefan Dziembowski, Lisa Eckey, Sebastian Faust, and Daniel Malinowski. 2017. PERUN: Virtual Payment Channels over Cryptographic Currencies. *IACR ePrint* (2017).

[47] Stefan Dziembowski, Sebastian Faust, and Kristina Hostáková. 2018. General state channel networks. In *Proceedings of the 2018 ACM CCS*.

[48] Daniel Ellsberg. 1961. Risk, ambiguity, and the Savage axioms. *The quarterly journal of economics* (1961), 643–669.

[49] Shayan Eskandari, Mehdi Salehi, Wanyun Catherine Gu, and Jeremy Clark. 2021. SoK: Oracles from the Ground Truth to Market Manipulation. *arXiv preprint arXiv:2106.00667* (2021).

[50] Ethereum. 2020. *Solidity Language*. https://github.com/ethereum/solidity

[51] etherscan.info. 2021. Ethereum Average Gas Price Chart. https://etherscan.io/chart/gasprice

[52] etherscan.io. [n. d.]. Ether Transaction Fees. https://etherscan.io/chart/transactionfee

[53] etherscan.io. 2021. Optimism 10.2M Gas Transaction. https://etherscan.io/tx/0x90ebd9630d98d5b0a186eec4c2382c296e5f41e828da910d76a53ab72ffe30e8

[54] Eugene F Fama. 1995. Random walks in stock market prices. *Financial analysts journal* 51, 1 (1995), 75–80.

[55] Ethereum Foundation. 2021. Ethereum London Hard Fork. https://ethereum.org/en/history/#london

[56] Ethereum Foundation. 2022. Smart Contract Wallets. https://docs.ethhub.io/using-ethereum/wallets/smart-contract-wallets/

[57] Emilio Frangella. 2020. Crypto Black Thursday: The Good, the Bad, and the Ugly. https://medium.com/aave/crypto-black-thursday-the-good-the-bad-and-the-ugly-7f2acebf2b83

[58] Georg Fuchsbauer. 2019. WI Is Not Enough: Zero-Knowledge Contingent (Service) Payments Revisited. In *Proceedings of the 2019 ACM CCS*.

[59] Drew Fudenberg and Jean Tirole. 1991. Game theory, 1991. *Cambridge, Massachusetts* (1991).

[60] Ben SC Fung and Hanna Halaburda. 2016. Central bank digital currencies: a framework for assessing why and how. *Available at SSRN 2994052* (2016).

[61] Alberto Garoffolo, Dmytro Kaidalov, and Roman Oliynykov. 2020. Zendoo: a zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 1257–1262.

[62] Goerli. 2018. *Ethereum Goerli Test Network*. https://goerli.net/

[63] Shafi Goldwasser, Silvio Micali, and Ronald L Rivest. 1988. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on computing* (1988).
[64] Neville Grech, Michael Kong, Anton Jurisevic, Lexi Brent, Bernhard Scholz, and Yannis Smaragdakis. 2018. Madmax: Surviving out-of-gas conditions in ethereum smart contracts. *Proceedings of the ACM on Programming Languages* 2, OOPSLA (2018), 1–27.
[65] Matthew Green and Ian Miers. 2017. Bolt: Anonymous payment channels for decentralized currencies. In *Proceedings of the 2017 ACM CCS*.
[66] Austin Thomas Griffith. 2022. Ethereum Meta Transactions.
[67] Shelly Grossman, Ittai Abraham, Guy Golan-Gueta, Yan Michalevsky, Noam Rinetzky, Mooly Sagiv, and Yoni Zohar. 2017. Online detection of effectively callback free objects with applications to smart contracts. *Proceedings of the ACM on Programming Languages* 2, POPL (2017), 1–28.
[68] Mudit Gupta. 2021. All TWAPs are subject to manipulation. https://tinyurl.com/5xv2nnpj
[69] Mark R. Hake. [n. d.]. Fees Threaten Ethereum's Perch as King of NFTs. https://www.nasdaq.com/articles/fees-threaten-ethereums-perch-as-king-of-nfts-2021-10-11
[70] Jona Harris and Aviv Zohar. 2020. Flood & Loot: A Systemic Attack On The Lightning Network. In *Proceedings ACM AFT*.
[71] David Haushalter. 2001. Why hedge? Some evidence from oil and gas producers. *Journal of Applied Corporate Finance* 13, 4 (2001), 87–92.
[72] Maurice Herlihy. 2018. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing*.
[73] Hermez. 2020. Scalable payments. Decentralised by design, open for everyone. https://hermez.io/hermez-whitepaper.pdf
[74] Jochen Hoenicke. 2021. Johoe's Mempool Statistics. https://jochen-hoenicke.de/queue/#ETH,all,fee Accessed: 2022-01-13.
[75] Shangrong Jiang, Yuze Li, Shouyang Wang, and Lin Zhao. 2022. Blockchain competition: The tradeoff between platform stability and efficiency. *European Journal of Operational Research* 296, 3 (2022), 1084–1097.
[76] Don Johnson, Alfred Menezes, and Scott Vanstone. 2001. The elliptic curve digital signature algorithm (ECDSA). *International journal of information security* 1, 1 (2001), 36–63.
[77] Jan Kallsen and Johannes Muhle-Karbe. 2015. Option pricing and hedging with small transaction costs. *Mathematical Finance* 25, 4 (2015), 702–723.
[78] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S Matthew Weinberg, and Edward W Felten. 2018. Arbitrum: Scalable, private smart contracts. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 1353–1370.
[79] Marek M Kamiński. 2017. Backward induction: Merits and flaws. *Studies in Logic, Grammar and Rhetoric* (2017).
[80] Maurice George Kendall and A Bradford Hill. 1953. The analysis of economic time-series-part i: Prices. *Journal of the Royal Statistical Society. Series A (General)* 116, 1 (1953), 11–34.
[81] Majid Khabbazian, Tejaswi Nadahalli, and Roger Wattenhofer. [n. d.]. Timelocked Bribing. ([n. d.]).
[82] Miles S Kimball. 1993. Standard risk aversion. *Econometrica: Journal of the Econometric Society* (1993), 589–611.
[83] Matter Labs. 2021. Matter Labs website. https://matter-labs.io/
[84] Ron Lavi, Or Sattath, and Aviv Zohar. 2019. Redesigning Bitcoin's fee market. In *The World Wide Web Conference*.
[85] Haim Levy. 2015. *Stochastic dominance: Investment decision making under uncertainty*. Springer.
[86] Fangxiao Liu, Xingya Wang, Zixin Li, Jiehui Xu, and Yubin Gao. 2020. Effective GasPrice Prediction for Carrying Out Economical Ethereum Transaction. In *2019 6th International Conference on Dependable Systems and Their Applications (DSA)*. IEEE, 329–334.
[87] Ayelet Lotem, Sarah Azouvi, Aviv Zohar, and Patrick McCorry. 2022. Sliding Window Challenge Process for Congestion Detection. In *Financial Cryptography and Data Security*.
[88] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. 2019. Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability.. In *NDSS*.
[89] Rawya Mars, Amal Abid, Saoussen Cheikhrouhou, and Slim Kallel. 2021. A Machine Learning Approach for Gas Price Prediction in Ethereum Blockchain. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 156–165.
[90] Frank J Massey Jr. 1951. The Kolmogorov-Smirnov test for goodness of fit. *Journal of the American statistical Association* 46, 253 (1951), 68–78.
[91] Gregory Maxwell. [n. d.]. The first successful Zero-Knowledge Contingent Payment. https://bitcoincore.org/en/2016/02/26/zero-knowledge-contingent-payments-announcement/
[92] Patrick McCorry. 2020. any.sender, transactions made simple. https://medium.com/anydot/any-sender-transactions-made-simple-34b36ba7519b
[93] Patrick McCorry, Chris Buckland, Bennet Yee, and Dawn Song. 2021. SoK: Validating Bridges as a Scaling Solution for Blockchains. *Cryptology ePrint Archive* (2021).
[94] Patrick McCorry, Malte Möser, and Syed Taha Ali. 2018. Why preventing a cryptocurrency exchange heist isn't good enough. In *Cambridge International Workshop on Security Protocols*.
[95] Patrick McCorry, Malte Möser, Siamak F Shahandasti, and Feng Hao. 2016. Towards bitcoin payment networks. In *Australasian Conference on Information Security and Privacy*.
[96] Andrew Miller, Iddo Bentov, Surya Bakshi, Ranjit Kumaresan, and Patrick McCorry. 2019. Sprites and state channels: Payment networks that go faster than lightning. In *Financial Cryptography and Data Security*.
[97] Mahdi H Miraz and David C Donald. 2019. Atomic cross-chain swaps: development, trajectory and potential of non-monetary digital token swap facilities. *Annals of Emerging Technologies in Computing (AETiC) Vol* (2019).
[98] Ayelet Mizrahi and Aviv Zohar. 2020. Congestion attacks in payment channel networks. *arXiv preprint arXiv:2002.06564* (2020).
[99] Malte Möser, Ittay Eyal, and Emin Gün Sirer. 2016. Bitcoin covenants. In *Financial Cryptography and Data Security*.
[100] Andrew Munro. 2018. *FOMO3D Ethereum ponzi game R1 ends as hot play outmaneuvers bots*. https://www.finder.com.au/fomo3d-ethereum-ponzi-game-r1-ends-as-hot-play-outmaneuvers-bots
[101] R Myerson. 1991. Game Theory: Analysis of Conflict Harvard Univ. *Press, Cambridge* (1991).
[102] Matthias Nadler. 2020. A quantitative analysis of the Ethereum fee market: How storing gas can result in more predictable prices.
[103] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. http://www.bitcoin.org/bitcoin.pdf
[104] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*.
[105] Ohad Barta. 2021. ZK Roll-Up Gas Consumption. https://twitter.com/OhadBarta/status/1463875770196049931
[106] OpenZeppelin. 2022. ECDSA Solidity Library. https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/cryptography/ECDSA.sol
[107] Optimism. 2021. Optimism website. https://www.optimism.io/
[108] Martin J Osborne and Ariel Rubinstein. 1994. *A course in game theory*.
[109] J François Outreville. 2014. Risk aversion, risk behavior, and demand for insurance: A survey. *Journal of Insurance Issues* (2014), 158–186.
[110] Paleko. 2020. The bZx attacks explained. https://www.palkeo.com/en/projets/ethereum/bzx.html
[111] Athanasios Papoulis and S Unnikrishna Pillai. 2002. *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education.
[112] Daniel Perez, Sam M Werner, Jiahua Xu, and Benjamin Livshits. 2021. Liquidations: DeFi on a Knife-edge. In *International Conference on Financial Cryptography and Data Security*. Springer, 457–476.
[113] Giuseppe Antonio Pierro, Henrique Rocha, Roberto Tonelli, and Stéphane Ducasse. 2020. Are the gas prices oracle reliable? a case study using the ethgasstation. In *2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 1–8.
[114] Joseph Poon and Vitalik Buterin. 2017. Plasma: Scalable autonomous smart contracts. *White paper* (2017), 1–47.
[115] Joseph Poon and Thaddeus Dryja. [n. d.]. The Bitcoin Lightning Network. http://lightning.network/lightning-network.pdf
[116] Joseph Poon and Thaddeus Dryja. 2016. The bitcoin lightning network: Scalable off-chain instant payments.
[117] John W Pratt. 1978. Risk aversion in the small and in the large. In *Uncertainty in economics*. Elsevier, 59–79.
[118] Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. 2021. An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. *arXiv preprint arXiv:2106.06389* (2021).
[119] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2021. Quantifying Blockchain Extractable Value: How dark is the forest? *arXiv preprint arXiv:2101.05511* (2021).
[120] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the defi ecosystem with flash loans for fun and profit. In *International Conference on Financial Cryptography and Data Security*. Springer, 3–32.
[121] Trevor A Reeve and Robert J Vigfusson. 2011. Evaluating the forecasting performance of commodity futures prices. *FRB International Finance Discussion Paper* 1025 (2011).
[122] Team Rocket. 2018. Snowflake to avalanche: A novel metastable consensus protocol family for cryptocurrencies. *Available [online]* (2018).
[123] Team Rocket, Maofan Yin, Kevin Sekniqi, Robbert van Renesse, and Emin Gün Sirer. 2019. Scalable and probabilistic leaderless BFT consensus through metastability. *arXiv preprint arXiv:1906.08936* (2019).
[124] Robert W Rosenthal. 1981. Games of perfect information, predatory pricing and the chain-store paradox. *Journal of Economic theory* (1981).
[125] Tim Roughgarden. 2010. Algorithmic game theory. *Commun. ACM* (2010).
[126] Tim Roughgarden. 2020. Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559. *arXiv preprint arXiv:2012.00854*

(2020).
[127] Mehdi Salehi, Jeremy Clark, and Mohammad Mannan. 2021. Red-Black Coins: Dai without liquidations. In *International Conference on Financial Cryptography and Data Security*. Springer, 136–145.
[128] Aetienne Sardon. 2021. Zero-Liquidation Loans: A Structured Product Approach to DeFi Lending. *arXiv preprint arXiv:2110.13533* (2021).
[129] Reinhard Selten. 1965. Spieltheoretische behandlung eines oligopolmodells mit nachfrageträgheit: Teil i: Bestimmung des dynamischen preisgleichgewichts. *Zeitschrift für die gesamte Staatswissenschaft/Journal of Institutional and Theoretical Economics* (1965).
[130] Andrey Shevchenko. 2021. Here are the best and worst times of the day to use Ethereum. https://cointelegraph.com/news/here-are-the-best-and-worst-times-of-the-day-to-use-ethereum
[131] Yoav Shoham and Kevin Leyton-Brown. 2008. *Multiagent systems: Algorithmic, game-theoretic, and logical foundations.*
[132] MacKenzie Sigalos. 2021. Ethereum had a rough September. Here's why and how it's being fixed. https://www.cnbc.com/2021/10/02/ethereum-had-a-rough-september-heres-why-and-how-it-gets-fixed.html
[133] Carl P Simon. 1994. *Mathematics for economists.* Norton & Company, Inc.
[134] Starkware. 2021. Starkware website. https://starkware.co/
[135] Nick T Thomopoulos, Nicholas T Thomopoulos, and Philipson. 2018. *Probability Distributions.* Springer.
[136] Kevin Tjiam, Rui Wang, Huanhuan Chen, and Kaitai Liang. 2021. Your Smart Contracts Are Not Secure: Investigating Arbitrageurs and Oracle Manipulators in Ethereum. In *Proceedings of the 3rd Workshop on Cyber-Security Arms Race.* 25–35.
[137] Ryan Todd. 2019. Synthetix suffers oracle attack, more than 37 million synthetic ether exposed. https://www.theblockcrypto.com/linked/28748/synthetix-suffers-oracle-attack-potentially-looting-37-million-synthetic-ether
[138] Christian P Traeger. 2014. Why uncertainty matters: discounting under intertemporal risk aversion and ambiguity. *Economic Theory* 56, 3 (2014), 627–664.
[139] Itay Tsabary and Ittay Eyal. 2018. The Gap Game. In *ACM CCS.*
[140] Itay Tsabary, Matan Yechieli, Alex Manuskin, and Ittay Eyal. 2021. MAD-HTLC: because HTLC is crazy-cheap to attack. In *2021 IEEE Symposium on Security and Privacy (SP).*
[141] Kemal Turksonmez, Marcin Furtak, Mike P Wittie, and David L Millman. 2021. Two Ways Gas Price Oracles Miss The Mark. In *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS).* IEEE, 1–7.
[142] UMA. 2020. How UMA solves the Oracle Problem. https://docs.umaproject.org/oracle/econ-architecture
[143] Pranay Valson. 2020. Transaction Fee Estimations: How To Save On Gas? https://medium.com/@pranay.valson/transaction-fee-estimations-how-to-save-on-gas-part-2-72f908b13d67
[144] Eric Van Damme. 2002. Strategic equilibrium. *Handbook of game theory with economic applications* (2002).
[145] Ron van der Meyden. 2019. On the specification and verification of atomic swap smart contracts. In *IEEE ICBC.*
[146] Sahana Venugopal. 2022. Users raise a stink over Sunflower Farmers NFT for gas fee spikes on Polygon. https://ambcrypto.com/users-raise-a-stink-over-sunflower-farmers-nft-for-gas-fee-spikes-on-polygon/
[147] Martin Swende Vitalik Buterin. 2021. EIP-3529: Reduction in Refunds. https://eips.ethereum.org/EIPS/eip-3529
[148] Helen M Walker and M Helen. 1985. De Moivre on the law of normal probability. *Smith, David Eugene. A source book in mathematics. Dover* (1985).
[149] Daniel Wang, Jay Zhou, Alex Wang, and Matthew Finestone. 2018. Loopring: A decentralized token exchange protocol. *URL https://github.com/Loopring/whitepaper/blob/master/en_whitepaper. pdf* (2018).
[150] Yuheng Wang, Jiliang Li, Zhou Su, and Yuyi Wang. 2022. Arbitrage attack: Miners of the world, unite!. In *Financial Cryptography and Data Security.*
[151] Zhipeng Wang, Kaihua Qin, Duc Vu Minh, and Arthur Gervais. 2022. Speculative Multipliers on DeFi: Quantifying On-Chain Leverage Risks. In *Financial Cryptography and Data Security.*
[152] Joel Watson. 2002. *Strategy: an introduction to game theory.*
[153] Sam M Werner, Paul J Pritz, and Daniel Perez. 2020. Step on the gas? A better approach for recommending the Ethereum gas price. In *Mathematical Research for Blockchain Economy.* Springer, 161–177.
[154] Fredrik Winzer, Benjamin Herd, and Sebastian Faust. 2019. Temporary censorship attacks in the presence of rational miners. In *2019 IEEE EuroS&PW.*
[155] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151, 2014 (2014), 1–32.
[156] Yingjie Xue and Maurice Herlihy. 2021. Hedging Against Sore Loser Attacks in Cross-Chain Transactions. *arXiv preprint arXiv:2105.06322* (2021).
[157] Anatoly Yakovenko. 2018. Solana: A new architecture for a high performance blockchain v0. 8.13. *Whitepaper* (2018).
[158] Alexei Zamyatin, Dominik Harz, Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, and William Knottenbelt. 2019. Xclaim: Trustless, interoperable, cryptocurrency-backed assets. In *2019 IEEE S&P.*
[159] Ming Zhao. 2021. Yield Farming is a Misnomer. https://twitter.com/FabiusMercurius/status/1454513434209312772
[160] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. 2021. On the just-in-time discovery of profit-generating transactions in defi protocols. *arXiv preprint arXiv:2103.02228* (2021).
[161] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. 2021. High-frequency trading on decentralized on-chain exchanges. In *2021 IEEE Symposium on Security and Privacy (SP).* IEEE, 428–445.
[162] Jean-Yves Zie, Jean-Christophe Deneuville, Jérémy Briffaut, and Benjamin Nguyen. 2019. Extending Atomic Cross-Chain Swaps. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology.*

A FUTURE-CONFIRMATION-DEPENDENT APPLICATIONS

We review two prevalent constructions whose security requires their future transactions to be confirmed in a timely manner. Failure of such confirmation can result in a safety violation, i.e., theft of tokens by unauthorized parties.

First, *roll-up* applications execute a bundle of transactions off-chain, and only publish on-chain the execution's summary for verification. There are two types of roll-ups, differing in their summary verification method: *Optimistic* roll-ups [78, 107] assume the published summary is correct, but include a dispute period in which transaction issuers can publish, on chain, proofs of fraud. Failing to include a proof of fraud during the dispute period can result with a safety violation, e.g., funds being stolen. *Zero-Knowledge (ZK)* roll-ups [11, 61, 73, 83, 134, 149] publish recurrent succinct correctness proofs along with the transaction summary, which are validated on-chain. Failing to include the transaction prevents the system progress, i.e., a liveness violation.

Additionally, *Hash Time Locked Contracts (HTLCs)* are an essential building block of cross-chain atomic swaps [72, 87, 88, 97, 145, 156, 162], off-chain state channels [41, 46, 47, 65, 95, 96, 116], vaults [19, 94, 99, 158], and contingent payments [9, 20, 23, 58, 91]. Conducted between two parties, an HTLC pays the first party for providing a suitable hash preimage (hash lock), or the other party after a timeout elapses (time lock). All these HTLC-based applications assume the first party is able to confirm the preimage transaction before the timeout elapses. If that assumption is not met, then the first party's tokens might be unjustly taken by the second party [81, 140, 154].

LedgerHedger allows all of these applications to reserve future transaction confirmation for when they will need it.

B PRICE-PREDICTION-MODEL VALIDATION

We compare Ethereum past *gas-price* measurements with a normal distribution, validating the random walk prediction model (§3.3).

First, we use Blockchair [16] to obtain measurements of Ethereum's blocks for September 2021, chosen arbitrarily. During this period, about 200K blocks (numbered 13136427 to 13330089) were created, for which we consider the *gas-price* as the ratio of the total paid fees and the total consumed gas (while ignoring empty blocks).

Then, we find the *gas-price* difference between each two consecutive blocks; the hypothesis is that these differences follow a normal distribution, i.e., they are each independently drawn from $N(\mu, \sigma^2)$, for some μ and σ^2 values.

To mitigate effects of long-lasting trends (e.g., *gas-price* increases at US day-time, where there is generally higher volume of trade

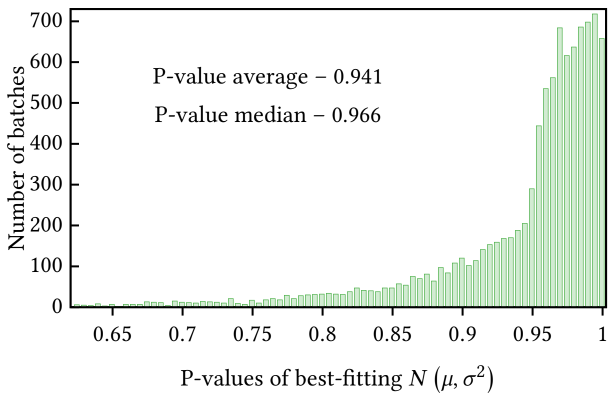


Figure 7: Kolmogorov–Smirnov test p-values for September 2021 Ethereum blocks and normal distributions.

and therefore higher demand), we split our samples to batches of 20 blocks, corresponding to an expected time period of 5 minutes. For each batch we numerically find μ and σ^2 values that maximizes the *p-value* for the Kolmogorov–Smirnov test [90], i.e., values of μ and σ^2 that maximize the probability that the *gas-price* change is drawn from $N(\mu, \sigma^2)$. We present histogram of the resultant *p-values* (significance levels) in Figure 7.

Figure 7 shows that, indeed, *gas-price* fluctuations for most of the examined batches can be modeled as drawn from a normal distribution with high probability, thus justifying the *gas-price* random walk model. Specifically, 99.8% of the batches are normally distributed with significance level of at least 0.5, 90.4% of batches are normally distributed with significance level of at least 0.85, and 66% of the batches are normally distributed with significance level of at least 0.95. Additionally, we note the average p-value is 0.941, and the median is 0.966, both indicating statistical significance that the samples were drawn from a normal distribution, verifying the hypothesis.

Finally, we consider the found normal distribution parameters μ and σ^2, presented (excluding a few outliers) in Figure 8.

Figure 8 shows the vast majority of batches are best-fitted with $\mu \approx 0$ and relatively low σ^2 values. Indeed, 98% of the examined batches are best-fitted with $\mu \in [-1, 1]$ and $\sigma^2 \leq 5$.

Repeating this analysis for different batch sizes (10, 40 and 80) yields similar results. We thus conclude that the random walk model describes with statistical significance the *gas-price* changes over the sampled period, and that each step has little drift, if any, and low variance.

C MODIFICATIONS

We present a few modifications to LedgerHedger that might be of practical interest. These focus on user experience in case of unintended usage, e.g., enabling *Buyer* to get the contract tokens earlier in case of no *Seller* accepting the contract. We also present a few modifications for reducing the contract overhead.

Enabling earlier refunds from a declined contract. First, one can consider a modification the *Recoup* function requires to be invoked after b_{acc} instead of during $[b_{start}, b_{end}]$. This allows *Buyer* to withdraw tokens from a declined contract at an earlier stage.

Note that initiating a contract that will not be accepted is not SPE – *Buyer* pays the initiation fees, and then later either forfeits her tokens or pays additional fees to withdraw them (Eq. 8).

Enabling refund from a non-depleted contract. Additionally, we can change the *Recoup* function to accept invocations after b_{end} if *Seller* accepted the contract, but then ignored it.

This allows *Buyer* to withdraw tokens in case *Seller* crashed. Similarly to the previous refund modification, initiating a contract that will be refunded is not SPE.

Higher ε values. Setting $\varepsilon = 1$ suffices to incentivize *Seller* to prefer confirming $tx_{payload}$ (assuming she meets the g_{alloc} quota). *Buyer* setting higher values for ε further improves this incentive, even in the presence of *Seller* having exogenous considerations for excluding $tx_{payload}$.

Setting $\varepsilon = 0$. Setting $\varepsilon = 0$ means *Buyer* has to pay (a single token) less for $tx_{payload}$. This, however, means *Seller* has the same benefit from confirming $tx_{payload}$ and from exhausting the contract (see Table .1). This change might be suitable if *Seller* is expected to prefer the former due to an exogenous consideration or due to being benign.

Hard coding block intervals. Our implementation takes as parameters b_{start} and b_{end}, indicating the block interval for transaction confirmation or contract exhaustion. However, this requires storing two values, and storing data is a rather costly operation [155]. Instead, one can create a contract with a hard coded interval length, and take only b_{start} as a parameter. This still enables enforcing the engagement interval, but requires storing one less variable.

D LEMMA 1 PROOF

Proof of Lemma 1. In the *PublishTx* subgame, *Buyer* chooses if to publish $tx_{payload}$ or not. Additionally, if she chooses to publish $tx_{payload}$ then she also decides what its gas consumption g_{pub} is.

Publishing $tx_{payload}$ (a_{pubTx}) leads to subgame $\Gamma^{Seller}_{FulfillTx}$. If so, her resultant wealth is $W_{Buyer}(\pi_{exec}, FulfillTx, \bar{s}_{\text{spe}}) = w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon + w^{exo}$ if $\pi_{exec} < \frac{payment+col+\varepsilon}{g_{pub}+g_{done}}$ and $g_{pub} \leq g_{alloc}$, and $w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon + \max(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0)$ otherwise (Eq. 4).

Alternatively, not publishing a transaction ($a_{noPubTx}$), leads to subgame $\Gamma^{Seller}_{FulfillNoTx}$. This results with wealth $W_{Buyer}(\pi_{exec}, FulfillNoTx, \bar{s}_{\text{spe}}) = w^{init}_{Buyer} - g_{init} \cdot \pi_{setup} - payment - \varepsilon + \max(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0)$ (Eq. 2).

Let us take note that $w^{exo} > 0$, $\pi_{exec} > 0$ and $g_{alloc} > 0$. Therefore, we get that $w^{exo} > \max(w^{exo} - g_{alloc} \cdot \pi_{exec}, 0)$. Subsequently, considering all the aforementioned options, the wealth of *Buyer* is maximized when $\pi_{exec} < \frac{payment+col+\varepsilon}{g_{pub}+g_{done}}$ and $g_{pub} \leq g_{alloc}$.

With that, let us consider the value of g_{pub}. First, setting $g_{pub} > g_{alloc}$ violates the mentioned condition, as *Seller* will not confirm $tx_{payload}$.

And, setting $g_{pub} < g_{alloc}$ is also unfavorable, as $g_{pub} \geq g_{alloc}$ is required to receive the w^{exo} tokens to begin with. Thus, publishing

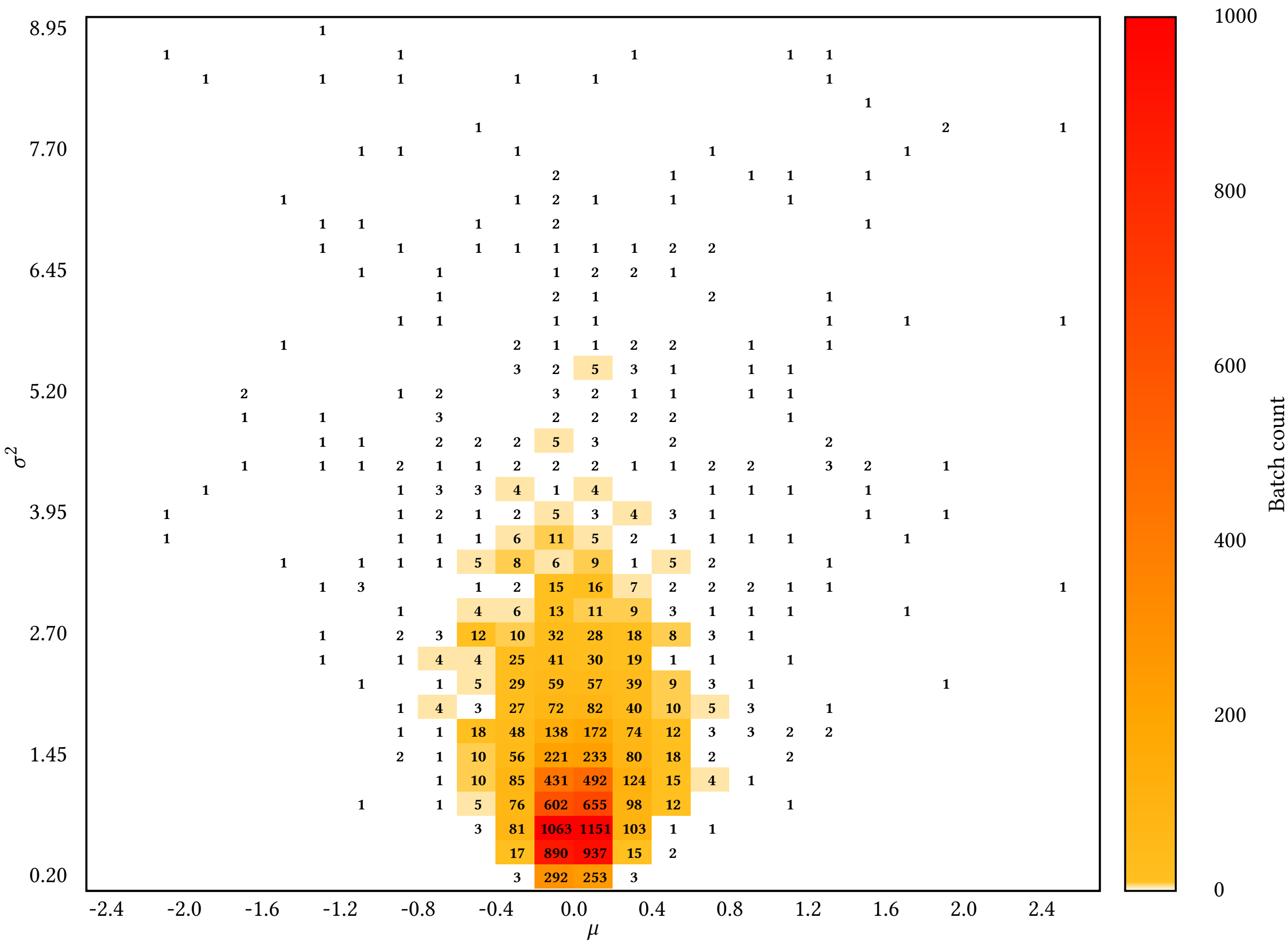


Figure 8: Best-fitted μ and σ^2 values for September 2021 Ethereum blocks.

a transaction that requires exactly $g_{pub} = g_{alloc}$ is the preferred action.

When $g_{pub} = g_{alloc}$, we get the condition for the preferable outcome is simply $\pi_{exec} < \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}}$, which is exactly the condition mentioned in the lemma, concluding its proof. □

E RESULTANT REQUIRED PRICE FOR LINEAR UTILITY FUNCTIONS

Recall Figure 5 shows that the required prices are fixed for the linear utility function, for both *Buyer* and *Seller*, for any considered $\mathcal{F}$. We thoroughly explain this result.

Broadly speaking, this holds due to $\Pr[\pi_{exec} < \pi_{bound}] = 1$, the linearity of the utility function, and the fact all considered distributions have the same mean value.

First, note that our parameter choice results in $\Pr[\pi_{exec} < \pi_{bound}] = 1$, where $\pi_{bound} = \frac{payment+col+\varepsilon}{g_{alloc}+g_{done}}$ (Lemma 1).

So, we get $W_{Seller}\left(\pi_{exec}, \Gamma^{Buyer}_{PublishTx}, \bar{s}_{\text{spe}}\right)$ (Eq. 5) and $W_{Buyer}\left(\pi_{exec}, \Gamma^{Buyer}_{PublishTx}, \bar{s}_{\text{spe}}\right)$ (Eq. 6) are *linear* in π_{exec}. This is in contrast to parameter values where $0 < \Pr[\pi_{exec} < \pi_{bound}] < 1$, resulting in *piece-wise linear* functions of π_{exec}.

Following that, consider the linear utility Linear is also a linear function, so both $U_{Seller}\left(\Gamma^{Buyer}_{PublishTx}, \bar{s}_{\text{spe}}\right)$ and $U_{Buyer}\left(\Gamma^{Buyer}_{PublishTx}, \bar{s}_{\text{spe}}\right)$ are also linear in π_{exec}.

When considering the expected utility (e.g., Eq. 10), the integration is therefore of a linear function. Let us denote that function as $a\pi_{exec} + b$ for some constants a and b, and note that $\int_{-\infty}^{\infty} (a\pi_{exec} + b) \cdot \mathcal{F}_{\text{pdf}}(\pi_{exec})\, d\pi_{exec} = a\int_{-\infty}^{\infty} \pi_{exec} \cdot \mathcal{F}_{\text{pdf}}(\pi_{exec})\, d\pi_{exec} + b\int_{-\infty}^{\infty} \mathcal{F}_{\text{pdf}}(\pi_{exec})\, d\pi_{exec}$.

The result of the first integral $\int_{-\infty}^{\infty} \pi_{exec} \cdot \mathcal{F}_{\text{pdf}}(\pi_{exec})\, d\pi_{exec}$ is the distribution's mean value, which is equal for all our considered distributions. The result of the second integral $\int_{-\infty}^{\infty} \mathcal{F}_{\text{pdf}}(\pi_{exec})\, d\pi_{exec}$ is exactly 1, as $\mathcal{F}_{\text{pdf}}(\pi_{exec})$ is a probability density function.

So, we get that the expected utility from the $\Gamma^{Buyer}_{PublishTx}$ subgame is equal for all distributions. Similar considerations apply to the expected utility from the Γ^{Buyer}_{NoLH} subgame, resulting with these expected utility differences being constant across the distributions, as indicated by Figure 5.

Table 2: Ethereum Goerli Network Deployment and Gas Requirements.

Invocation	Transaction Identifier	Consumed Gas
Initiate	`37d4a7332ad18753277c62b96f9e8b97` `d2f59c7aa22126dd23fe6825c361743f`	$g_{init} = 117e3$
Recoup	`e8b69c4ae70f40e72e3a8df353c38e44` `9c176d9a4d7aee86b073e3a3a6a55531`	$g_{done} = 57.3e3$
Initiate	`7a47b67e574b748105ef31f6ebed8990` `c17a96f19ef01307779a6119edf2318f`	$g_{init} = 37.4e3$
Accept	`b5607e9c499279c7bd4b0abf2f3d212b` `b3c294c684d87678cd06dd5d049a6b26`	$g_{accept} = 50e3$
Exhaust	`c482ad2b3bfc1ca64b83e8fcdc29fe82` `652ef7d839fc24323d035f8aba0b66b0`	$g_{alloc} + g_{done} = 3.021e6$
Initiate	`9fee96dcfedd8f94e5442c1d8d50c92e` `40bcfbf27ae512f9e2e3b01e670b005f`	$g_{init} = 37.4e3$
Accept	`b0f3cd808d5ad637b94541f3519614dc` `444d2c76eaf60e4917f32bfc57df6eb9`	$g_{accept} = 50e3$
Apply	`facb062758d24a2266b3e6d989ffe430` `202fdc2f23f4f73a585945e132fe0d7b`	$g_{pub} + g_{done} = 2.668e6$
Arbitrary *tx* without *Apply*	`27b4ad41e814d432a6c3e060eee6c6e7` `f7e8fdc615b904548dfd9387db79020a`	$g_{pub} = 63e3$
Arbitrary *tx* with *Apply*	`b8a45902b247cd812e784e940ed822c3` `cf8155a732b09ced2823fc27265fb7e2`	$g_{pub} + g_{done} = 75e3$

F GOERLI TEST NETWORK DEPLOYMENT

Table 2 presents our deployment of LedgerHedger on the Goerli Ethereum test network. It lists the invoked contract function, the transaction identifiers, and the consumed gas.

We took the following approach to verify the gas overhead of *Apply* produced by our local profiler. We created another meta-transaction, and performed its operations both with and without the contract. The gas consumption difference is $12e3$, matching the local profiler measurement $g_{done} = 12e3$. Table 2 includes the relevant transaction identifiers for this experiment as well.

G LEDGER-HEDGER SOLIDITY IMPLEMENTATION

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/utils/cryptography/ECDSA.sol";

struct MetaTx {
    uint256 nonce;
    address to;
    uint256 value;
    bytes callData;
}

enum State {
    INIT,
    REGISTERED,
    IDLE
}

contract GasFuture {
    uint256 public nonce;

    uint32 public startBlock;
    uint32 public endBlock;
    uint32 public regBlock;

    address public buyer;
    address public seller;
    uint256 public gasHedged;

    uint256 public collateral;
    uint256 public payment;
    uint256 public eps;

    State public status;

    constructor(address _owner) public {
        buyer = _owner;
        status = State.IDLE;
    }

    receive() external payable {}

    function init(
        uint32 _regBlock,
        uint32 _startBlock,
        uint32 _endBlock,
        uint256 _gasHedged,
        uint256 _col,
        uint256 _eps
    ) external payable {
```

```
    require(buyer == msg.sender, "Not␣owner");
    require(block.number <= _regBlock && _regBlock < _startBlock
                && _startBlock <= _endBlock, "block␣out␣of␣bound");
    // NOTE: Optionally let this be reinitiated if depeleted
    require(status == State.IDLE, "Contract␣already␣initialized");
    require(_gasHedged > 0, "Hedged␣amount␣can't␣be␣negative");
    require(_col >= 0, "Collateral␣can't␣be␣negative");
    require(_eps > 0, "Epsilon␣can't␣be␣negative");
    require(msg.value > eps, "Payment␣can't␣be␣negative");

    regBlock = _regBlock;
    startBlock = _startBlock;
    endBlock = _endBlock;

    gasHedged = _gasHedged;

    eps = _eps;
    payment = msg.value - eps;
    collateral = _col;

    status = State.INIT;
}

// The callers of the function sets themselves as the gasPayer
function register() external payable {
    require(block.number <= regBlock, "Register␣block␣expired");
    require(status == State.INIT, "Contract␣not␣initialized");
    require(msg.value >= collateral, "Insufficient␣collateral␣provided");
    seller = msg.sender;
    status = State.REGISTERED;
}

function refund() external {
    require(block.number >= startBlock
                && block.number <= endBlock, "Block␣must␣be␣between␣start␣and␣end");
    require(status == State.INIT, "Contract␣must␣be␣only␣initiated");
    require(msg.sender == buyer, "Not␣owner");
    status = State.IDLE;
    buyer.call{ value: payment + eps }("");
                // the payment is sent to the buyer anyway
}

function execute(MetaTx memory _metaTx, bytes memory _sig) external {
    require(block.number >= startBlock
                && block.number <= endBlock, "Block␣must␣be␣between␣start␣and␣end");
    require(status == State.REGISTERED, "Contract␣not␣registered");
    require(msg.sender == seller, "Wrong␣seller");
    status = State.IDLE;
    verifyAndExecute(_metaTx, _sig);
    seller.call{ value: collateral + payment + eps }("");
                // the payment is sent to the seller anyway
}
```

```
    function exhaust() external {
        require(block.number >= startBlock
                        && block.number <= endBlock, "Block␣must␣be␣between␣start␣and␣end");
        require(status == State.REGISTERED, "Contract␣not␣registered");
        require(msg.sender == seller, "Wrong␣seller");
        loopUntil();
        status = State.IDLE;
        seller.call{ value: collateral + payment }("");
                        // the payment is sent to the seller anyway
    }

    function verifyAndExecute(MetaTx memory _metaTx, bytes memory _sig)
                        public returns (bytes memory) {
        require(_metaTx.nonce == nonce, "Nonce␣incorrect");
        bytes32 metaTxHash = keccak256(abi.encode(_metaTx.nonce,
                        _metaTx.to, _metaTx.value, _metaTx.callData));
        address signer = ECDSA.recover(ECDSA.toEthSignedMessageHash(metaTxHash), _sig);
        require(buyer == signer, "UNAUTH");
        nonce++; // We up the nonce regardless of success
        (bool _success, bytes memory _result) = _metaTx.to.call{
                        value: _metaTx.value }(_metaTx.callData);
        if (status == State.INIT) {
            require(address(this).balance >= payment + eps,
                                "cannot␣spend␣locked␣funds");
        } else if (status == State.REGISTERED) {
            require(address(this).balance >= payment + eps + collateral,
                                "cannot␣spend␣locked␣funds");
        }
        return _result;
    }

    function loopUntil() public {
        uint256 i = 0;
        uint256 times = (gasHedged - 23330) / 117;
        for (i; i < times; i++) {}
    }
}
```