

Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts

Kushal Babel* Philip Daian* Mahimna Kelkar* Ari Juels

Cornell Tech, Cornell University, and IC3

September 9, 2021

Abstract

We introduce the *Clockwork Finance Framework* (CFF), a general purpose, formal verification framework for mechanized reasoning about the economic security properties of *composed decentralized-finance (DeFi) smart contracts*.

CFF features three key properties. It is *contract complete*, meaning that it can model any smart contract platform and all its contracts—Turing complete or otherwise. It does so with asymptotically *optimal model size*. It is also *attack-exhaustive by construction*, meaning that it can automatically and mechanically extract all possible economic attacks on users’ cryptocurrency across modeled contracts.

Thanks to these properties, CFF can support multiple goals: economic security analysis of contracts by developers, analysis of DeFi trading risks by users, and optimization of arbitrage opportunities by bots or miners. Because CFF offers composability, it can support these goals with reasoning over any desired set of potentially interacting smart contract models.

We instantiate CFF as an executable model for Ethereum contracts that incorporates a state-of-the-art deductive verifier. Building on previous work, we introduce *extractable value* (EV), a new formal notion of economic security in composed DeFi contracts that is both a basis for CFF analyses and of general interest.

We construct modular, human-readable, composable CFF models of four popular, deployed DeFi protocols in Ethereum: Uniswap, Uniswap V2, Sushiswap, and MakerDAO, representing a combined 17 billion USD in value as of August 2021. We use these models to show experimentally that CFF is practical and can drive useful, data-based EV-based insights from real world transaction activity. *Without any explicitly programmed attack strategies*, CFF uncovers on average an expected \$56 million of EV per month in the recent past.

*The first three authors contributed equally to this work.

Contents

1	Introduction	3
2	Background and Related Work	6
2.1	Blockchain and Smart Contracts	6
2.2	Decentralized Finance	6
2.3	Formal Verification Tools	7
3	Clockwork Finance Formalism	8
3.1	Decentralized Finance Instruments	10
4	DeFi Composability	13
4.1	Characteristics of Contract Composition	14
4.2	Uniswap as a Price Oracle	15
4.3	Composition of multiple AMMs	16
4.4	MEV Bribery Contracts	17
4.5	Remarks on Composability	18
5	Clockwork Exploration in K	18
5.1	Why K?	18
5.2	Scaling Formal Verification for CFF	19
5.3	CFF Uniswap Model	20
6	Experimental Evaluation	21
6.1	Execution Validation and Performance Experiments	21
6.2	Mechanized Proofs of Non Composability	23
6.3	AMM Experiments	24
6.4	Composability Experiments	28
7	Conclusion	29
A	DeFi Exploits Background	32
A.1	Case Study on bZx attacks	33
B	Generalized MEV and Composability Definitions	33
C	CFF Details	34
C.1	Writing a CFF Model	34
C.2	Refinements to the Abstract Model	35
C.2.1	AMM Refinements	35
C.2.2	MakerDAO Refinements and Liquidation Auction	35
C.3	Mechanized Proofs	35
C.4	CFF Limitations	36
C.5	MEV Deep Dive	37
C.6	Bounding the MEV for AMMs	38

1 Introduction

The innovation of smart contracts has resulted in an explosion of decentralized applications on blockchains. Abstractly, smart contracts are pieces of code that run on blockchain platforms, such as Ethereum. They support rich (even Turing-complete) semantics, can trade in the underlying cryptocurrency, and can directly manipulate blockchain state. While early blockchains were built primarily to support currency transfer, newer ones with smart contracts have enabled a wide range of sophisticated and novel decentralized applications.

One particularly exciting area where smart contracts have been influential is decentralized finance (or *DeFi*), a general term for financial instruments built on top of public decentralized blockchains. DeFi contracts have realized a number of financial mechanisms and instruments (e.g., automated market makers [12], atomic swaps [34], and flash loans [40]) that cannot be replicated with fiat or real world assets, and have no analog in traditional financial systems. These innovations usually take advantage of two distinctive properties of smart contracts. These are *atomicity*, which means (potential) execution of multi-step transactions in an all-or-nothing manner, and *determinism*, meaning execution of state transitions without randomness and thus a unique transaction outcome for a given blockchain state. Smart contracts can also intercommunicate on-chain, which has led to DeFi instruments that can interoperate and *compose* to achieve functionality that transcends their independent functionalities.

Recent years, however, have seen a plethora of high-profile attacks on DeFi contracts (see, e.g., [14] for a recent survey), with attackers stealing billions in the aggregate. These attacks are primarily financial in nature and not pure software exploits; they leverage complex financial interactions among multiple DeFi contracts whose composition is poorly understood. Existing notions of software security and traditional bug-finding tools are insufficient to reason about or discover such attacks.

A range of literature [20, 21], has attempted to apply formal verification techniques to the study of DeFi security. These works, though, have typically been used to check for attack heuristics [48] that represent conventional software bugs in smart contracts or to validate formal security properties [28, 37] akin to those in standard software verification tools. More recently, some work [49] has applied formal verification tools to the economic security of DeFi contracts, quantifying such security by identifying optimum arbitrage strategies. While an important initial step, this work has focused on predetermined, known attack strategies, and lacks the generality to discover new economic attacks, rule out classes of attack, or provide upper bounds on the exploitable value of DeFi contracts.

Clockwork Finance. Motivated by the little-explored question of DeFi contracts’ economic security, in this paper we present *Clockwork Finance*¹ (*CF*), an approach to understanding the economic security properties of DeFi smart contracts and their composition. CF addresses the inherently economic nature of DeFi security properties by codifying the use of formal verification techniques to reason about the *profit* extractable from the system by a participant, rather than in terms of more traditional descriptions of software bugs as error states. CF relies on, and we

¹Our name comes from the Enlightenment notion of the cosmos as a clock, i.e., a fully deterministic and predictable machine, like the smart contract systems we consider. The Wikipedia definition of *clockwork universe* [1] notes: “In the history of science, the clockwork universe compares the universe to a mechanical clock ... making every aspect of the machine predictable.”

introduce in this paper, the first formal definition for the economic security of composed smart contracts, which we call *extractable value* (EV). EV generalizes *miner-extractable value* (MEV)—a metric previously used in [17] to study DeFi protocol impact on consensus security.²

Clockwork Finance Framework (CFF). We realize CF in the form of a powerful mechanized tool that we call the *Clockwork Finance Framework (CFF)*. To use CFF, a user wishing to analyze the economic security of a contract creates or reuses an existing formal model of the contract, as well as models for potentially composed contracts. CFF then offers three key functional properties:

- *Contract completeness:* CFF is *contract complete* in the sense that it can model DeFi (and other) contracts, such as those in Ethereum, with equivalent execution complexity to the native platform. That is, for all possible transactions (inputs), executing the formal CFF model of a contract requires time $\mathcal{O}(1)$ in its platform execution time. CFF introduces no execution blow-up or time penalty even for complex compositions of contracts. CFF also has **equal expressive power** as the contract platform to which it’s applied—again, such as Ethereum.
- *Optimal model size:* The model for a DeFi instrument is asymptotically optimal, in that there is at most a (small) constant-size increase in the size of the model compared to the target contract. One practical effect, as we show, is a need for minimal manual effort by users in creating contract models.
- *Attack-exhaustive by construction:* CFF can mechanically reason about the full space of possible state transitions for models and their compositions. CFF can in principle—given sufficient computation—identify any attack expressible as a condition of mempool transaction activity and target contract models. To achieve this property, CFF takes advantage of the determinism of smart contracts: it is generally much harder to reason exhaustively about probabilistic systems.

CFF also offers two important usability features:

- *Modularity:* CFF models are *modular*, meaning that once a model is realized for a particular contract, it can be used for any CFF execution involving that contract. Modularity also means that models are arbitrarily composable in CFF: Any and all models in a library can be invoked for a CFF analysis without customization.
- *Human-readability:* Although we do not show this experimentally, we show by example that CFF models are typically easier for human users to read, understand, and reason about than contract source code.

Taken together, these properties and features make CFF highly versatile and able to support a range of different uses. Designers of DeFi contracts can use CFF to reason about the economic security of their contracts and do so, critically, while reasoning about interactions with other contracts. Arbitrage bots and miners can use the same contract models to find profitable strategies

²CF can be extended to other metrics of economic security, e.g., arbitrageurs’ profits, profits of permissioned actors, etc., but we leave extensions to future work.

in real-time. Users can use CFF to reason about guarantees provided by the transactions they execute in the network, including the value at risk of exploits by miners, bots, and other network participants—which today is considerable in practice [17, 48]. We explore these various use cases in the paper.

CFF achieves more than mere measurement of economic security: It can *prove bounds* on the economic security of contracts, i.e., the maximum amount adversaries can extract from them. Furthermore, it can do so using only the formally specified models of interacting contracts. CFF *does not require manual coding of adversarial strategies*.

Notably, this means that CFF can illuminate potential adversarial strategies even when they were *not previously exploited* in the wild. This stands in contrast to existing work, where the focus has often been on specific predefined strategies encoded manually [48], or which has required error-prone effort to define an action-space manually beyond the mere contract code executing on the system [49]. We believe that use of CFF would be a helpful part of the standard security assessment process for smart contracts, alongside bug finding, auditing, and conventional formal verification.

Contributions. We summarize three concrete contributions and insights from our paper below:

- **Security Definitions** (Sections 3 and 4). We provide the first formal definitions for the economic security of smart contracts and their composition and thus the first principled basis for DeFi contract designers to reason about the economic security of their protocols. Our definitions are general enough to model different types of players with different capabilities (e.g., transaction reordering, censorship, inserting malicious transactions) for influencing the system state.
- **Clockwork Finance Framework (CFF) and Concrete Models** (Sections 3 and 5). We instantiate our definitions in our CFF tool in order to find arbitrage strategies and prove bounds on the economic security of smart contracts. We model within CFF and analyze four popular real-world contracts: Uniswap V1, Uniswap V2, SushiSwap, and MakerDAO. We compare our results against direct on-chain Ethereum Virtual Machine execution, showing that CFF execution of our models yields high-fidelity results.
- **Practical Attacks and Formal Proofs** (Section 6). Our CFF tool automatically discovers the main attack patterns seen in practice, uncovering highly profitable attacks in an automated way for the four contracts we model. These attacks exploit the price slippage or the lack of secure financial composition of DeFi contracts, and can be used by malicious miners (or others) to profit at the expense of ordinary users. Our tool also yields formal mathematical proofs for the upper bound on the value extractable from these attacks. By our conservative estimate, the potential impact of these attacks frequently exceeds the Ethereum block reward by two orders of magnitude (i.e., 10,000%). We also validate our attacks by simulating them on an archive node and have contributed the implementation of our simulation method into the latest public release of the Erigon client software.

CFF is the first smart-contract analytics tool to achieve contract completeness, optimal model size, and attack-exhaustive by construction, enabling it to bring new capabilities to ecosystem participants. Our CFF code is available at <https://github.com/defi-formal/cff/>.

2 Background and Related Work

Our work intersects with several well-studied areas which we briefly introduce here as background.

2.1 Blockchain and Smart Contracts

Smart contracts are executed in *transactions*, which, like ACID-style database transactions [44], modify the state of a cryptocurrency system atomically (that is, either the entire transaction executes or no component of the transaction executes). A transaction’s output and validity depends on both the system’s state and the code being executed, which can read and respond to this state. The state may also include user balances of tokens representing assets or of cryptocurrencies in the underlying system. In the smart contract setting, the primary purpose of the underlying blockchain is to order transactions. The execution of a transaction sequence is then deterministic, and can be computed by all parties. The sequencing of transactions is done by actors known as *miners* (or *validators* or *sequencers*, terms we use interchangeably).

A unique attribute of smart contract transactions that proves critical to decentralized finance is their ability to throw an unrecoverable error, reverting any side-effects of a transaction until that point and converting the transaction into a no-op. This allows actors to execute transactions in smart contracts that are reverted if some operation fails to complete as expected or yield desired profit.

2.2 Decentralized Finance

Decentralized Finance, or *DeFi*, is a general term for the ecosystem of financial products and protocols defined by smart contracts running on a blockchain. As of August 2021, the Ethereum DeFi space contains roughly 80bn USD of locked capital in smart contracts [2]. DeFi protocols or instruments have already been deployed for a wide range of use cases, and allow users to borrow, lend, exchange, or trade assets on a blockchain. Abstractly, a key goal of DeFi is to create composable and modular financial instruments that do not rely on a centralized issuing party. DeFi instruments can thus interoperate programatically without human intervention or complex cooperation among issuing entities. We provide a brief background on the two specific classes of DeFi instruments featured in this work.

Lending contracts. Some DeFi contracts lend a certain cryptocurrency (such as DAI in the Maker protocol [32]) to a user, with another user-supplied cryptocurrency (such as ETH) held by the contract as collateral. If the value of the collateral falls below a system-defined threshold, the financial instrument can automatically foreclose on the collateral to repay the loan without the cooperation of the borrower. This automated loan guarantee mitigates risk in a way attractive to lenders. Lending contracts can also underlie “stablecoin” protocols, which support tokens pegged to real-world currencies such as the U.S. dollar (e.g., as in the Maker protocol).

Decentralized exchanges. Another example of a DeFi instrument is a *decentralized exchange* (“DEX”). In a DEX, users can trade between different assets that have a digital representation (e.g., on a blockchain). A DEX facilitates the exchange of assets without the risk that one party in the exchange defaults or fails to execute their end of the asset swap. This guarantee protects users from counterparty risk present in traditional exchanges, especially cryptocurrency exchanges,

which have often violated users’ trust assumptions by absconding with funds [33, 36] or incorrectly executing user orders through technical errors and even fraud [43]. A special class of DEX called Automated Market Maker (“AMM”) eliminates the need for a counterparty to execute a swap. An AMM (like Uniswap or Sushiswap) maintains reserves of liquidity providers’ assets and allows swaps with a user’s assets at programatically self adjusting prices.

Miner extractable value. A notion called *MEV*, or *miner-extractable value*, introduced in [17], measures the extent to which miners can capture value from users through strategic placement and/or ordering of transactions. Miners have the power to dictate the inclusion and ordering of mempool transaction in blocks. (Thus MEV is a superset of the front-running/arbitrage profits capturable by ordinary users or bots, because miners have strictly more power.) Previous studies of MEV have performed transaction-level measurements of the outcome of specific strategies (e.g., sandwiching attacks in [48] and pure revenue trade composition in [17]). Other work has abstracted away transaction-level dynamics, analyzing DeFi protocols such as AMMs using statistical modeling and economic agent-based simulation [6].

2.3 Formal Verification Tools

Formal verification is the study of computer programs through mathematical models in well-defined logics. It supports the proof of mathematical claims over the execution of programs, traditionally to reason about program safety and correctness. Formal verification has been applied to traditional financial systems in the past (like [38]) but as noted in Section 1, DeFi systems have novel properties not present in these older systems. Most formal verification works for smart contracts (such as [5, 7, 21, 37, 48]) do not reason about economic security and hence cannot characterize financial exploits in DeFi (i.e., they are not attack-exhaustive by construction). Recent work [49] has attempted to apply formal verification to find profitable arbitrage strategies but does not provide formal proofs of economic security. Moreover, the tool covers only certain types of manually encoded smart contract actions, so that the tool lacks contract completeness and optimal model sizes.

Our work aims to establish a clear translation interface between existing program verification tools and the unique security requirements of DeFi. We develop our models in the K Framework [42], which provides a formal semantics engine for analyzing and proving properties of programs. K allows developers to define models that are *mathematically formal*, *machine-executable*, and *human-readable*.

By *mathematically formal*, we mean that K uses an underlying theory called “matching logic” that allows claims expressed about programs in programming languages defined by K to be proven formally. Such proofs have been used in industry to verify the practical security properties of smart contracts that hold billions of dollars [23].

By *executable*, we mean that K provides concurrent and non-deterministic rewrite semantics [16] that allow for efficient execution of large programs in the developer-specified programming language model. Figure 1 shows the high-level goals of the K Framework, which include deriving an interpreter and compiler for a specified language semantics, as well as model-checking tools. We will show how these tools are useful for reasoning about DeFi contracts.

By *human-readable*, we mean that K provides output in a form that can serve as a reference for other mathematical models, as it uses only abstract and human-readable mathematical opera-

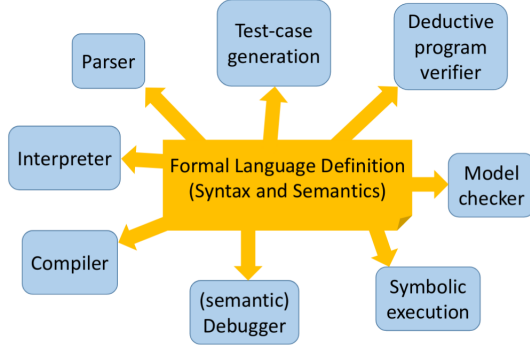


Figure 1: K Framework Fundamentals: In this figure from [42], the yellow box is a user-specified language model (like that in Section 5); blue boxes are tools generated automatically by the framework.

tions. Examples of human-readable K semantics include the Jello Paper for the Ethereum VM.³ Because DeFi contracts today lack standardized abstract models, we believe K’s abstract models are especially suitable to DeFi and hope they can ease both security analysis and communication of protocol functionality to users.

K is one of a number of formal verification tools; other common tools include Coq, Isabelle, etc. Indeed, several have been applied to model Ethereum-based systems in the past [5, 7, 21]. We refer the reader to [15, 16, 42] for details on the mathematical and formal foundations of K. We emphasize that our MEV-based secure composability definitions and general results are not specific to K.

3 Clockwork Finance Formalism

We introduce our formalism for Clockwork Finance in this section. It underpins the definition of *extractable value* (EV) we introduce in this paper. Our contract composability definitions in Section 4 are based in turn on that of EV. We let λ throughout denote the system security parameter.

Accounts and balances. We use A to denote the space of all possible accounts. For example, in Ethereum, accounts represent public key identifiers and are 160-bit strings (in other words, $A = \{0, 1\}^{160}$). We define two functions, **balance**: $A \times \mathbf{T} \rightarrow \mathbb{Z}$ and **data**: $A \rightarrow \{0, 1\}^d$ (where d is $\text{poly}(\lambda)$), that map an account to its current balance (for a given token \mathbf{T}) and its associated data (e.g., storage trie in Ethereum) respectively. For $a \in A$, as shorthand, we let **balance**(a) denote the balance of all tokens held in a and **balance**(a)[\mathbf{T}] denote the account balance of token \mathbf{T} . We use **balance**(a)[0] denote the balance of the primary token (e.g., ETH in Ethereum⁴).

³The “Jello Paper” (<https://jellopaper.org/>), based on [20], reimplements the original Ethereum yellow paper [45] in a machine executable, mathematically formal manner and can generate an Ethereum interpreter and contract proofs.

⁴We note that our usage of *token* to denote ETH is non-standard. While the ETH balance is stored differently than the balance of other tokens in Ethereum, we choose to model them using the same **balance** function for a cleaner (although equivalent) formalism.

We define the current *system state mapping* (or simply *state*) s as a combination of the account balance and data; that is, for an account a , $s(a) = (\text{balance}(a), \text{data}(a))$. We use \mathcal{S} to denote the space of all state mappings.

Smart contracts. As smart contracts in the system are globally accessible, we model them within the global state through the special 0 account. We let $\mathcal{C}(s)$ denote the set of contracts in state s of the system, which may change as new contracts are added. We use $\text{balance}(C, s)$ and $\text{data}(C, s)$ to denote the balance of tokens and the data (e.g., contract state and code) associated with a contract C in state s respectively.

Transactions. Transactions are polynomial-sized (in the security parameter) strings constructed by some player that are executed by the system and can change the system state. Abstractly, a transaction tx can be represented by its *action*: a function from \mathcal{S} to $\mathcal{S} \cup \{\perp\}$ transforms the current state mapping into a new state mapping. We denote this action function by $\text{action}(\text{tx})$. We say that a transaction tx is valid in state s if $\text{action}(\text{tx})(s) \neq \perp$ and use \mathcal{T}_s to denote the set of all valid transactions for state s . Our formalism is general enough to also allow transactions that add smart contracts to the system or interact with existing ones.

Blocks. We define a block $B = [\text{tx}_1, \dots, \text{tx}_l]$ to be an ordered list of transactions. We disregard block contents regarding consensus mechanics, e.g., nonce, blockhash, Merkle root which are not relevant for our framework. Of the block metadata, we only model the block number, denoted by $\text{num}(B)$. The action of a block can now be defined as the result of the action of the sequence of transactions it contains. We use $\text{action}(B)(s)$ to denote the state resulting from the action of B on starting state s . That is, $\text{action}(B)(s) = \text{action}(\text{tx}_l)(s_{l-1})$ where $s_0 = s$ and $s_i = \text{action}(\text{tx}_i)(s_{i-1})$. A block is said to be valid if all of its transactions are valid w.r.t. their corresponding input state (i.e., the state resulting from executing prior transactions sequentially).

We can analogously define the action of any sequence of transactions (even spanning multiple blocks)—a concept useful for analyzing reordering across blocks.

Network actors and mempools. Let \mathcal{P} denote the (unbounded) set of players in our system, and $P \in \mathcal{P}$ denote a specific player. We use \mathcal{T}_s to denote the global set of all valid transactions for state s , but note that not all transactions can be validly generated by all players. For a player $P \in \mathcal{P}$, we define a set $\mathcal{T}_{P,s} \subseteq \mathcal{T}_s$ as the transactions that can be validly created by P when the system is in state s . Transactions created by players are included in a mempool for the current state. A player P working as a miner to create a block may include any transactions currently in the mempool (i.e., transactions generated by other players) as well as any transactions in $\mathcal{T}_{P,s}$ that P generates itself. Abstractly, a “valid block” for a miner is any sequence of transactions that the miner has the *ability* to include. We use $\text{validBlocks}(P, s)$ to denote the set of all valid blocks that can be created by player P in state s if it could work as a miner. We use $\text{validBlocks}_k(P, s)$ to denote the set of valid k length block sequences (B_1, \dots, B_k) such that $B_1 \in \text{validBlocks}(P, s)$ and the other $B_i \in \text{validBlocks}(P, s_{i-1})$ where $s_0 = s$ and $s_j = \text{action}(B_j, s_{j-1})$.

Extractable value. Equipped with our basic formalism, we now define extractable value (EV), which intuitively represents the maximum value, expressed in terms of the primary token, that

can be extracted by a given player from a valid sequence of blocks that extends the current chain. Formally, for a state s , and a set \mathcal{B} of valid block sequences of length k , the EV for a player P with a set of accounts A_P is given by:

$$\text{EV}(P, \mathcal{B}, s) = \max_{(B_1, \dots, B_k) \in \mathcal{B}} \left\{ \sum_{a \in A_P} \text{balance}_k(a)[0] - \text{balance}_0(a)[0] \right\}.$$

where $s_0 = s = (\text{balance}_0, \text{data}_0)$, $s_i = \text{action}(B_i)(s_{i-1})$, and $s_k = (\text{balance}_k, \text{data}_k)$.

We also define miner-extractable value, which computes the maximum value that a *miner* can extract in a state s . Consider a player P working as a miner. The k -MEV of P in state s can now be defined as:

$$k\text{-MEV}(P, s) = \text{EV}(P, \text{validBlocks}_k(P, s), s).$$

Note that the parameter k is the length by which the current chain is extended. The most common scenario will be extension by a single block for which we will simply use MEV as shorthand henceforth. k -MEV does not account for how difficult it is to mine the k consecutive blocks, but it is sufficient for our purpose to understand the value that can be extracted if a single miner could append multiple blocks. In Appendix B, we define a weighted notion of miner-extractable-value that takes the probability of appending multiple blocks into account. We call this “weighted MEV” or WMEV.

3.1 Decentralized Finance Instruments

DeFi instruments. We define DeFi instruments quite broadly, as smart contracts that interact with tokens in some way other than through transaction fees. We provide three concrete examples of DeFi instruments, which we use in running examples throughout the paper and as building blocks to discuss properties at higher levels of abstraction.

In particular, we specify here: (1) A simplified Uniswap contract; (2) A simplified Maker contract; and (3) A simple betting contract. We note that while we use simplified versions of the original contracts, they are still useful as didactic tools and for analyzing the core semantic properties underlying contract composition. *Note, however, that our instantiations of the contracts in the CFF (see Section 5) include the missing details, i.e., are complete and usable for real-world data.*

Uniswap contract. The Uniswap automated market maker contract [3] allows a player to execute exchanges between two tokens (usually ETH and another token), according to a market-driven exchange rate. The contract assumes the role of the counterparty for such an exchange. Uniswap uses an automated market maker formula, called the $x \times y = k$ formula or the *constant product* formula. We discuss a simplified version here that does not deal with liquidity provisions, transaction fees, and rounding. Abstractly, for tokens \mathbf{X} and \mathbf{Y} , the number of coins x and y for these tokens in the contract always satisfies the invariant $x \times y = k$, where k is a constant. This equation can be used to determine the exchange rate between \mathbf{X} and \mathbf{Y} . If Δx coins of \mathbf{X} are sold (to the contract), Δy coins of \mathbf{Y} will be received (by the user) so as to satisfy:

$$x \times y = (x + \Delta x) \times (y - \Delta y).$$

Contract $C_{\text{uniswap}}^{(\mathbf{X}, \mathbf{Y})}$

```

function exchange(InToken, OutToken, InAmount):
  if balance(acccaller)[InToken] ≥ InAmount then
     $x = \text{balance}(C_{\text{uniswap}})[\text{InToken}]$ 
     $y = \text{balance}(C_{\text{uniswap}})[\text{OutToken}]$ 
    OutAmount =  $y - xy/(x + \text{InAmount})$ 
    balance(acccaller)[InToken] -= InAmount
    balance(acccaller)[OutToken] += OutAmount
    balance( $C_{\text{uniswap}}$ )[InToken] += InAmount
    balance( $C_{\text{uniswap}}$ )[OutToken] -= OutAmount
  else Output  $\perp$ 

```

Figure 2: Simplified abstract Uniswap contract

Figure 2 shows the pseudocode for our simplified Uniswap contract $C_{\text{uniswap}}^{(\mathbf{X}, \mathbf{Y})}$ for the tokens \mathbf{X} and \mathbf{Y} . It contains a function `exchange()` which allows a user to sell InAmount tokens of InToken to the contract in exchange for OutToken tokens where $(\text{InToken}, \text{OutToken}) \in \{(\mathbf{X}, \mathbf{Y}), (\mathbf{Y}, \mathbf{X})\}$. The number of OutToken tokens received by the user is determined by the $x \times y = k$ market maker formula.

Maker Contract. The Maker protocol allows users to generate and redeem the collateral-backed “stablecoin” Dai through Collateralized Debt Positions (CDPs). Users can take out a loan in Dai by depositing the required amount of an approved cryptocurrency (e.g., ETH) as collateral, and can pay back the loan in Dai to free up their collateral. If a user’s collateral value relative to their debt falls below a certain threshold called the “Liquidation Ratio” (> 1), then their collateral is auctioned off to other users in order to close the debt position. Maker uses a set of external feeds as price oracles to determine the value of the collateral. A separate governance mechanism is used to determine parameters like the Liquidation Ratio, stability fees (interest charged for the loan), etc., and also to approve external price oracle feeds and valid collateral types. We consider here a simplified version of Maker’s single-collateral CDP contract that does not model stability fees, or liquidation penalties. The contract $C_{\text{maker}}^{(\mathbf{X}, \mathbf{Y})}$ allows users to take out (or pay back) loans denominated in token \mathbf{X} by depositing (or withdrawing) the appropriate collateral in token \mathbf{Y} , and allows for liquidation as soon as the debt-to-collateral ratio drops below the Liquidation Ratio. The contract is detailed in Figure 3.

It should be noted that the amount of collateral liquidated and received by the liquidator as well as the debt (in Dai) paid off by the liquidator in exchange for the collateral depends on the outcome of a 2-phase auction. If the auction is perfectly *efficient*, the winning bidder pays off an equivalent amount of debt for receiving the offered collateral. On the other hand, when the auction is inefficient due to system congestion, collusion, transaction censoring, etc., the winning bidder can receive the entire collateral on offer without paying off an equivalent amount of debt. In our simplified Contract $C_{\text{maker}}^{(\mathbf{X}, \mathbf{Y})}$, we assume that liquidation is perfectly efficient.

```

Contract  $C_{\text{maker}}^{(X,Y)}$ 

threshold = 1.5; collateral = {}; debt = {};

function deposit_collateral(qty) :
  if balance(acccaller)[Y] ≥ qty then
    balance(acccaller)[Y] -= qty
    balance(Cmaker)[Y] += qty
    collateral[caller] += qty

function deposit_loan(qty) :
  if balance(acccaller)[X] ≥ qty and debt[caller] ≥ qty then
    balance(acccaller)[X] -= qty
    debt[caller] -= qty

function withdraw_collateral(qty) :
  if collateral[caller] ≥ qty and getprice(Y, X) * (collateral[caller] - qty) - threshold * debt[caller] ≥ 0
  then
    balance(acccaller)[Y] += qty
    balance(Cmaker)[Y] -= qty
    collateral[caller] -= qty

function withdraw_loan(qty) :
  if getprice(Y, X) * collateral[caller] - threshold * (debt[caller] + qty) ≥ 0 then
    balance(acccaller)[X] += qty
    debt[caller] += qty

function liquidate(acc) :
  if getprice(Y, X) * collateral[acc] - threshold * debt[acc] < 0 then
    balance(acccaller)[X] -= debt[acc]
    balance(acccaller)[Y] += debt[acc]/getprice(Y, X)
    balance(Cmaker)[Y] -= debt[acc]/getprice(Y, X)
    debt(acc) = 0
    collateral[acc] -= debt[acc]/getprice(Y, X)

function getprice(Y, X) :
  return  $\frac{\text{balance}(C_{\text{uniswap}})[X]}{\text{balance}(C_{\text{uniswap}})[Y]}$ 

```

Figure 3: Maker contract

Betting contract. To better understand composition failures, we introduce a simple betting contract and study its interaction with the previous contracts. Abstractly, the betting contract allows a user to place a bet against the contract on a future token exchange rate as determined by using Uniswap as a price oracle. By price oracle, we mean that the exchange rate between tokens

```

Contract  $C_{\text{pricebet}}^{\mathbf{X}}$ 

hasBet = false; player =  $\perp$ 
// Contract also initialized with 100 ETH tokens when created.

function bet():
  if (hasBet = false) and balance(acccaller)[ETH]  $\geq$  100 then
    balance(acccaller)[ETH] -= 100
    balance( $C_{\text{pricebet}}$ )[ETH] += 100
    hasBet = true; player = caller
  else Output  $\perp$ 

function getreward():
  if (hasBet = true) and  $\frac{\text{balance}(C_{\text{uniswap}}^{(\mathbf{X}, \text{ETH})}[\text{ETH}]}{\text{balance}(C_{\text{uniswap}}^{(\mathbf{X}, \text{ETH})}[\mathbf{X}]} > 1$  and (player = caller) and (current time is at most  $t$ )
  then
    balance(acccaller)[ETH] += 200
    balance( $C_{\text{pricebet}}$ )[ETH] -= 200
  else Output  $\perp$ 

```

Figure 4: Betting Contract C_{pricebet}

as determined by the Uniswap contract is used to drive decisions in another contract.

In Figure 4, we specify the contract $C_{\text{pricebet}}^{\mathbf{X}}$ that takes bets on the relative future price of token \mathbf{X} to ETH. Specifically, suppose that $C_{\text{pricebet}}^{\mathbf{X}}$ is initialized with a deposit of 100 ETH tokens. A user Alice can now call `bet()` and deposit 100 of her own ETH tokens to take a position against the contract. If at some point before the expiration time t , the Uniswap contract $C_{\text{uniswap}}^{(\mathbf{X}, \text{ETH})}$ contains more ETH tokens than \mathbf{X} tokens, (i.e., the Uniswap contract values \mathbf{X} more than ETH), Alice can call `getreward()` to claim 200 ETH from the contract, which includes her initial 100 ETH bet, along with her 100 ETH reward. Otherwise, Alice loses her initial bet.

For simplicity, our contract only contains a single bet, but it is straightforward to design similar contracts with more restrictions and/or functionalities (e.g., allowing another user to play the counterparty in the bet).

4 DeFi Composability

Smart contracts don't exist in isolation. A natural question, therefore, is when contracts “compose securely.” Abstractly, for a particular notion of security, does the security of a contract C_1 change when another contract C_2 is added to the system? In this paper, since our primary motivation is to analyze DeFi instruments, we focus on an economic notion of composable security. In particular, we look at how the extractable value of the system changes when new contracts are added to it. The *economic* composability of an existing DeFi instrument C_1 w.r.t. C_2 now pertains to the added monetary value that can be extracted if C_2 is introduced into the system. That is, C_1 is composable w.r.t. C_2 if adding C_2 to the system does not give an adversary significantly higher extraction gains.

For brevity, throughout this paper, we let *composability* refer to this specific notion, but note that it is orthogonal to previously considered notions (in, e.g., [27, 31]).

Ideally, we want contracts to be “robust” enough to compose securely with all other contracts. Unfortunately, this may be too strong a notion in practice. We thus parameterize our definitions to allow restricted or partial notions of composability. Definition 1 defines the simplest notion of contract composability.

Definition 1 (Defi Composability). Consider a state s and a player P . A DeFi instrument C' is ε -composable under (P, s) if

$$\text{MEV}(P, s') \leq (1 + \varepsilon) \text{MEV}(P, s).$$

Here s' is the state resulting from executing a transaction that adds the contract C' to s (no-op if C' already exists in the system). Although the composability of C' pertains to all contracts in $\mathcal{C}(s)$, when looking at the specific interaction with a $C \in \mathcal{C}(s)$, we may also write that C' is ε -composable with (C, P, s) .

In other words, allowing a player to interact with contract C' in a limited capacity (using at most the tokens that the player controls in s) does not significantly increase the profit the player can extract from the system. Note that Definition 1 can easily be extended to consider several states and or players.

4.1 Characteristics of Contract Composition

We find that DeFi instruments that are secure under composition according to Definition 1 are surprisingly uncommon, especially when two instruments depend on each other (e.g., one contract using the other as a price oracle). Intuitively, manipulating one contract can change the execution path of the other contract. In this section, we analyze the composition among the contracts (C_{uniswap} , C_{pricebet} , and C_{maker}) introduced in Section 3.1 to highlight interesting characteristics that can arise from smart contract composition. Note that for this simplified, didactic analysis, we do not make use of our CFF tool. We summarize our observed characteristics below.

Characteristic 1. Composability is state dependent, i.e., contracts may be ε -composable in some state s but not in another state s' .

Characteristic 2. Composability depends on the actions allowed for a player. For instance, contracts may be composable if only transaction reordering is allowed but not if the creation of new transactions is allowed as well.

Characteristic 3. A contract may not be composable with another instance of itself.

Characteristic 4. It is often possible to introduce *adversarial* contracts that break composability with minimal resources. Thus it is important to consider composability not just of existing contracts, but also over such adversarial contracts.

To provide intuition for these properties, we will analyze the following contract compositions. First, Section 4.2 considers the use of C_{uniswap} as a price oracle for either C_{pricebet} or C_{maker} . Section 4.3 analyzes the composition between multiple independent instances of C_{uniswap} . Finally, in Section 4.4, we introduce a new bribery contract that can be used to inject non-composability into the system.

4.2 Uniswap as a Price Oracle

Example 1 (C_{uniswap} as a price oracle for C_{pricebet}). Consider a simplified Uniswap contract (C_{uniswap}) that exchanges the tokens BBT and ETH, and a betting contract (C_{pricebet}) that uses it as a price oracle.

In particular, consider a system state s such that $\mathcal{C}(s) = \{C_{\text{uniswap}}\}$ (or alternatively $\mathcal{C}(s)$ contains other contracts that do not affect the composability). Suppose that in state s , C_{uniswap} contains b BBT tokens and e ETH tokens such that $b > e$. To denote the Uniswap transactions contained in the mempool in state s :

- Let $\mathcal{T}_{B \rightarrow E}$ be the set of transactions that sell BBT tokens to the contract in exchange for ETH tokens. Suppose the total number of BBT tokens transacted is b' .
- Let $\mathcal{T}_{E \rightarrow B}$ be the set of transactions that sell ETH to the contract in exchange for BBT tokens. Suppose that the total number of ETH transacted is e' .

For a player P , let p_e and p_b be the number of ETH and BBT tokens held by P in the state s that are not within pending transactions in the mempool. Note that P can use transactions from other accounts within the mempool as well as any transactions it can create with its own capital to create a block. Note that even if P does not have the hash power to mine blocks, it can pay some other miner to order transactions according to its preference. Let s' be the state resulting from adding C_{pricebet} to state s .

Composability is state dependent. It is easy to see that contracts that are independent of each other and provide orthogonal functionalities should compose securely in all states. In most real-world cases, however, we want to analyze the composability of contracts that are not independent and may in fact depend on each other's state. In such situations, whether two contracts compose securely will almost always depend on the characteristics of the current system state.

We use Example 1 to provide intuition to this observation. Specifically, we show that C_{uniswap} and C_{pricebet} are composable in states with a small number of available tokens, while in other states, an adversary can extract more MEV from the composition. Suppose that we define the number of *liquid tokens* in the Uniswap contract as follows: For player P and state s , we say that there are $l_b = l_b(P, s) = b' + p_b$ liquid BBT tokens and $l_e = l_e(P, s) = e' + p_e$ liquid ETH tokens. We will now show how composability can be affected by the number of liquid tokens in the current state.

a) *Composability in states with a small number of liquid tokens.* When $l_e \leq b - e$, i.e., the number of liquid tokens is sufficiently small, C_{uniswap} and C_{pricebet} do in fact compose securely. This is because regardless of what transactions P creates or how it orders existing transactions in the transaction pool, at no point in the execution of a created block can the number of ETH tokens in C_{uniswap} exceed the number of BBT tokens in it. In other words, P cannot maliciously create a short term fluctuation in the exchange rate in order to claim a reward from C_{pricebet} . Note that while P can still cause the exchange rate to be manipulated even if it cannot cause the number of ETH tokens to exceed the number of BBT tokens, since we are focusing only on composability with C_{pricebet} here specifically, P will not be able to claim the reward from C_{pricebet} .

Consequently, any value that P can extract in state s' (which adds the C_{pricebet} contract to state s) can also be extracted in state s . Equivalently, it holds that $\text{MEV}(P, s') = \text{MEV}(P, s)$ we conclude that C_{uniswap} is 0-composable under $(C_{\text{pricebet}}, P, s)$.

b) *Non-composability in other states.* Suppose now that our low liquidity assumption was no longer valid. In particular, we will consider states s such that $e' > b - e$, and $p_e \geq 100$. At least 100 ETH is necessary in our example to actually take a bet against the betting contract. To extract more value in state s , a malicious miner P can proceed as follows:

- 1) P inserts a transaction that takes a bet against the contract C_{pricebet} by depositing 100 ETH.
- 2) P orders all transactions in the set $\mathcal{T}_{E \rightarrow B}$. This raises the amount of ETH in C_{uniswap} temporarily.
- 3) P inserts a transaction (a call to `getreward()`) to claim the reward of 100 ETH (in addition to its original bet) from C_{pricebet} due to the short term fluctuation in the number of ETH in C_{uniswap} .
- 4) P orders the transactions in $\mathcal{T}_{B \rightarrow E}$ that buy ETH from C_{uniswap} .

Abstractly, by ordering all transactions that sell ETH to C_{uniswap} first, P can create a short-term volatility in the exchange rate between ETH and BBT, allowing P to claim the reward from C_{pricebet} . When the block created by P executes, since all transactions that add ETH to C_{uniswap} are ordered first, there will be more ETH tokens than BBT tokens by the time the P 's transaction to claim the reward from C_{pricebet} executes. This sudden change in the amount of ETH is only temporary as the remaining transactions in the block will reduce the number of ETH tokens. Note that this reordering attack is still possible in the case that $b' \approx e'$ and the natural or "fair" transaction order would not cause such a large change in the exchange rate during normal execution. Yet, the malicious miner P was able to profit simply by reordering user transactions.

Composability depends on the allowed actions. In the context of Example 1, if P cannot insert its own transactions for C_{uniswap} , then composability holds even if $p_e + e' - 100 > b - e > e'$ and $p_e \geq 100$, since P cannot create a large enough price fluctuation simply from the transactions in the mempool. However, if P has the ability to insert its own transactions, it can use the previously mentioned procedure to extract the reward from C_{pricebet} . P can also insert its transactions before and after user transactions to take advantage of the short term slippage in the Uniswap price. This strategy resembles the sandwiching attack described in [48], which combines frontrunning and backrunning. It also allows P to capitalize on the price differential between limit orders and market orders.

Uniswap as a price oracle for Maker. Similar problems arise when Uniswap is used as a price oracle in the Maker contract. By reordering Uniswap transactions, and thereby manipulating the currency exchange rate, a miner can cause the value of a user's collateral to fall below the acceptable threshold, and trigger a liquidation event. Furthermore, the miner can buy the user's collateral tokens in the liquidation event, and later sell them for a profit when the exchange price returns to normal.

4.3 Composition of multiple AMMs

Perhaps surprisingly, we find that even multiple contracts deployed with the same code need not be composable with each other. An interesting example of this non-composability is seen when two automated market makers (AMM) contracts co-exist in a system. Example 2 highlights this observation.

Example 2. Suppose that a state s contains two instances, C_{uniswap} and C_{uniswap}^* , of the Uniswap contract that exchange between the same two tokens (BBT and ETH). Let b, e be the number of BBT and ETH tokens respectively in C_{uniswap} , and let b^*, e^* be the number of BBT and ETH tokens respectively in C_{uniswap}^* .

Lemma 2. *If $be^* \neq b^*e$, then there exists a $\delta > 0$ such that for any $0 < \alpha < \delta$, a miner with at least α ETH (equiv. BBT) tokens can achieve an end balance of more than α ETH (equiv. BBT) tokens by only interacting with C_{uniswap} and C_{uniswap}^* .*

Proof. We prove for ETH tokens but note that the proof is exactly the same for BBT tokens. Let $U = \{C_{\text{uniswap}}, C_{\text{uniswap}}^*\}$. Consider the following sequence of transactions: (1) Deposit ETH in contract $A \in U$ to retrieve tokens of BBT; (2) Deposit the BBT tokens in $A' \in U \setminus A$ to get tokens of ETH. We will show that when $be^* \neq b^*e$, there exists a $\delta > 0$ such that depositing α ($0 < \alpha < \delta$) tokens in step (1) results in more than α tokens in step (2).

First, suppose that α_0 ETH tokens are deposited in C_{uniswap} in the first step. This results in $\frac{b\alpha_0}{e+\alpha_0}$ BBT tokens, which when deposited in C_{uniswap}^* gives back $\frac{be^*\alpha_0}{b^*e+b^*\alpha_0+b\alpha_0}$ ETH tokens. Similarly, if α_0 ETH tokens were first deposited in C_{uniswap}' , then the user would end up with $\frac{b^*e\alpha_0}{be^*+b\alpha_0+b^*\alpha_0}$ ETH tokens. Now, we consider the following cases:

Case (1) $be^* - b^*e > 0$. Let $\delta = \frac{be^* - b^*e}{b+b^*}$. Therefore, $b^*e + b\alpha + b^*\alpha < be^*$ which gives $\alpha < \frac{be^*\alpha}{b^*e+b\alpha+b^*\alpha}$. In other words, depositing first in C_{uniswap} and then in C_{uniswap}^* yields more ETH tokens than the initial deposit.

Case (2) $be^* - b^*e < 0$. This is analogous to the first case. Let $\delta = \frac{b^*e - be^*}{b+b^*}$. Therefore, $be^* + b\alpha + b^*\alpha < b^*e$ which gives $\alpha < \frac{b^*e\alpha}{be^*+b\alpha+b^*\alpha}$. In other words, depositing first in C_{uniswap}^* and then in C_{uniswap} yields more ETH than the initial deposit. \square

4.4 MEV Bribery Contracts

New contracts can be introduced into the system specifically with the goal of breaking composability. One such example is that of *bribery contracts*. The existence of MEV in a system can give rise to new bribery-based incentives for miners to choose the final transaction ordering. For instance, a user could bribe a miner to give her transactions preferential treatment (e.g., a better exchange rate for Uniswap transactions). Such bribes can be carried out securely through bribery contracts. Consider the following simple example.

Example 3. A user U and a miner P enter into a bribery smart contract with a payout as follows: P submits two valid transaction orderings, O_1 and O_2 , such that O_1 is preferred by U ; if O_1 is the order finalized by the ledger, P receives a payout proportional to the difference to the user U in value of O_1 and O_2 .

Intuitively, U is “bribing” the miner to provide U with a more profitable transaction ordering. To maximize its profit, a miner may potentially enter into multiple such bribery contracts with other users, and pick the best one to complete. Bribery contracts could also pose a threat to the long term stability of the system; given enough incentive, it could be worthwhile to mine a consensus block on a stale chain, thereby attempting to rewrite blockchain history. This is similar to time-bandit attacks, which as observed in [17] can be highly detrimental for current blockchain consensus protocols.

4.5 Remarks on Composability

We end with some remarks on our composition examples.

Takeaways for smart contract developers. Unfortunately, as our composition examples show, the security of a DeFi smart contract may not always depend solely on the contract’s code; design flaws in other contracts—even those deployed much later—may cause composability failures. This is problematic for contract developers since it implies that security of their contracts may in fact be out of their hands.

Remark on capital requirements. Several of our DeFi composability attacks in this section require the miner to possess some initial capital to carry out malicious transaction reorderings and extract MEV. Despite this, we note that in the real world, capital requirements will rarely be barriers to exploiting the system, even for smaller players, particularly due to the availability of flash loans. Flash loans are essentially risk-free loans that can be offered any time arbitrage or other profitable system behavior can be executed atomically, which is often the case. Flash loans also do not compose with contracts that were designed without flash loans; the attacks in [40] are an example of this. Consequently, adding flash loans to any of our non-composability examples in this section will only exacerbate the impact of malicious transaction reordering.

5 Clockwork Exploration in K

Equipped with our formalism for reasoning about the security of DeFi instruments, we now discuss how best to apply it to real-world contracts. To establish a formal methodology for DeFi security, we instantiate our Clockwork Finance Framework (CFF) into a mechanized proof system and symbolic execution engine using the K framework.

We start with an overview of design considerations for CFF and challenges with formal verification and how we overcome them. We then use the Uniswap contract (Figure 2) as an example to describe our CFF executable models.

5.1 Why K?

A natural question is why we chose the K framework specifically, among the plethora of available formal verification tools, for our implementation of the CFF. While CFF is suitable for instantiation using any good formal verification tool, we found K code to be especially human readable and intuitive (mainly because of its concurrent semantics) for developers who may not be experts in formal verification, making it likely to spur broader adoption. We chose K for a set of qualitative reasons, detailed in Section 2.3. Nevertheless, we emphasize that our results are not tool-specific, and should be straightforward to replicate using other tools.

K vs. Coq. As a specific comparison point, we explain our choice of K over Coq [30], another popular formal verification tool. A comparison in [4] found similar performance numbers for the proving engines of both K and Coq; simple formal proofs took approximately the same amount of real time on the test hardware. We posit (though defer detailed study) that performance differences between both these tools for our application would be minor.

As [4] points out, however, the models in the K framework are always executable, and allow for concrete inputs to programs to be evaluated. On the other hand, in Coq, such an execution must be defined separately as its own function and proved equivalent to the relational definition of the relevant models. We believe that this additional step would impose substantial overhead, especially on third-party developers of models for our framework (we discuss creating third-party models in Appendix C.1).

5.2 Scaling Formal Verification for CFF

Unfortunately, simply applying formal verification tools out-of-the-box to our models turns out to be impractical. To understand why, we need to step back and consider the number of paths from the start of model execution to termination of execution that must be explored by any formal verification tool, in an attempt to exhaustively prove a specific property holds in all possible executions. While general sound formal verification techniques are known to be undecidable, in practice they usually suffice for typical programs, where execution semantics are primarily linear. Branching conditions (e.g., control-flow branches) generally cause an increase in the number of paths to explore. Here, the number of paths that must be explored could be exponential in the number of branches in the program.

However, in our setting, miners can choose *any* any ordering of given transactions when creating a block. This means that the number of unique paths needed to fully explore the search space is $O(t!)$ where t is the number of transactions to which we apply the CFF. This is asymptotically and concretely more expensive than usual program verification proofs, and consequently impractical for even a modest number of transactions. One existing parallel in the literature is to semantics of concurrency (see e.g., [22]), in which many possible interleavings must be reasoned about. Nonetheless, most such tools either work with a small concurrency parameter, or do not attempt to exhaustively analyze the full state space of interleavings. They attempt only to find plausible bugs based on observed behavior.

Search-space reduction. To make formal verification practical, we must first reduce the search space to a tractable set of paths. We found that reasoning about all possible transaction orders in the formal model directly results in a large amount of repeated computation as equivalent states are explored (e.g., by re-ordering non-dependent transactions). Therefore, we apply simple lossless heuristics based on the specific DeFi instruments we are analyzing, to reduce the number of paths by excluding semantically equivalent orderings.

While we would ideally like to avoid encoding even these simple lossless heuristics, and our tool does allow us to do this, avoiding exploration of equivalent orderings proves to be a substantial optimization. Consider Uniswap trading for instance: if a miner makes multiple sequential trades selling an asset, exploring their re-orderings will have no effect, as Uniswap’s AMM function is path independent [12]. Even this simple optimization cuts the work required by our tool down by orders of magnitude, and renders the state space of larger problem instances feasible for CFF.

We encode several such optimizations manually in the `run_uniswapv2_experiments` and the `run_mcd_experiments` files provided in our repository. Similar optimizations will likely be helpful for any MEV analysis in our framework.

```

1 <k> exec(Address:ETHAddress in TokenIn:ETHAddress swaps TradeAmount:Int input for
   ↪ TokenOut:ETHAddress) =>
2   AmountToSend = (TradeAmount *Int USwapBalanceOut) /Int (USwapBalanceIn +Int TradeAmount);
3   Address in TokenIn gets 0 -Int TradeAmount;
4   Address in TokenOut gets USwapBalanceOut -Int var(AmountToSend);
5   Uniswap in TokenIn gets TradeAmount;
6   Uniswap in TokenOut gets 0 -Int var(AmountToSend);
7   ...
8 </k>
9 <S> ... (Uniswap in TokenOut) |-> USwapBalanceOut (Uniswap in TokenIn) |-> USwapBalanceIn ... </S>
10 <B> ... .List => ListItem(Address in TokenIn swaps TradeAmount input for TokenOut) </B>

```

Figure 5: Simplified Uniswap contract implemented in CFF. Ellipses match the rest of the program state in each cell.

5.3 CFF Uniswap Model

Figure 5 shows an implementation (in K) of a snippet of our abstract Uniswap contract from Figure 2. This takes our presented abstract contract and formalism and transforms it into a computer-readable executable model, capable of being symbolically and concretely reasoned about by the symbolic execution engine and deductive verifier bundled with K.

A few key differences exist between our abstract contract and executable CFF models. The first is that our executable CFF models contain an XML-like configuration consisting of *cells*, or mathematical objects in the K Framework. The *k*, *S*, and *B* cells of our executable model are featured in Figure 5. Recall that our model represents a state machine executing Uniswap transactions. The *k* cell specifies the transactions left to execute in the model and not yet included in a block, and can be viewed similarly to a program tape in a Turing-style execution machine. Note that execution of these transactions by CFF takes different paths corresponding to different orderings (including the original order in *k* cell) and censoring combinations of these transactions. The *S* cell represents the space of state mapping *S* in CFF (Section 3), and stores a mapping of addresses to balances (state entries). The *B* cell represents the prefix of the block that has been constructed thus far by CFF. The model is consistent with our formalism by maintaining the invariant $S = \text{action}(B)(s_0)$ where s_0 is the initial state. When no instructions are left to execute by CFF (empty *k* cell), the *B* cell will represent a valid block. The final state and the contents of the valid block potentially vary for different execution paths.

Another key difference is that our abstract contract has imperative semantics while K is fundamentally rewrite-based [16] using “ $A \Rightarrow B$ ” as a special operator meaning “*A* rewrites to *B*”. Lines 1-6 in Figure 5 correspond to one of the rewrite operators in our CFF Uniswap model. Line 1 in Figure 2 then corresponds to “*A*”, or the initial configuration of our model when this semantic rule applies. This semantic rule describes execution when the next instruction to execute (first transaction in the *k* cell, wrapped in an “exec” keyword) is a token swap on Uniswap for swapping a symbolic amount `TRADEAMOUNT` of the input token denoted by symbol `TOKENIN` for an output token denoted by symbol `TOKENOUT`. This swap rewrites to (“ \Rightarrow ”) a series of statements (Lines 2-6) that will execute one at a time with separate operational semantic rules in CFF. The ellipsis in the *k* cell signifies the remaining transactions, in *S* cell signifies the rest of the state mapping, and in the *B* cell signifies the prefix of the block constructed so far.

We leave further exploration of our executable models to the interested reader, and provide some more notes on K-specific keywords in the above model in Appendix C.1. We also describe some refinements necessary for a model that behaves the same as deployed DeFi contracts and discuss subtleties of modeling MakerDAO liquidations in Appendix C.2.

6 Experimental Evaluation

Using our full CFF models (not the simplified ones presented above), we ran several experiments on data from Uniswap V1, Uniswap V2, SushiSwap, and MakerDAO, which we detail here. We aim to experimentally address several key questions:

1. Are our CFF models accurate in reproducing the on-chain behavior of corresponding contracts? How efficient is this execution?
2. Can our models yield mechanized proofs about the extent of security of DeFi contracts and their composition while handling transaction reorderings and generic transaction insertions by miners?
3. Is use of our CFF models economically sensible in uncovering DeFi exploits on-chain?

Experimental setup. We ran most of our experiments on a mid-range server, equipped with an AMD EPYC 7401P 24-core server processor, 128GB of system memory, and a solid-state drive. For our computations, only the result is written to disk, and therefore our code is primarily CPU-intensive. We did not observe substantial memory overhead. For our parallelism experiments only, we used an AWS cluster of c5 instances with 256 vCPUs unless specified otherwise.

Dataset collection. We used Google’s BigQuery Ethereum to download every swap and liquidity event generated (until May 16, 2021) by Uniswap V1, Uniswap V2, and SushiSwap. These are three Uniswap-like AMMs that see substantial volume and are relevant to our analyses. In total, we collected 50,038,981 swaps, 2,317,917 liquidity addition events, and 844,709 liquidity removal events traded for 39,329 token pairs. For each token pair, we created a chronological log of all the events generated.

For MakerDAO, we used BigQuery to download all the log events generated (until May 16, 2021) by its core smart contract⁵ which manipulates CDPs (“vaults”) and updates stability fees and oracle prices. This data includes 322,771 CDP manipulation events (including 284 liquidations) across 18,642 CDPs and 25 collateral types. For each collateral type, we created a chronological log of all relevant events.

6.1 Execution Validation and Performance Experiments

We start with experiments to validate our CFF models with on-chain data and show the performance of our CFF tool.

⁵<https://github.com/makerdao/dss/blob/master/src/vat.sol>

CFF model validation. We empirically evaluated our CFF models on the collected data to ensure that our framework computes the correct final state, i.e., actual on-chain state. For the data from the three AMMs, we ran our executable semantics and inspected the resulting chain. We found that the chain state from our CFFs models differs minimally from the on-chain state. We discuss in Appendix C.4 the technical reasons for the small differences that do occur.

We evaluated our CFF Maker model similarly. We found that the stability fees and final debt and collateral values for each CDP before liquidation exactly match the chain state. Since we do not model the liquidation auction mechanism, we do not expect the Maker model to accurately derive the state after liquidation events. MEV reported in our experiments only depends on the state before the first liquidation. The state after liquidation does not affect our results.

We provide scripts to download, process, and validate data for each protocol in the `all-data` subfolder of our repository. This validation mechanism highlights the importance of executable formal semantics: execution is a key requirement for validating abstract formal models against real-world data. Our models do come with some important caveats, described in Appendix C.4.

CFF performance and parallelism. We evaluate the performance of our CFF for two types of functionalities. First, for different UniswapV2 token pairs, we execute all the on-chain UniswapV2 transactions that manipulate the state in the same order as they happened. This measures the execution time of our model, or the time to derive the full on-chain state from the list of transactions. In Figure 6, we show the time taken for our CFF to derive the state for different pairs as a function of the number of transactions executed for the pair. K’s internal execution engine intrinsically gives roughly a 4x parallel speedup, which can be seen in the figure as a speedup of real/wall execution time over the amount of total CPU time required to compute model state. These results, combined with our model validation, answer our first experimental question. Our modeling execution engine is sufficiently performant to ensure that our models’ output matches the full chain state on Ethereum for all relevant transactions using only commodity hardware. For instance, the most active pairs traded on any AMM contained about 100k transactions in our data, and it took under 2 hours of CPU time to parse this data and perform end-to-end model validation.

Second, we evaluate the performance for exploring all possible reorderings available to a miner as part of their extraction of MEV, and analyze how the computation of optimal miner orderings can be efficiently parallelized. This will allow us to use our models to also find transaction orderings not exploited by past miners. For these experiments, we use an AWS `c5.metal` bare metal instance optimized for computation. This machine features 96 3.9 GHz cores running on Intel’s Second Generation Xeon Cascade Lake processors, with 192GiB of available memory.

In Figure 7, we report the average execution times for attacks with 7, 8 and 9 transactions to be reordered using different number of CPU cores. As discussed in Section 6.3, blocks with 10 or more relevant transactions are rare. Transactions chosen for this particular figure are UniswapV2 transactions and MakerDAO transactions explored using a composition of our UniswapV2 and MakerDAO models, so as to be representative of our MEV extraction experiments described in Section 6.4 ; changing to a different transaction type that deals with our other models does not have any material impact on the reported numbers. Since we used a 96-core machine for our experiments, and given that K provides a 4x parallel speedup, we find that the real wall clock time converges to the fastest execution speed at around 24 worker threads before CPU limitations are reached. Given that our parallel exploration of possible state spaces has no synchronization between parallel workers, the embarrassingly parallel nature of this problem suggests future scaling

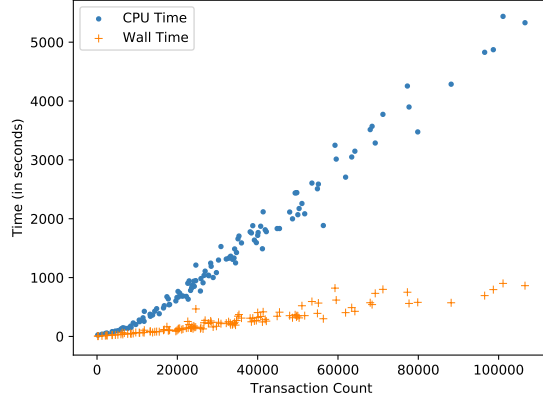


Figure 6: CFF execution time to evaluate and validate resultant state for a transaction sequence.

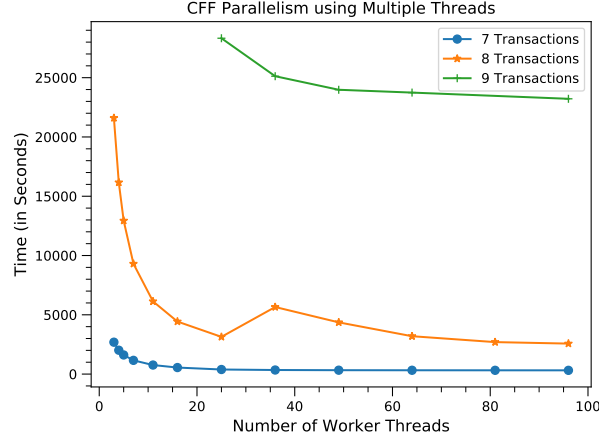


Figure 7: CFF Parallelism: Time taken to explore all reorderings with varying number of transactions (7,8,9) as a function of the number of threads used.

across machines to be a natural direction for handling larger problem instances. Before the scale ceiling of 24 parallel workers is hit, approximately linear scaling is visible in Figure 7, with some overhead associated with scheduling threads and managing shared system resources.

6.2 Mechanized Proofs of Non Composability

We now use the deductive program verifier (`kprove`) from the K framework along with our refined CFF models to assess the security of the composition of Sushiswap and UniswapV2. To achieve this, we specify the initial symbolic state to our CFF along with the set of relevant transactions available to the miner including generic transactions inserted by the miner. If the two contracts compose securely as per our definition in Section 3, then running `kprove` generates a deductive proof of the absence of MEV. On the other hand, when the composition under the specified initial state is insecure, `kprove` generates a counterexample MEV attack. The counterexample is a set of satisfiable formulae representing the amount of MEV in terms of the variables appearing in the

specified initial state and the transactions applied to it.

While our CFF can reason about the security of any specification of initial state and set of transactions, we describe an example detailed specification in Appendix C.3 capturing one of the biggest arbitrage opportunities⁶ observed on-chain involving two AMMs as reported in [39]. The attacker in this arbitrage made a profit of 76 ETH, while our CFF reports a higher MEV of 123 ETH *not captured by miners*. This example illustrates the power of CFF in finding opportunities left on the table by arbitrageurs currently. We plot the counterexample formula output by our CFF representing the available MEV opportunity as a function of the size of the trades inserted by the miner in Appendix C.3. Note that our refined mechanized models account for fees, slippage, and integer rounding and hence, the deduced size of the opportunity available to the miner is slightly less than the theoretical value derived in Section 4. We provide the full specification in the **proofs** sub-folder of our repository.

CFF can mechanically reason about the security of many disparate AMMs composed together, as well as more complex composed smart contracts, but we leave this to future work.

6.3 AMM Experiments

We ran a series of experiments on our CFF models for the three AMMs to understand the extent of MEV extractable from them, and prove the utility of our models further by furnishing real-world insights into available MEV. Our experiments are intended to validate the ability of our tool to uncover profit-seeking miner strategies, and can easily be used for other DeFi smart contracts.

Reordering to lower-bound MEV. We consider all possible transaction reorderings that can be performed by a miner. For this, we do not consider insertion of transactions by miners, and therefore we will find a lower bound on the MEV by computing the difference between the most profitable and least profitable transaction ordering with respect to a user who colludes with the miner to get the most profitable ordering. Effectively, this is the profit that a miner can make without needing any skin in the game, through a bribe from the user to provide her with the best possible ordering. We highlight in Appendix C.6 why this is a good proxy for MEV. In certain cases of restrictions imposed by other (wrapper) contracts involved in the transaction, not all reorderings might be valid. We validate the optimal ordering output by our tool by simulating it on an archive node. We have contributed our implementation for simulating historical reorderings into the latest public release of the Erigon client software and is now accessible via the `eth_callBundle` JSON-RPC API. Note that providing our CFF tool with the models of the other (wrapper) contracts interacting with the AMM contracts would ensure that the optimal reorderings output by our tool are automatically valid, however we defer this to future work.

For each AMM that we support, we conduct two kinds of analysis: First, we analyse the average MEV in a randomly sampled block (having transactions for any token pair) obtained by sampling 1000 blocks per month that have at least 2 relevant transactions. We report the 7-day moving average of MEV found per block as a time series plot in Figure 8. For the current calendar year, total MEV across all the AMMs in our random sample is 1.5 million USD, which by extrapolation comes to about 56 million USD per month in 2021. Second, we examine the token pairs with the top 10 highest number of transactions, and randomly sample 30 blocks involving these token pairs. Our tool can fully explore the state space for blocks with 9 or fewer AMM transactions; we call

⁶0x2c79cdd1a16767e90d55a1598c833f77c609e972ea0fa7622b70a67646a681a5

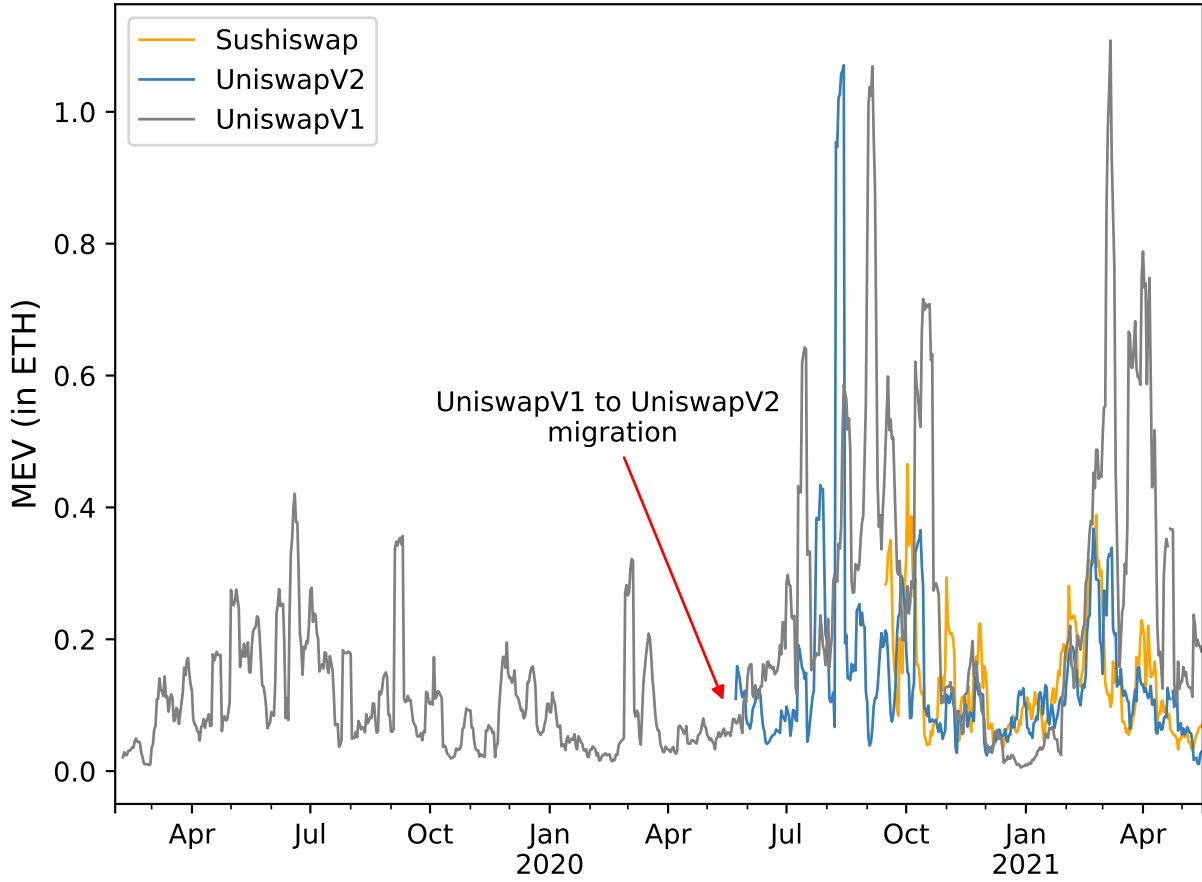
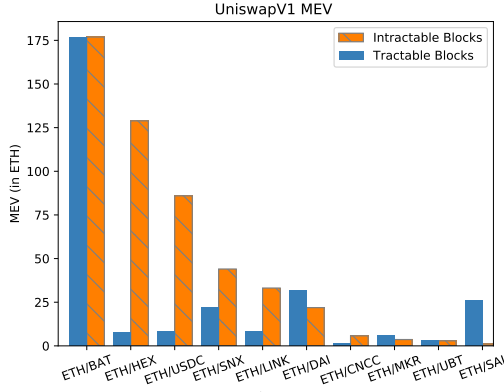


Figure 8: 7-day moving average of MEV per block in a random sample of 1000 random blocks in each month. 1 ETH \sim 3200 USD at the time of writing.

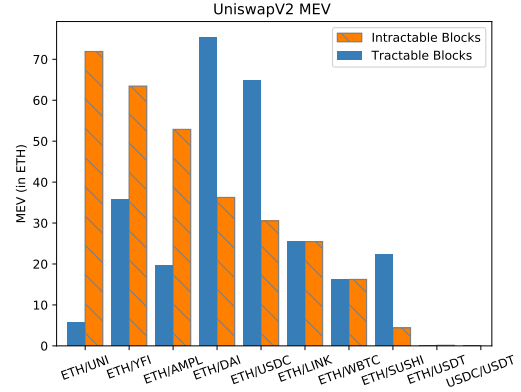
these blocks “tractable”. We report the average MEV found per block (for each token pair) in our random sample in Figure 9.

Intractable-block exploration. For blocks with 10 or more relevant AMM transactions, we do not explore the full search space. Instead, for these “intractable blocks,” we compute the MEV through a randomized search. We explore 400,000 paths, but randomize which paths are explored. The average MEV values for intractable blocks in our random sample are also reported in Figure 9. Because our primary aim was developing and validating our models’ ability to find attacks, we did not optimize this search for performance further. Using further optimization or more parallel computation could likely yield more accurate estimates for intractable blocks, but we defer this to future work. We found that “intractable” blocks are rare in our dataset. Figure 11 shows a histogram of number of blocks as a function of number of relevant AMM transactions they contain.

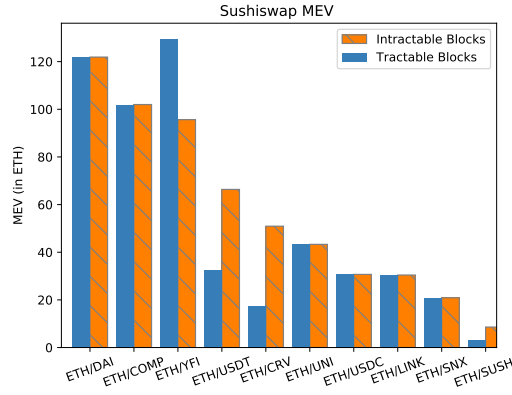
Approximate Convergence. To support our exploration of intractable blocks, a natural question is to what extent a random search on a sample of orderings approximates the MEV for a given



(a) Uniswap V1 MEV



(b) Uniswap V2 MEV

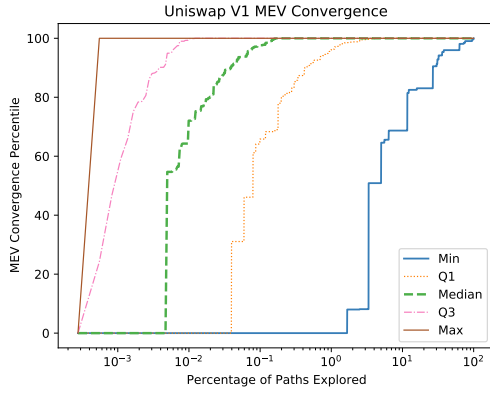


(c) Sushiswap MEV

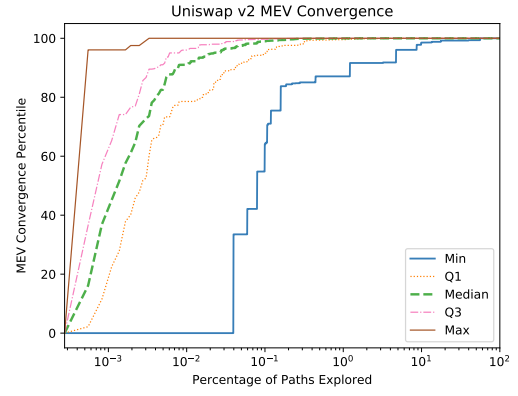
Figure 9: Highest observed MEV blocks for the top 10 most active token pairs in our dataset. Intractable blocks have 10 or more transactions involving the pair, and are partially explored by our tool through a random search.

block. For this, we look at how the MEV converges for tractable blocks as more paths are explored iteratively. For each AMM, we randomly explore the same tractable blocks in our random sample, and report the quartiles for MEV convergence in Figure 10. On average, we uncover 70% of the optimal MEV in more than 90% of the instances by exploring just 1% of the total paths. Since we explore 400,000 paths for intractable blocks, we explore roughly 11% of the total paths for blocks with 10 transactions, and roughly 1% of the total paths for blocks with 11 transactions. As evident from Figure 11, blocks with more than 11 transactions are even more rare among the intractable blocks.

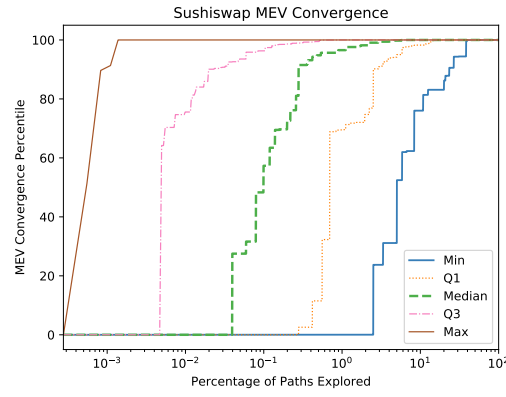
Reordering insights. Our results show that UniswapV2 exposes significantly less MEV compared to UniswapV1 and Sushiswap, thanks to the huge liquidity on UniswapV2. It is interesting to note that some of the token pairs have negligible MEV compared to the rest. It turns out that all of these pairs include a stablecoin (or are both stablecoins, e.g., USDC/USDT), which exposes only small price fluctuations for users across reorderings. On the other hand, pairs with unstable



(a) Uniswap V1 Convergence



(b) Uniswap V2 Convergence



(c) Sushiswap Convergence

Figure 10: Convergence towards the optimal MEV for different quartiles across the random sample vs Percentage of total paths explored for tractable blocks

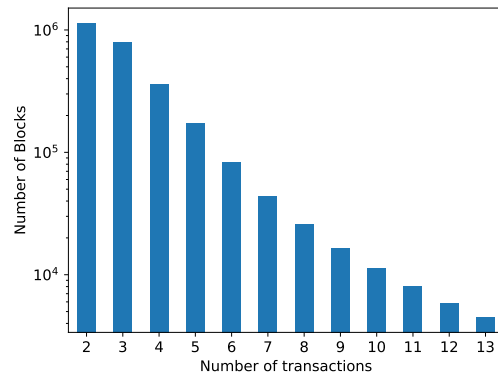


Figure 11: Histogram of number of blocks vs number of relevant AMM transactions they contain

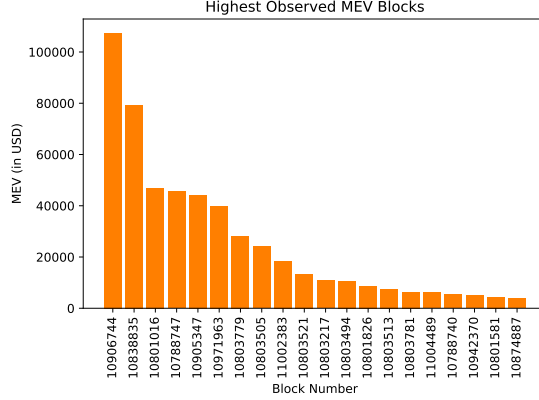


Figure 12: MEV for Maker composed with Uniswap V2

prices (UNI, YFI, BAT) expose the highest MEV (75-175 ETH). On manual examination, we find that the blocks exposing huge MEV (~ 100 ETH) often involve a user making a big purchase of token X with token Y and being either frontrun or backrun by an arbitrager. We provide a deep dive into a backrunning example—one of the highest MEV instances uncovered by our tool—in Appendix C.5.

6.4 Composability Experiments

To highlight the capability of our tool in finding MEV in the composition over multiple contracts, we consider our running example of the composition between MakerDAO and Uniswap. Here, we use the price from Uniswap V2 instead of the one from Maker’s oracle module. Although MakerDAO does not currently use Uniswap as a price oracle, making the attacks in this section purely theoretical, this change reflects similar proposals from over 60 projects (enumerated at <https://debank.com/ranking/oracle>), as well as academic results suggesting a possible security argument for such a change [6]. Using our tool, we can compute the MEV exposed as a result of MakerDAO adopting this potential composition.

Oracle attacks. We extend the AMM reordering experiments from Section 6.3 to allow for an additional miner action, where the miner can liquidate under-collateralized CDPs. Formally, if CDPs with index $1, \dots, n$ are open in the system, the set of transactions s is extended to include a liquidation of all n CDPs by a miner account M . We then compute the total amount of profit earned by M from any successful liquidations as a lower-bound metric for MEV.

To quantify this, we examine the on-chain data for the top 100 CDPs and blocks in MakerDAO when the CDPs are at the highest risk of liquidation (i.e. CDPs with the least collateral-to-debt ratio). For a given block, we consider possible reorderings over all Uniswap V2 and MakerDAO transactions, and then compute the MEV as a result of a miner possibly inserting a CDP liquidation transaction. We report this in Figure 12 for the top 20 blocks with the largest CDP liquidations (calculated using the value of the collateral at the time of liquidation). We found a total MEV of 542,827 USD in these blocks—orders of magnitude larger than the block rewards and transaction fees for these blocks. These experiments can be reproduced using the `run_mcd.experiments` script we provide in our Github repository.

7 Conclusion

We have introduced a powerful and novel approach—that adopts the lens of miner-extractable value (MEV)—for reasoning about and quantifying security guarantees for DeFi contracts and their interaction. We have instantiated a number of semantic models in a new computational framework, the Clockwork Finance Framework (CFF)—an executable proof system that allows us to reason about the financial security of smart contracts. We have provided open-source models, both abstract and executable, that represent key MEV-exposing deployed smart contracts. We have shown how our definitions enable powerful proofs of composition for popular smart contract protocols, a missing ingredient in the current deployment of DeFi contracts. We believe that MEV, smart contract composition, and formal verification can serve as viable key ingredients for empirically and rigorously measuring and improving DeFi contract security.

Acknowledgments

We thank Alexander Frolov for his contribution in developing the infrastructure needed to scale our experiments to an AWS cluster. This work was funded by NSF grants CNS-1564102, CNS-1704615, and CNS-1933655 as well as generous support from IC3 industry partners. Any opinions, findings, conclusions, or recommendations expressed here are those of the authors and may not reflect those of these sponsors.

References

- [1] http://wikipedia.org/wiki/Clockwork_universe.
- [2] <https://defipulse.com/>.
- [3] Hayden Adams. *Uniswap*. <https://uniswap.org/docs>. 2019.
- [4] Musab Alturki and Brandon Moore. *K vs. Coq as Language Verification Frameworks (Part 1 of 3)*. <https://runtimeverification.com/blog/k-vs-coq-as-language-verification-frameworks-part-1-of-3/>. 2019.
- [5] Sidney Amani et al. “Towards verifying Ethereum smart contract bytecode in Isabelle/HOL”. In: *CPP*. 2018, pp. 66–77.
- [6] Guillermo Angeris and Tarun Chitra. *Improved Price Oracles: Constant Function Market Makers*. 2020. arXiv: 2003.10001.
- [7] Andrei Arusoaie. *A Formal Semantics of Findel in Coq (Short Paper)*. 2019. arXiv: 1909.05464.
- [8] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. “A survey of attacks on Ethereum smart contracts (sok)”. In: *POST*. 2017, pp. 164–186.
- [9] Osato Avan-Nomayo. “\$100M Liquidated From Compound Following Flash Loan Exploit”. In: *beincrypto*. March 3 (2020).
- [10] Lorenz Breidenbach et al. “Enter the hydra: Towards principled bug bounties and exploit-resistant smart contracts”. In: *USENIX Security*. 2018, pp. 1335–1352.

- [11] Lorenz Breidenbach et al. *To sink frontrunners, send in the submarines*. <https://hackingdistributed.com/2017/08/28/submarine-sends/>. 2017.
- [12] Vitalik Buterin. *On Path Independence*. <https://vitalik.ca/general/2017/06/22/marketmakers.html>. 2017.
- [13] Vitalik Buterin. *Thinking about smart contract security*. <https://blog.ethereum.org/2016/06/19/thinking-smartcontract-security>. 2016.
- [14] Huashan Chen et al. “A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses”. In: *ACM Computing Surveys (CSUR)* 53.3 (2020), pp. 1–43.
- [15] Xiaohong Chen, Dorel Lucanu, and Grigore Roşu. *Matching Logic Explained*. Tech. rep. <http://hdl.handle.net/2142/107794>. 2020.
- [16] Xiaohong Chen and Grigore Roşu. “A Language-Independent Program Verification Framework”. In: *ISoLA*. 2018, pp. 92–102.
- [17] Philip Daian et al. “Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges”. In: *IEEE SP*. 2020.
- [18] Brady Dale. *DeFi Insurance Firm Nexus Mutual Makes Its First Payout Following bZx Attacks*. <https://www.coindesk.com/defi-insurance-firm-nexus-mutual-makes-its-first-payout-following-bzx-attacks>.
- [19] Ilya Grishchenko, Matteo Maffei, and Clara Schneidewind. “A semantic framework for the security analysis of Ethereum smart contracts”. In: *POST*. 2018, pp. 243–269.
- [20] Everett Hildenbrandt et al. “Kevm: A complete formal semantics of the ethereum virtual machine”. In: *CSF*. 2018, pp. 204–217.
- [21] Yoichi Hirai. “Defining the Ethereum virtual machine for interactive theorem provers”. In: *FC*. 2017, pp. 520–535.
- [22] Jeff Huang, Patrick O’Neil Meredith, and Grigore Rosu. “Maximal sound predictive race detection with control flow abstraction”. In: *Proceedings of the 35th ACM SIGPLAN conference on programming language design and implementation*. 2014, pp. 337–348.
- [23] Runtime Verification Inc. *Verified Smart Contracts*. <https://github.com/runtimeverification/verified-smart-contracts>. 2020.
- [24] Mahimna Kelkar, Soubhik Deb, and Sreeram Kannan. *Order-Fair Consensus in the Permissionless Setting*. Cryptology ePrint Archive, Report 2021/139. <https://eprint.iacr.org/2021/139>. 2021.
- [25] Mahimna Kelkar et al. “Order-Fairness for Byzantine Consensus”. In: *CRYPTO*. 2020, pp. 451–480.
- [26] Kyle J Kistner. *Post-Mortem [of the bZx Attack]*. <https://bzx.network/blog/postmortem-ethdenver>. 2020.
- [27] Ahmed Kosba et al. “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts”. In: *IEEE S&P*. 2016, pp. 839–858.
- [28] Johannes Krupp and Christian Rossow. “Teether: Gnawing at ethereum to automatically exploit smart contracts”. In: *USENIX Security*. 2018, pp. 1317–1333.

- [29] Klaus Kursawe. “Wendy, the Good Little Fairness Widget: Achieving Order Fairness for Blockchains”. In: *AFT*. 2020, pp. 25–36.
- [30] Xavier Leroy. “Formal verification of a realistic compiler”. In: *Communications of the ACM* 52.7 (2009), pp. 107–115.
- [31] Kevin Liao, Matthew A. Hammer, and Andrew Miller. “ILC: A Calculus for Composable, Computational Cryptography”. In: *PLDI*. 2019, 640–654.
- [32] MakerDAO. *The Maker Protocol: MakerDAO’s Multi-Collateral Dai (MCD) System*. <https://makerdao.com/en/whitepaper/>. 2020.
- [33] Robert McMillan. “The inside story of Mt. Gox, Bitcoin’s \$460 million disaster”. In: *Wired*. March 3 (2014).
- [34] Ron van der Meyden. “On the specification and verification of atomic swap smart contracts”. In: *ICBC*. 2019, pp. 176–179.
- [35] Andrew Miller et al. “The Honey Badger of BFT Protocols”. In: *ACM CCS*. 2016, pp. 31–42.
- [36] Tyler Moore and Nicolas Christin. “Beware the middleman: Empirical analysis of Bitcoin-exchange risk”. In: *FC*. 2013, pp. 25–33.
- [37] Daejun Park, Yi Zhang, and Grigore Rosu. “End-to-End Formal Verification of Ethereum 2.0 Deposit Smart Contract”. In: *CAV*. 2020, pp. 151–164.
- [38] Grant Olney Passmore and Denis Ignatovich. “Formal Verification of Financial Algorithms”. In: *CADe*. 2017, pp. 26–41.
- [39] Kaihua Qin, Liyi Zhou, and Arthur Gervais. *Quantifying Blockchain Extractable Value: How dark is the forest?* 2021. arXiv: 2101.05511.
- [40] Kaihua Qin et al. *Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit*. 2020. arXiv: 2003.03810.
- [41] Haseeb Qureshi. “A hacker stole \$31M of Ether—how it happened, and what it means for Ethereum”. In: *Freecodecamp.org, Jul 20, 2017* (2017).
- [42] Grigore Rosu. “K: A semantic framework for programming languages and formal analysis tools”. In: *Dependable Software Systems Engineering* 50 (2017), p. 186.
- [43] David Twomey and Andrew Mann. “Fraud and manipulation within cryptocurrency markets”. In: *Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation*. 2019. Chap. 8, pp. 205–250.
- [44] Gottfried Vossen. “Database transaction models”. In: *Computer Science Today*. 1995, pp. 560–574.
- [45] Gavin Wood. *Ethereum yellow paper*. <https://github.com/ethereum/yellowpaper>. 2014.
- [46] Insu Yun et al. “{QSYM}: A practical concolic execution engine tailored for hybrid fuzzing”. In: *USENIX Security*. 2018, pp. 745–761.
- [47] Yunhao Zhang et al. “Byzantine Ordered Consensus without Byzantine Oligarchy”. In: *OSDI*. 2020, pp. 633–649.
- [48] Liyi Zhou et al. *High-Frequency Trading on Decentralized On-Chain Exchanges*. 2020. arXiv: 2009.14021.

- [49] Liyi Zhou et al. *On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols*. 2021. arXiv: 2103.02228.

A DeFi Exploits Background

Attacks and arbitrage. A number of practical issues arise in the deployment of secure DeFi systems. The first carries over from traditional software systems, since the guarantees upheld by any financial instruments are only as good as the software that underlies them. Both smart contracts in general and DeFi instruments have seen a wide number of software failures that eroded their security guarantees (e.g., [8, 40, 41]), as well as corresponding academic and practical interest in rectifying these failures (e.g., [10, 14, 19, 20, 28]).

Further security concerns occur when the intended design and functional guarantees provided by DeFi systems do not align with the financial guarantees desired by users. For instance, in decentralized exchanges, while some users may assume that “secure” exchange implies fair execution of their submitted orders, recent work [17] finds that the core system design itself could prove unfair to its users, detailing how inefficiency can be exploited by arbitrageurs to introduce systematic security failures. In many instances, because “attacks” (e.g., arbitrage) involve exploiting inefficiencies in DeFi systems in unexpected ways to profit financially, it makes sense to express security properties from an economic standpoint. Consequently, for DeFi systems, the distinction between profit-seeking techniques like arbitrage, and security failures can become difficult to draw.

Sometimes, the distinction is obvious. A typographical error in the program of a smart contract (as described in [13]) is one common source of funds-loss that can be clearly categorized as a “code bug.” Similarly, a decentralized exchange that is designed to allow arbitrage by programmatic actors analogous to those in traditional financial exchanges can be clearly classified as “financial arbitrage” [17], and therefore not a security vulnerability.

Unfortunately, many DeFi exploits fall less clearly into either category. A noteworthy example is the string of recent high-profile attacks on the bZx DeFi protocol, which relied on data from several external DeFi instruments. An attacker was able to break the invariants of the external contracts and use them to profit from the bZx protocol. Now, invariant checks could easily have been done within the bZx protocol code, in which case the root cause would be a software failure of the bZx contract. At the same time, the exploit could also be viewed as a design flaw since it is impossible to determine during the execution of a DeFi transaction, whether the external feed has been manipulated through arbitrage. In Appendix A.1, we use the bZx attacks as a case study to understand how the distinction between software exploits and fundamental design failures manifests in the real world.

Fair ordering consensus protocols. Motivated by frontrunning attacks, recent work (e.g., [24, 25, 29, 47]) has attempted to solve the transaction reordering problem at the consensus layer by introducing new consensus protocols with useful fair ordering properties. Other techniques (e.g., [11, 35]) aim to hide transaction contents before they are sequenced to prevent some forms of adversarial frontrunning. Fair ordering protocols have not yet been deployed, and current techniques require substantial design changes, and add significant latency to the system, which could be undesirable. Furthermore, a constrained level of arbitrage may actually be deemed acceptable, or even necessary to provide financial incentives for users.

Our work does not focus on solving the problem of MEV-based attacks. Instead, we provide the formal tools necessary for smart contract designers to understand the extent of MEV exposed by their systems, and evaluate the design and usability tradeoffs that suit their specific applications.

A.1 Case Study on bZx attacks

In this section, we use the attacks on the bZx protocol to understand the nuances between security vulnerabilities in smart contracts, and arbitrage-like design choices. The bZx protocol was originally designed to allow decentralized margin trading and lending, and was the target of recent high-profile attacks. The core of one of these attacks was the ability of a malicious attacker to use flash loans to perform a massive short in the bZx protocol. The bZx contract relied on Uniswap, a decentralized exchange, to sell coins at what it assumed was market price. But, because the size of the attacker’s flash-loan-based short order exceeded the amount that could be safely traded using the liquidity in the Uniswap exchange, the short increased the price of wBTC (wrapped Bitcoin) tokens on the Uniswap platform for this transaction. The attacker was then able to use this false rate to borrow wBTC against ETH (Ethereum, the native currency of the Ethereum blockchain), selling the newly borrowed wBTC into this falsely inflated price and obtaining ETH profit. A comprehensive post-mortem exposé summarizing the attack is available in [26].

The bZx attack blurs the line between arbitrage and code vulnerabilities. One can easily view the failure of the bZx protocol to check that the Kyber/Uniswap order routing had sufficient liquidity to complete its order as a code failure in the bZx protocol, in which case the attack represents a software exploit against bZx. But, one can also view this failure as a fatal design flaw, as it is impossible to determine during the execution of a DeFi transaction whether a given price represents the true market price outside the system in which the transaction is executing, in which case the attack represents financial arbitrage that more closely resembles the activity in traditional financial markets when inefficient financial products operate as intended.

This debate is not purely theoretical. One DeFi insurance product, Nexus Mutual, insured users of the bZx protocol against losses stemming from failures in the correct operation of the underlying smart contracts. Nexus Mutual however did not cover issues in design, and would not need to pay out to its users if the smart contracts were deemed to be operating as intended. After some debate, the Nexus Mutual fund decided to pay out to users who lost money in the bZx attack, as they reasoned that the bZx smart contract designers *intended* to check the slippage the attacker took advantage of, and the attacker bypassed this check due to a coding error [18]. While in this case the Nexus Mutual operators were able to come to a determination, we expect that future DeFi attacks will continue blurring the line between design and implementation issues, especially at the interfaces between various composable interoperable financial components. In a DeFi context, both types of attacks can be viewed as a programmatic search for a reachable final state in the system in which the attacker profits. The attack is far from unique; for example, just a few months later, \$100M was drained from a similar protocol in a similar exploit pattern [9].

B Generalized MEV and Composability Definitions

In Section 3, we defined k -MEV which computes the MEV for a miner if it appends k consecutive blocks to the chain and can change the transaction ordering across those k blocks. In this section,

we define weighted miner-extractable value, or WMEV, which is weighted by the probability that a miner can mine k consecutive blocks.

Formally, for a miner P , let p_k be the probability that it mines exactly k consecutive blocks. For simplicity, we assume that p_k is not state dependent (at least in the short term). p_k may be a function of the mining difficulty or the fraction of hash power owned by the miner. We can now define weighted MEV as follows:

Definition 3 (Weighted MEV).

$$\text{WMEV}(P, s) = \sum_{k=1}^{\infty} p_k \cdot k\text{-MEV}(P, s)$$

As a simple example, consider a miner P who controls a fraction f of the total hash power. If we assume that mining is modeled as a random oracle and that there is no selfish mining, then the probability p_k that P mines exactly k consecutive blocks is $p_k = f^k(1 - f)$. Suppose further that the extra MEV obtained per extra mined block is a constant m . For this simplified example, we can compute the WMEV as:

$$\text{WMEV}(P, s) = \sum_{k=1}^{\infty} f^k(1 - f)(km) = \frac{fm}{(1 - f)}$$

Equipped with this, we can also generalize the definition of Defi composability to include WMEV. For this, MEV in Definition 1 will be replaced by WMEV.

Miner cost. All of our notions of extractable value abstract out the actual cost incurred by the miner (e.g., the cost of equipment, electricity). We do this to make our definitions more broadly applicable. We note that the cost of a specific miner can be calculated independently, and subtracted from the extractable value to obtain the profit a miner could make from transaction reordering.

C CFF Details

C.1 Writing a CFF Model

We now provide additional description of the operations executed by our model in Figure 5, which may prove helpful when defining your own CFF model.

Line 2 is the first such operation, and creates a local variable in the model state which binds the amount to send according to the AMM formula in a variable called AmountToSend. USwapBalanceIn and USwapBalanceOut, the balance of the Uniswap contract in the input and output tokens, are used in this calculation. These variables are sourced from Line 9, where they are matched in the global Ethereum state S .

Lines 3-6 use the special “gets” operator, which we give operational semantics to separately, to change the system state by debiting and crediting the appropriate balances from Uniswap and the user in the traded asset; the user here receives AmountToSend tokens for TradeAmount tokens sent as input. The var function is a built-in function indicating that a variable bound in the current scope (rather than the Ethereum state) should be used.

Note some special K keywords are required for our semantic rule. Firstly, the `...` keyword specifies that anything can successfully match in this location when applying the rule. We do not care what operations after the first execution are pending in the model when applying the rule, for example (Line 7). The rule also applies regardless of the contents of `S` outside of `USwapBalance` (Line 9), and regardless of what transactions the miner has already included in their block `B` in the model (Line 10).

Further such details on K can be found at the K tutorial at <http://kframework.org/>, or by reading our modeling code and documentation on Github.

C.2 Refinements to the Abstract Model

C.2.1 AMM Refinements

We now refine the abstract model, intended to illustrate the core functionality of a Uniswap-like AMM, to be fully faithful to the deployed Uniswap contract. To do so, we must refine our trade rule to take into account the rounding used in the real-world Uniswap trade functions, which come with some degree of error/imprecision. This imprecision is described and formalized in the model in [23], a superset of the formal semantics in our work that was used to verify the Uniswap protocol before deployment.

We must also add semantic rules for liquidity provision and removal transactions, which further affect the Uniswap contract and drive relevant state updates. Lastly, we must take into account all code paths in the Uniswap deployed Solidity contract. Our fully refined model that accurately reflects real-world Uniswap arithmetic is available in `models/uniswap` on our Github repository.

C.2.2 MakerDAO Refinements and Liquidation Auction

We refine our abstract MakerDAO model by adding a rule to update stability fees and account for this stability fees to calculate the CDP debt accurately. We also combine the CDP manipulation actions into one single rule, to accurately reflect the deployed contract. Next, we add rules for CDP fungibility, i.e. transferring debt and collateral between CDPs. We now discuss the subtleties of MEV extraction in a liquidation auction and replace the efficient auction outcome in our abstract model accordingly.

We analyze the optimum MEV assuming that all network miners are behaving to maximize total MEV – a rational decision from a miner standpoint. Optimum MEV is achieved when the miner is able to censor competing bids, and win the entire collateral on offer in the second phase of the auction. We thus refine the liquidation auction outcome in our abstract model to receive the entire collateral on offer. Note that if some miners defect to reduce the efficiency of MEV extraction, it is possible that only some constant percentage of the optimum MEV will remain extractable.

C.3 Mechanized Proofs

We now provide the details of an example specification used to check the security of the composition of Sushiswap and UniswapV2 in Figure 13. This example captures one of the biggest arbitrage captures⁷ observed on-chain involving two AMMs as reported in [39]. The hex addresses for users

⁷<https://etherscan.io/tx/0x2c79cdd1a16767e90d55a1598c833f77c609e972ea0fa7622b70a67646a681a5>

```

1 claim <k>
2   On UniswapV2 697323163401596485410334513241460920685086001293 swaps for ETH by providing
      ↳ 1300000000000000000000000000000000 COMP and 0 ETH with change 0 fee 1767957155464 ;
3   On Sushiswap Miner swaps for ETH by providing Alpha:Int COMP and 0 ETH with change 0 fee 0 ;
4   On UniswapV2 Miner swaps for Alpha COMP by providing ETH fee 0 ;
5
6   => .K
7 </k>
8 <S> (Sushiswap in COMP) |-> 107495485843438764484770 (Sushiswap in ETH) |->
      ↳ 49835502094518088853633 (UniswapV2 in COMP) |-> 5945498629669852264883 (UniswapV2 in
      ↳ ETH) |-> 2615599823603823616442 => ?S:Map </S>
9 <B> .List => ?_ </B>
10 requires (Alpha >Int 0) and Bool (Alpha <Int 10000000000000000000000000000000000) //10**22
11 ensures ({?S[Miner in COMP]}:>Int <=Int 0 ) and Bool ({?S[Miner in ETH]}:>Int <=Int 0 )

```

Figure 13: Specification for Composition of UniswapV1 and UniswapV2

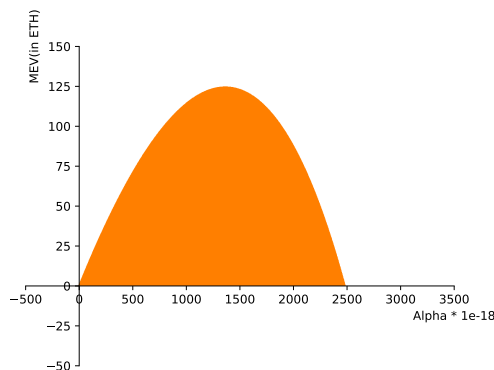


Figure 14: Satisfiable region for MEV. The region represents MEV extractable by the miner as a function of the size of its trade.

are converted to base 10 integers. The initial state for Sushiswap and UniswapV2 is specified in the **S** cell. The last two transactions in the **k** cell represent the transactions inserted by the Miner according to the strategy described in Section 4. Note that the Miner transaction can be symbolic, Alpha being the symbol representing the size of the swap Miner does (denominated in Wei (1 ETH = 1e18 Wei)). The **requires** clause specifies the constraints on Alpha, essentially denoting the Miner budget. Finally, the **ensures** clause represents the claim that the Miner is not able to extract any value regardless of the way specified transactions are reordered.

Our tool derives a counterexample to the claim with a MEV of 123 ETH as shown in Figure 14.

C.4 CFF Limitations

Unfortunately, while the CFF provides a powerful way to reason about smart contract security, it does come with some limitations. The first major limitation is in the fidelity of the models themselves: because we are providing abstract, somewhat simplified models of the code that is actually executing on the blockchain, there may be sources of MEV that we overestimate, or miss.

While for our particular MEV analyses herein, we validated our results to ensure they represented real exploitable MEV on the part of the miners, it would be far more convenient to use a model that operated with 100% accuracy, such as [20], which is already defined in K.

Unfortunately, because the semantics in [20] are an order of magnitude larger than our specialized models, they are also far costlier to execute. We believe there is substantial room and demand to optimize the backend state space search in the K Framework, so fully faithful semantic models of the EVM can be used for reordering exploit detection. We also believe there is room for a wide range of hybrid approaches, including randomized testing / fuzzing, symbolic execution, concolic execution [46], and machine learning, to attempt to learn and optimize for this state transition model.

A number of limitations also come from our approach of crawling and extracting Uniswap transactions on-chain, which we do through Ethereum logs. Unfortunately, Uniswap does not log all information relevant to the execution of a transaction in our model. For example, slippage limits are not reflected in the Uniswap logs, and may cause a transaction to fail when reordered to receive a worse price. While in the instances we validated, this was not prohibitive to MEV extraction, it speaks to the requirement for adding a layer of manual or automatic validation based on the full EVM rules for any attack evaluated through the CFF methodology.

C.5 MEV Deep Dive

In this section, we will explore in more detail our top MEV example, which occurred in Ethereum block 10968577 in the YFI-WETH pair on Sushiswap, primarily surrounding MEV-creating transaction 0x8a9d88084eb3a451fcd1c28f1851d0-ced03e7665499a362942978ff13d5c19d4.

In this transaction, a user sold 40 YFI tokens, a popular and extremely valuable Ethereum token that was in the middle of an upwards price rally, on an automated decentralized exchange liquidity aggregator called 1inch.exchange. As part of this aggregation, 1inch chose to execute a sale of 22 YFI tokens on SushiSwap, worth USD\$550,000 at the then-price of USD\$25,000 per token.

User	Swap Performed	Amount of Input Token
A	YFI → WETH	22000000000000000000
B	WETH → YFI	53788258395569781028
B	WETH → YFI	6784028349336991312
C	WETH → YFI	103266050000000000000
D	WETH → YFI	300000000000000000000
D	WETH → YFI	4970140364366149478
D	WETH → YFI	6984067876806377830
D	WETH → YFI	300000000000000000000
D	WETH → YFI	150000000000000000000

Figure 15: Mined actual transaction ordering of the top MEV block in our sample

Because the user placed a large market order on a set of automated market makers, this naturally

created an arbitrage opportunity to buy YFI at this newly-depressed price, selling it into more liquid off-chain and on-chain markets which still reflected the real market valuation. Figure 15 shows the ordering of transactions on the network, with user “A” being the user selling YFI tokens on 1inch, and users B-D representing a set of arbitrage bots that programatically bought and re-sold tokens from SushiSwap when user A created an arbitrage opportunity.

The MEV here is obvious, as the ability for a miner to essentially take the trades performed by the bots furnishes a more profitable opportunity for the miner than the bots, who can also execute the bots’ failed transactions.

The optimal ordering found by our tool for user A is $D \rightarrow D \rightarrow D \rightarrow C \rightarrow B \rightarrow B \rightarrow D \rightarrow D \rightarrow A$, where the user’s trade is executed after the trade of the arbitrage bots. This makes sense, as the arbitrage bots cannot take advantage of the user’s price movement to re-arbitrage Uniswap back to market parity. Conversely, the worst order for user A is $A \rightarrow D \rightarrow D \rightarrow D \rightarrow C \rightarrow B \rightarrow D \rightarrow B \rightarrow D$, which is very similar to the order actually mined by the miner.

Note that the arbitrage on the network are already somewhat effective at extracting MEV from Uniswap, a result that is expected given the conclusions of [17]. However, the miner can still increase profit even further over these bots, due to the fine-grained control it can exercise in ordering that is likely hard to achieve through the public priority gas auctions described in [17]. We thus posit that this example shows not only the existence of MEV that can be exploited through generic tooling, but also the relative inefficiencies of current arbitrage bots on the network, who are unable to achieve the maximally optimal order even when opportunity sizes are large.

C.6 Bounding the MEV for AMMs

Although the price offered by the AMMs we study at the end of a given set of transactions is independent of the order of the transactions [12], individual users’ transactions get different prices depending on the order of the transactions. A miner can thus influence the value individual users get for their trades by choosing a different order for the transactions. For each user, there is an optimal and a worst case ordering.

Let b_h be the highest ETH-value of a trader’s account after a block has elapsed, assuming access to a price oracle for pricing a user’s tokens at an invariant market price for the time of trade execution. Let b_l be the lowest such value. It is therefore rational for the trader to pay $b_h - b_l - \epsilon$ to miners as a bribe. For miners to elicit this bribe, they would deploy a contract allowing each user of an AMM to deposit ETH. They would then credibly commit to mining the order resulting in b_l if no funds were available. Otherwise, they would submit both b_l and b_h , along with associated proofs, to the smart contract, which would enforce the order resulting in b_h , pay the miner $b_h - b_l - \epsilon$, and pay the trader ϵ . Note that paying such a contract is a strictly dominant from a trader point of view, as the trader profits ϵ more than without paying into such a contract. Introducing this new contract increases MEV by exactly $b_h - b_l - \epsilon$ through a direct payment by inspection; in our experiments, we assume ϵ is negligible when compared to $b_h - b_l$: since being paid this ϵ is a strictly dominant strategy, miners need only compensate users for the low cost of locking capital (which can be removed freely) in the bribery contract.

When analyzing attacks like this on DeFi protocols, a natural question becomes how to efficiently and thoroughly uncover reordering-based differences that would allow for an accurate measurement of b_h and b_l , and therefore the MEV in the presence of such contract composition. It is this measurement on which we focus in our AMM experiments.