DeFi composability as MEV non-interference

Does a new contract interact safely with the rest of the blockchain?

Massimo Bartoletti
Università di Cagliari

Riccardo Marchesin
Università di Trento

Roberto Zunino
Università di Trento

DeFi composability

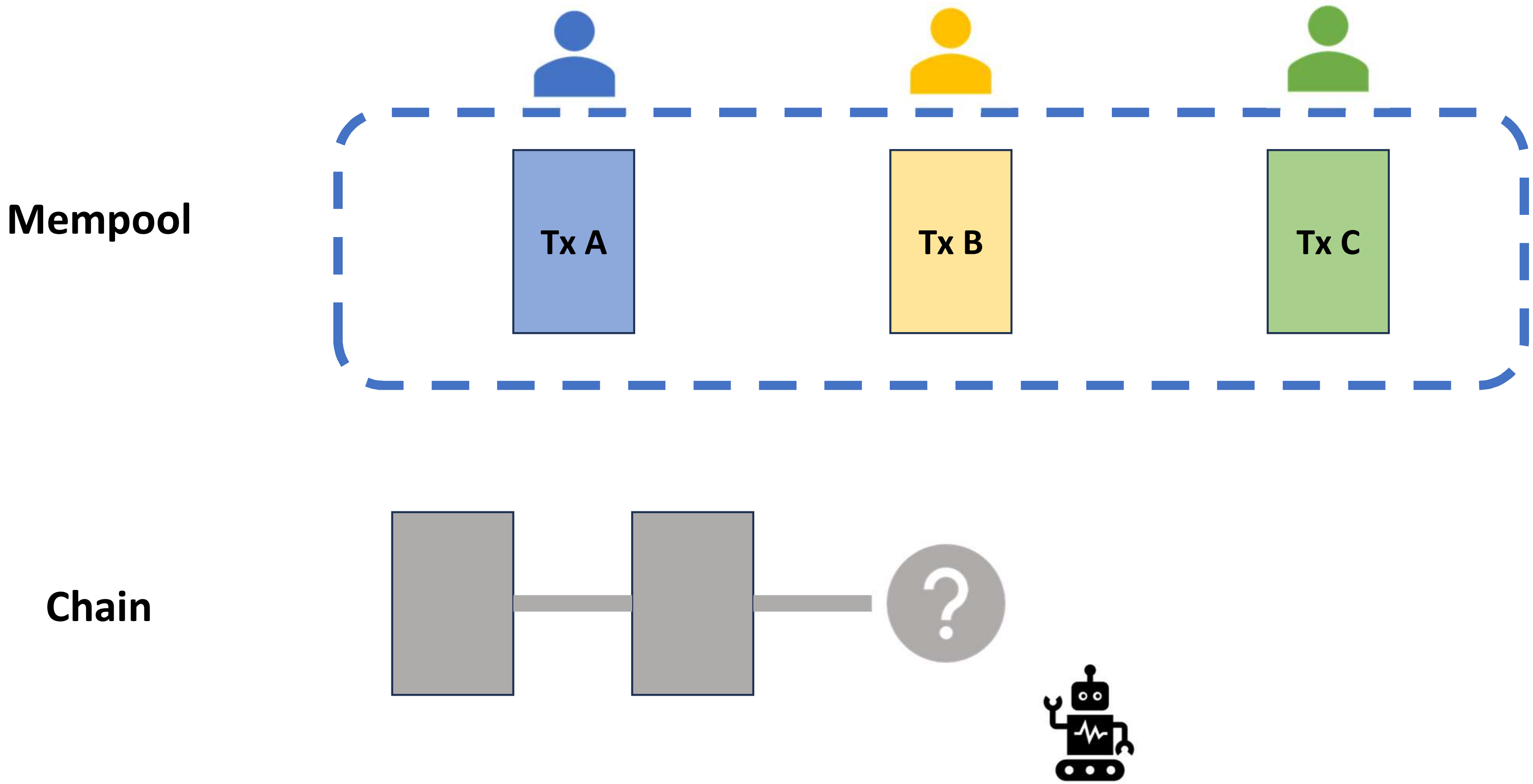
DeFi ecosystems have complex interactions and dependencies between protocols

Malicious users may exploit unintended forms of interaction

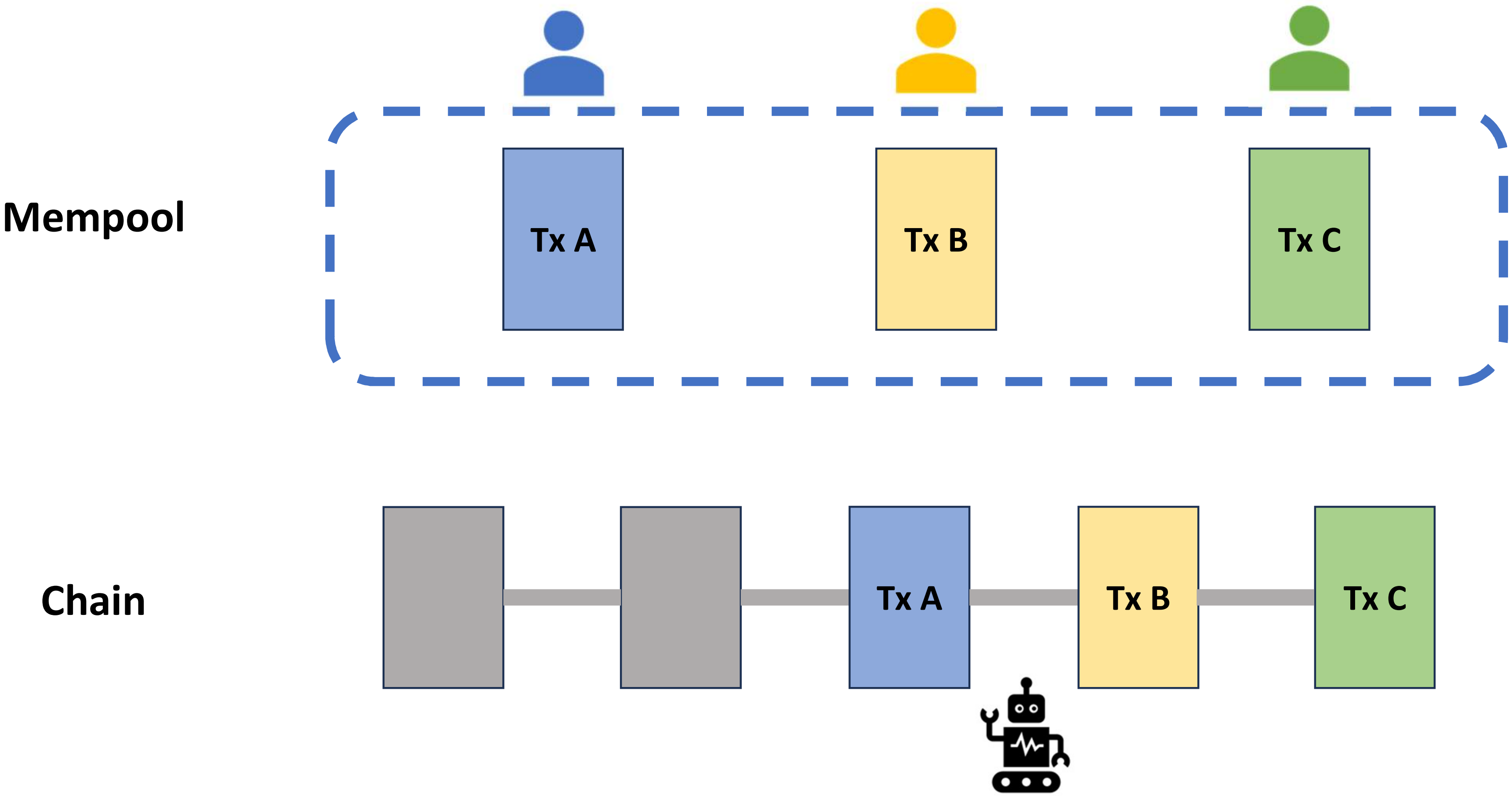
This is not limited to bugs: we also consider economic attacks

Background: MEV attacks

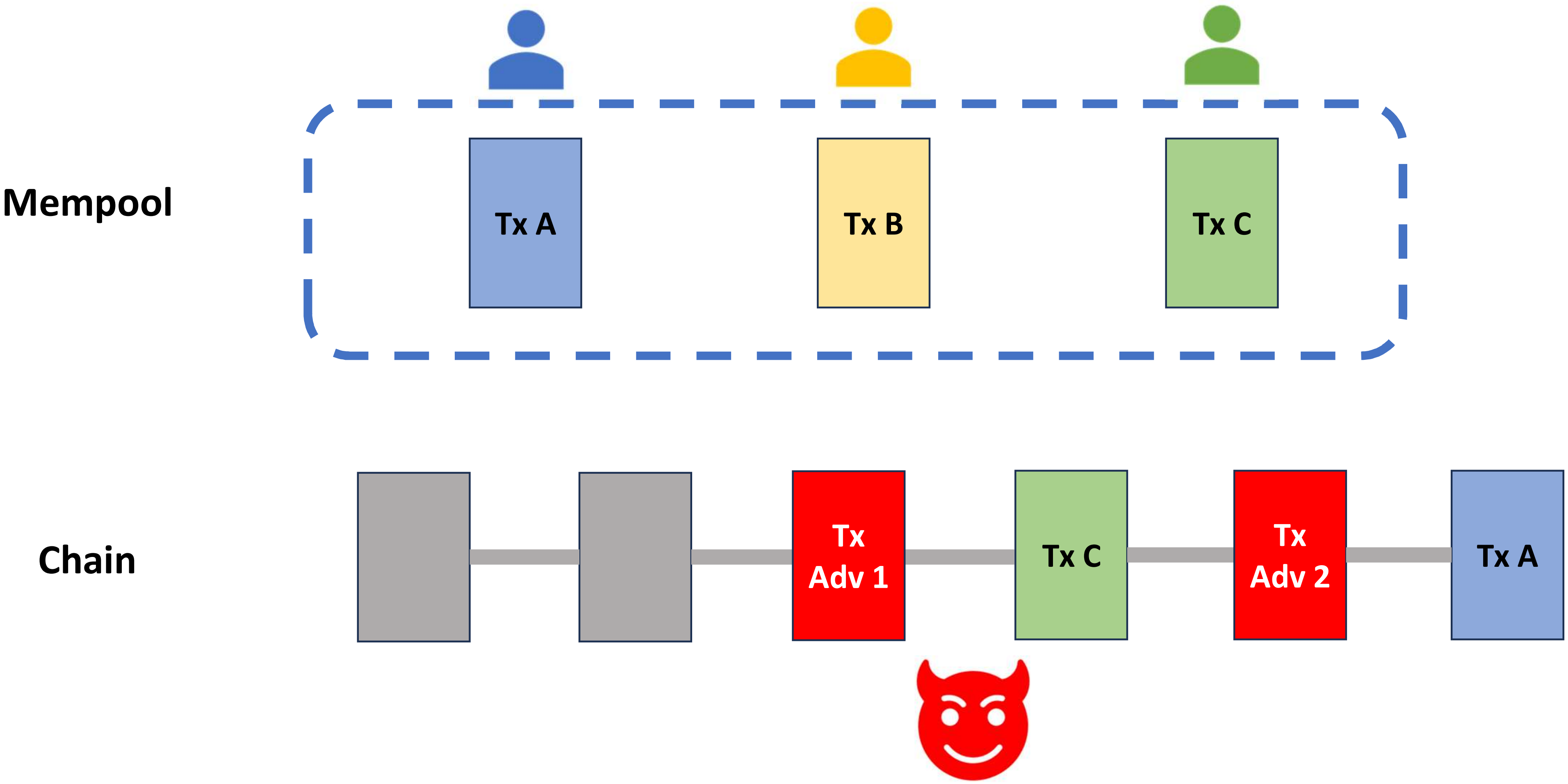
Transaction Ordering



Transactions ordering: expectation

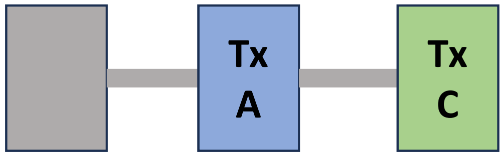


Transactions ordering: reality

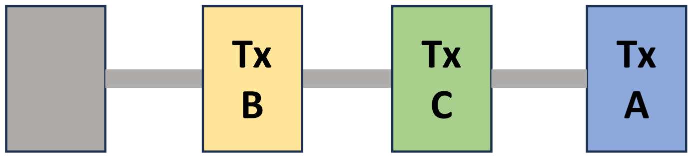


A malicious validator can…

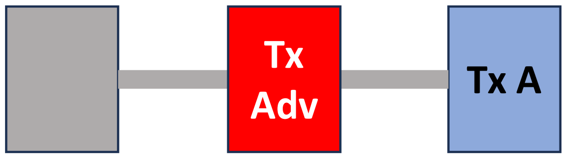
Drop transactions



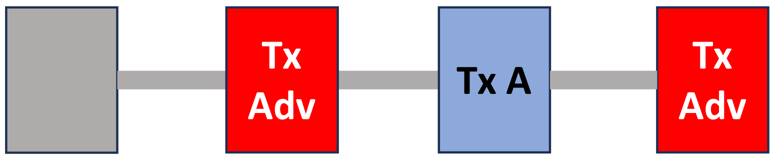
Rearrange transactions



Front-run transactions



Sandwich transactions



A vulnerable contract: the AMM

AMMs (Automated Market Makers) exchange two token types T0, T1 algorithmically adjusting the exchange rate (e.g. constant product between the amount of T0 and T1)

These attacks are **zero-risk** if performed by a validator

Attacks:

- A sends a transaction X to sell T0 and buy T1
- T0 will "lose value", T1 will "gain value"
- **Frontrunning**: Adv sell T0 to buy T1 before they gain value with X
- **Sandwiching**: Adv makes X unfavourable, put X, then balance AMM

Defining MEV

MEV = Maximal Extractable Value

$$MEV(S) = \max \{ gain_{Adv}(S, \underline{X}) \mid \underline{X} \in K(Adv)^* \}$$

- S is the blockchain state
- $\underline{X}$ is a sequence of transactions
- K(Adv) is the set of transactions craftable by Adv

Back to composability

ε-composability

A contract Δ is composable with a blockchain state S when it does not **significantly increase** MEV:

$$MEV(\, S \mid \Delta \,) \;\leq\; (1 + \varepsilon)\, MEV(S)$$

[“Clockwork Finance” paper by Babel, Daian, Kelkar, and Juels]

Drawbacks of ε-composability

- Computes the MEV of the **whole** blockchain state

  ➔ Inefficient

  ➔ Does not tell *from where* the MEV is extracted

- If Δ has MEV on its own, and does not interact with the rest of the system, is it fair to say it is non composable with S?

Composing AMMs (1)

- Adv[2:T0] | AMM[2:T0, 12:T1]

  Adv can sell 2:T0 and buy 6:T1

- Adv[2:T0] | AMM[2:T0, 12:T1] | AMM[2:T0, 12:T1]

  Adv can sell 1:T0 in each AMM and buy 4:T1 from each

Attacking both gives Adv more gain, but extracts less from each.

Are they composable?

Composing AMMs (2)

S = Adv[1:T0] | AMM1[1:T0, 2: T1] | AMM2[1:T1, 20:T2]

Adv can spend 1:T0, get 1:T1 and spend it again to get 10:T2

Attacking only AMM2 gives nothing. Having access to AMM1 helps Adv to extract a lot from AMM2.

Is AMM2 composable in S?

PriceBet

Consider a composed contract **PriceBet(C)**: bets on the exchange rate between two tokens, where the exchange rate is given by **C**

- PriceBet(AMM) where rate = ratio between amounts of tokens
- PriceBet(Exchange) where rate is set by an oracle

Are these compositions secure?

Hint: Adv can create volatility in the AMM to win the bet

(Bad) idea: adding MEVs

$$S = W \mid \Gamma \mid \Delta \quad \text{(W are wallets)}$$

Γ, Δ are composable iff

$$\mathrm{MEV}(S) \leq \mathrm{MEV}(\, W1 \mid \Gamma\,) + \mathrm{MEV}(\, W2 \mid \Delta)$$

(where $W1+W2 = W$)

Problem: We can’t always “break” S.

The expression MEV(Δ) is problematic when Δ that depends on Γ.

Local MEV

Local MEV = maximal loss of Δ

$$MEV(S,\Delta) = \max \{ loss_{\Delta}(S, \underline{\mathbf{X}}) \mid \underline{\mathbf{X}} \in K(Adv)^{*} \}$$

We are assuming a (potentially irrational) Adv who just wants to cause harm to the contract.

Restricted Local MEV

Restricted Local MEV = local MEV that Adv can extract from Δ by only targeting the contracts in Δ

$$MEV_{alone}(S,\Delta) = \max \{ loss_{\Delta}(S,\underline{\mathbf{X}}) \mid \underline{\mathbf{X}} \in (K(Adv) \cap tx(\Delta))^{*} \}$$

It is the loss caused to Δ "without help" from other contracts

Restricted local MEV

Restricted local MEV = value that an adversary can extract from Δ while only targeting contracts in Δ.

$$MEV_{alone}(S, \Delta) = \max\{ loss_{\Delta}(S, \underline{X}) \mid \underline{X} \in K_{\Delta}(Adv)^* \}$$

It is the loss caused to Δ “without help” from other contracts.

Composability as MEV non-interference

The state S does not interfere with new contracts Δ if

$$MEV(S \mid \Delta, \Delta) = MEV_{alone} (S \mid \Delta , \Delta)$$

Properties:

- Zero tokens in Δ implies non-interference
- Δ is independent from S (token & contract independence) implies non-interference

Composability w.r.t. rich adversaries

We also model a stronger adversary, with unbounded wealth.

Local MEV w.r.t. rich adversaries:

$$MEV^{\infty}(\Gamma, \Delta) = \max\{ MEV(S, \Delta) \text{ where } S = W|\Gamma \}$$

Non-interference w.r.t. rich adversaries:

$$MEV^{\infty}(\Gamma| \Delta, \Delta) = MEV^{\infty}_{alone}(\Gamma |\Delta, \Delta)$$

Non-interference w.r.t. rich adversaries

Results:

- $MEV^{\infty}(\Gamma, \Delta) = MEV^{\infty}(deps(\Delta), \Delta)$

  Front-running resistance: if Γ does not interfere with Δ then Γ| Γ’ does not interfere with Δ

- Zero-token composability
- Contract independence implies non-interference

A possible riformulation

States form a transition system, labeled by the transactions.

$\mathcal{T}$ set of transactions, $\mathcal{T}_\Delta$ transactions targeting delta.

Γ is MEV non-interfering with Δ

iff

$\forall\, W\ \forall\, \boldsymbol{T} \subseteq \mathcal{T}\ \exists\, \boldsymbol{T}' \subseteq \mathcal{T}_\Delta$ such that

$$W|\Gamma \xrightarrow{\boldsymbol{T}} S \ ,\ \ W|\Gamma \xrightarrow{\boldsymbol{T}'} S' \ \text{ and } \ \$(\Delta, S') \preccurlyeq \$(\Delta, S \quad)$$

Challenges

- Use more sofisticated non-interference methods to study attacks
- Model a rational adversary, while keeping some results
- Weaken well-formedness assumption on states/contracts

References

DeFi composability as MEV non-interference: https://arxiv.org/abs/2309.10781

Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts: https://arxiv.org/abs/2109.04347