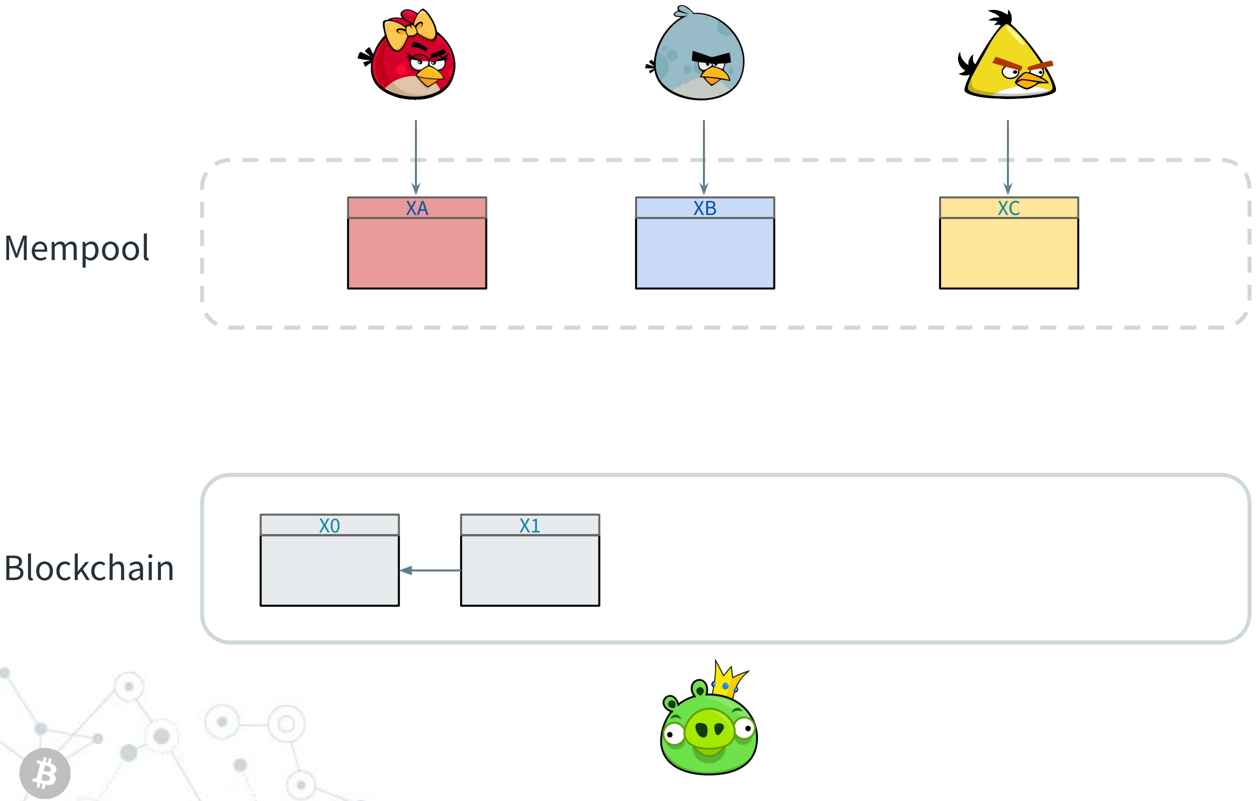
A theoretical basis for Blockchain Extractable Value

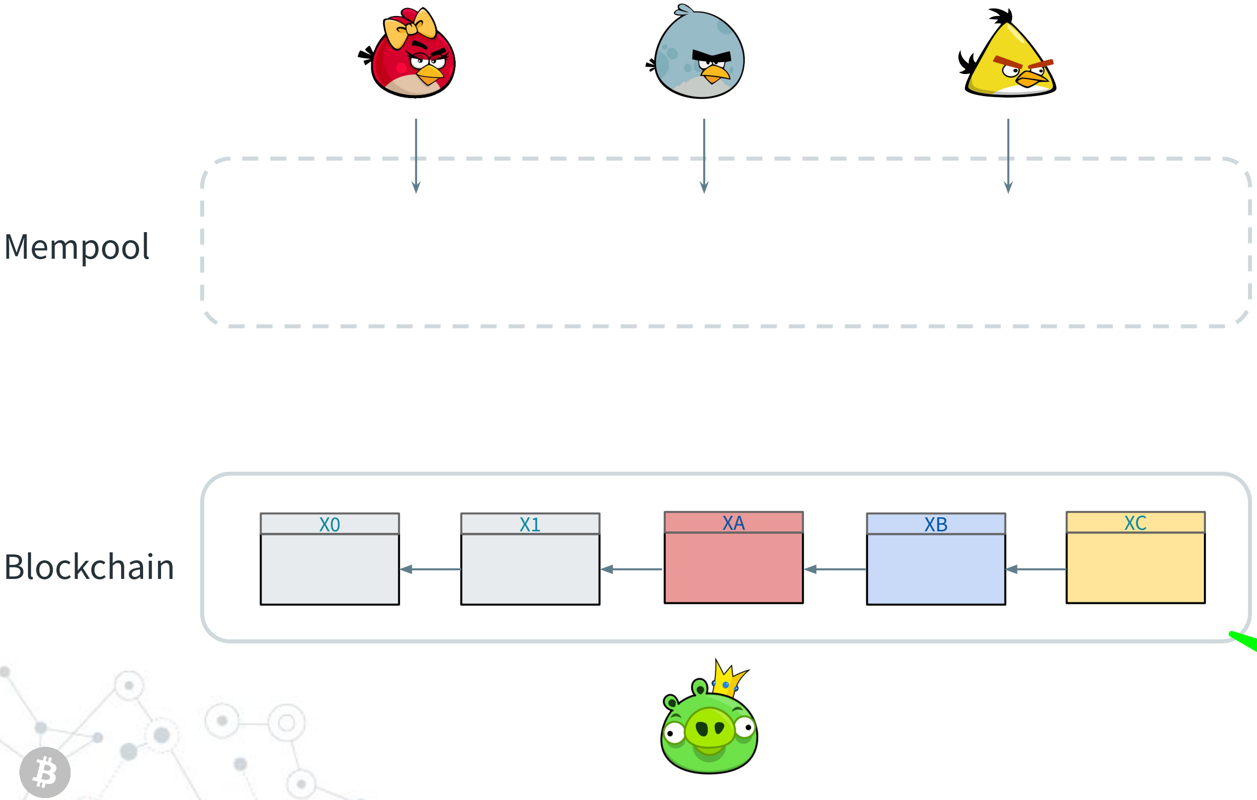
Massimo Bartoletti
University of Cagliari

Roberto Zunino
University of Trento

Transaction ordering



Transaction ordering



Mempool

Blockchain

X0

X1

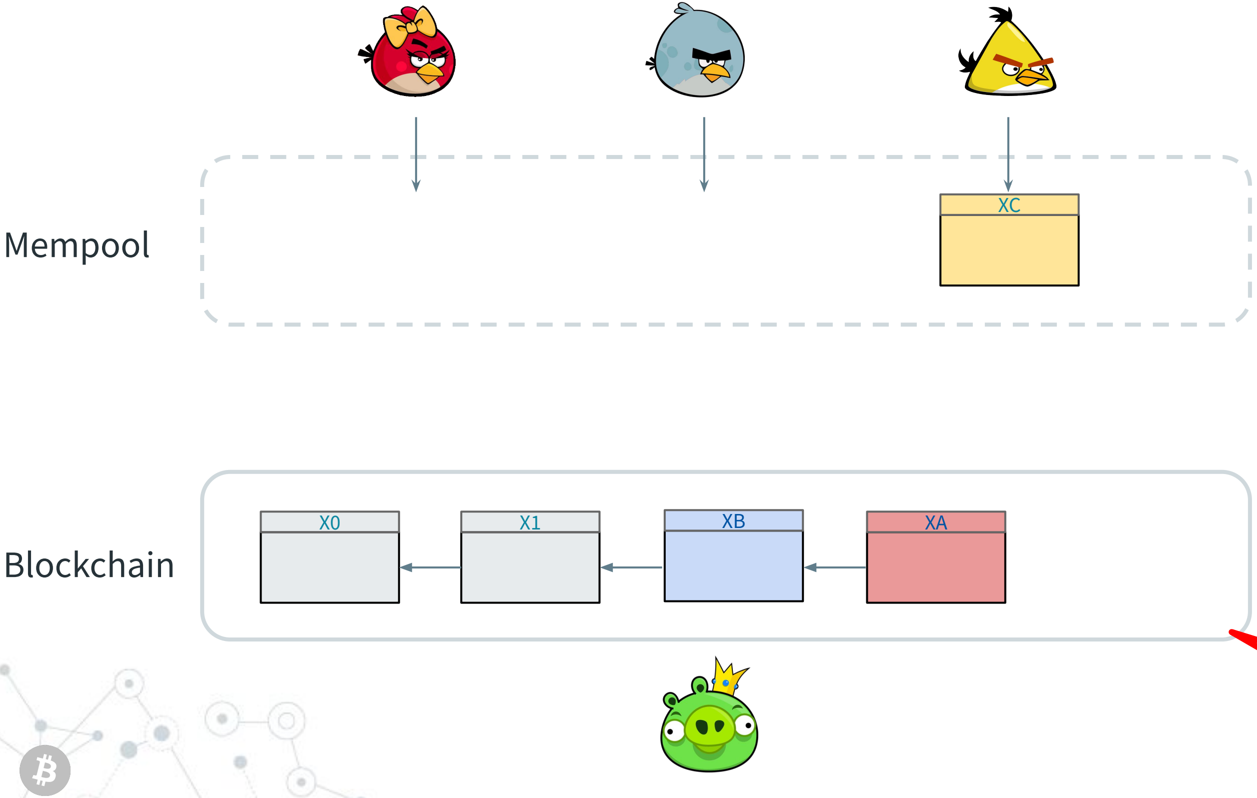
XA

XB

XC

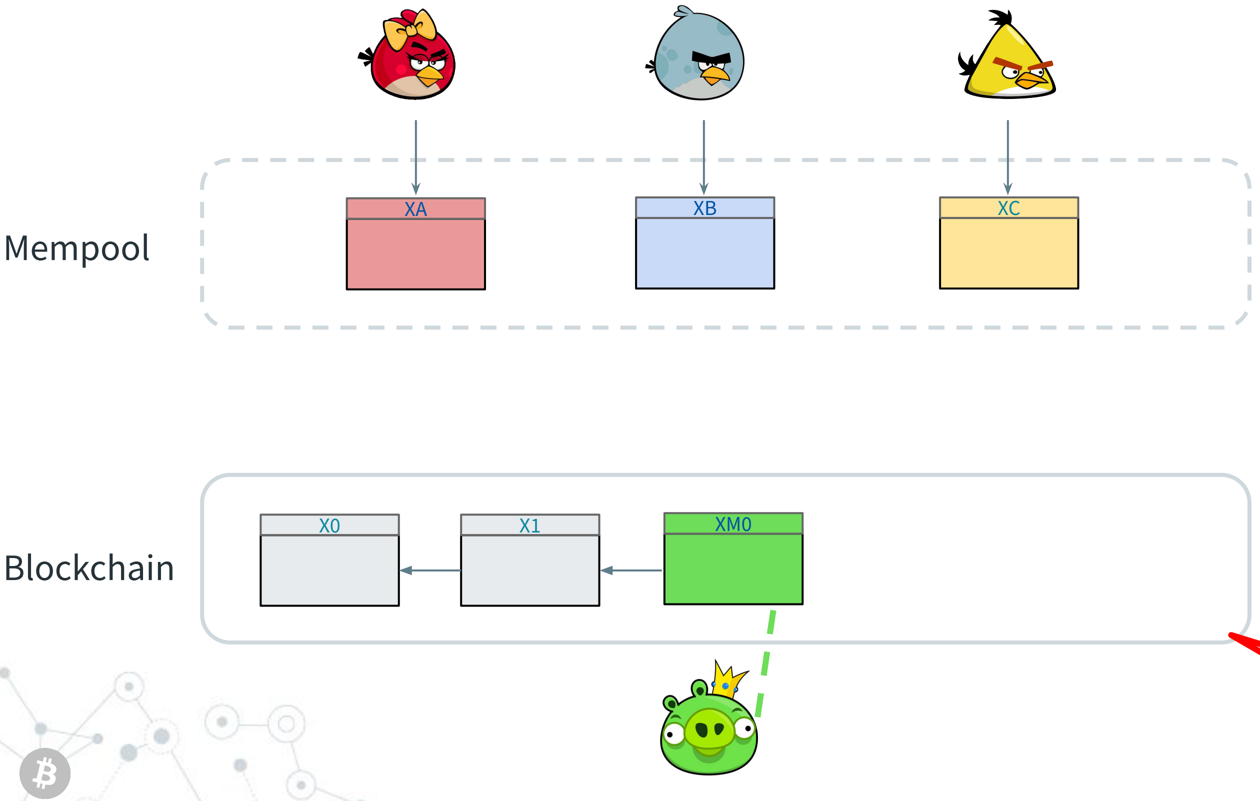
ideally: **fair** ordering

Transaction ordering



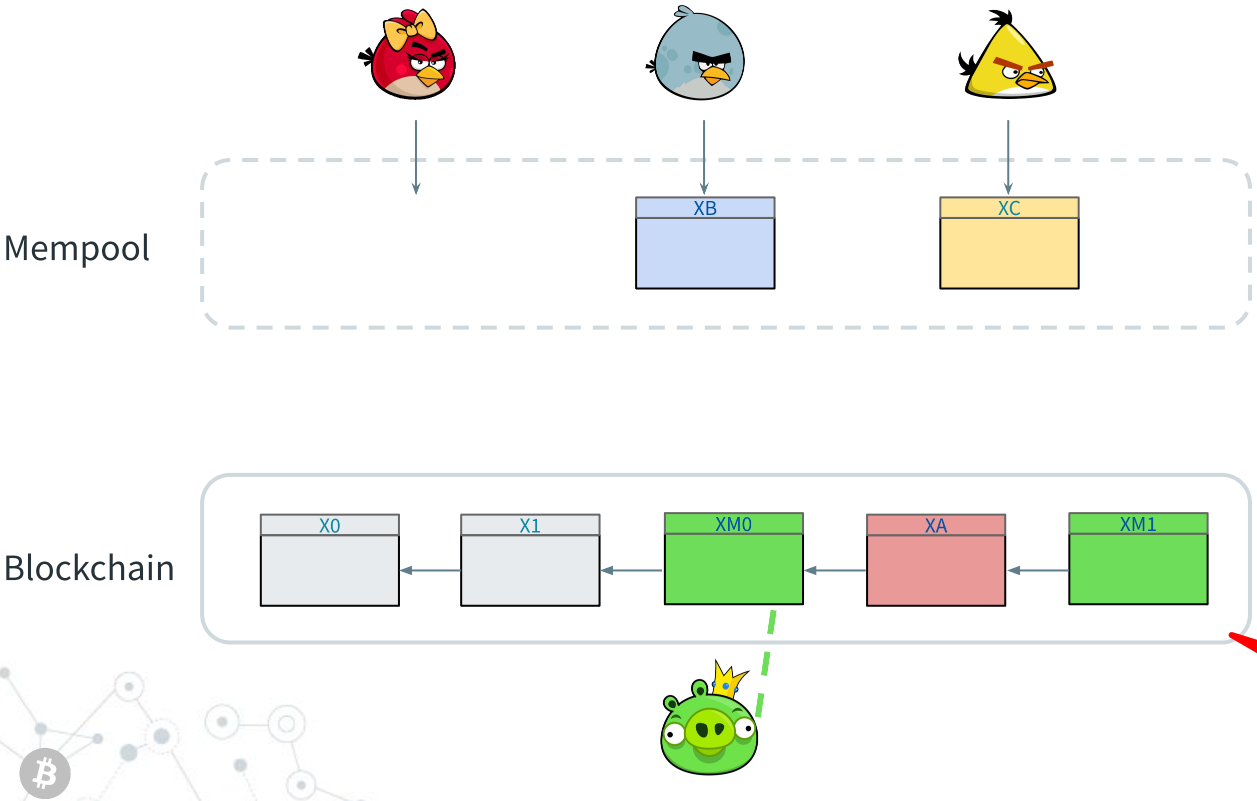
reorder & drop tx

Transaction ordering



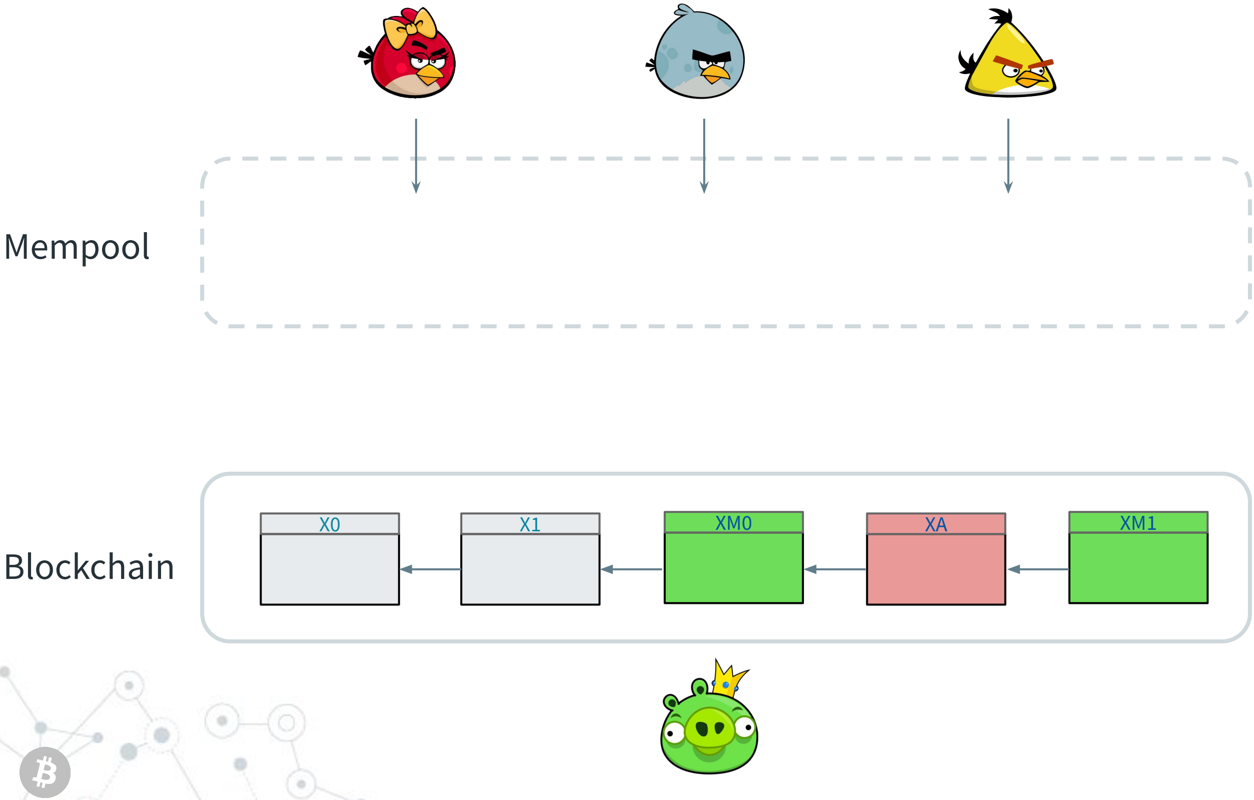
front-run users’ tx

Transaction ordering



“sandwich” users’ tx

Transaction ordering



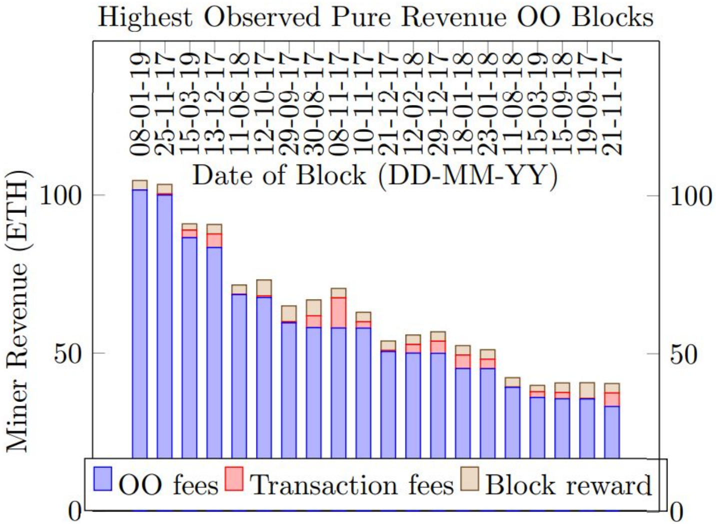
Rational miners exploit users’ tx to gain $$$

… usually, to the detriment of users’!

MEV attacks

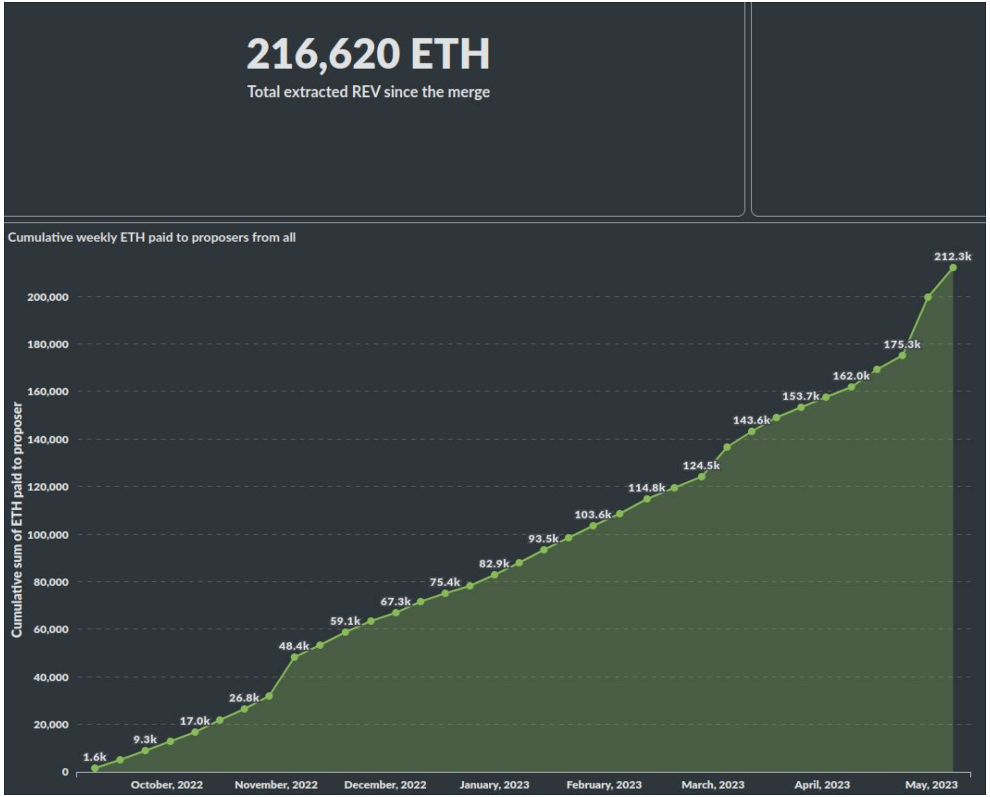
Drawbacks of MEV

- Decreased “goodput”
  - → user tx marginalised by MEV tx
- Increased tx fees
  - → front-running tx via priority fees
- Solution to increasing tx fees: Flashbots
  - → large **private** network implementing a sort of “MEV market”
  - → advertised as “democratising MEV” (?)



Source: Daian *et al*. “Flash Boys 2.0”

FlashBots statistics



216,620 ETH

Total extracted REV since the merge

Cumulative weekly ETH paid to proposers from all

~ USD 400M

Source: https://explore.flashbots.net/

Contribution: a theoretical basis for MEV

- General model of contracts
  - → State transition systems + wealth
  - → Abstracts from blockchain design (account-based, UTXO, …)
- **Adv knowledge**: tx deducible by Adv from mempool
- MEV & **Adversarial MEV**:
  - → $\text{MEV}_{\boldsymbol{A}}(S,\boldsymbol{P})$: extractable by users ***A*** in state S and mempool ***P***
  - → $\text{MEV}(S,\boldsymbol{P})$: extractable by **any** Adv (regardless of id & wealth)

MEV

A single user

A set of users

$$\mathrm{MEV}_{\boldsymbol{A}}(S,\boldsymbol{P}) = \max \{ \mathrm{gain}_{\boldsymbol{A}}(S,\underline{X}) \mid \underline{X} \in K_{\boldsymbol{A}}(\boldsymbol{P})^{*} \}$$

This definition is not yet completely satisfactory:

1. how to formalise $K_{\boldsymbol{A}}(\boldsymbol{P}) = \{ X \mid \boldsymbol{A} \text{ can craft } X \text{ from } \boldsymbol{P} \}$?

   → axiomatization of Adv knowledge

2. $\mathrm{MEV}_{\boldsymbol{A}}$ is the gain of a *given* set ***A***

   → Adv MEV = MEV extractable by anyone

Adversarial Knowledge

```
contract HTLC {
    commit(b,c) {
        require cmt==null && msg.value>0;
        rcv=b; cmt=c
    }
    reveal(s) {
        require H(s)==cmt;
        to=msg.sender;
        to.transfer(this.balance);
    }
    ...
}
```

$\boldsymbol{P} = \{\, A{:}\text{reveal}(\text{”hello”}) \,\}$

$M{:}\text{reveal}(\text{”hello”}) \in K_M(\boldsymbol{P})$

Adversarial Knowledge & MEV

$$\mathrm{MEV}_{A}(S,P) = \max \{ \gamma_{A}(S,\underline{X}) \mid \underline{X} \in K_{A}(P)^{*} \}$$

$$\mathrm{MEV}_{A}(S,P) = \mathrm{MEV}_{A}(S,P \setminus K_{A}(\varnothing))$$

mono | exts | idem

$$P \subseteq P' \Rightarrow \quad \mathrm{MEV}_{A}(S,P) \leq \mathrm{MEV}_{A}(S,P')$$

mono

$$A \subseteq A' \not\Rightarrow \quad \mathrm{MEV}_{A}(S,P) \leq \mathrm{MEV}_{A'}(S,P)$$

$$\forall A \,.\, \exists A0 \subseteq_{\mathrm{fin}} A \,.\; \mathrm{MEV}_{A}(S,P) = \mathrm{MEV}_{A0}(S,P)$$

mono | fin.cs | no.ss

$$\forall P \,.\, \exists P0 \subseteq_{\mathrm{fin}} P \,.\; \mathrm{MEV}_{A}(S,P) = \mathrm{MEV}_{A}(S,P0)$$

cont

$$C \text{ wallet mono} \Rightarrow \mathrm{MEV}_{A}(S,P) \leq \mathrm{MEV}_{A}(S + W_{\Delta},P)$$

Adversarial MEV

- In MEV$_{\boldsymbol{A}}$(S,***P***): the set ***A*** in is fixed;
- In practice: the identity of the adversary is immaterial!

MEV(S,***P***) = value that can be extracted by **anyone** with the power to reorder, drop or insert tx!

Adversarial MEV

Idea: min-max game between honest users and Adv

- **min**: honest users choose Adv (any cofinite set ***B***)
- **max**: Adv chooses $\boldsymbol{A} \subseteq \boldsymbol{B}$ and redistributes tokens:

  S ~ S' iff W(S) and W(S') have the same tokens

$$\mathrm{MEV}(S,\boldsymbol{P}) = \min_{\boldsymbol{B}\text{ cofinite}} \ \max_{\substack{\boldsymbol{A}\subseteq\boldsymbol{B}\\ S\sim S'}} \ \mathrm{MEV}_{\boldsymbol{A}}(S',\boldsymbol{P})$$

Properties of adversarial MEV

$$\mathrm{MEV}(S,\boldsymbol{P}) = \min_{\boldsymbol{B}\text{ cofinite}} \; \max_{\substack{\boldsymbol{A}\subseteq\boldsymbol{B}\\ S\sim S'}} \; \mathrm{MEV}_{\boldsymbol{A}}(S',\boldsymbol{P})$$

$$\boldsymbol{P} \subseteq \boldsymbol{P'} \quad \Rightarrow \; \mathrm{MEV}(S,\boldsymbol{P}) \leq \mathrm{MEV}(S,\boldsymbol{P'})$$

$$\mathbf{C}\text{ wallet mono} \Rightarrow \; \mathrm{MEV}(S,\boldsymbol{P}) \leq \mathrm{MEV}(S + W_{\Delta},\boldsymbol{P})$$

Adversarial MEV on real-world contracts

MEV-leaking:

- Automated Market Maker
- Lending pool
- …

MEV-free:

- HTLC
- Bank
- Crowdfunding
- Bounty contract
- …

Conclusions

- MEV not easy to capture formally!
  - → time? (clogging)
  - → probabilistic strategies? (lottery)
  - → contract composition?
  - → computational *vs.* symbolic?
- MEV-freedom *vs.* MEV mitigation

M. Bartoletti, R. Zunino.
A theoretical basis for Blockchain Extractable Value
https://arxiv.org/abs/2302.02154