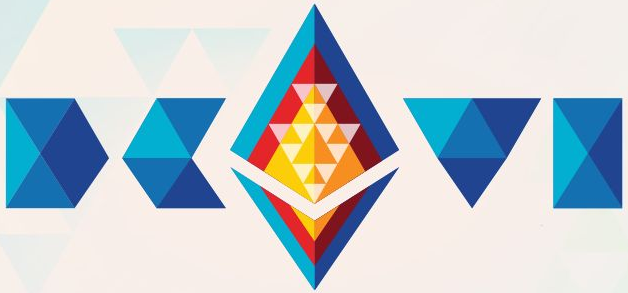


Smart Transactions:

Prophecy of a New Paradigm

Vlad Zamfir

Your title, your organization

Section 1

The Prophecy

The Prophecy

Ethereum transactions will become **smart**

Programmable, networked, and **context aware**

- Of the way they are treated
  - Over time of their actual and possible futures
  - Over space of their actual and possible context

Where today they are relatively **dumb** and **blind**

Ethereum is being profoundly disrupted by unexpected transactional semantics

This has long been the case due to EVM quirks

But unexpected transaction execution due to MEV has become a blockchain constitutional crisis, and not just to the Ethereum blockchain

It is forcing all blockchain communities to reckon with the possibility of reintermediation, censorship, and worst-case executions

Transactions face evolutionary pressure due to unexpectedly changing semantics,

and in response they will gradually (then suddenly) become

Smart Transactions

Some MEV search awareness is going to balloon into a lot

The MEV search looks into the possible futures of transactions, and chooses one to maximize MEV

Transactions can already use this to their advantage, by paying out more MEV in case of favorable execution

This search result quality awareness and passive interactivity with the MEV search will develop into much more search awareness and interactivity

Section 2

The Past

The Past

Transactions fell prey to ethereal predators in the dark forest

- Worst-case slippage
- Freak liquidations
- Stolen arbitrage
- Hijacked hacks

And they have went into hiding

- Avoiding the mempool
- Using trusted searchers
- Trying to eliminate their MEV

And transactions strategically exposing MEV also emerged

The history of “Good MEV” may have begun with bundle searchers providing MEV “tips” or “bribes”

These MEV payments redistributed power from upstream searchers to downstream searchers

This allowed searchers to provide valuable services, especially notably gas savings on OOG

It has been observed that “Good MEV” also reduces the gas cost of successful transactions

Following this research, I discovered MEV-time I/O

During the MEV search, earlier transactions of a bundle or block are often included as a function of the behaviour of later transactions

In fact, earlier transactions can directly interact with later transactions through EVM storage, and this can be used in many ways, including to

- give more up-to-date oracle values
- modify the EVM's control flow
- time travel

MEV-time I/O

bestows non-deterministic semantics on the EVM, unlocking tremendous potential for gas savings,

And for transactions to have access to more information about their place in the MEV Search

MEV-time interaction dramatically changes transaction semantics

If this interaction can be secured and validated so that virtually anything a searcher knows a transaction can also demand to know (or revert),

then transactions can become aware both of their and their transaction peers' actualized trace and also of unactualized counterfactual timelines

even giving them shockingly quantum-like execution semantics (for preprocessing cost), observably interacting with its multiverse of possible futures, pasts, and presents

However, MEV-time I/O today is not secure

transactions within bundles and blocks can also be executed against the MEV-time I/O of counterfactual bundles and blocks

Smart transactions rely on MEV search result security

Because otherwise they can't safely raise their awareness very far beyond what is observable and verifiable by the EVM from within the EVM

This led me down a very long journey of research into protecting bundle search

Very thankfully, I have been able to prospect MEV search protection infra that does not require EIPs, in large part by leveraging a cumulation of validation and fault tolerance research

When a prospect is competitive enough, its viability secures its inevitability

This argument thereby underwrote the smart transaction prophecy

Section 3

The State of the Art

Smart transactions pull themselves up by their bootstraps

One bit of awareness can buy two bits of awareness

Smart transactions infrastructure roadmap

Phase 0: saving gas via virtual/actual invalidation
Phase 1: semi-atomicity via cumulative validation
Phase 2: atomicity via essential proposer services
Phase 3: rm'ing proposer trust with virtual services
Phase 4+: opening up smart tx development, virtual service provision, and search participation

Formal Semantics of Smart Transition Systems

In this example a VLSM, V, is going to be validating for its embedding in a corresponding speculative execution VLSM, V^r:

$$V = (L, S, S_0, M, M_0, \tau, \beta)$$
$$V^r = (L^r, S^r, S_0, M^r, \{M_0\}, \tau^r, \beta^r)$$
$$S^r = S \cup (S \times S \times 2^M)$$
$$M^r = 2^M$$
$$L^r = \{\text{duplicate}, \text{speculate}, \text{validate}\} \times L$$

Smart transactions validate far and wide, into the past, present, and the future

Formal Semantics of Smart Transition Systems

Specifically where only embeds transitions in V if it first find a valid speculative execution which is at least two transitions long.

$$\tau^r((\text{duplicate}, l), \gamma, m) = (\langle \gamma, \gamma, \varnothing \rangle, \text{✖})$$
$$\tau^r((\text{duplicate}, l), \langle \gamma, \gamma', K \rangle, m) = (\langle \gamma, \gamma', K \rangle, \text{✖})$$

$$\tau^r((\text{speculate}, l), \gamma, m) = (\gamma, \text{✖})$$
$$\tau^r((\text{speculate}, l), \langle \gamma, \gamma', K \rangle, m) = (\langle \gamma, \tau^s(l, \gamma', m), K \cup \{\tau^m(l, \gamma', m)\} \rangle, \text{✖})$$

$$\tau^r((\text{validate}, l), \gamma, m) = (\gamma, \text{✖})$$
$$\tau^r((\text{validate}, l), \langle \gamma, \gamma', K \rangle, m) = (\gamma, \text{✖}) \quad \text{if } \neg\beta(l, \gamma', m)$$
$$\tau^r((\text{validate}, l), \langle \gamma, \gamma', K \rangle, m) = (\langle \gamma, \tau^s(l, \gamma', m), K \cup \{\tau^m(l, \gamma', m)\} \rangle, \text{✖}) \quad \text{if } \beta(l, \gamma', m)$$

$$\beta^r((\text{duplicate}, l), \gamma, m) = \gamma \in S$$
$$\beta^r((\text{speculate}, l), \langle \gamma, \gamma', K \rangle, m) = \beta(l, \gamma', m)$$
$$\beta^r((\text{validate}, l), \rangle \gamma, \gamma', K \rangle, m) = \gamma' \neq \gamma$$

Formal Semantics of Smart Transactions

Refinements of this model can be used to specify additional constraints, for example, we can implement Ethereum's Out-Of-Gas (OOG) transactional semantics by allowing "duplicate" after subtracting gas from the transacting account's state, and invalidating the whole multi-step transaction execution if it runs out of gas before it terminates.

We can thereby see that Ethereum transaction semantics are already using smart transitions, with respect to validating gas limits.

Section 4

Use Cases, Challenges, and Implications

Bundle/search protection infrastructure is built on more primitive smart transactions infrastructure, and allows for many much smarter transactions

- We can build true ACLs w.o. code analysis,
- we can save gas and pay without ETH,
- rent as expected MEV to justify state in RAM,
- automated collective bargaining
- direct micro/meso/macroecon interventions
- just-in-MEV-time LP pools
- 0-capital, 0-credit trading
- “hedge” exact end-of-block costs perfectly
- ....and many more!

Smart transactions are useful for infrastructure development, for all prior blockchain use cases, and shiny new smart-transaction-only features

Smart transactions need efficient solutions for:

- simultaneous search of inter-dependent smart transactions
- verifiable counterfactual claims, summaries, statistics
- multi-block smart txs/validation
- search/searcher organization
- gas and DOS insurance markets

Considerable Challenges Remain, in Smart Transaction Infrastructure and Search,

To make sure that smart transactions don't fail to execute even as demand for preprocessing increases

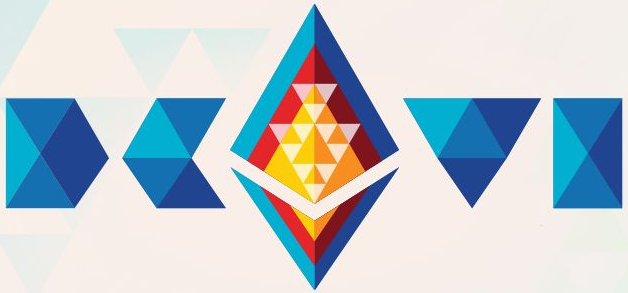
Smart, beyond MEV

Smart transactions are defined in terms of the wide scope of their validation capacities, more than the MEV for which their valid traces are optimized, at MEV-time

Smart transactions semantics are innovative in computer science, they reduce costs and have quantitatively qualitatively better risk managent than traditional economic transactions, they increase the power of transactions and create very low liability virtual service transaction provider roles, and open up transaction semantics

Smart Transactions have implications far outside of their MEV-time birthplace

Smart Transactions Revolutionize Ethereum's Transcational Semantics



Thank you!

Your Name

Your title, your organization

email@emailaddress.com

@twitterhandle