WebAssembly in Blockchains

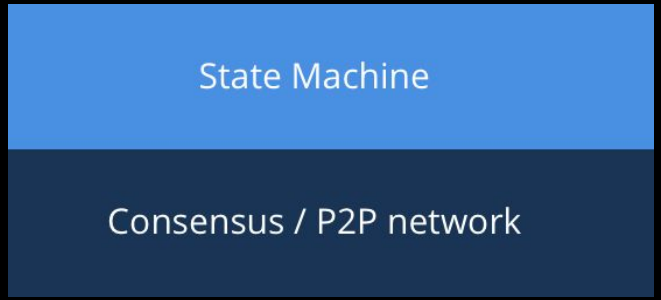
Sina Habibian
Truebit

Intro

- WebAssembly is finding a home within blockchains.
- Research with Ethereum, Parity, Dfinity, and Truebit.
- Goal: give a sense of the platform, approaches, and challenges.

Blockchain overview

- Replicated state machine.
- State machine : consensus



Metering

- Users need to pay for how much they use shared resources.
- The concept of “gas”
- Metering for instructions & memory.
- The mechanics: insert metering instructions per block of code & keep a tally.

Nondeterminism

- Blockchains need **consensus =>** the blockchain VM needs to be deterministic.

Nondeterminism – resource limits

- Resource limits:
  - Stack depth
    - Different clients on different operating systems.
    - Helpful: stack-balancing feature.
    - Solution: gas
  - Memory

Nondeterminism – floating point

- Current solution: reject contracts that have floating point operations or globals at validation.

- Idea: canonical definitions for floating point / NaNs – “a deterministic subset of WASM”

Instrumentation

- Two parts: 1) what to collect, 2) how to collect it – could go in the Javascript spec
- Introducing ways to inspect the stack.
  - State snapshotting.

Imports

- A spec for non-browser-based VMs.

Typed traps

- Getting more info out of the WASM runtime.
- To enable symbolic execution and static analysis tools: “is this type of exception possible?”
- Maybe related:

Trap versus embedder-specific error #1070

Open jfbastien opened this issue on May 22, 2017 · 2 comments

jfbastien commented on May 22, 2017 Owner

Over in WebAssembly/spec#483 (comment) @rossberg-chromium and I discuss what should generate a trap versus an embedder-specific error.

Backward compatibility

Things aren’t too bad.

- WASM binaries starts with a distinct flag.
- Existing projects: JULIA, evm2wasm.

New WASM developments which will be helpful

- Multi-values
- References types
- Annotations

New WASM developments which may not be helpful

Will lead to nondeterminism:

- Threads (with shared memory).
- GC

Thank you!

Ping me at: sina@truebit.io