What is the EVM?

Michael Yuan, PhD

https://www.secondstate.io/

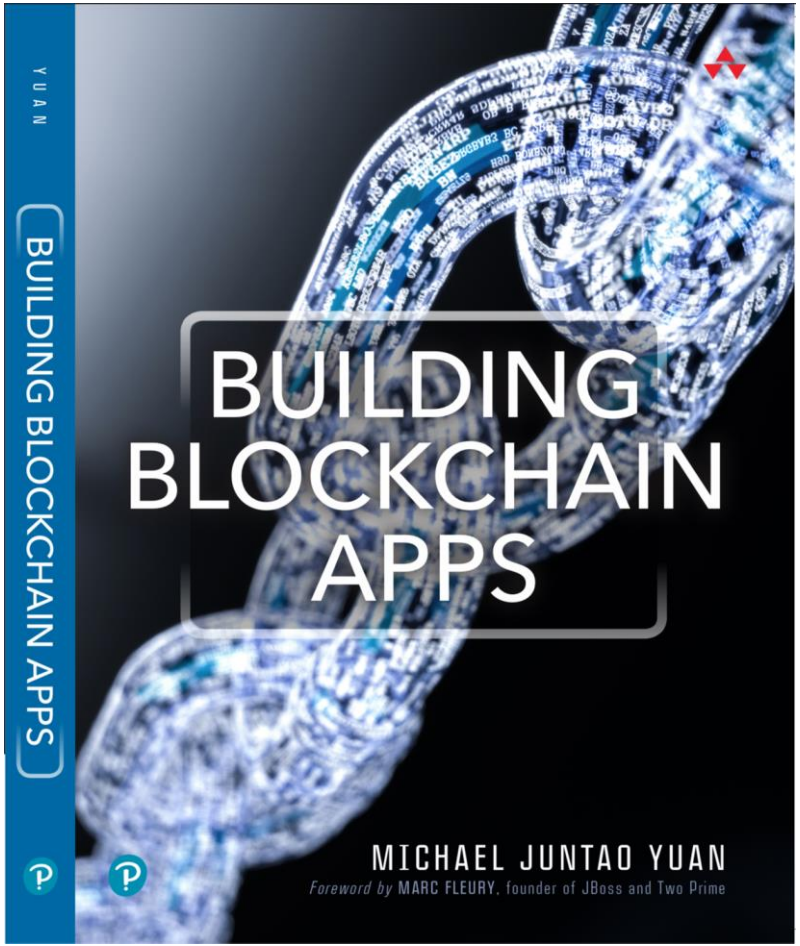
Who am I

- Open source veteran
  - Red Hat
  - JBoss
  - Mozilla
- CEO at Second State
  - http://www.SecondState.io/
  - **VC-funded software startup here in Austin!**
- Co-founder of CyberMiles
- Author of 5 books on software
- Principle Investigator for NIH

SECOND STATE

Play a game to get 35% OFF

http://secondstate.io/book



“

Ethereum is a global, open-source platform for decentralized applications. On Ethereum, you can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world.

Ethereum.org

It is already a $20+ billion dollar ecosystem.

SECOND STATE

Ethereum Virtual Machine

1. A Turing complete VM that runs on a server
2. Operation System and hardware agnostic
3. Access to persistent data storage
4. Very lightweight

SECOND STATE

Developer experience

Upload a compiled application to the cloud, and receive a pointer to the deployed application.

Execute a function, and get the result. Application state is persisted between function calls.

SECOND STATE

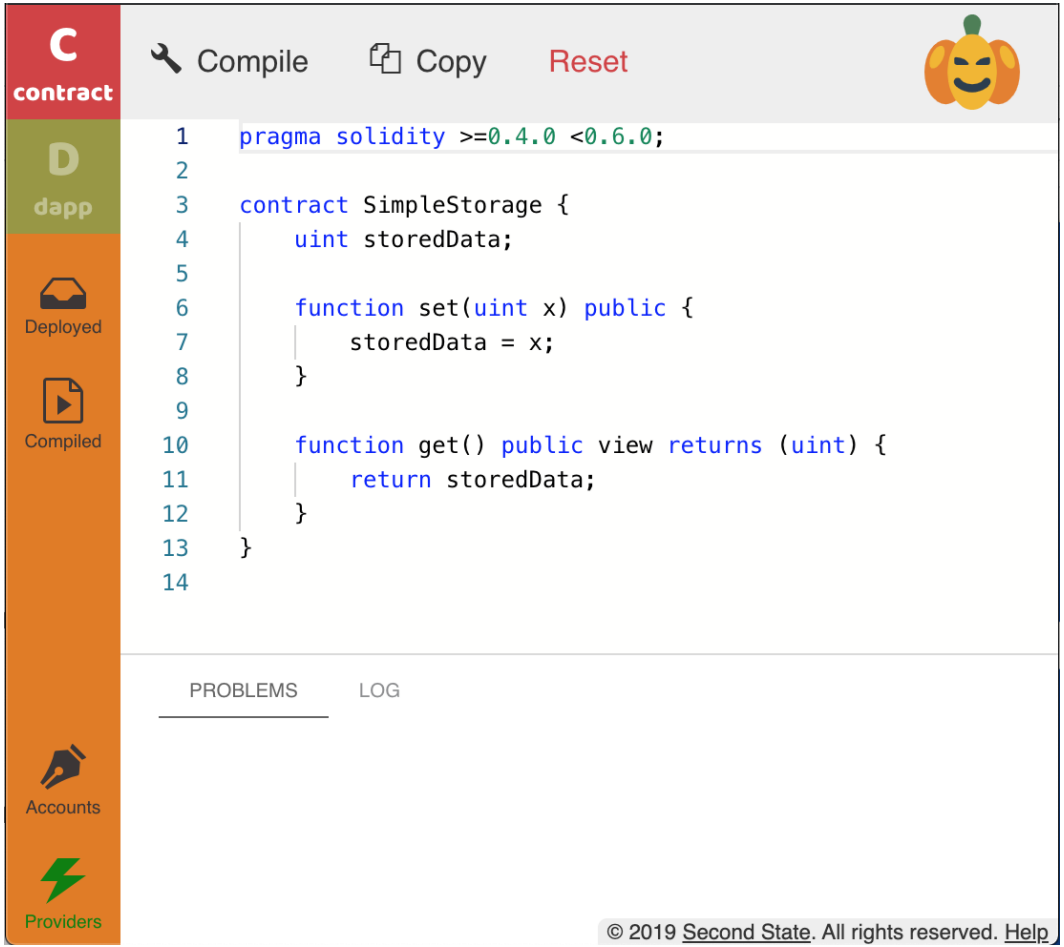
Wait … Isn’t this the same as

cloud-native microservice?

DEMO

http://buidl.secondstate.io/

SECOND STATE



SECOND STATE

Blockchain & dapp

SECOND STATE

Decentralized ledger

- Not just distributed, but decentralized
- A small subset of database functions, but without the DBA
- Key features
  - Consensus without authority
  - Impossible for small groups to cheat
  - Very difficult to change past history
- NOT optimized for performance

SECOND STATE

SECOND STATE

The smart contract

- The genius idea behind Ethereum
  - Bitcoin TXs are just for coin transfers. The consensus is the account state after the TX
  - Why not execute code inside TX and reach consensus on the results?
  - The virtual machine to execute code could be Turing complete
- How it works
  - The smart contract is “backend” software residing on blockchain
  - It is automatically executed by all nodes when the transaction is included
  - Majority of nodes must agree on the execution results
- Implications
  - Automation, transparency, correctness
  - Code is law
  - Machines and humans

EVM is designed for the blockchain use case

- Deterministic behavior
  - Supports specialized programming languages
- Integration with cryptocurrency
  - Addresses, public key, private key, hash functions etc.
  - Supports payable functions
  - Transfers between accounts
- Support gas computation and operations
  - Requires “gas” to operate
  - Prevents infinite loops

SECOND STATE

Future of EVM

SECOND STATE

Ethereum is not World computer

> At the moment, Ethereum can handle about 13 transactions per second, which cuts in half to about **7 transactions per second** for tokens (4.7m gas limit, 21k avg gas price for standard txn = ~220 standard txns every block, current avg block time 17s = 13 txns/sec, gas requirement roughly doubles for token transactions). And this doesn't include more expensive smart contract execution.

Smart contracts on Ethereum are worse than even non-financial commercial code; as of May 2016, Ethereum contracts averaged 100 obvious bugs (so obvious a machine could spot them) per 1000 lines of code.[6] (For comparison, Microsoft code averages 15 bugs per 1000 lines, NASA code around 0 per 500,000 lines.)

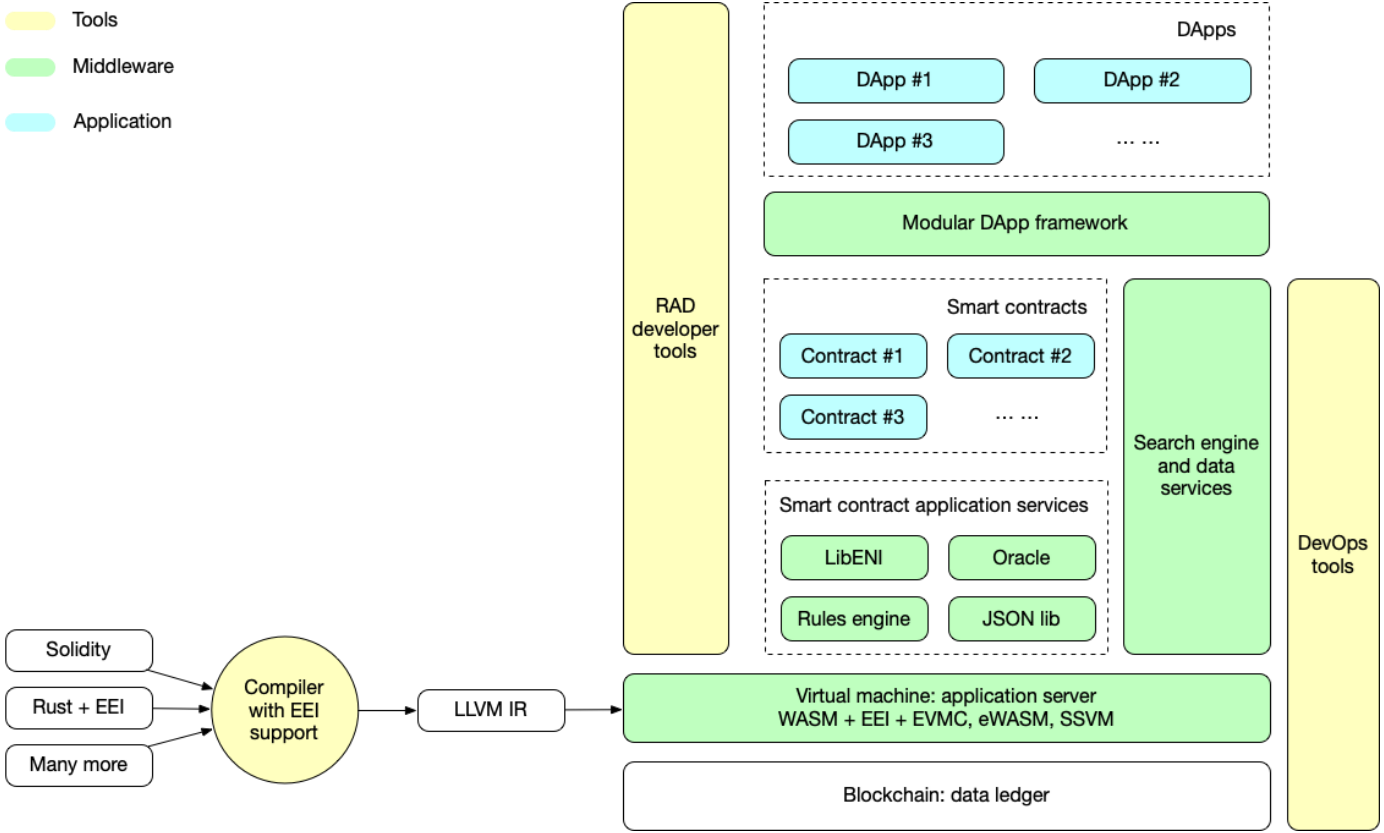
SECOND STATE

The twin challenges of Solidity (and any smart contract language, really)

The language is generic (Turing complete) and difficult to optimize for domain-specific applications and use cases.

To support both consensus and non-consensus computing in the same program drives the language design toward the lowest common denominator.

Ewasm (Ethereum flavored WebAssembly)



SECOND STATE

WASM beyond the blockchain

SECOND STATE

WebAssembly (WASM) on the server?

1. Language agnostic (compare with JVM and JS VM)
2. High level of abstraction (compare with OS containers)
3. Native performance with very small footprint
4. Ideal for microservices

“

If WASM+WASI existed in 2008, we wouldn't have needed to created Docker. That's how important it is. WebAssembly on the server is the future of computing.

Solomon Hykes, Co-founder of Docker

Ethereum innovations for enterprise IT

Digital currencies

Account & security infrastructure for centralized digital currencies

- Facebook Libra
- DECP

Formal verification

Formally verify the correctness of source code and bytecode. Many solutions now.

Zero knowledge

Compute results without knowing the input data.

- Oasis Labs

SECOND STATE

The Second State Solution

For blockchains

- Ewasm runtime module
- LLVM compiler for Solidity & YUL

Customers & Partners:

- Ethereum Foundation
- Ethereum Classic Labs
- CyberMiles Foundation
- Oasis Labs

For enterprise IT

- Server-optimized WASM engine
- Storage and persistence
- RPC services

Customers & Partners:

- Qualcomm
- Tianjin University

Voice your opinion

& record it on the public blockchain

Are you interested in deploying microservices written in Rust / Go / Swift / Python / TypeScript in WebAssembly (WASM) runtimes on the server-side?

http://secondstate.io/demo/2019-austin.html

SECOND
STATE

Thanks !