LLVM x Blockchain

A New Ecosystem of Decentralized Applications

Robin Zhong

About Me

Robin Zhong
robin@nebulas.io

Nebulas

Co-founder and CTO of Nebulas

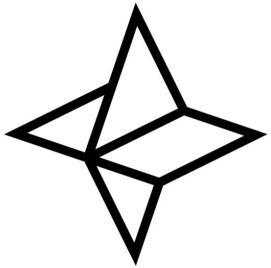
Alibaba Group 阿里巴巴集团

Former architect of Alibaba Blockchain Department

dolphin

Former Senior Engineering Director of Dolphin Browser

About Nebulas



NEBULAS

Decentralized Search Framework

Nebulas is an open source Public Blockchain project, aims to provide search framework for blockchains.

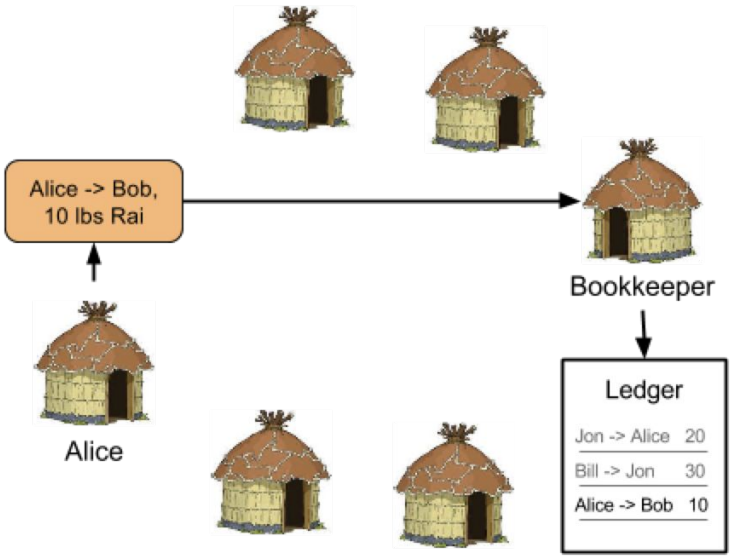
https://nebulas.io/

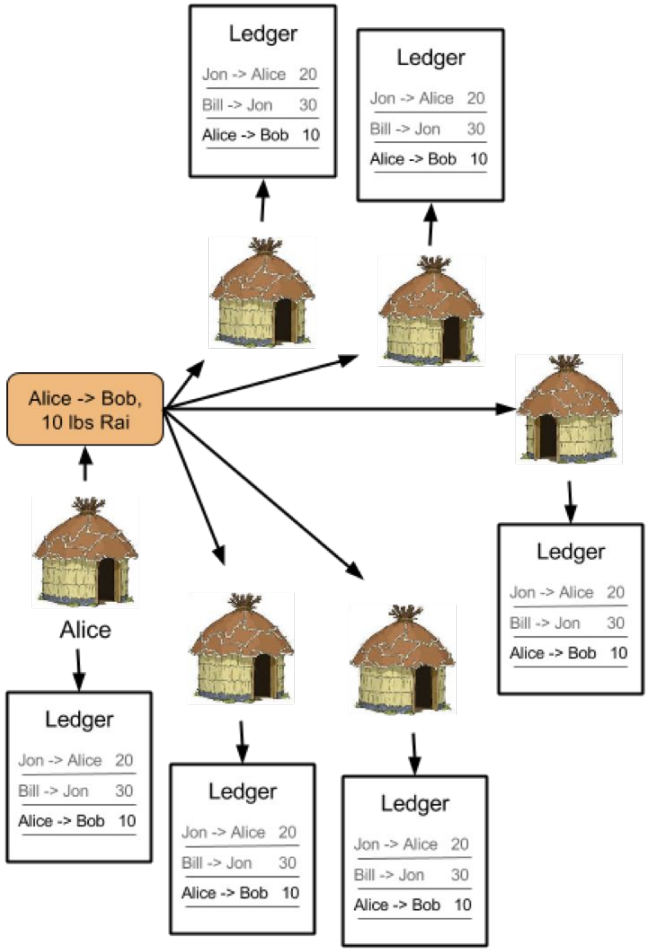
https://github.com/nebulasio

Agenda

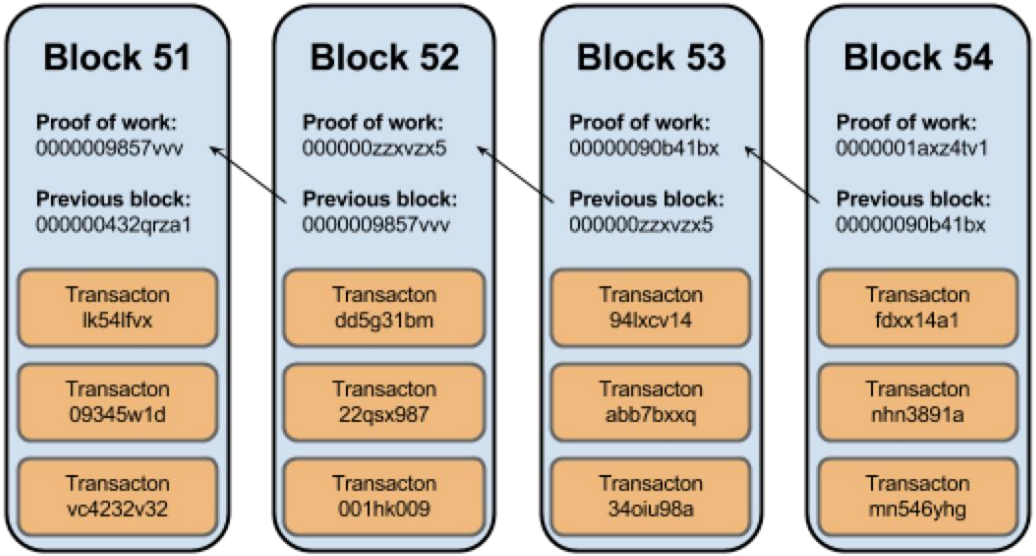
- What’s the Blockchain
- How Decentralized Applications works
- Why LLVM + Blockchain
- What is Nebulas doing

What's the Blockchain

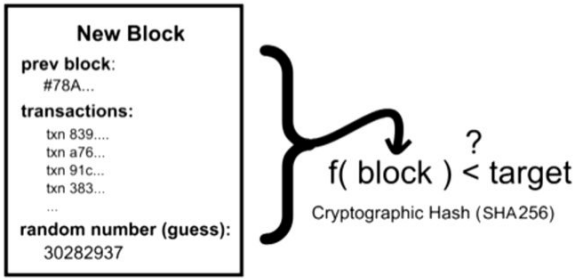




What's the Blockchain

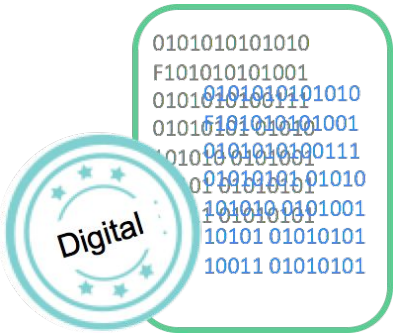


POW (proof-of-work) is one of most popular Consensus algorithm



What’s the Blockchain

Blockchain ensure the ownership of data



Token reveals the value of data

Blockchain industry

Cryptocurrencies: 1568
Markets: 10328

Market Cap: $332,039,265,018
24h Vol: $16,238,332,425

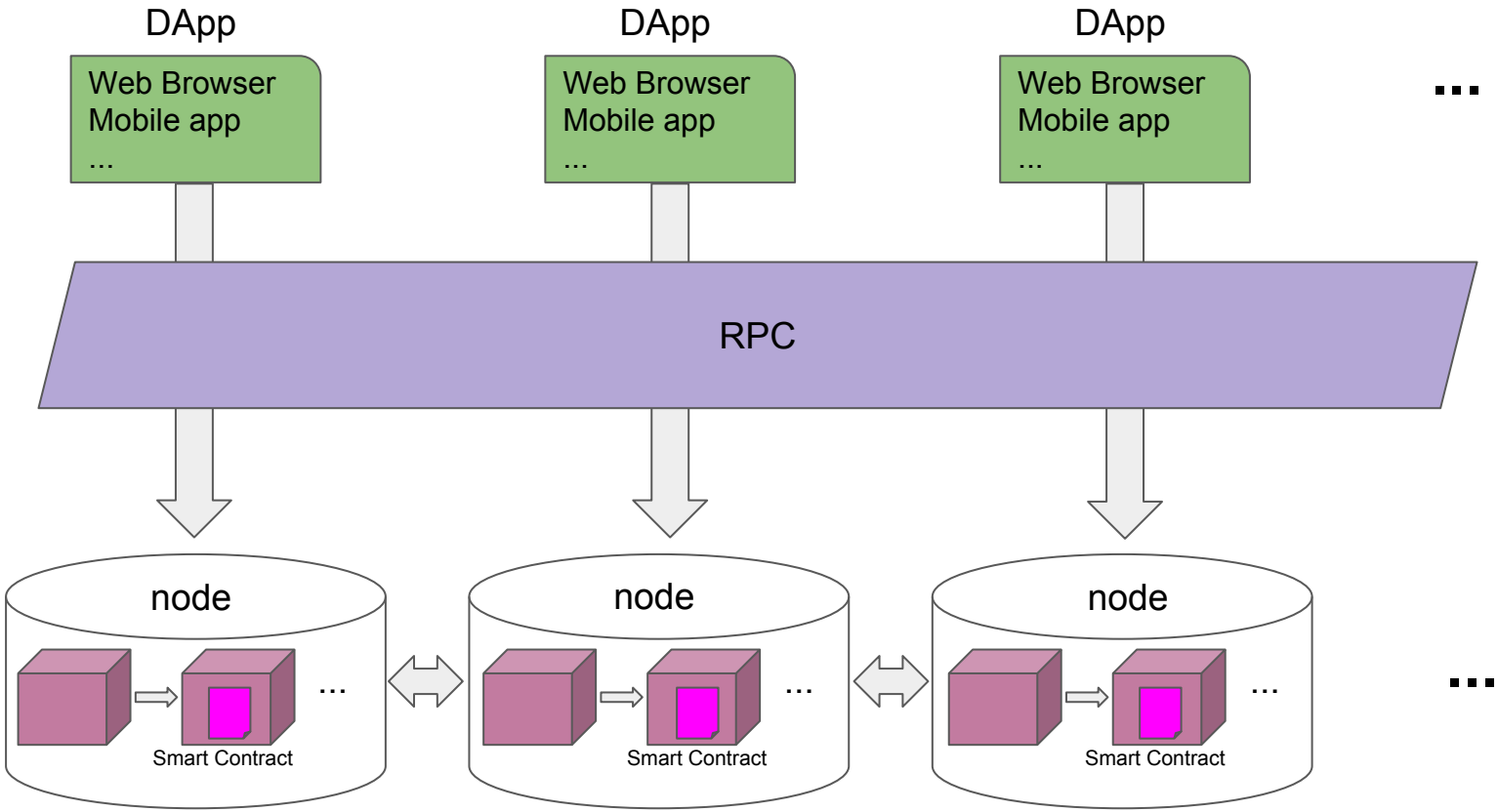
Bitcoin - E-cash system

Market Cap: $138,246,955,744

Ethereum - Decentralized Application Platform by introducing Smart Contract

Market Cap: $50,851,932,229

How Decentralized Application works



Generic architecture of DApps

Features of Decentralized Applications

- Smart Contract must be open source
  - The application must be completely open-source, it must operate autonomously, and with no entity controlling the majority of its tokens. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by consensus of its users.
- Data must be stored in a public blockchain
  - The application's data and records of operation must be cryptographically stored in a public, decentralized blockchain in order to avoid any central points of failure.
- App must use a cryptographic token
  - The application must use a cryptographic token (bitcoin or a token native to its system) which is necessary for access to the application and any contribution of value from (miners / farmers) should be rewarded in the application’s tokens.
  - The application could issue their tokens according to a standard cryptographic algorithm acting as a proof of the value nodes are contributing to the application.

Show cases of Decentralized Application

- Steam
  - https://steem.io
  - Steem is a blockchain-based rewards platform for publishers to monetize content and grow community.
  -
- Cryptokitties
  - https://www.cryptokitties.co/
  - Collect and breed digital cats.

Pains of Decentralized Applications

- No security guarantee mechanism
- Toolchains are unfriendly
- Execution environments are vary
- Performance is always important

No Security Guarantee Mechanism

- State-of-art:
  Nothing is done yet.
  A concrete example: Over 3000 ethereum contracts have major security flaws.

- Problem:
  Platform is vulnerable to malicious applications
  Code/contract is written by human-being, it's not bug-free
  Existing contracts cannot be amended if there's security flaw

Toolchains are unfriendly

Different platforms are using different programming languages for application development, lack of complete documents, need more development tools as well.

- State-of-art:
  Ethereum → Solidity, Serpent, Mutan, LLL
  Ripple → C++
  EOS → C++
  Fabric → Go, Java
  Corda → Kotlin, Java

- Problems:
  Developers need to learn a new programming languages in order to develop the applications on those platforms. Time-consuming, yet with low productivity.
  Lack of complete documents and development tools are also pain points to developers.

Execution Environments are Vary

DApps are running on variety of execution environments:

- State-of-art:
  Ethereum → Ethereum Virtual Machine (EVM)
  EOS → Webassembly
  Corda → Java Virtual Machine (JVM)

- Problems
  Nearly impossible to migrate application to different platforms, and we need a standard

Performance is always important

How about the performance?

- State-of-art
  Bitcoin: ave. 5TPS in real use case
  Ethereum: 10TPS in real use case
  Fabric: 1000TPS (consortium chain)

- Problems
  Significant limitation on applying blockchain technology in real life

Benefits of LLVM x Blockchain

No Security Guarantee Mechanism ?

Built up on LLVM front end and IR, we may have different ways to guarantee security:

- Program level, we can leverage program annotation, program verification technologies to guarantee the DApp is secure even it’s written by ordinary developers
- Runtime level, we can limit the system resources that the DApps can access to avoid potential secure flaws.
- Protocol wise, security rules are built in, malicious applications can easily be filtered out and not eligible to be run on platform.

Benefits of LLVM x Blockchain

Toolchains are unfriendly ?

LLVM front end can easily support main programming languages that developers are familiar with.

C/C++, Java, Go, C#, Kotlin, … can all be supported using LLVM front end.

Benefits of LLVM x Blockchain

Execution Environments are Vary ?

LLVM JIT for all platforms, including different OS and different arch

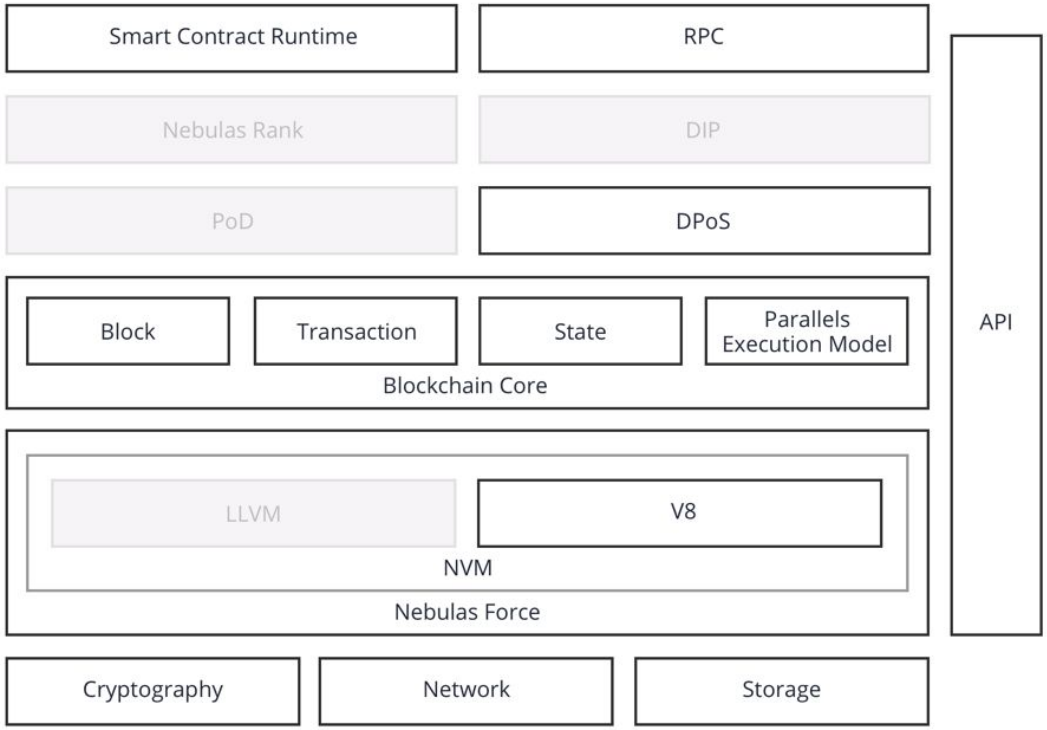
Benefits of LLVM x Blockchain

Performance is always important?

Parallel processing of smart contracts through horizontal scalability can be a good way to improve performance.

Rely on LLVM and it’s powerful tool chain, it is promising to build high performance DApps on top of it.

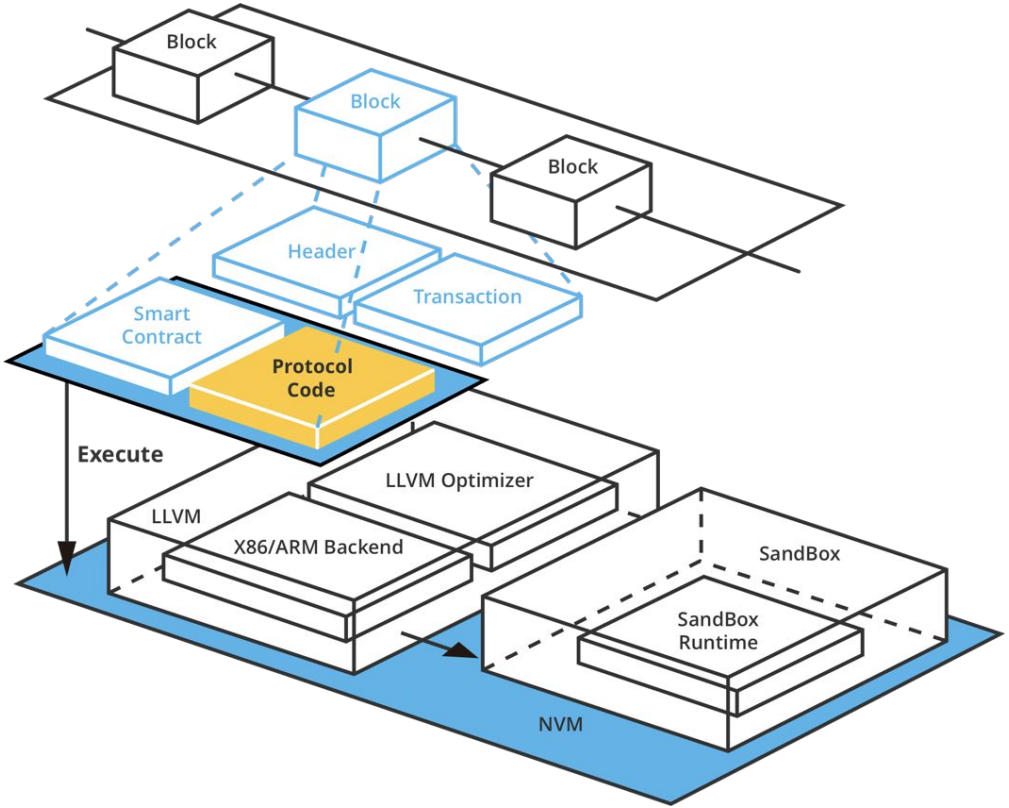
What is Nebulas doing



Nebulas release v1.0 & mainnet https://mainnet.nebulas.io

- Fully functional blockchain system
- JavaScript is the smart contract language
- Up to 2000 TPS

Nebulas Virtual Machine = Nebulas + LLVM



NVM

- A blockchain compatible execution sandbox
- Build on top of LLVM
- Inspired by MinSFI with trusted compiler and trusted call stack

Source code (under development):
https://github.com/nebulasio/go-nebulas/tree/develop/nf/nvm/llvm
https://github.com/nebulasio/nvm

Challenges of NVM

- Security
  - Blockchain requires a safe sandbox to execute smart contract, which may harmful for both system and host (node)
  - Developers need a secure toolchain to help them write secure smart contract, especially the value managed by smart contract is so high

- More Languages, toolchain, and performance

Website:	https://nebulas.io
Contact:	contact@nebulas.io
Blog:	https://medium.com/nebulasio
Github:	https://github.com/nebulasio
Slack:	https://nebulasio.herokuapp.com