

# GBA

RESTON CHAPTER

**Michael Adams, Co-Organizer**  
**February 26, 2020**

[www.GBAglobal.org](http://www.GBAglobal.org)

1

## About Tuan Phan



# GBA

- Partner at Caplock Security LLC
- Builds several proofs of concept using Hyperledger Fabric and Ethereum private blockchains
- Advises clients on the security implementation of smart contracts and blockchain infrastructure.
- Speaker on numerous topics on cybersecurity, blockchain security, smart contract auditing, IT governance, and regulatory compliance at several industry conferences and seminars.
- Developed and taught ISACA GWDC Blockchain Security Seminar
- Authored several articles on blockchain and regulatory compliance topics for industry magazines and journals
- Members of ISACA 2020 Emerging Technology Advisory Group
- SME reviewer for ISACA Blockchain Audit Program



2

2



# Ethereum Blockchain Ecosystem

February 26, 2020

Tuan Phan, CISSP, PMP, CBSP, Security+, SSBB

Partner, Caplock Security LLC

202-780-5455

[tphan@caplocksecurity.com](mailto:tphan@caplocksecurity.com) [@ChainOpSec](https://twitter.com/ChainOpSec) [LinkedIn.com/in/tuanphan/](https://www.linkedin.com/in/tuanphan/)

3

3

## Agenda



- What is Ethereum
- Ethereum Roadmap
- Why Ethereum
- Decentralized Applications (DApp)
- DApp Showcases
  - Jordi Guirao – CityBetter , <https://www.linkedin.com/in/jordiguiraomuns/>
  - Ali Kalkanel – LOANER Dapp , <https://www.linkedin.com/in/ali-kalkanel/>
  - Steve Despres – Smart Name System, <https://www.linkedin.com/in/steve-despres-9b443bb1/>
  - Tuan Phan – ETH Fund Me, <https://www.linkedin.com/in/tuanphan/>

4

4

## Why Ethereum



- Promote the growth of Ethereum ecosystem
  - Robust and growing community
  - Viable for public as well as private blockchain
  - Variety of use cases
- Bring awareness on the robust capabilities
  - Key tools
  - Security best practices
  - Smart contracts & Dapp development
  - Rapid development and prototyping
- Encourage learning and onboarding of new developers

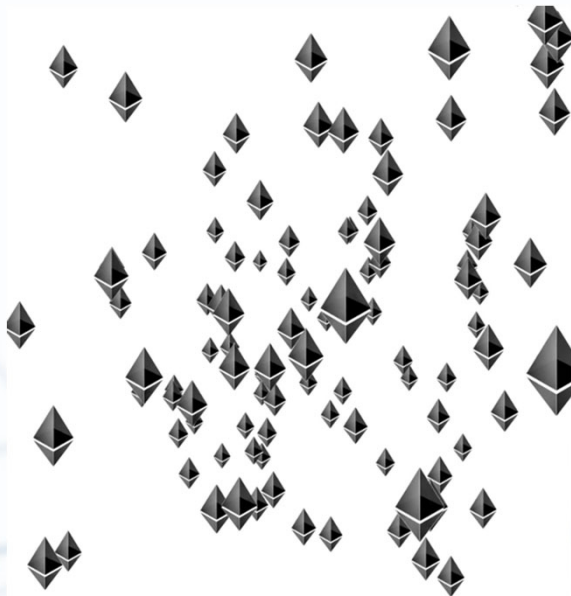
5

5

## What is Ethereum



- Open source, public network
- Permissionless
- Provide:
  - State management
  - Trustlessness
  - Trackability
  - Irreversible (immutability)
- Ethereum Virtual Machine
  - Execution environment
- Ideal system for smart contracts



6

6

## Components of Ethereum

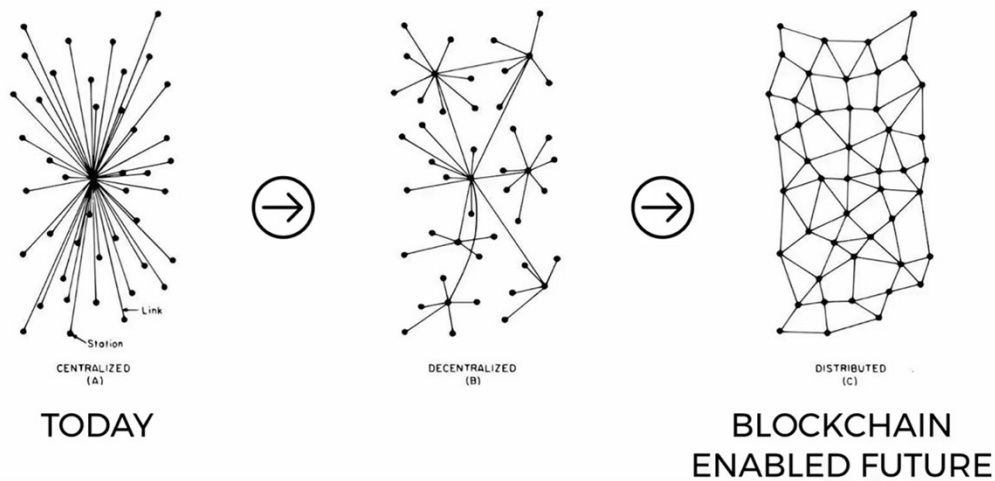


- P2P network
- State machine
- Transactions
- Data structures
- Consensus rules
- Consensus algorithm
- Economic security
- Clients

7

7

## P2P Network

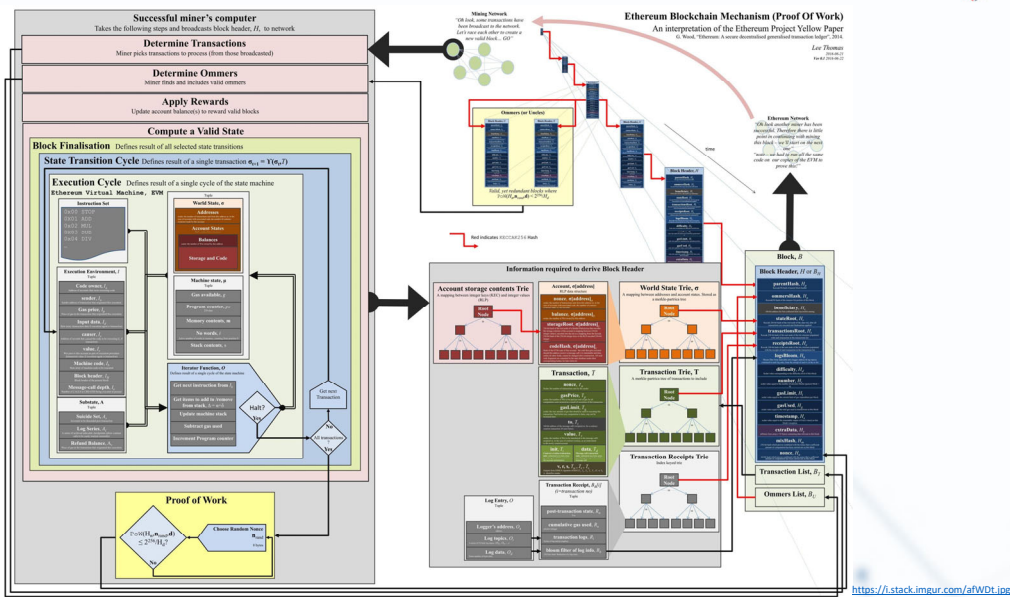


ConsenSys Academy

8

8

## Consensus Algo & Rules



9

## Ethereum Virtual Machine (State Machine)



- Runs on every node
- Handles all transaction processing
- Turing complete
- Solidity/Vyper/LLL → Smart contracts
- Operates on bytecode



ConsensSys Academy

10

10

## Transactions & Data Structures



### Transactions

- Function calls
- Contract, sender, recipient addresses
- Value
- Data payload

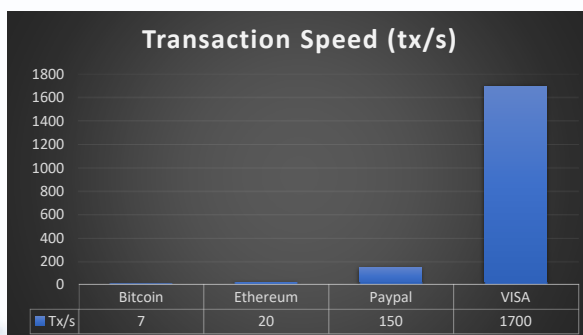
### Data Structures

- Each node's database (LevelDB)
- Merkle Patricia Tree

11

11

## Current Challenges



- EVM as bottleneck
- Inefficient
- Monopolization
- Environmentally unfriendly

12

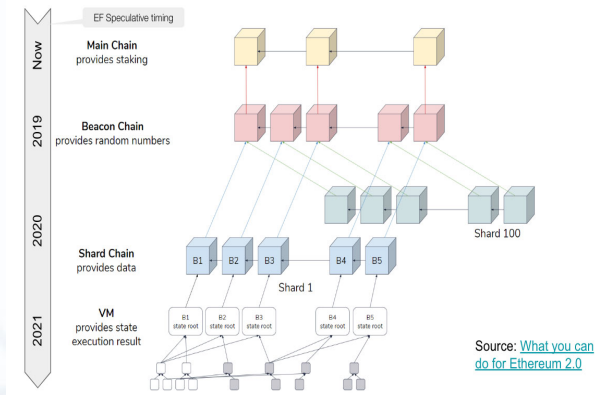
12



## Ethereum Roadmap → Ethereum 2.0



- Availability of developers, tools, and resources
- Ongoing project activities
- Alternative short-term scaling solutions:
  - Plasma (<https://plasma.io/plasma.pdf>)
  - ZK-Rollups
  - State Channels
  - Payment Channels
  - ZK-STARKS
  - Optimistic Rollups (Arbitrum)
  - Commit-chains
- Proof of stake
- eWASM



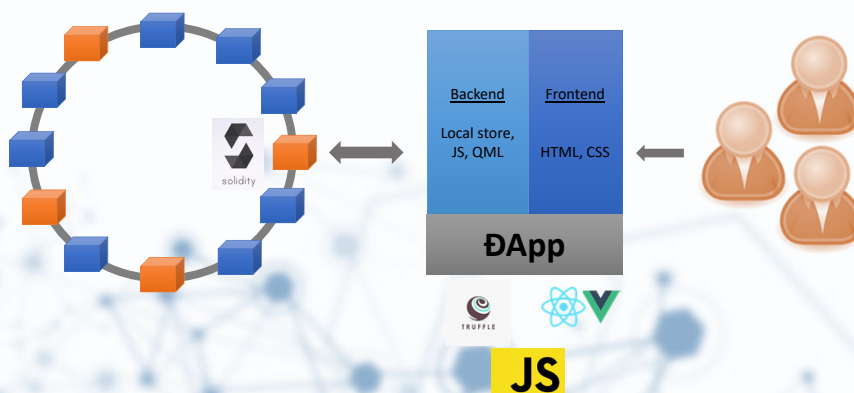
13

13

## Ɗapps and Smart Contracts



- [ƊApps](#) are blockchain-enabled applications/websites
- Rely on [smart contracts](#) for logic processing.



14

14

## Ethereum Ecosystem



- Open finance



- Oracles Provable

- Decentralized Exchanges



- Governance

- Infrastructure

- Developer Tools



- Gaming

- Collectibles

- Marketplaces

- Identity



- Token Curated Registries

15













15

## Ethereum DApps

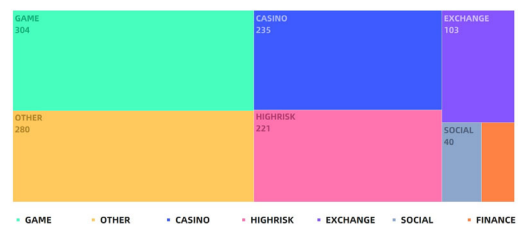


### 2019 Dapp Market Summary - By Blockchain

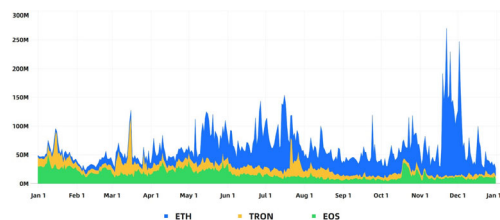
Dapp Review

	Dapps	Active Dapps	New Dapps	Active Users	Volume (USD)
 ETH	2146	1223	668	1.82M	12.81B
 TRON	663	637	579	989.28K	4.42B
 EOS	668	633	408	779.45K	6.10B
 IOST	49	34	49	37.27K	109.38M
 STEEM	97	92	60	18.62K	48.22M
 NEO	36	25	25	74.46K	99.51M
 ONT	63	59	57	201.51K	8.92M
 LOOM	16	14	16	29.40K	618.75K
 TOMO	22	5	22	6402	59.43M
 WICC	21	4	21	18.03K	2.36M
 WAVES	24	23	24	13.22K	12.18M
 WAX	26	26	26	62.92K	2.10M

### 2019 ETH Active Dapps - by Category



### 2019 Daily Txn Volume - By Blockchain (USD)



Data Source: dapp.review

Dapp Review

16

16



## CityBetter

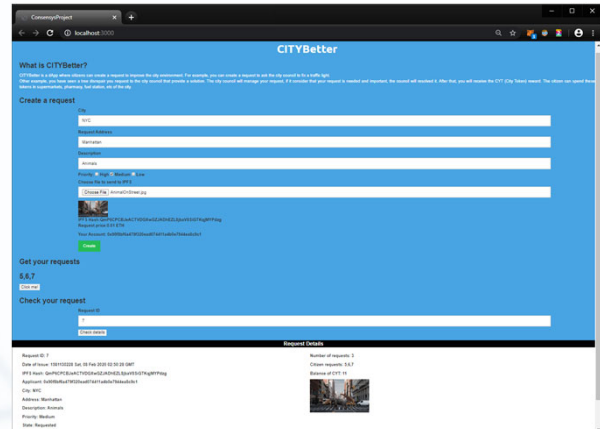
By Jordi Guirao



CITYBetter is a dApp where citizens can create a request to improve the city environment.

CityBetter could be a good way to introduce the Blockchain ecosystem to citizens.

CityBetter encourages citizen collaboration with the City Councils and the City to create a better economy and better city!



<https://www.linkedin.com/in/jordiguiraomuns/>



17

17

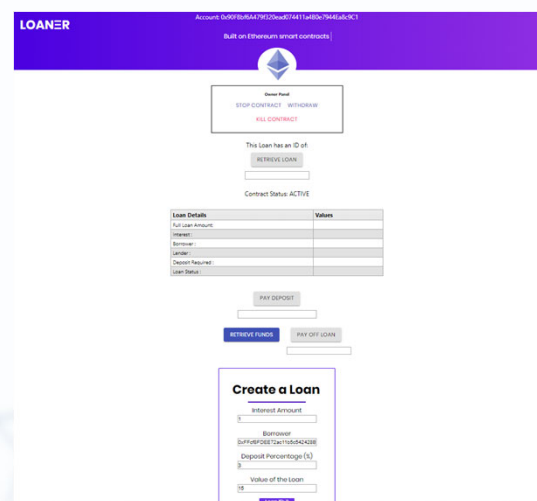
## LOANER

By Ali Kalkanel

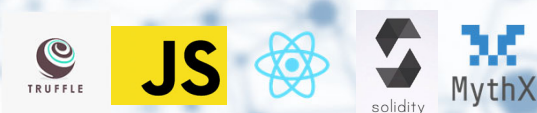


Loaner is a lending dApp that allows one to create a loan and/or borrow ETH via the LOANER platform.

This allows people to create peer to peer lending agreements in a secure and transparent way using Blockchain and Smart Contracts.



<https://www.linkedin.com/in/ali-kalkanel/>



18

18

## Smart Name System

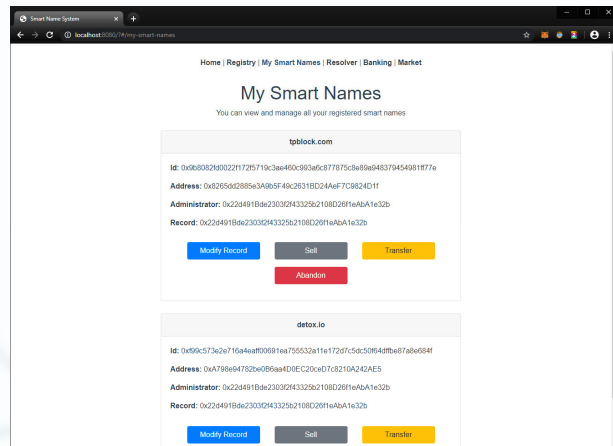
By Steve Despres



Smart Name System is a decentralized application built with Solidity for Ethereum Blockchain. It provides a name registry and some services and is composed of several smart contracts and a web application.

<https://www.linkedin.com/in/steve-despres-9b443bb1/>

<https://github.com/stevedespres/smart-name-system>



19

19

## ETH Fund Me

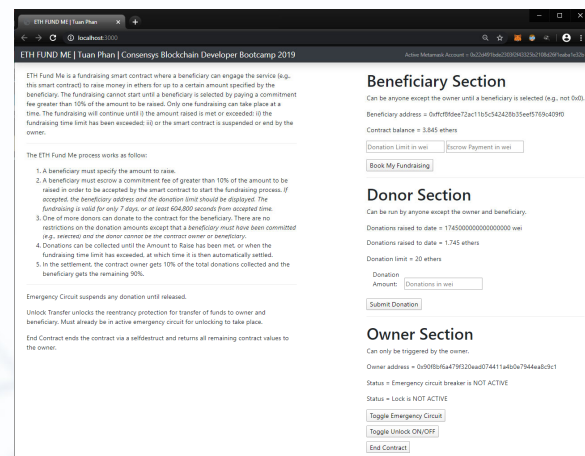
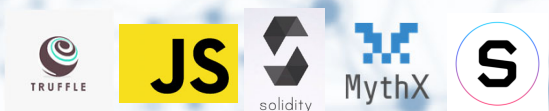
By Tuan Phan



ETH Fund Me is a fundraising smart contract where a beneficiary can engage the service (e.g., this smart contract) to raise money in ethers for up to a certain amount specified by the beneficiary.

<https://www.linkedin.com/in/tuanphan/>

<https://github.com/Tuanp703/Donations>



20

20



## Demo of Ethereum DApps

Jordi Guirao – CityBetter , <https://www.linkedin.com/in/jordiguiraomuns/>

Ali Kalkanel – LOANER DApp , <https://www.linkedin.com/in/ali-kalkanel/>

Steve Despres – Smart Name System, <https://www.linkedin.com/in/steve-despres-9b443bb1/>

Tuan Phan – ETH Fund Me, <https://www.linkedin.com/in/tuanphan/>

21

21



# Thank you for your time!

Tuan Phan, CISSP, PMP, CBSP, Security+, SSBB

Partner, Caplock Security LLC

202-780-5455

[tphan@caplocksecurity.com](mailto:tphan@caplocksecurity.com) @ChainOpSec [LinkedIn.com/in/tuanphan/](https://www.linkedin.com/in/tuanphan/)

22

22