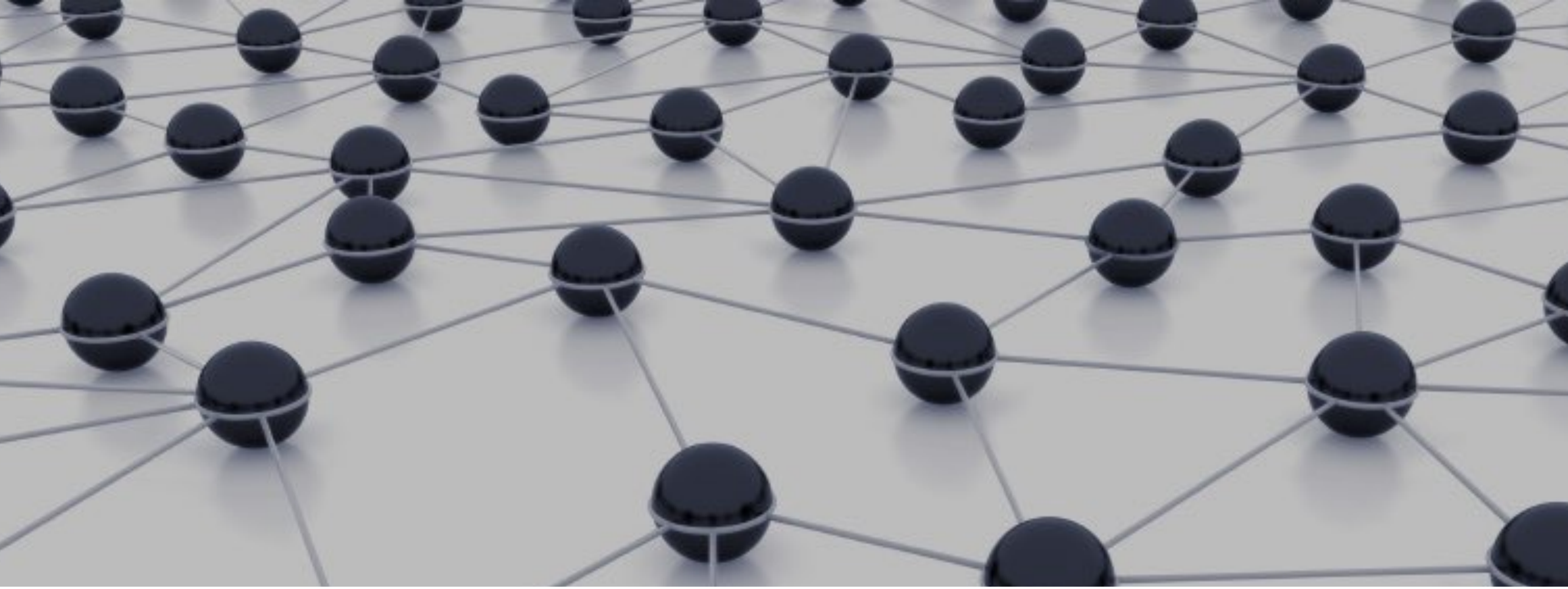
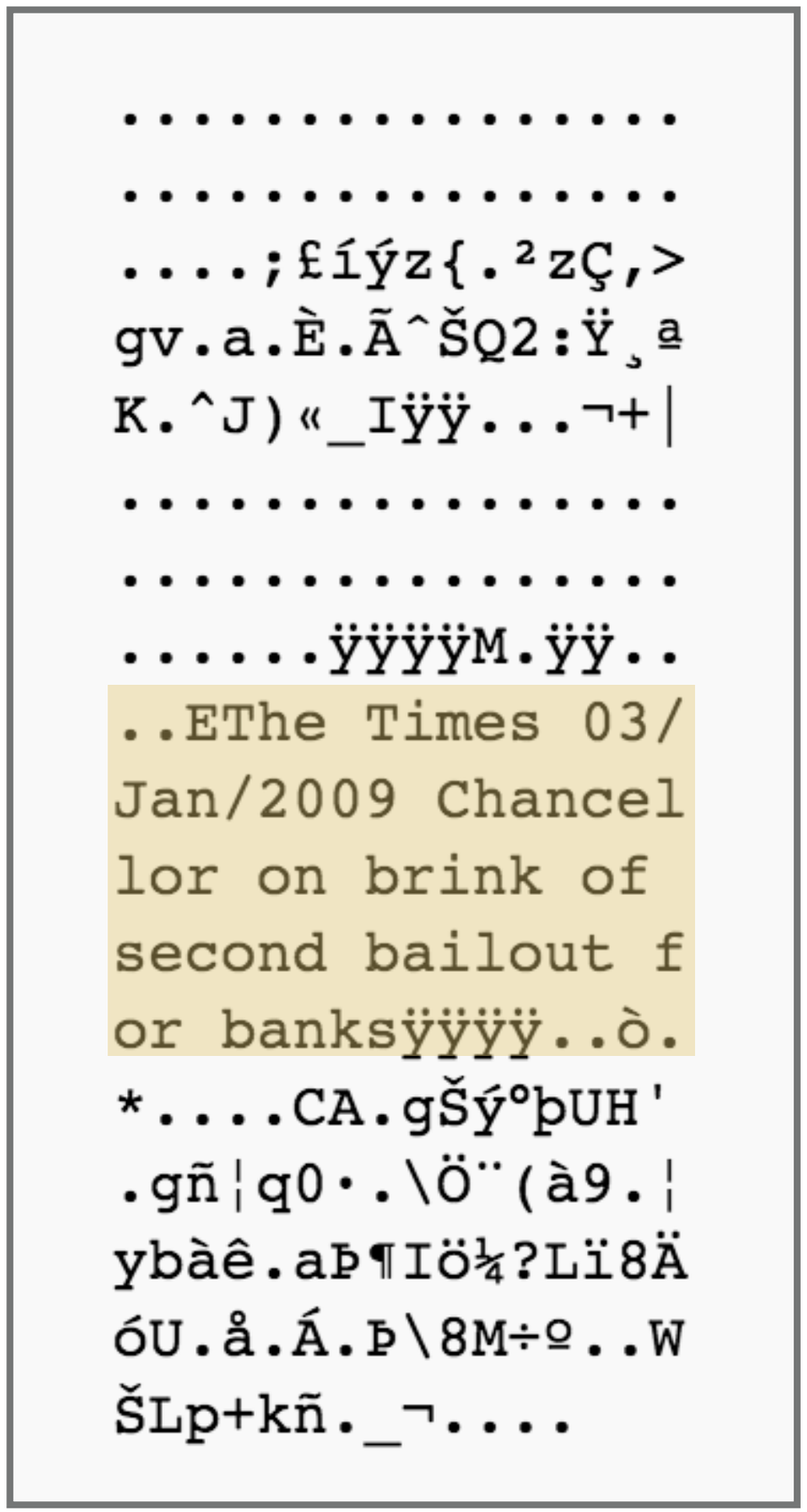


BLOCKCHAINS 101

Decentralisation for developers



GENESIS BLOCK

A little backstory…

PRELUDE

- Internet
- Databases
  - SQL
  - NoSQL
  - Big data
- Cryptography
  - Hash trees
  - PGP
- Peer-to-peer networks
  - DHT
  - BitTorrent

> Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.
>
> *-Satoshi Nakamoto*

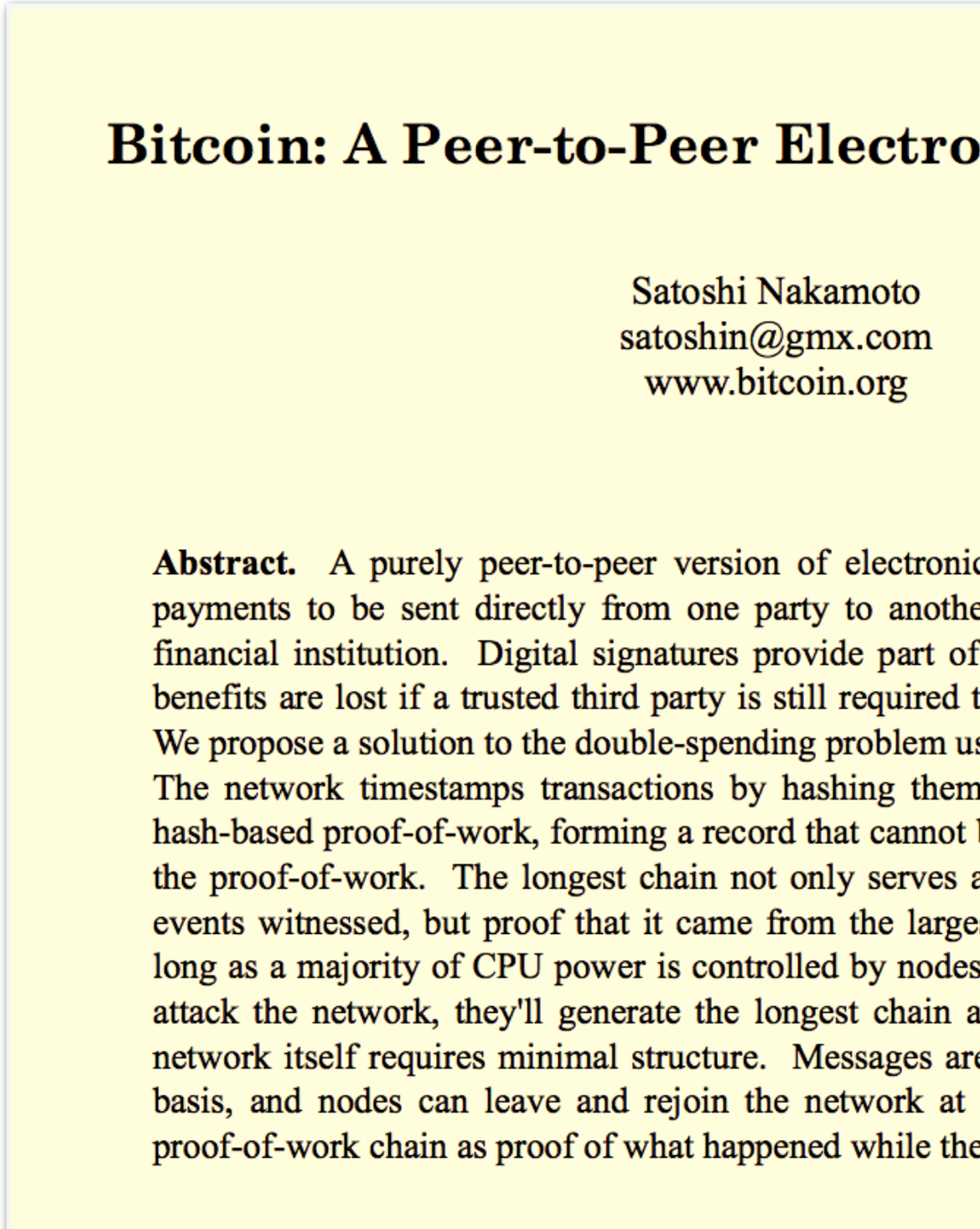
BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM

- "chain of blocks"
  - immutable Merkle data trees

- Censorship-resistant
  - P2P communication

- Coordination
  - Byzantine General
  - Prisoner's Dilemma

- Protocol governs compliance
  - Incentivised validators
  - Preventing tragedy of the commons



Bitcoin: A Peer-to-Peer Electro

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic
payments to be sent directly from one party to anothe
financial institution. Digital signatures provide part of
benefits are lost if a trusted third party is still required t
We propose a solution to the double-spending problem us
The network timestamps transactions by hashing them
hash-based proof-of-work, forming a record that cannot
the proof-of-work. The longest chain not only serves a
events witnessed, but proof that it came from the large
long as a majority of CPU power is controlled by nodes
attack the network, they'll generate the longest chain a
network itself requires minimal structure. Messages are
basis, and nodes can leave and rejoin the network at
proof-of-work chain as proof of what happened while the

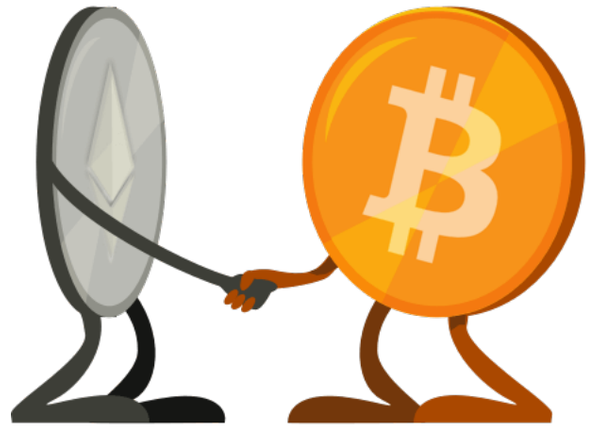
BEYOND BITCOIN

- Proliferation of “alts”
  - Litecoin / 2.5 block time
  - Dogecoin / fun
  - Darkcoin / private

- Not just value transfer
- Innovation in all industries
- Generalised state transition machine as “DApp platform”

BLOCKCHAIN PROJECTS

- Value
  - Bitcoin
  - DASH
- Processing
  - Ethereum
- Storage
  - ~~Namecoin~~
  - IPFS
  - Maidsafe/Storj
  - BigchainDB
- Messaging
  - ~~BitMessage~~



WUT!

Not only for buying drugs?

KEY FEATURES

- Immutable
  - Create Read ~~Update Delete~~
- Non-repudiable
  - Digital signatures
    - Sign & Verify
- Fault-tolerant
  - Censorship resistant
  - Partially-connected mesh resilience

BENEFITS

- Zero infrastructure
  - Scaling for free
  - Resilience for free
- Jurisdiction
  - Estonia e-Residency
  - Everywhere/nowhere
- Identity built-in
  - Sharable reputation
  - No more passwords
- Auditable
  - Triple-entry accounting
  - If you want it
- Censorship-resistant
  - State & corporate actors
  - Controversial ideas
- M2M transactions
  - Internet of things (IoT)
  - Microtransactions

CAVEATS

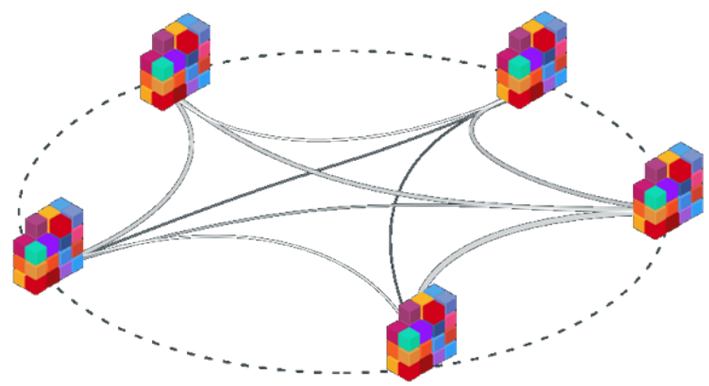
- External data
  - System does not know about outside world
  - Oracles

- Privacy
  - External now
  - Zero Knowledge later?

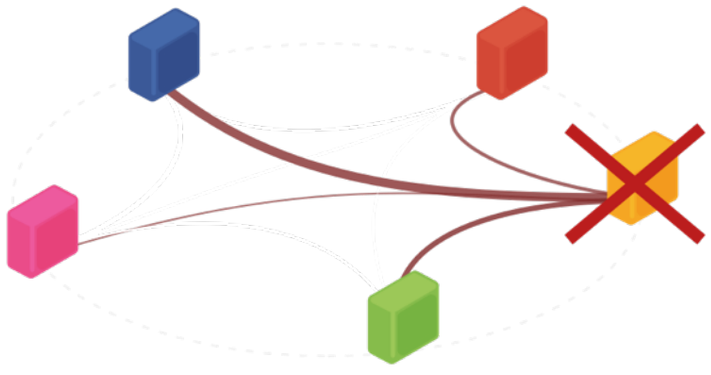
- Scalability
  - Increase transactions per second
  - Decrease time to finality

PUBLIC, PRIVATE, AND CONSORTIUM CHAINS

- Public chains are secured by pseudonymous validators
  - Proof of Work
  - Proof of Stake



- Consortium chains are secured by known entities
  - Require partial or full approval
  - May disregard unknown entities



- Private chains are… a fuzzy idea?
  - Privacy & fungibility with public chains unknown
  - Not clear if ledger is private or participants are exclusive

UGG WANT MORE

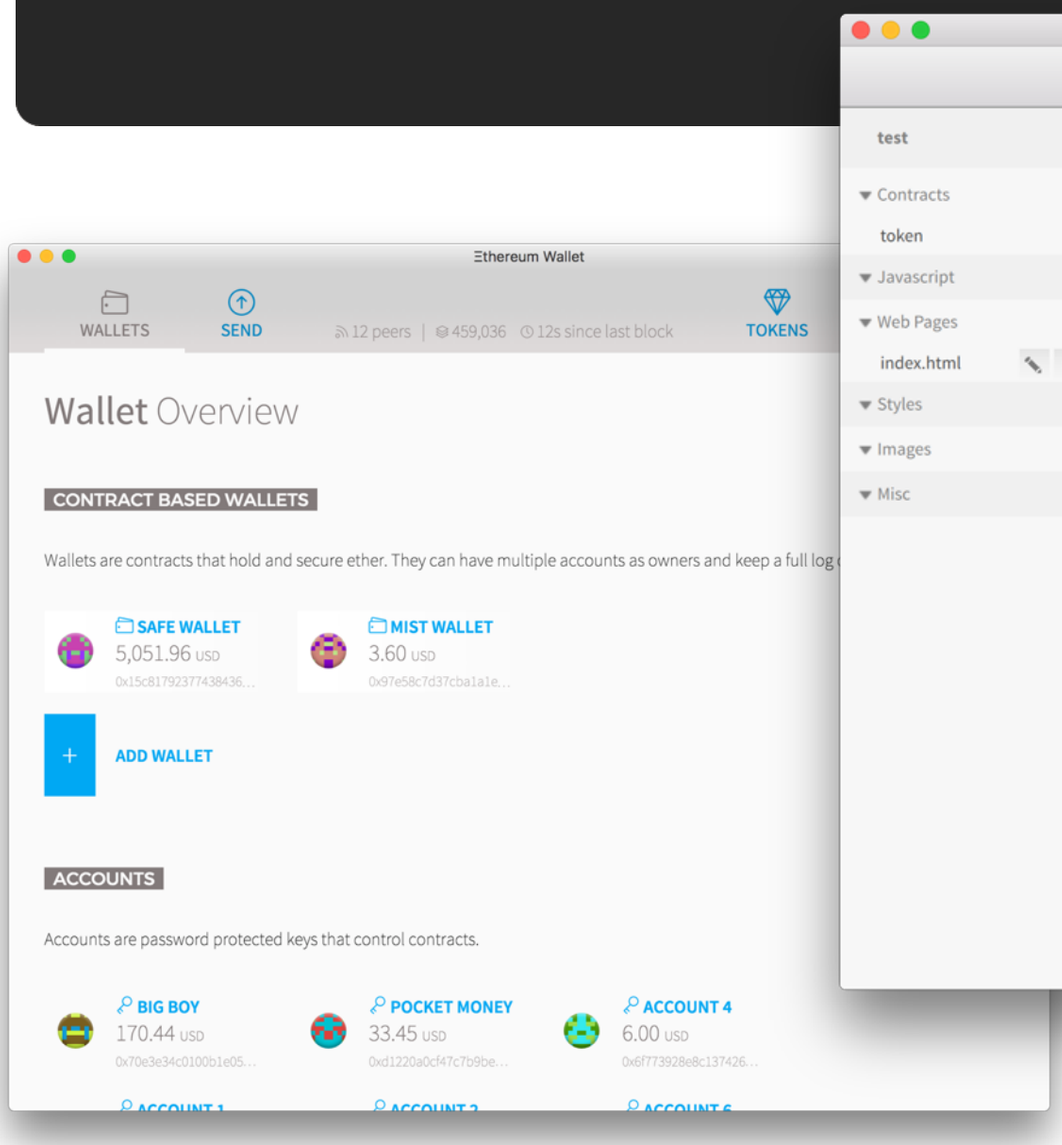
ETHEREUM ECOSYSTEM

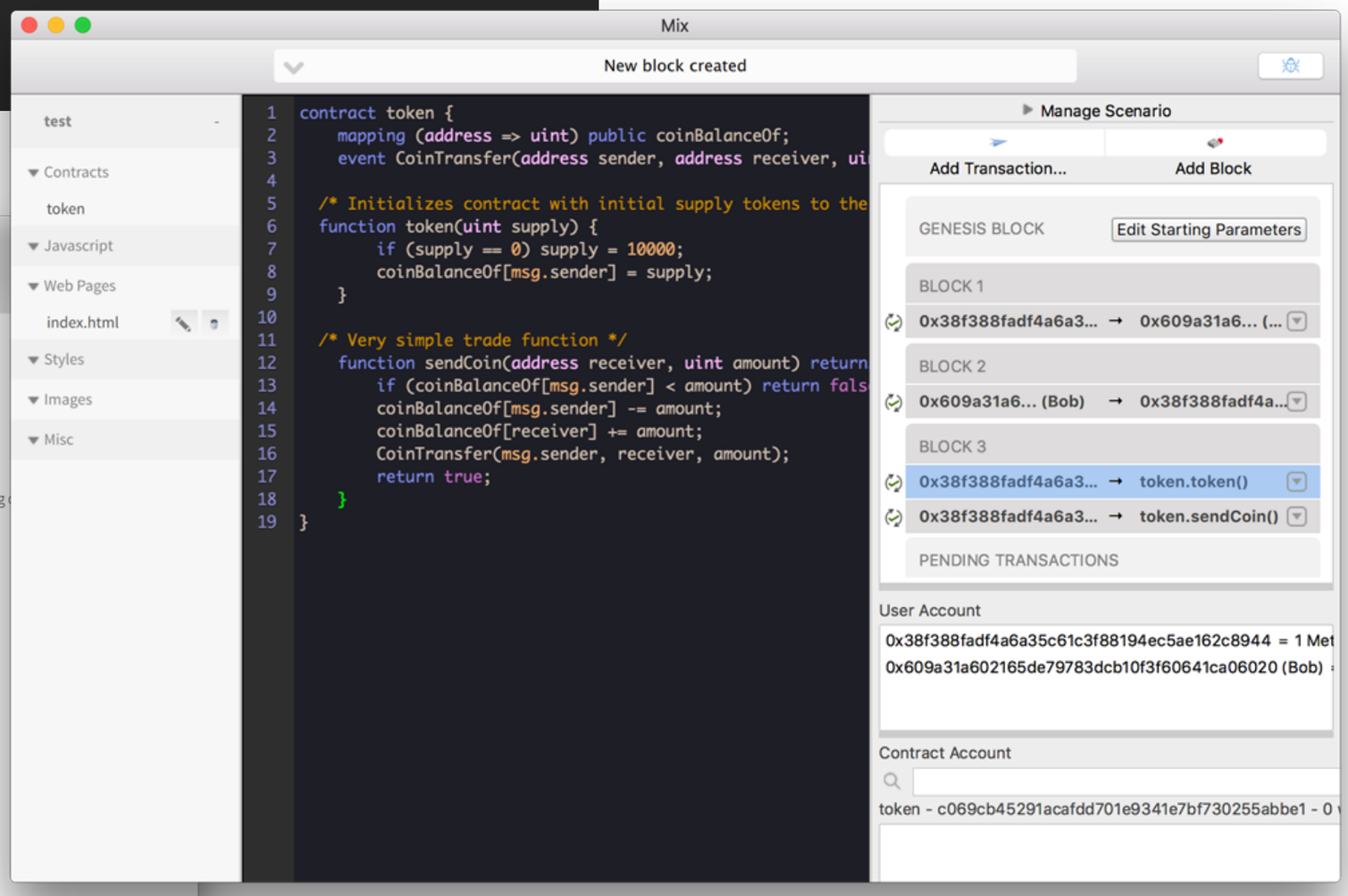
- Ethereum Virtual Machine implemented in 7 languages!
  - Python, Java, C++, Haskell, Go, JavaScript, Rust
  - Partial support: .NET, Ruby
- JSON-RPC
  - Tranport agnostic (HTTP, IPC, …)
  - Suited for automated processes
- web3.js JavaScript library
  - Use JavaScript to interact with the blockchain DApp
  - No complicated crypto maths!

Console: Geth

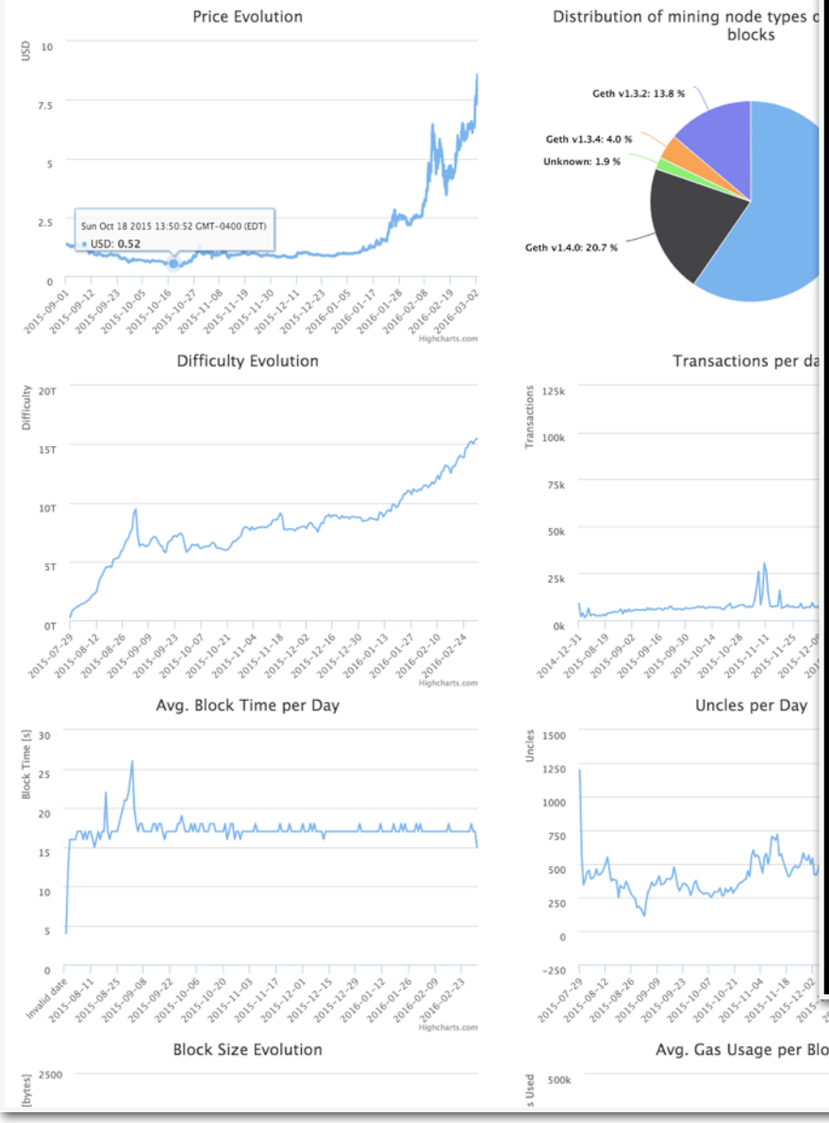
```
> listProposal(42)
Proposal #42 Send 100 ether to “Bob” for “Website Design”. 4 votes for, 2 against, 6 hours remaining.
> MyVote = Against
> MyOwnDemocracy.vote.sendTransaction(42, MyVote, {from: me}) |
```

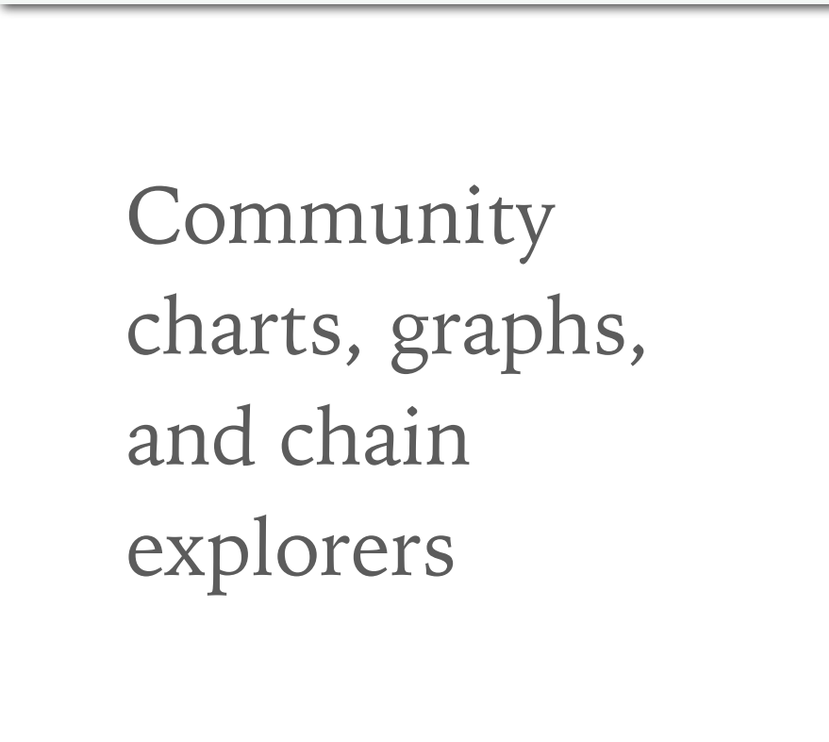
- Geth Console
- Mix IDE
- Mist GUI

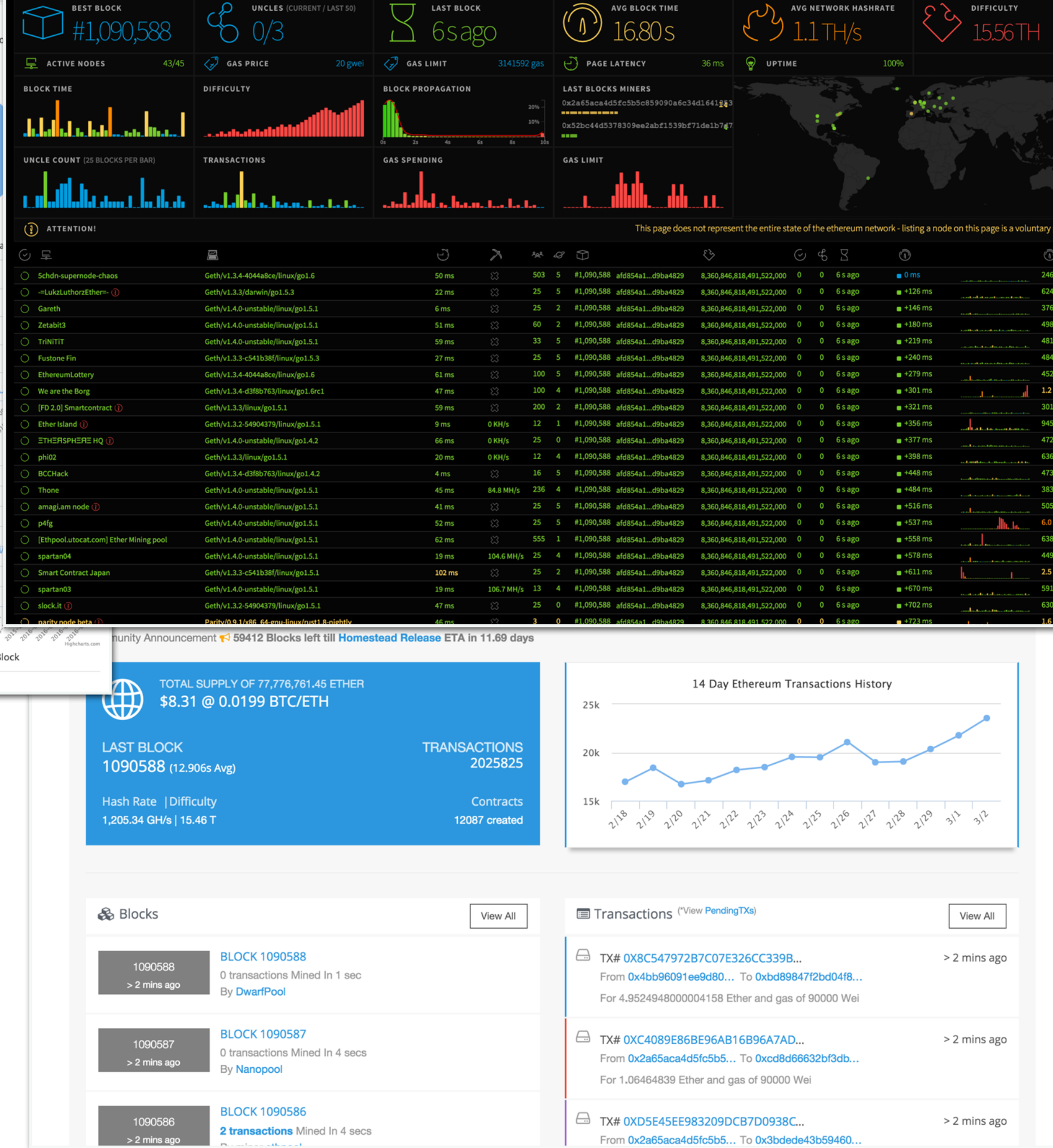




Basic Statistics







Community charts, graphs, and chain explorers

STATE OF THE ĐAPPS

Search

m
H in/ETH out
2016-03-02

Etheroll
James Britt
Ether dice game casino / gamble ether
proprietary
Live 2016-03-02

Syng
Jarrad Hope
open source mobile ethereum client
GPL
Working Prototype 2016-02-26

EthereumWall
LPMitchell
Decentralized unmoderated public message board
Live 2016-02-25

LΞTH
Inzhoop
LΞTH is the first hybrid mobile app to manage an Ethereum wallet
GPL
Working Prototype 2016-02-25

A smart co
Stealth Mod

reum
2016-02-18

EtherDoubler
Satoshi :)
The first doubler with verified contract
Live 2016-02-17

Solether
Francesco 'makevoid' + KristinaB
Autonomous Electrical Energy Entities - Prototype +EntityConcept
Unlicense
Working Prototype 2016-02-17

EtherAPIs
Péter Szilágyi & Jeffrey Wilcke
Micropayment platform for generic API calls
GPL
Working Prototype 2016-02-16

btcrelay
Joseph Chow
A bridge between the Bitcoin blockchain & Ethereum smart contracts
MIT
Working Prototype 2016-02-15

Ethere
Verifiable o
Working Pro

2016-02-15

Icebox
Christian Lundkvist
A cold storage solution for Ether
MIT
Live 2016-02-11

KingOfTheEtherThrone
Kieran Elby
Will make you a King or Queen, might grant you riches, and will immortalize your name.
proprietary
Working Prototype 2016-02-06

Dactuary
Vignesh Sundaresan
Decentralized actuary built on Ethereum
Concept 2016-02-04

insurETH
Thomas Bertani, Kristina Butkute, Francesco Canessa
P2P flight insurance
Apache
Work in Progress 2016-01-21

Ventu
Ry
Decentrali
Stealth Mod

dresses via
2016-01-05

dappsys
Nexus Dev
Solidity Contract System Framework
MIT
Working Prototype 2016-01-02

Dapple
Nexus Dev
smart contract package manager and build tool
MIT
Live 2016-01-02

Maker / Dai
Maker
Stable Cryptocurrency
MIT
Work In Progress 2016-01-02

KYC-chain
Edmund John
Proof of KYC Requirements
Concept 2015-12-27

Decentralize
Working Pro

Decentralized Twitter
etherforum
ethID
4G Capital Smart Contra

I CAN HAZ?

- ethereum.org
- ethereum.stackexchange.com
- reddit.com/r/ethereum
- ethstats.net
- etherchain.org
- etherscan.io

ETHEREUM

TAYLOR GERRING

DIRECTOR OF TECHNOLOGY
ETHEREUM FOUNDATION

@TaylorGerring

github.com/tgerring

blockchainconsulting.expert