Ethereum: Past, Present, & Future

Blockchain Roadmap

Zurich Meetup: 2016.04.19

How we got here…

A look at Bitcoin's past

- Slow development of core protocol (for good reason)
- Sidechains promoted as extensibility / testing ground
- Wallet UI / UX stalled by protocol limitations
- Forming consensus around proposals difficult
- Ivory-tower design & architecture

Stumbling blocks

- Dark Wallet event in Milan late 2013
  - Multiple wallets represented: Qt, libbitcoin, Hive, Electrum
  - Goal: Improve user experience & privacy
  - Result:
    - github.com/darkwallet/dat.wallet (universal “unwallet”)
    - Plans for ecosystem improvement (coin mixing, etc)
    - ???

Dec 2013

Vitalik's response…

Ethereum

- Generalized blockchain
- Turing-complete (support any conceivable operation)
- Account-based instead of UTXO-based
- Most protocols designed from the ground-up
- White paper released in December 2013
- Public announcement January 2014 in Miami, FL, USA

Jan 2014


ethereum.org
hive
NO, I WILL NOT
SETUP YOUR
BITCOIN
WALLET.
ethereum.org
ethereum.org

Jan 2014

Ethereum!!!1!!1one!!

Roadmap (past)

- Proof of Concept series
  - Released throughout 2013-2015
  - Roughed-out concepts
- Olympic testnet
  - PoC 10 (“X”)
  - Activated 2015.03.09

Nov 2014

Roadmap (present)

- Frontier
  - Main public network
  - “Beta” / use at your own risk
  - Activated 2015.07.30 (~4.5 months after Olympic)
- Homestead
  - Public network considered “stable”
  - Integrate critical protocol changes discussed at Devcon1
  - Activated 2016.03.14 (~7.5 months after Frontier)

Roadmap (future)

- Metropolis
  - Improved GUI experience (Dapp browser + IDE)
    - Release TBD
- Serenity
  - Scalability & beyond
  - Release TBD

State of the community

Nov 2015

Right now

- 8+ months public network
- Dapps (~200 on dapps.ethercasts.com)
- Transactions (~0.40 TPS)
- Node count (~5000 nodes)
- Accounts (150,000+)
- Over 200 meetups with 40,000 people (and growing!)

Immediate future

- Pending Geth 1.4.0 feature update
  - Push RPC!
- Incremental Ethereum Wallet/Mist improvements
  - Fast sync/light-client
- Expanded builds
  - Arm, Android, iOS, etc.

On the horizon

Protocol improvements

- EIP 101: Condense 2 types of accounts into 1
  - Externally-owned (“human”)
  - Contracts
- Origin address of 0x0^40 ?
- Security mechanisms move into EVM

Client improvements

- LES (light client)
- State tree pruning (light client)
- Natspec (natural language prompts)
- Swarm (storage) & Whisper (messaging)
- Dev tools
  - Mix IDE
  - Formal verification
  - Compiler improvements


ethereum
HOMESTEAD RELEASE
BLOCKCHAIN APP PLATFORM
「以太坊爱好者」线下活动
以太坊官网: https://ethereum.org
以太坊爱好者: https://ethfans.org
主办方：ethfans 以太坊爱好者社区
协办方：万向区块链实验室 区块铅笔

Opportunities

Privacy

- Now: None (use externals tools like PGP)
- Eventually: Zero-knowledge proofs
- Maybe: Homomorphic cryptography
- ???

Efficiency

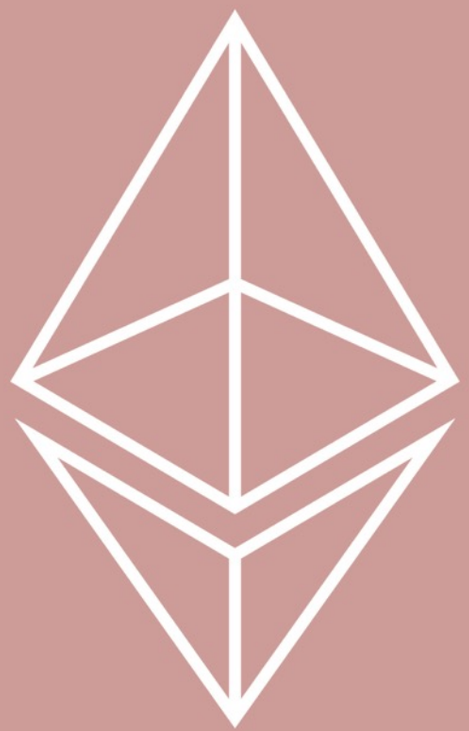
- Decrease block times
  - 600 sec → 15 sec → ???
- Improve Merkle tree structures
- Consensus switch
  - PoW to PoS (less wasteful energy expenditure)

Scalability

- Lightning network/State channels (i.e. Raiden)
- Sharding (Ethereum 2.0)
- Casper / Proof-of-Stake
  - Virtual Mining
  - Consensus by bet

Proof-of-Agility

- Phase 1
  - PoS votes on state roots only. Parallel with PoW. Delay "ice age"
  - EIP 101 (Changes to state tree), EIP 105 (Scalability)
- Phase 2
  - PoS voting on block hashes. PoW continues as "bivalence breaker"
  - Deprecate old-style transactions, introduce precompile opcodes
  - Ethereum 2.0 (Basic sharding)
- Phase 3
  - Discontinue PoW/pure PoS
  - Ethereum 3.0 (infinite sharding)



devcon two

Ethereum Developer Conference, September 19th - 24th, Shanghai, China

Shanghai International Blockchain Week

Taylor Gerring

Director of Technology
Ethereum Foundation