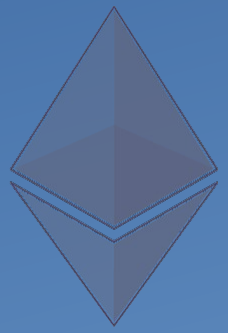
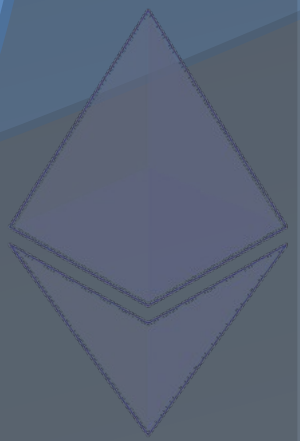
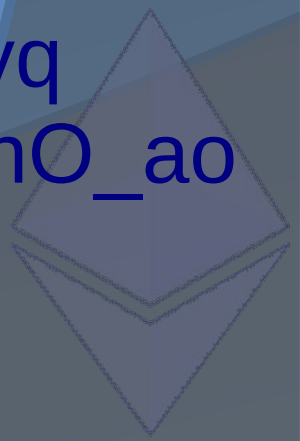
5th Ethereum Meetup



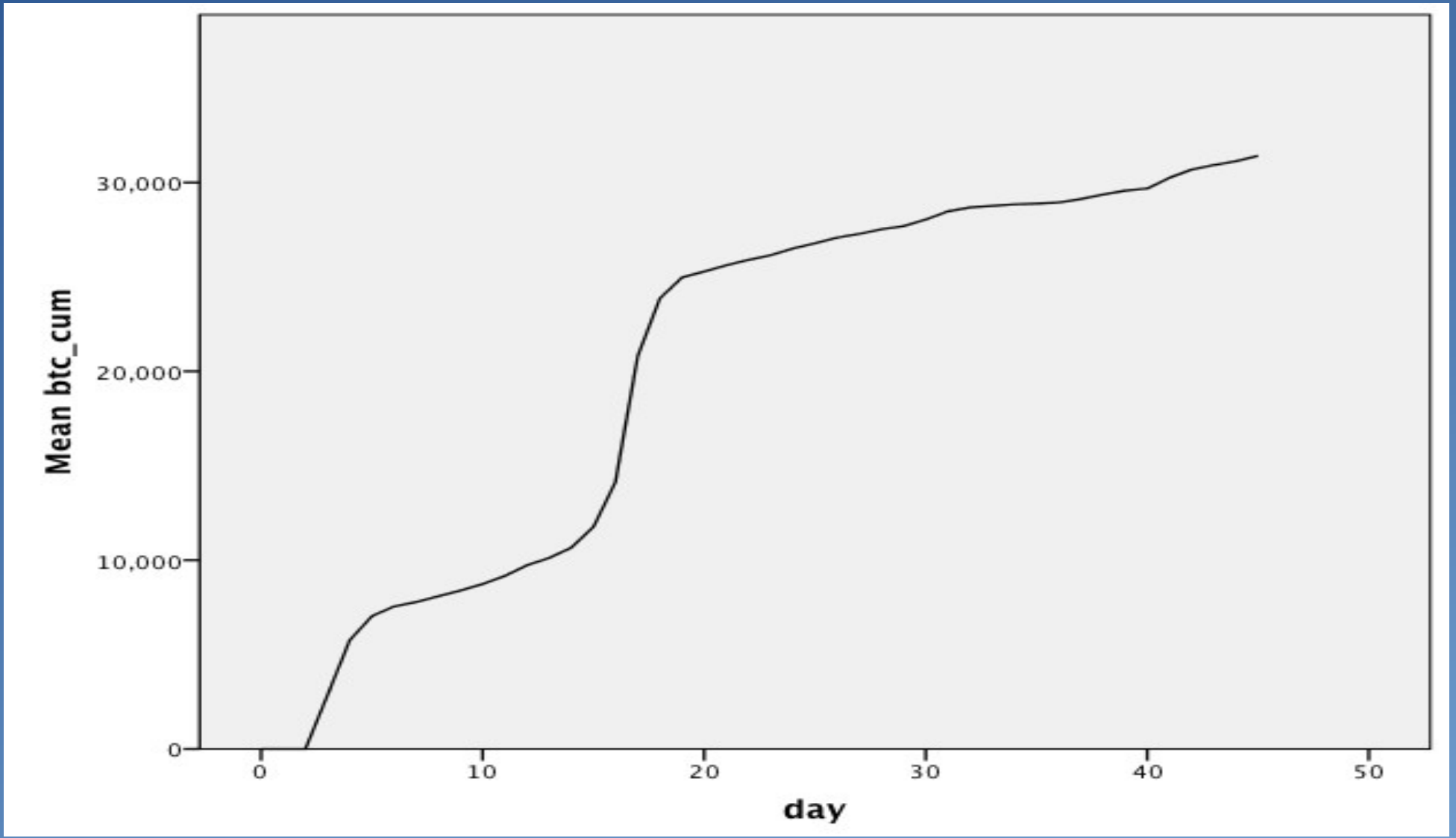


Ether Sale

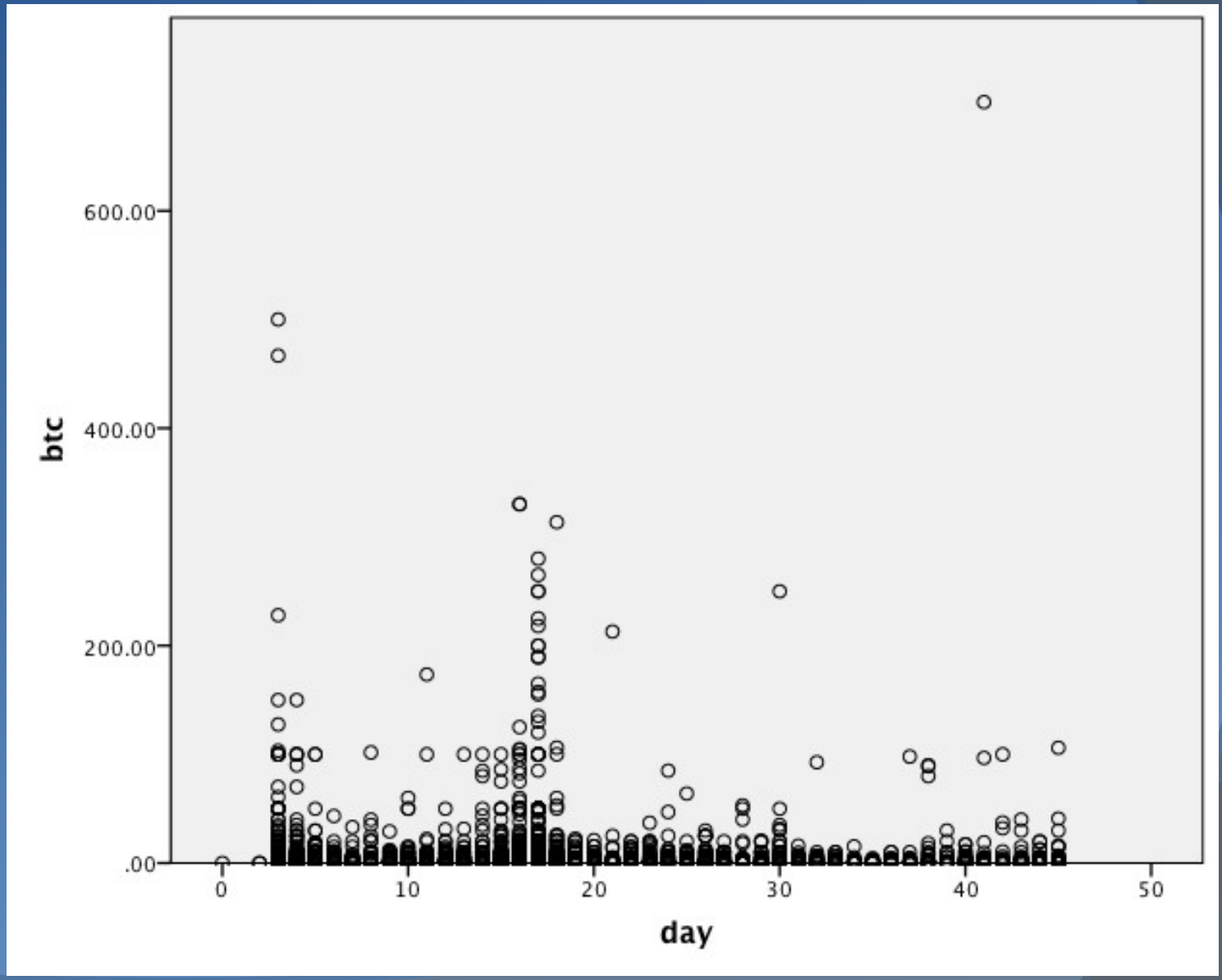
- 60,102,216 ETH
- 31,529 BTC (~12.5m USD) @ 400 BTCUSD
- Over 9000 transactions
- 2nd biggest crowdfunder
- 36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2
- Public expenses: https://docs.google.com/spreadsheets/d/1yqymLKNf9tIbArjYrKhEf-IvNmgA6FfvhjnqH_nO_ao



Ether Sale

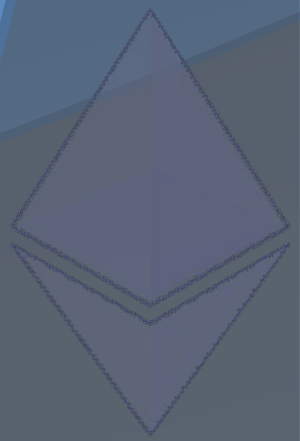


Ether Sale



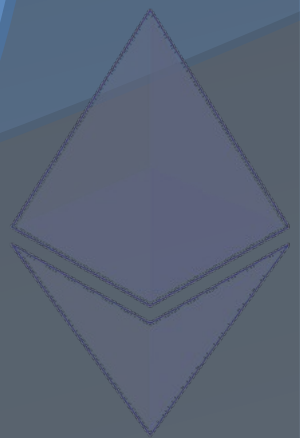
libp2p – a generic P2P protocol

- Same peer network for multiple decentralized protocols
- Automatic negotiation of message id ranges
- No centralized authority in charge of supported protocols



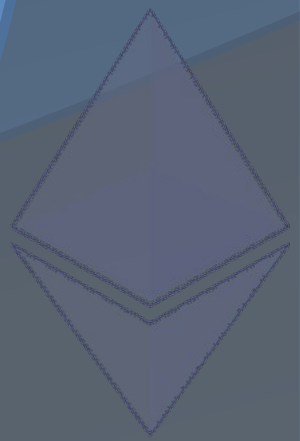
Swarm & Whisper

- Whisper built on top of libp2p
- Whisper – “shh”
- Swarm – “bzz” (probably canceled)
- Basic info at https://github.com/ethereum/cpp-ethereum/wiki (outdated)



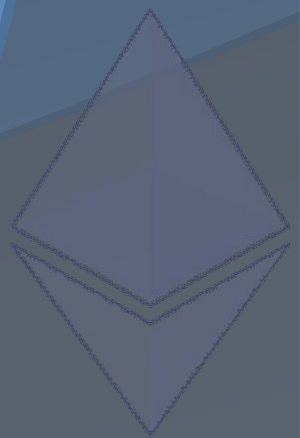
Whisper

- Currently in early stage of development (C++ client tree)
- Should become usable before poc7



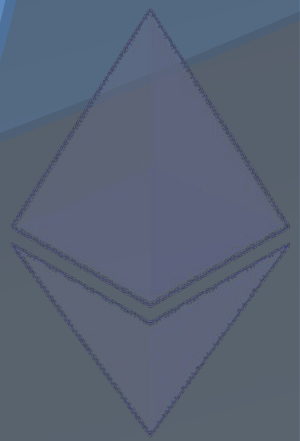
Contract ABI

- Contracts as Objects Paradigm
- New Language – Solidity
  - Static typing
  - Contract as “objects”
  - Invariants
- Strongly typed
- 1 byte method id



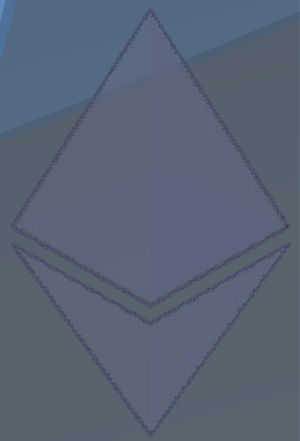
Solidity

- contract Foo
- {
- function sam(string32 in1) { ... }
- function bar(uint256 in1, string in2) returns (string out1, bool out2) { ... }
- function baz(uint32 in1, real in2) returns bool { ... }
-
- state:
- uint256 tom;
- }
-



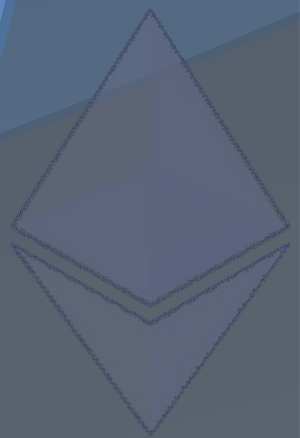
Contract ABI “Header”

```
[
  { "name": "send", "input": [ { "name": "to", "type":
"address" }, { "name": "valueInmGAV", "type":
"uint256" } ], "output": [] },
  { "name": "balance", "input": [ { "name": "who",
"type": "address" } ], "output": [ { "name":
"balanceInmGAV", "type": "uint256" } ] }
]
```



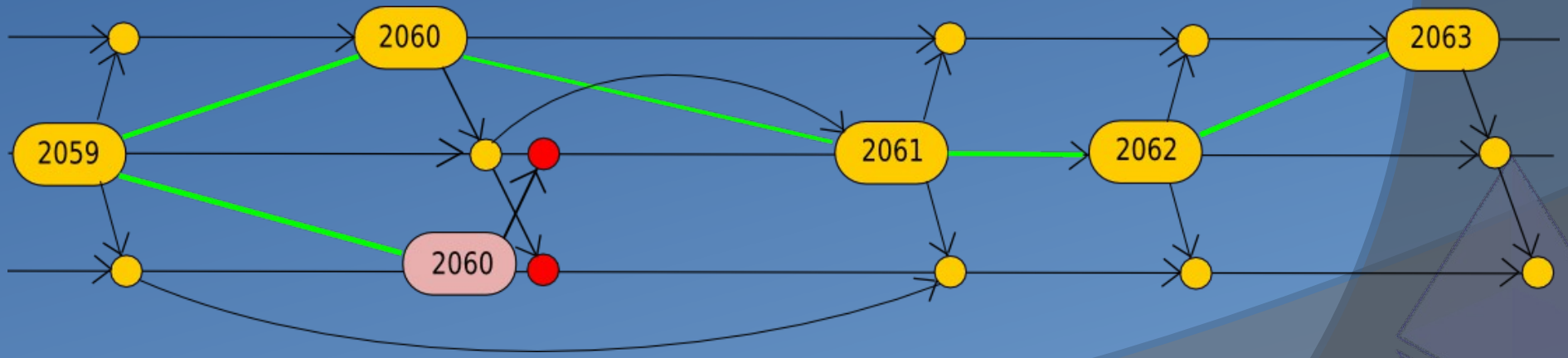
Blockchain

- Micro Chains (probably won't happen)
  - Small chain used for mining
  - Contains references to subchains
  - One consensus system for multiple chains



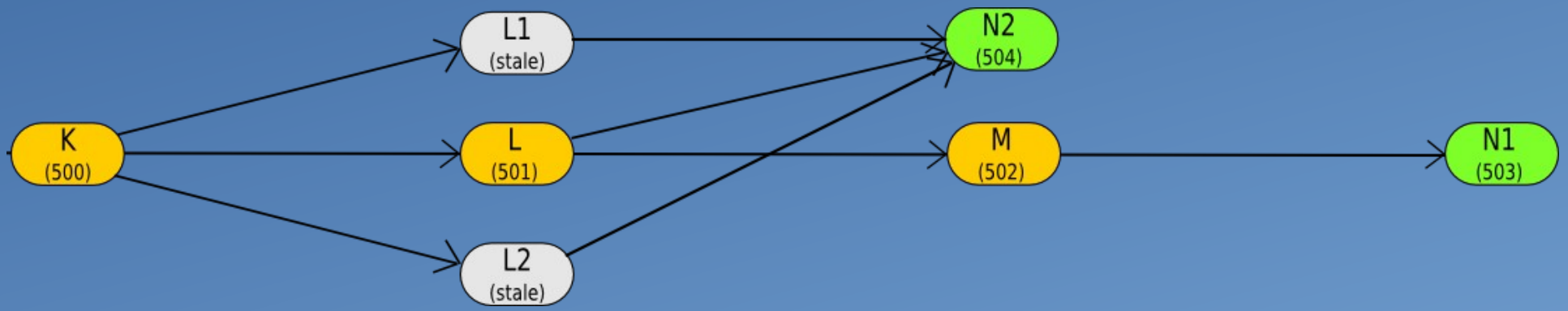
Blockchain

- Block Time:
  - Testnet: 6s
  - Release (planned): 12s
  - Lower stale rate through adapted GHOST-Protocol



Blockchain GHOST

- Uncle:
  - Child of parent of parent
  - Can be included into a block to increase score
  - Reduced reward for uncle, increased reward for real block

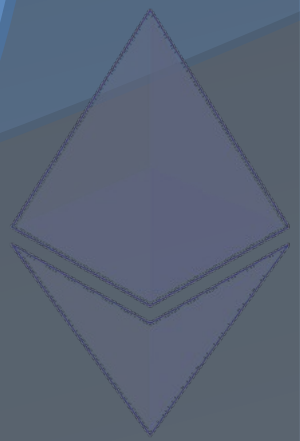


Blockchain Adapted GHOST

- Uncle:
  - Child of an (non-parent) ancestor up to a certain depth

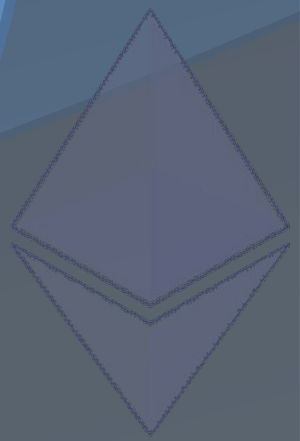
Blockchain Stuff

- Hybrid PoW / PoS
  - Slasher with exponential subjective scoring
  - Blocks contain both PoS Signatures and PoW
  - Signers for PoS determined 1000s of blocks in advance (by PoW)
  - NaS-Attacks can be punished via evidence
  - LRNaS-Attacks stopped by ESS



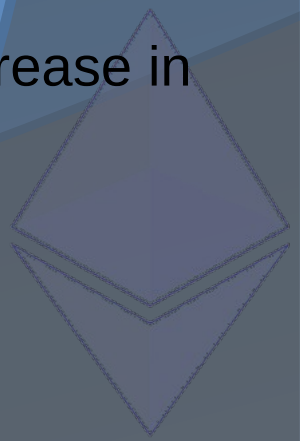
Ecosystem

- Default contracts
  - Namereg: associates an address with a name
  - MetaCoin: standard interface for subcurrencies
  - Coins: registers MetaCoins
  - Exchange: standard interface for a MetaCoin Exchange



Other Developments

- Native extensions
  - Native code for certain contracts in clients
  - Sender uses lower gasprice
- Micropayments (Idea)
  - Payer opens a channel with a recipient and id
  - Payer regularly sends a signed message containing id and an increasing value
  - Recipient send signed message to the contract
  - Contract pays out after a certain number of blocks after the increase in value

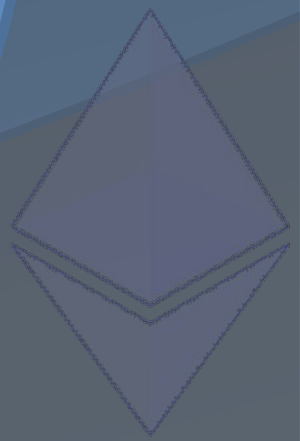


Other Developments

- Offchain Oracles (Idea)
  - Calculate state offchain
  - Have security deposit
  - Users can make auditing transaction
  - Gets reward if Oracle cheats

Adept

- Ethereum Fork by IBM
- Uses Telehash instead of Whisper
- Uses bittorrent instead of Swarm
- Intended for IoT



github.com/dafcok/ethereum