Introduction to Blockchain

Lecture 3: From Bitcoin to Ethereum

Ras Dwivedi

Indian Institute of Technology Kanpur

May 22, 2018

Outline

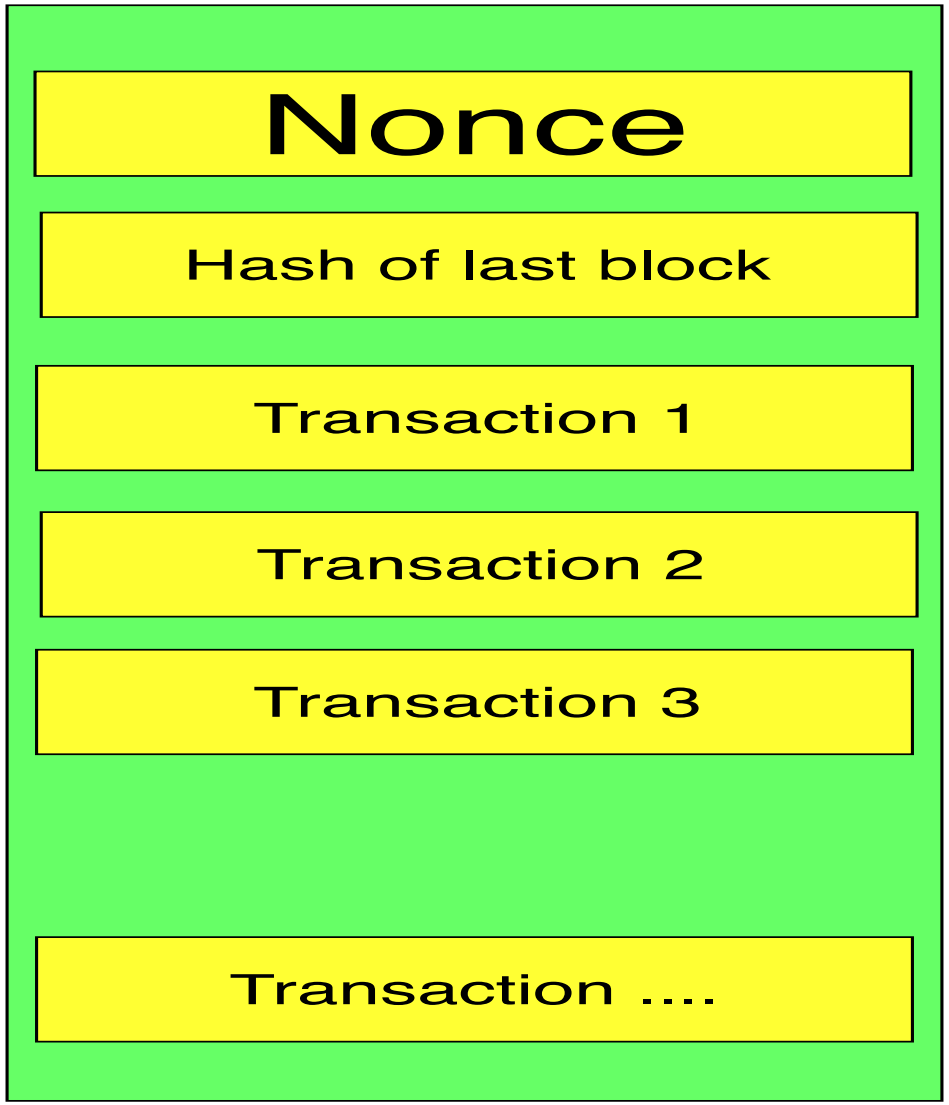
A Decentralized Ledger

Transactions

Transaction 4

Input: Trans 3, output 1	**Send:** 2 bitcoins
Signed: [Signature D]	**To:** [Public Key E]
	Send: 0.5 bitcoins
	To: [Public Key F]

Block


Nonce
Hash of last block
Transaction 1
Transaction 2
Transaction 3
Transaction ....

Proof of work

Mining rewards

Longest chain

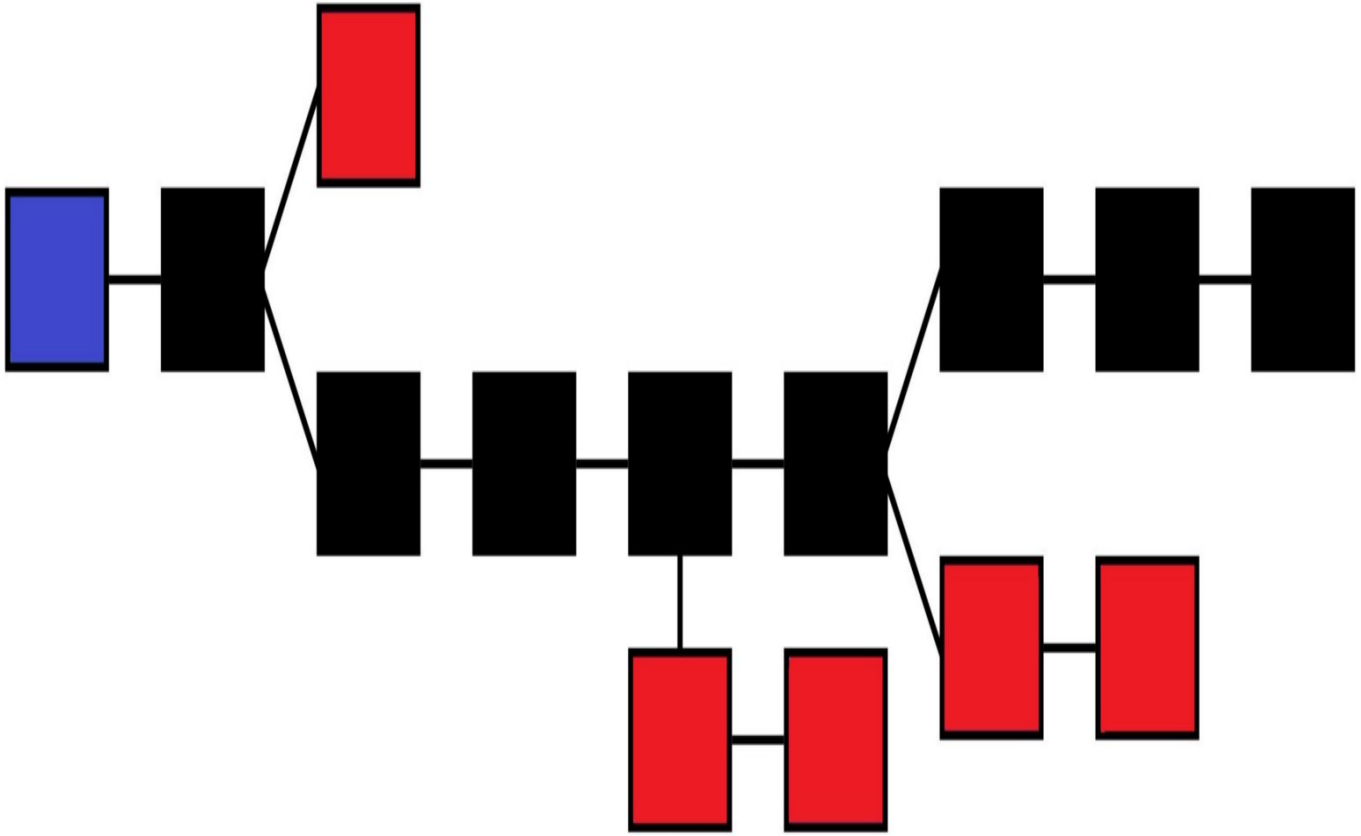


Figure: Blockchain

Bitcoin: Advantages

- Secure:
- transparency
- no counterpart risk
- decentralized
- Privacy
- low transaction cost

Bitcoing is Awesome! But...

- Block creation time is very high 10 mins/block

Bitcoing is Awesome! But...

- Block creation time is very high 10 mins/block
- Block confirmation time is very high 60 mins/block

Bitcoing is Awesome! But...

- Block creation time is very high 10 mins/block
- Block confirmation time is very high 60 mins/block
- can only do one function: Cryptocurrency

Bitcoing is Awesome! But...

- Block creation time is very high 10 mins/block
- Block confirmation time is very high 60 mins/block
- can only do one function: Cryptocurrency
- uses too much of energy: by 2020 electricity equivalent to entire Denmark
- Enters...

Introducing Ethereum

A planetary scale computer build on blockchain technology

permision-less

Turing complete language

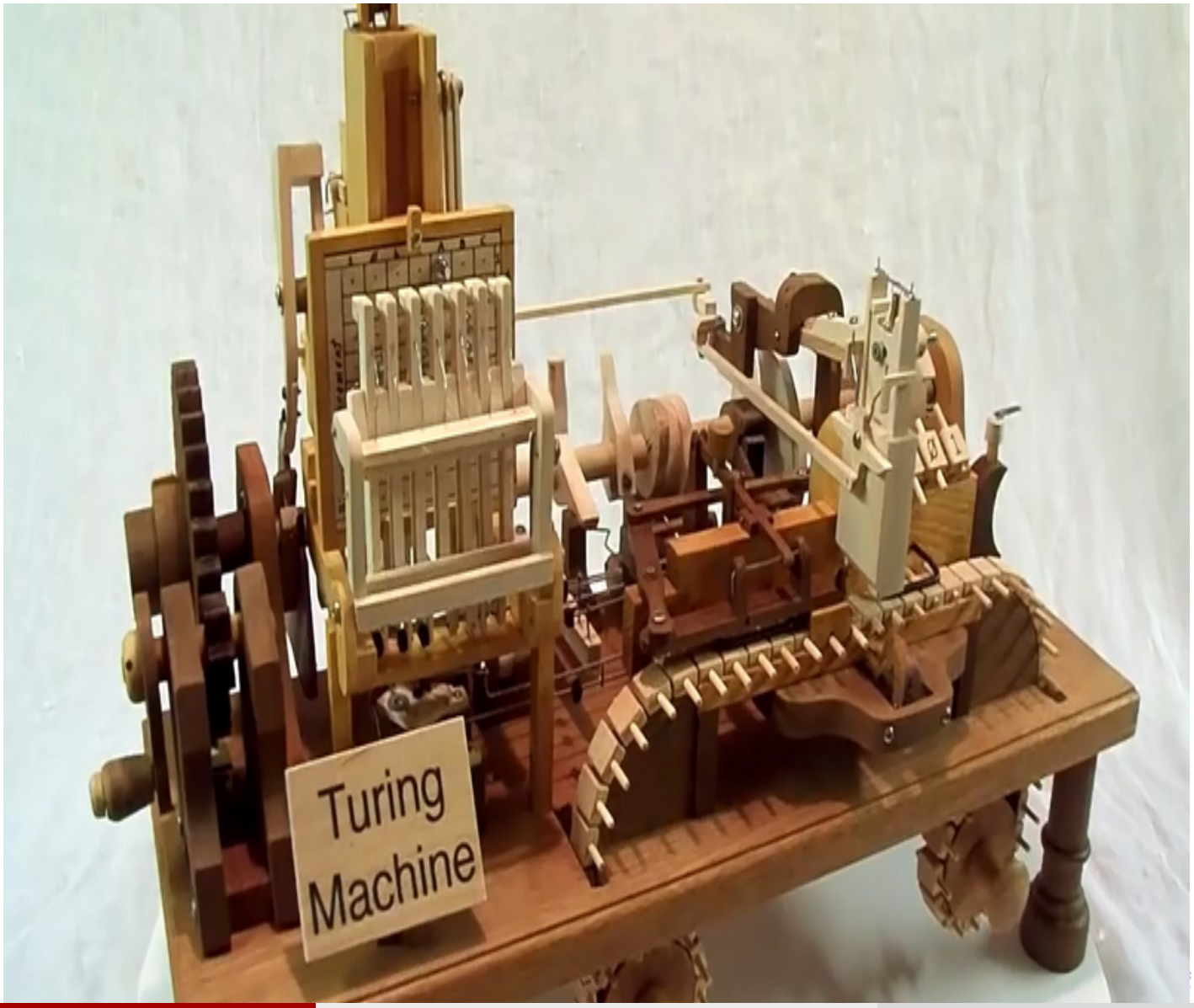
Introducing Ethereum

A planetary scale computer build on blockchain technology

permision-less

Turing complete language

Turing Machine



Introducing Ethereum

A planetary scale computer build on blockchain technology

permision-less

Turing complete language

Introducing Ethereum

A planetary scale computer build on blockchain technology

permision-less

Turing complete language

Begins the era of Decentralized app

Introducing Ethereum

A planetary scale computer build on blockchain technology

permision-less

Turing complete language

Begins the era of Decentralized app : Program that can run without failure, without any downtime, censorship, fraud or third party inference

EVM: Ethereum Virtual Machine

Ethereum Blockchain is

Blockchain with built in programming languagedecentralized massive database, where the current state of every account is stored EVM handles internal state and computationComputation is paid in Ether, per computation stepeach account object have:

- Its own internal state
- have 32 byte key/value called storage
- Can call or send messages to other node

Bitcoin vs Ethereum

Bitcoin

Ethereum

Figure: Bitcoin Vs Ethereum

Basics of Ethereum

- **Ether**: the underlying cryptocurrency of Ethereum
- **Gas:** Gas is a basic unit of computation
- **Smart contract:**
  - Pre-written logic (code)

Basics of Ethereum

- **Ether**: the underlying cryptocurrency of Ethereum
- **Gas:** Gas is a basic unit of computation
- **Smart contract:**
  - Pre-written logic (code)
  - stored and replicated on blockchain

Basics of Ethereum

- **Ether**: the underlying cryptocurrency of Ethereum
- **Gas:** Gas is a basic unit of computation
- **Smart contract:**
  - Pre-written logic (code)
  - stored and replicated on blockchain
  - self executing by running the code

Basics of Ethereum

- **Ether**: the underlying cryptocurrency of Ethereum
- **Gas:** Gas is a basic unit of computation
- **Smart contract:**
  - Pre-written logic (code)
  - stored and replicated on blockchain
  - self executing by running the code
  - can update blockchain
  - can do transfer of assets,
  - run code to make payment

Account types

- Externally Owned Accounts
- Contract Accounts

Externally owned Accounts

- Has ether Balance

Externally owned Accounts

- Has ether Balance
- Can send transactions

Externally owned Accounts

- Has ether Balance
- Can send transactions (Ether transfer or trigger Contract code)
- Is controlled by private keys
- has no associated code

Contract Accounts

- Has associated Ether balance
- Has associated code
- code execution is triggered by transaction or messages received from other accounts
- can execute code of arbitrary complexity (Turing Completeness) and manipulate data in blockchain

Transaction

Contains:

- receipt of the message
- signature
- Value: amount of wei to be transferred from sender to recipient
- option data field: which contains message to be send to recipient
- Startgas value:representing the maximum number of computational steps the transaction execution is allowed to take

Message

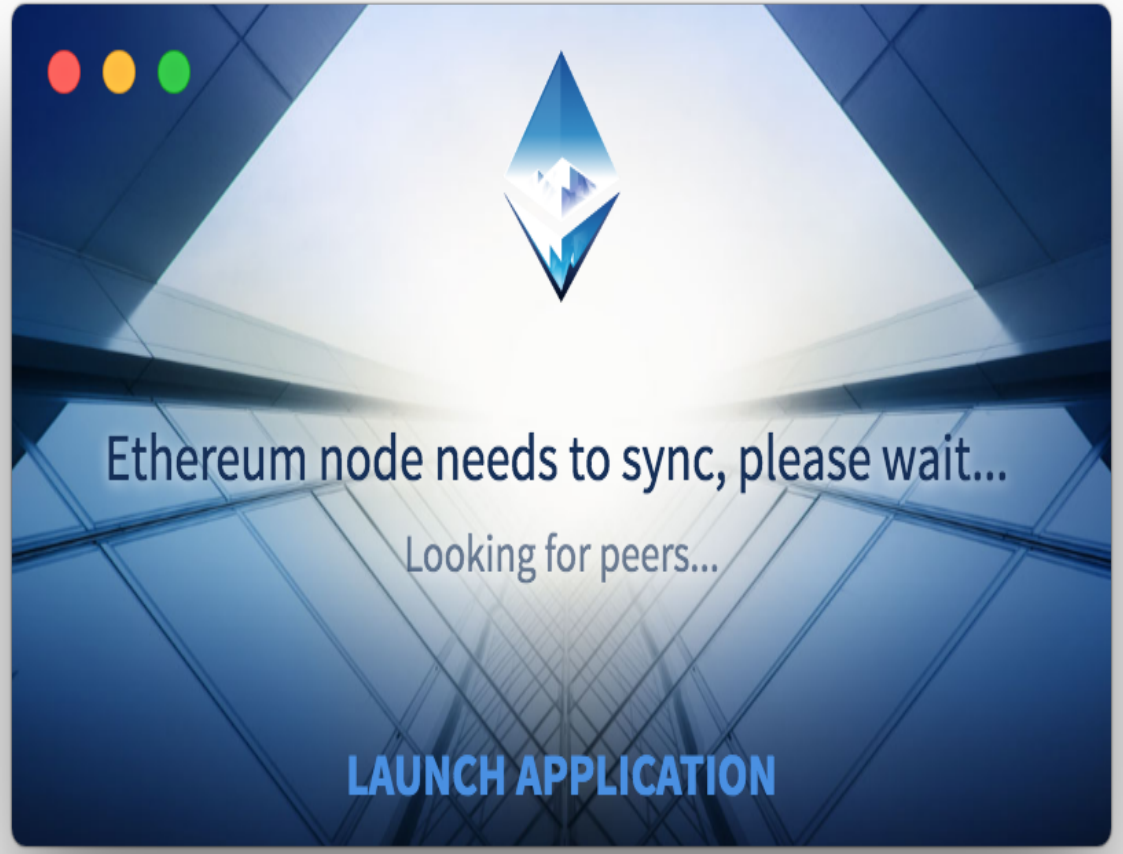
Mist

Mist: Introduction

Mist Ethereum wallet is a Desktop hybrid application which is both Ethereum node and client. Aim: to install mist and run a Faucet account

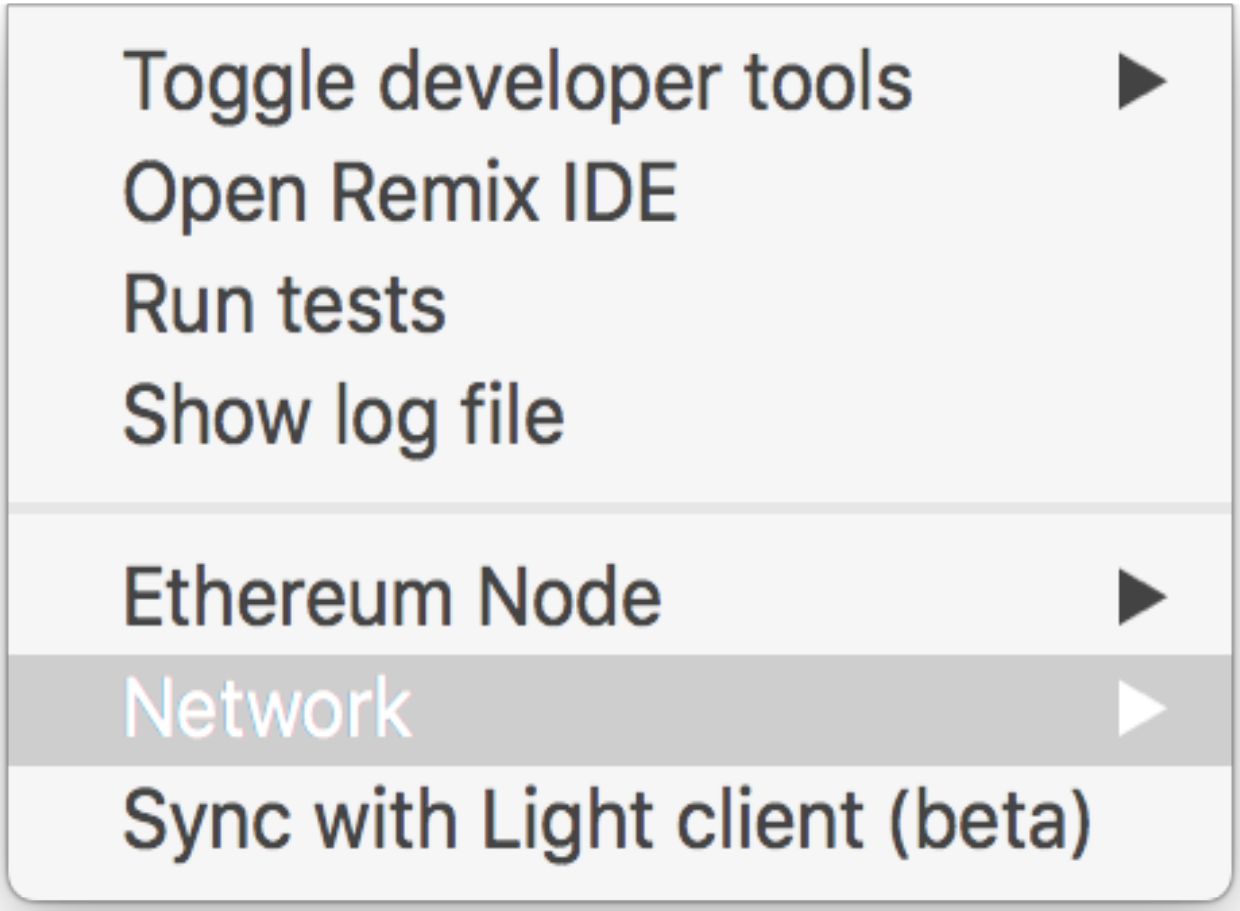
Discover Mist

Download, install and start mist. You should see the following



Mist

synchronization to the main net would take a lot of the time, so you should switch to the testnet



Mist

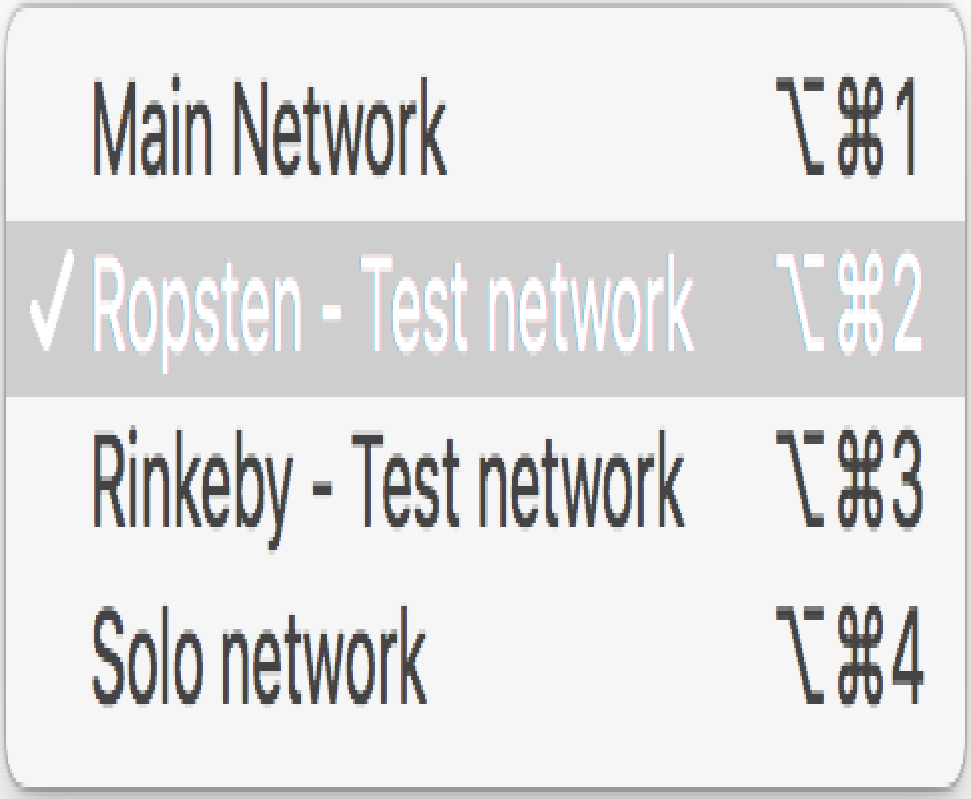
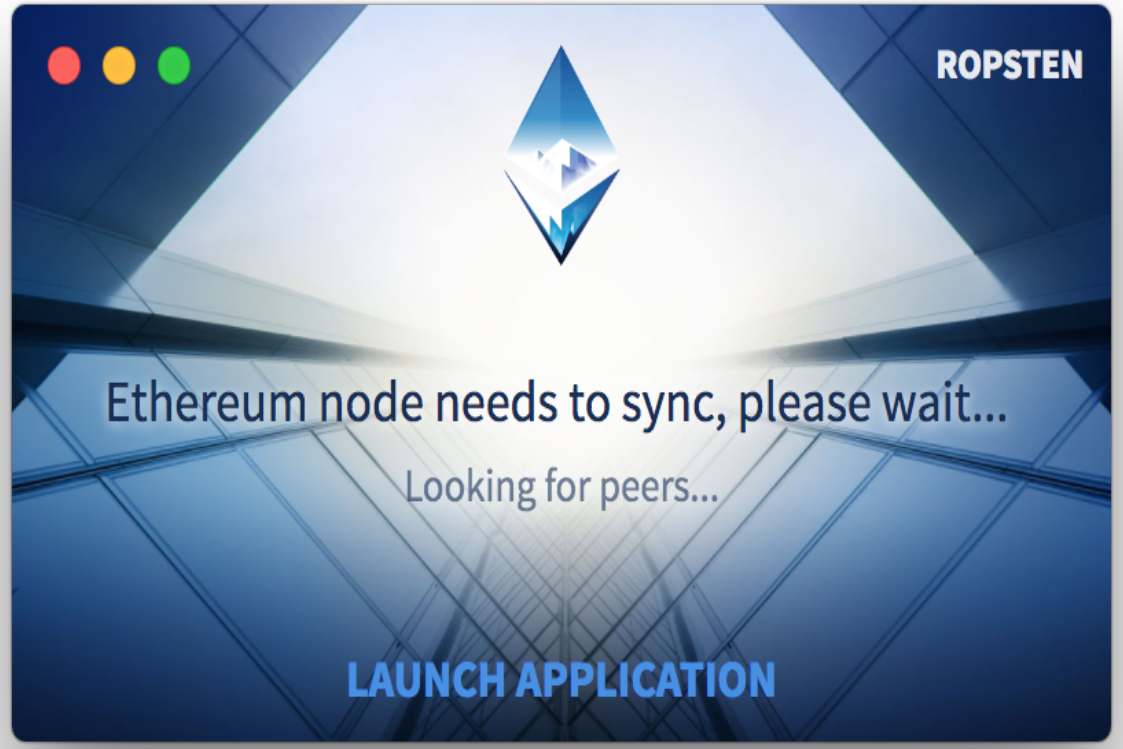


Figure: Caption

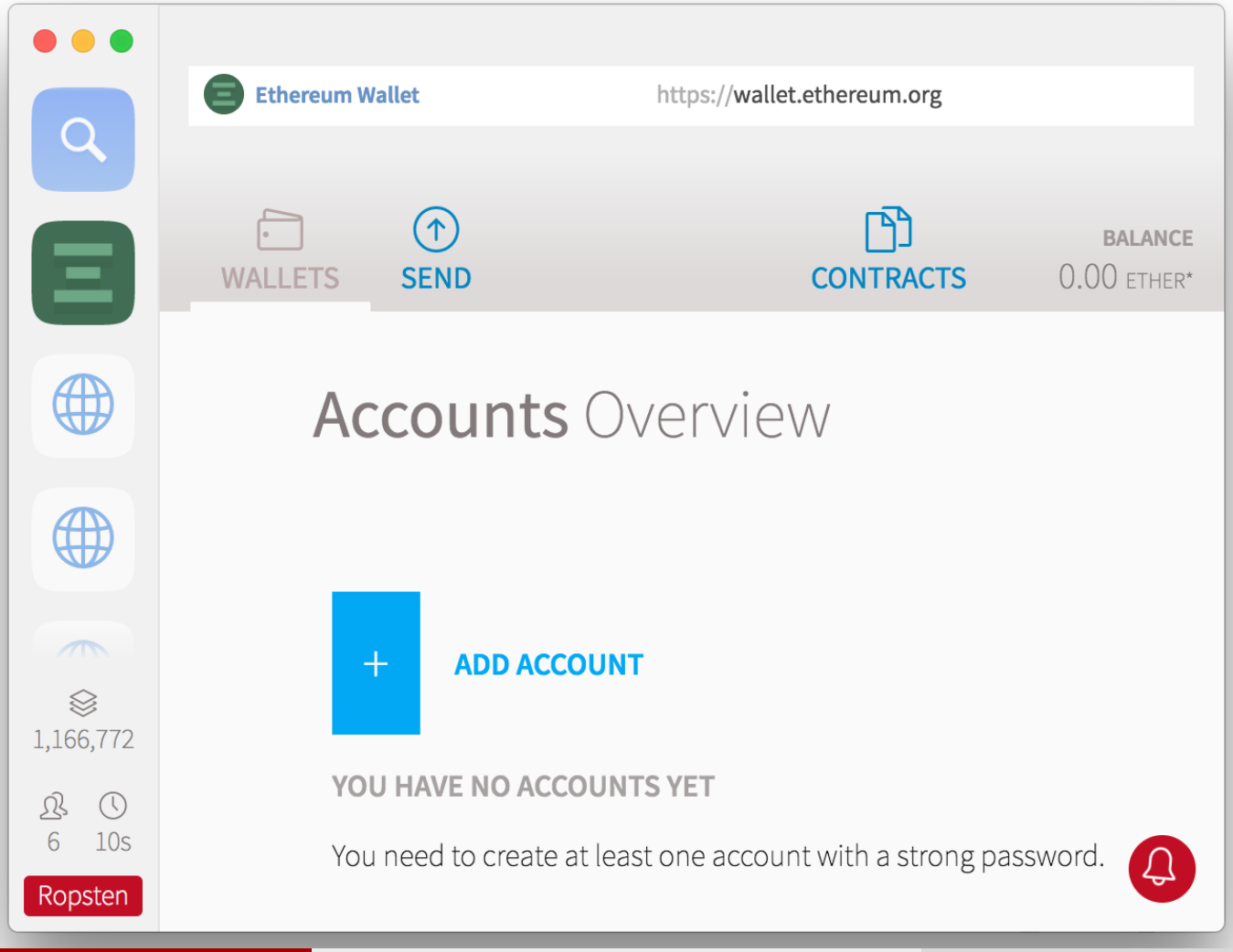
Mist

And then you'll see Mist syncing with test net



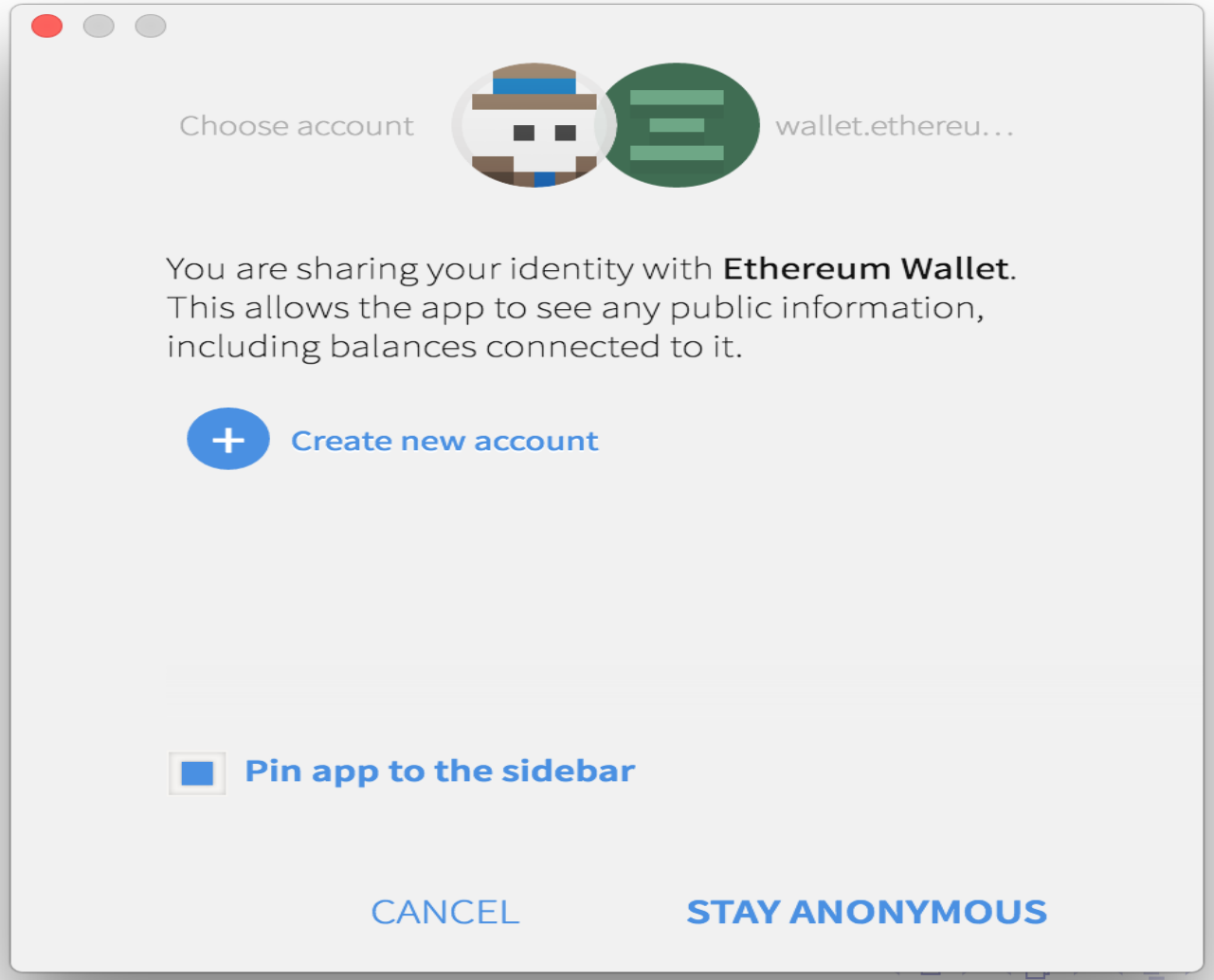
Mist

Lets click on launch application

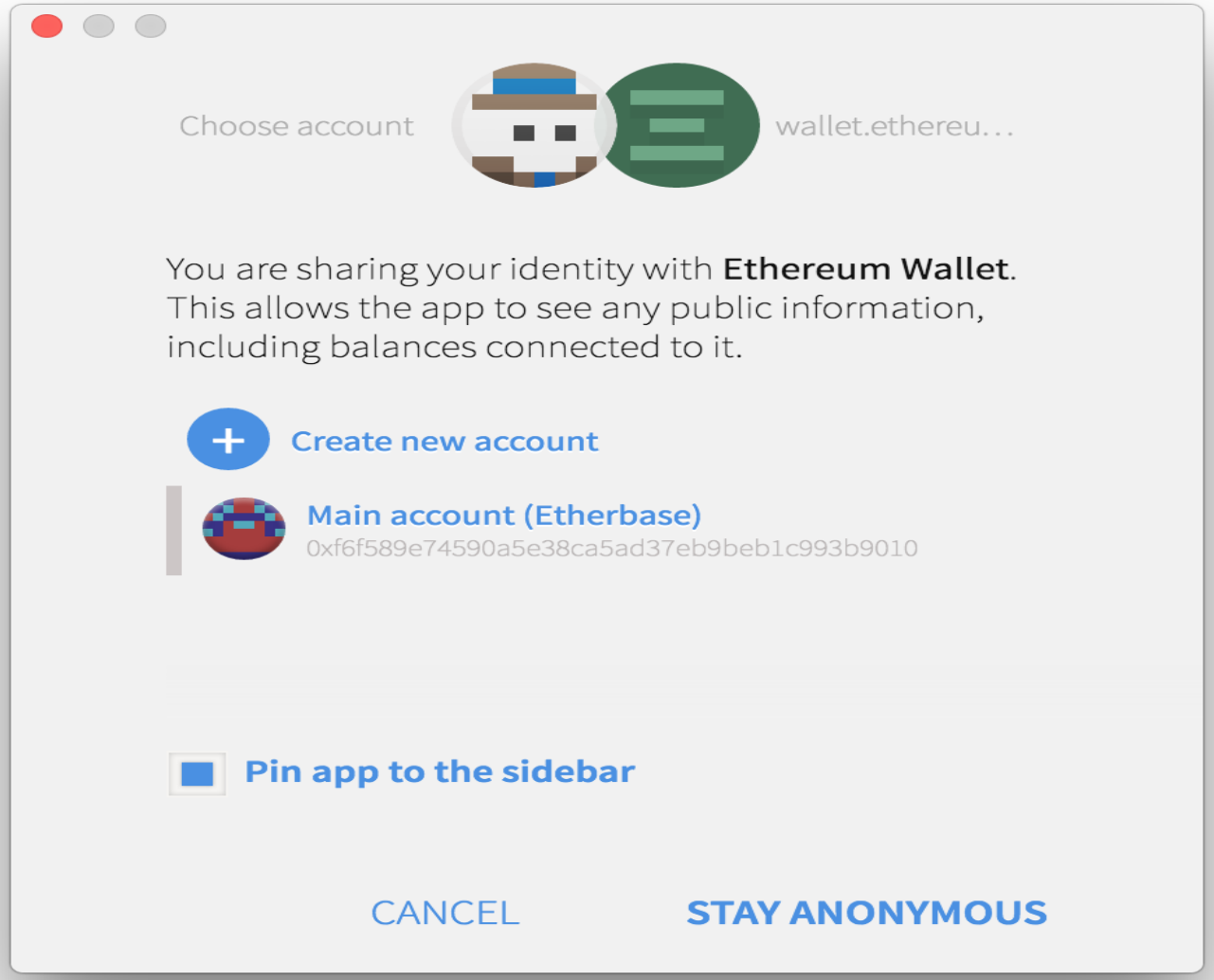


Mist

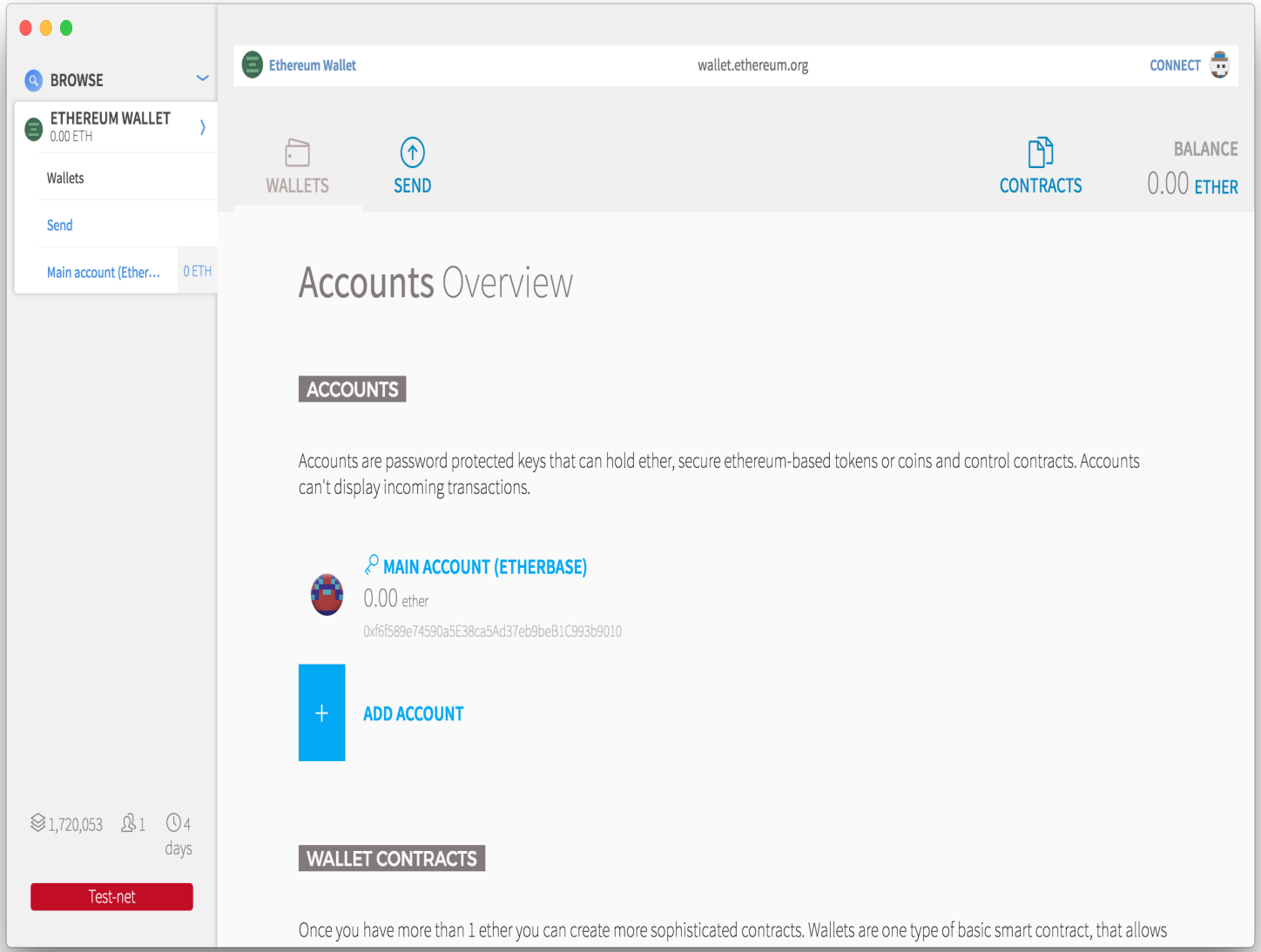
Create new account



Mist


Choose account
wallet.ethereu...
You are sharing your identity with **Ethereum Wallet**.
This allows the app to see any public information,
including balances connected to it.
Create new account
Main account (Etherbase)
0xf6f589e74590a5e38ca5ad37eb9beb1c993b9010
Pin app to the sidebar
CANCEL
STAY ANONYMOUS

Mist


BROWSE
ETHEREUM WALLET
0.00 ETH
Wallets
Send
Main account (Ether...
0 ETH
1,720,053
1
4 days
Test-net
Ethereum Wallet
wallet.ethereum.org
CONNECT
WALLETS
SEND
CONTRACTS
BALANCE
0.00 ETHER
Accounts Overview
ACCOUNTS
Accounts are password protected keys that can hold ether, secure ethereum-based tokens or coins and control contracts. Accounts can't display incoming transactions.
MAIN ACCOUNT (ETHERBASE)
0.00 ether
0xf6f589e74590a5E38ca5Ad37eb9beB1C993b9010
ADD ACCOUNT
WALLET CONTRACTS
Once you have more than 1 ether you can create more sophisticated contracts. Wallets are one type of basic smart contract, that allows

Bibliography