ethereum

vienna

11th Meetup

DEVCON-1 and UI Wallet

ethereum

Agenda

Introduction

DEVCON-1 recap

UI Wallet

Other

Let’s talk Bitcoin : Ether Review

ethereum

vienna

DEVCON-1 Recap

ethereum DEVCON-1

First open conference for developers

London Nov 9th - 13th

>30 h of content

Days 2-5 on youtube

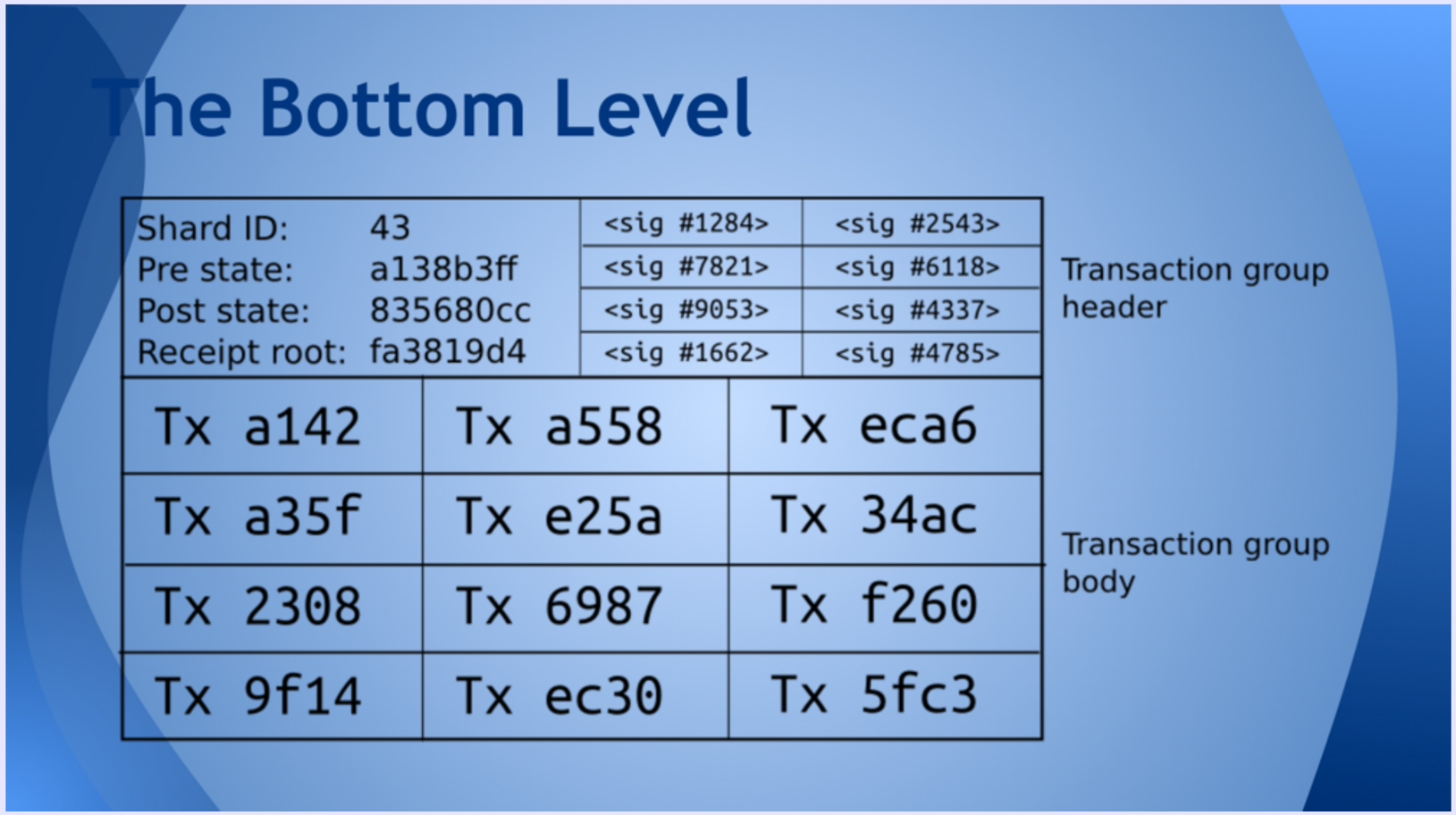
Day 1 to follow

ethereum Scalability

Scalability through sharding

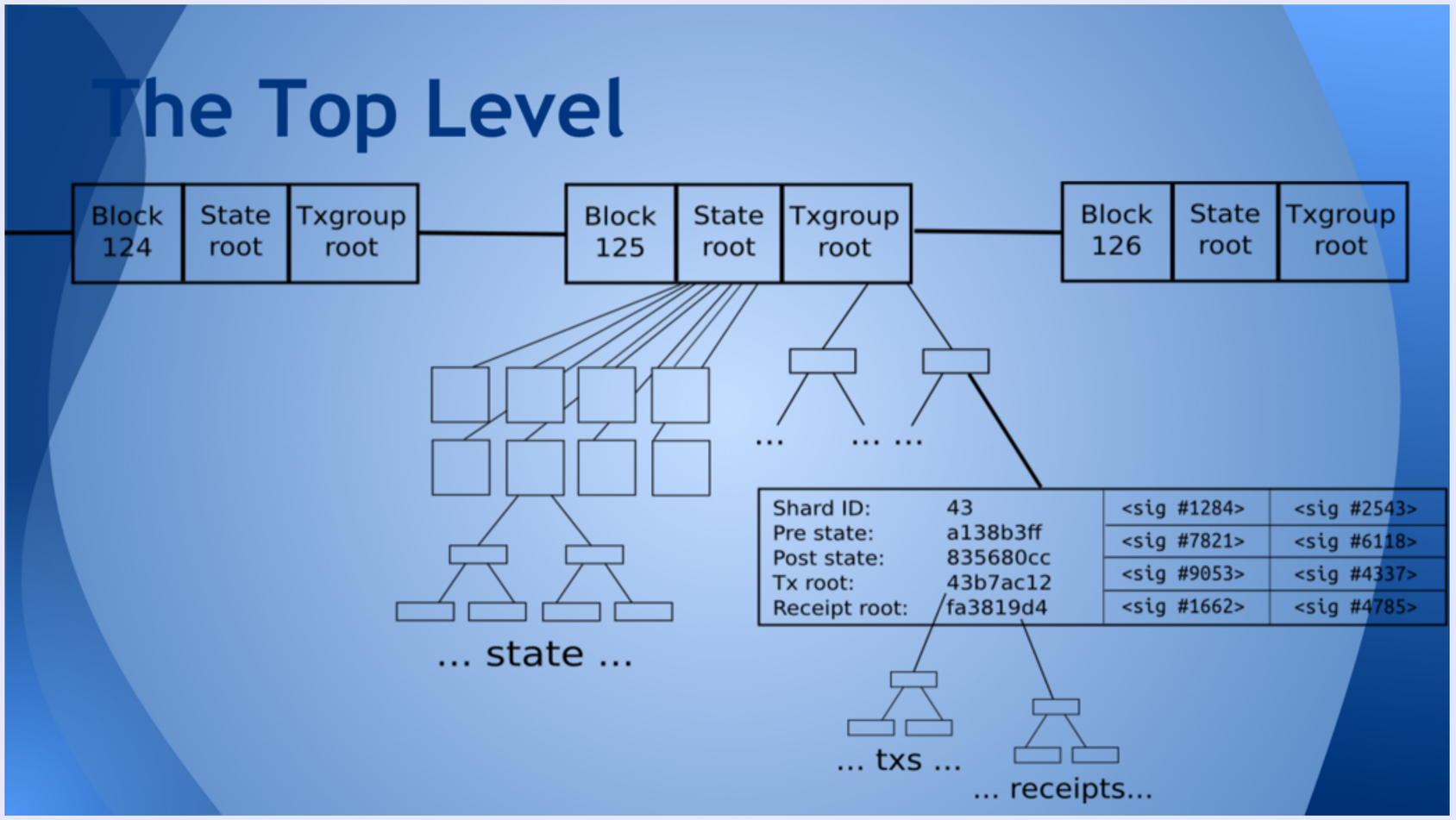
- State split into shards
- Each account in one shard
- Transactions only within one shard

ethereum Scalability



Monday: Vitalik Buterin - Scalable Blockchains & Asynchronous Programming

ethereum Scalability



Monday: Vitalik Buterin - Scalable Blockchains & Asynchronous Programming

ethereum Scalability

Cross shard transactions using

Asynchronicity by using call receipts (3 txs)

Sender writes call info into call receipt

2nd tx in target shard reads receipt and executes

Target writes return value into call receipt

3rd tx in original shard reads receipt

Finishes execution

ethereum Scalability

Fees paid to group creators

Group creators pay fees to blockmakers

Details:

- Upcoming blog post by Vitalik (blog.ethereum.org)
  - Scalable Blockchains & Asynchronous Programming (DEVCON-1, Monday)

ethereum CASPER

Consensus Protocol

based on PoS with security deposits

ethereum

CASPER

Traditional PoS: Nothing at stake problem

- signatures can be produced at very low cost
- no disadvantage from working on multiple chains

PoS with security deposits

- deposit is lost completely on proof of bad behaviour
- other nodes submit evidence transactions

ethereum CASPER

PoS with security deposits: Long range NaS

- Usage of old keys (with no more deposit) to create a competing version of events

Casper: Weak Subjectivity

- Clients only use signatures from nodes currently at stake
- Up to date list of nodes required

ethereum CASPER

Client that knows the current list of bonded nodes can learn future list

Clients need to be online regularly

Clients who are not, need to authenticate the list out-of-band

Details: see CASPER talk by Vlad (Monday)

Microsoft - Blockchain as a Service

Creating private ethereum environments

Prepackaged VMs setup with go-ethereum

Rapid experimenting

1 click private network, prefueled

up and running in 20min

BlockApps STRATO

Ethereum Haskell

Spinning up private chains

API Connector

Wallets

Faucets

bloc command line tool

IBM MTN

Multiplying Things Needlessly
Research Project

IoT devices communicate autonomously
Constrained by user defined policy

No central servers need to be maintained
No central servers need to hold sensitive data

Canonical also working on IOT + ethereum

Verification

Verification of Solidity using Why3

Only a subset of solidity supported as of now

```
contract BinarySearch {
 ///@why3
 /// requires { forall i j: int. 0 <= i <= j < @data.length ->
 ///                                    @data[i] <= @data[j] }
 /// variant { @end - @begin }
 /// ensures { @ret < UInt256.max_uint256 ->
 ///           (@begin <= @ret < @end && @data[@ret] = @value) }
 function find(uint[] data, uint begin, uint end, uint value)
       internal returns (uint ret) {
   uint len = end - begin;
   if (len == 0 || (len == 1 && data[begin] != value)) return uint(-1);
   uint mid = begin + len / 2;
   if (value < data[mid]) return find(data, begin, mid, value);
   else if (value > data[mid]) return find(data, mid + 1, end, value);
   else return mid;
 }
}
```

Verification

Solidity verification by Imandra by Aesthetic Integration

Proprietary proof generator
Open source proof checker

Light Client

Stage 1 - Probably in geth 1.4

- On demand retrieval of data
- Transaction relaying

Stage 2

- log filters
- multi-sampling header retrieval

Stage 3

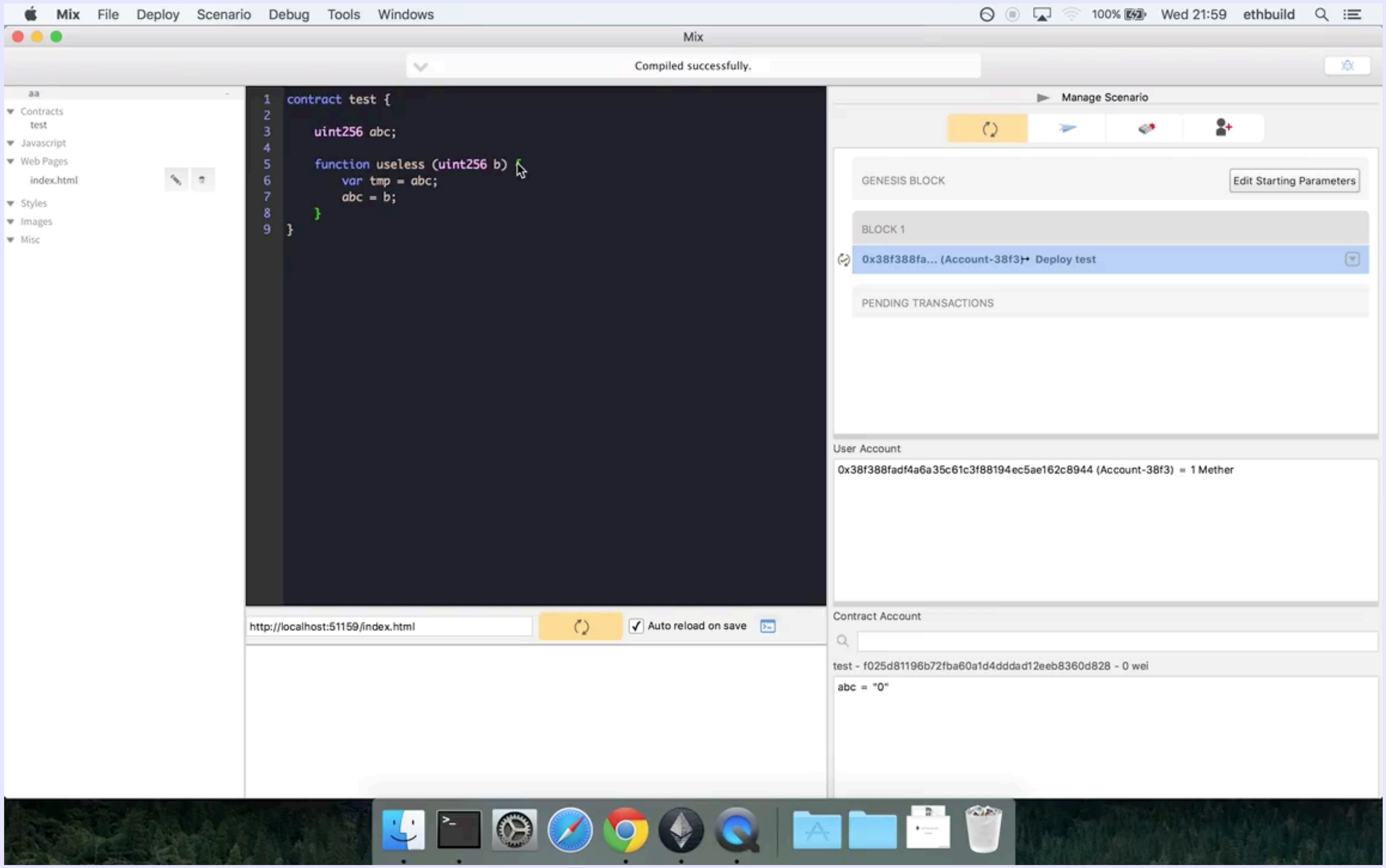
- distributed protocol
- micropayment

hack.ether.camp

Web IDE for DApp development

DApp Hackathon - December 1st

Mix


Mix File Deploy Scenario Debug Tools Windows
100% Wed 21:59 ethbuild
Mix
Compiled successfully.
aa
Contracts
test
Javascript
Web Pages
index.html
Styles
Images
Misc
1 contract test {
2
3 uint256 abc;
4
5 function useless (uint256 b) {
6 var tmp = abc;
7 abc = b;
8 }
9 }
http://localhost:51159/index.html
Auto reload on save
Manage Scenario
GENESIS BLOCK
Edit Starting Parameters
BLOCK 1
0x38f388fa... (Account-38f3) Deploy test
PENDING TRANSACTIONS
User Account
0x38f388fadf4a6a35c61c3f88194ec5ae162c8944 (Account-38f3) = 1 Mether
Contract Account
test - f025d81196b72fba60a1d4dddad12eeb8360d828 - 0 wei
abc = "0"

DApps

Oraclize

For querying data from external services
Verification using TLSnotary proofs

DApp Store

Marketplace / Registry for DApps
Early release on main chain: dappstore.io

DApps

WeiFund

Decentralised crowdfunding
with token issuance

Boardroom

Decentralised governance platform

DApps

Maker

Dai Stablecoin, pegged to SDR
Deployed on main chain

Gnosis / **Augur**

Decentralised prediction markets
Gnosis live since frontier
Augur (Ether Review)

DApps

Ujo Music

Music distribution and rights management
Imogen Heap

Slock.it

Locking / Unlocking rights in the blockchain

DApps

Colony

decentralised governance, community collaboration platform

Ether Review #5

Provenance

transparency for supply chains

ethereum

vienna

UI Wallet

Live-Demo

Presentations

https://github.com/ahirner/ethereum