ethereum

vienna

The Road to 2.0: Abstractions
More DAO drama

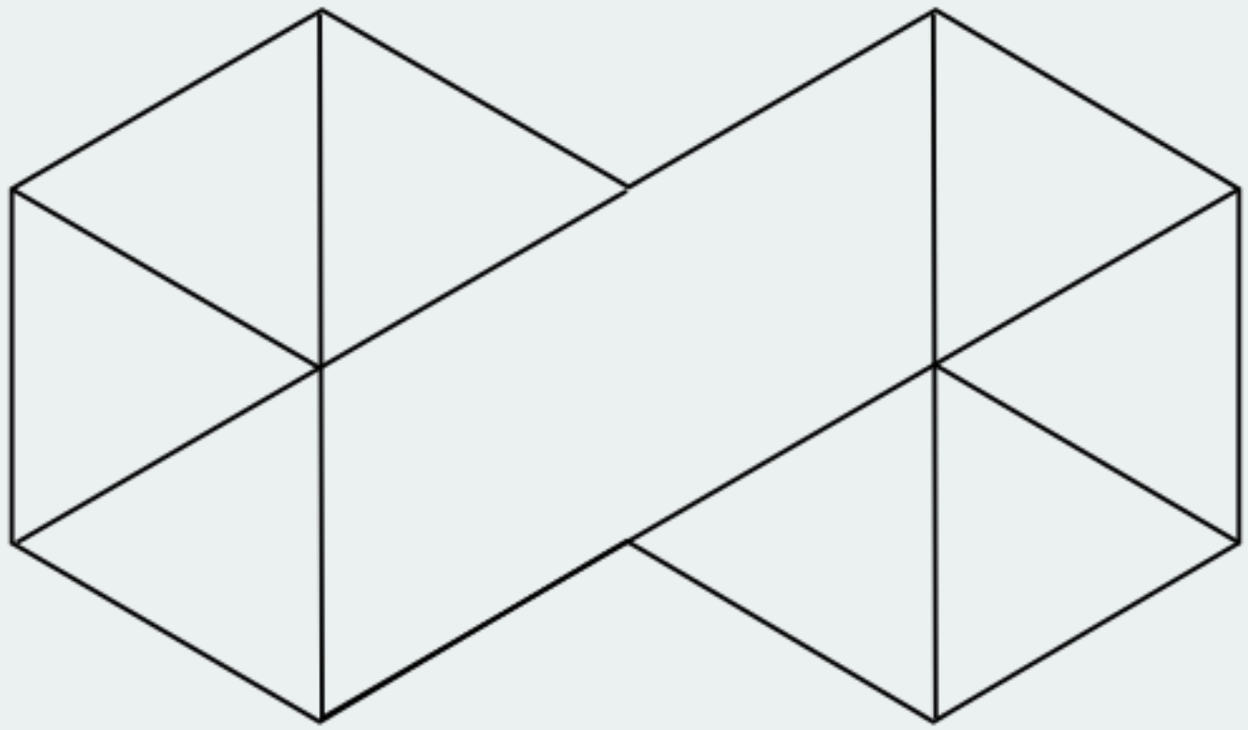
Agenda

General Introduction

Updates

The Road to 2.0: Abstractions

Socialising



RIAT

RESEARCH INSTITUTE FOR ARTS AND TECHNOLOGY

ethereum

vienna

The Road to 2.0: Abstractions
More DAO drama

ethereum

vienna

Updates

RIAT Events

September 7th	Ethereum Vienna Meetup Abstractions and DAO Drama
September 8th	First Fintech Academy Meetup AppCoins and launch of the waggawagga gaming portal
September 10th	Ethereum Vienna Workshop Contract Development for Beginners
September 12th	Ethereum: Meet Nick Dodson from Consensys!
September 13th	Bitcoin Austria Meetup
October 5th	Ethereum Vienna Meetup DEVCON-2 Recap

Nick Dodson

CONSENSYS

WeiFund

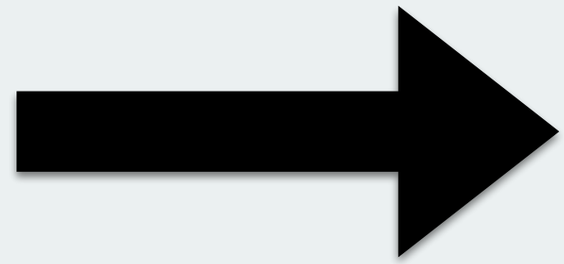
decentralised crowdfunding

BoardRoom

blockchain governance

ATM

Over there



and it still doesn't work

but there is hope (at least for the buying part)

DAO Refund

Trusted Child DAOs	**COMPLETE (~70 ETH unclaimed)**
Untrusted Child DAOs	**COMPLETE** as of late last night
Infiltrated Child DAOs	should happen any moment
Extra Balance	coming very soon

ETC DAO Refund

RHG secured 7m etc

Some sent to to exchanges

=> etc frozen

plan was supposedly to sell etc and return eth

was changed to withdrawal contract

ETC DAO Refund

Bug in withdrawal contract

=> withdrawal was cancelled

=> a few hours later reinstated

RHG	**COMPLETE**
RHG - Additional GCDAO	**COMPLETE** as of today
kraken	**COMPLETE**
poloniex	**COMPLETE** exchange balances converted

ETC DAO Refund

on september 6th

3.6M etc withdrawn from DAO by attacker

first action was a 1000 etc donation to etc devs

no further actions since

Ethereum Classic

	Hard fork	Non-fork
Block	0x6a1750da	0x8f263f06
Block Number	2215865	2212898
Difficulty	100.00%	12.40%
Total Difficulty	100.00%	13.51%
Block interval	13.3 sec	13.6 sec
Hash rate	5257.5 GH/s	635.6 GH/s

Mist Beta

Not much extra functionality

No accounts exposed to dapp

Must be requested and manually confirmed

Example DApp "Stake Voice"

Mist Beta

DEMO

[–] **vbuterin** Just some guy **10 points** 3 months ago*

As it turns out, with the change in the difficulty adjustment algorithm brought about in the last hardfork, the ice age will come very slowly indeed. Originally, the maximum amount by which the difficulty could adjust was 1/2048x, and so given a natural mining difficulty of ~2**45 (where it is now), after around block 3500000, it would go up faster than it goes down, and the protocol would quickly freeze. Now, difficulty can adjust down faster than that if the block time is slow enough, and so even after this point there is an equilibrium. At block 3.5m (1 year from now), we would have an equilibrium block time of 25s for 100k blocks (~1 month); then we would see 35s for 100k more blocks (now ~1.4 months); then ~55s for ~2.2 months, then ~95s for ~3.8 months, and so forth until we get ~655s for ~26 months (ie. slightly worse than bitcoin), and only after that does the protocol break because of the cap of ~99/2048 downward adjustment, and that final doom does not take place until 2021 (though it certainly gets very annoying by the second half of 2017).

Homestead HF changed the Ice Age

no longer at the end of the year

25s in 9 months

gets "annoying" by second half of 2017

no final doom till 2021

but bomb might already get defused in Metropolis

LES

Light Client is ready for testing

see 'Light Client Public Test' in wiki at
github zsfelfoldi/go-ethereum

Events don't work yet

Can use trusted headers for speedup

Requires **much less** space

DEVCON-2

Starts in <2 weeks

All tickets sold out (maybe the foundation still has some?)

DEMO Day

Premium Sponsors

- Microsoft
- Banco Santander

DEVCON-2

Demo of RAIDEN

Latest developments in sharding / casper

Zcash

Start of Metamask beta

Crowdsale of Gnosis

Release of Digix 2.0

ethereum

vienna

The Road to 2.0: Abstractions

Metropolis, EIP101 and beyond

Ethereum 2.0

Casper	Abstractions	Scalability
April Meetup	Now	November Meetup

Abstractions

Enable new possibilities

Simplify client codebases

Less potential consensus issues

Some changes necessary for casper or sharding

Metropolis

2nd scheduled Hardfork

Several EIPs have been proposed

Mostly by Vitalik

picked out EI**P**s with METROPOLIS_FORK_BLKNUM

some are a reaction to the DAO Attack

Metropolis

Substitute call stack limit with child gas restriction

Remove 1024 stack limit

Once the stack goes deeper, limit maximal gas

=> Contracts only have to worry about gas

and not stack depth

Metropolis

New opcode: STATIC_CALL

New CALL-like OpCode

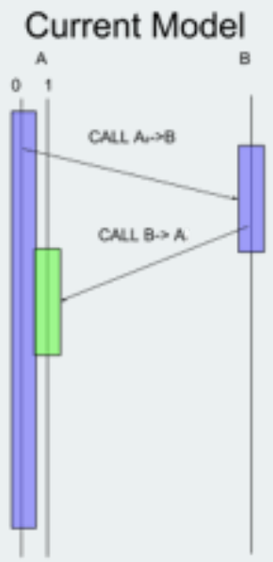
Prohibits any state change

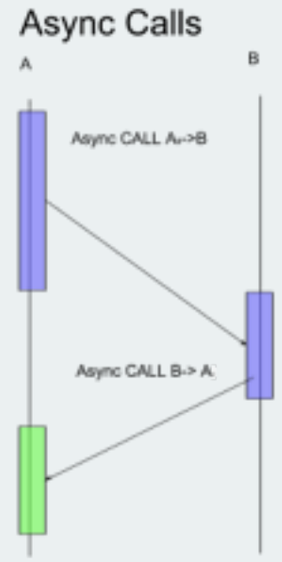
Metropolis

New Opcode ASYNC_CALL

New CALL-like OpCode

CALL is only executed after contract terminates





Metropolis

Proposal: Bomb 2.0

Removes the ICE Age and puts 10^18 into the bomb

Ether-based voting mechanism

if (Y - 2 * N) > 5000000

    a 60 day countdown is introduced

    then 1000 ether dispersed per call

Metropolis

Proposal: Bomb 2.0

Enforces HF by a vote of economic supermajority

HF should then

- move 10^18 ether to another address
- disable the 1000 ether transfers
- lock ether for yes votes for a week

Metropolis

Removal of medstate in receipts

Change of difficulty adjustment (again, uncles)

Integration of bigint arithmetic with precompiles

ECADD, ECMUL precompiles

BLAKE2b hashing (for zcash, by consensys)

Ethereum 2.0

Mauve Paper

Not related to abstractions

CASPER / Sharding etc.

Ethereum 1.0

Account	Balance
0x1350cf34d093953ce0d280364	100
0xd5f9d8d94886e70b06e474c3f	2500
0xd2963cd505c94dbf3bc663bdd	23290
0xd2963cd505c94dbf3bc663bdd	123809
…	…

Internal Accounts

External Accounts

Account	Balance	Code	Storage
0x1350cf34d093953ce0d280364	100	data	data
0xd5f9d8d94886e70b06e474c3f	2500	data	data
0xd2963cd505c94dbf3bc663bdd	23290	data	data
0xd2963cd505c94dbf3bc663bdd	123809	data	data
…	…	…	…

Serenity

Only one account type: contracts

One special "entry point" account (e.g. 0x0)

Anyone can send from entry point

External Account

=> Contract with signature verification and gas payment logic

Serenity

=> all transactions (that satisfy basic formatting checks) are valid

=> inclusion of a tx in chain no guarantee of execution

new receipt entry to indicate execution success

auto logged return values

Ethereum 2.0

This abstraction enables:

- Bitcoin-style multisig
  - also means multisig can be tx origin
- Elliptic curves other than secp256k1
- Better integration for more advanced crypto
  - ring signatures, threshold signatures, zkSNARKs, Lamport Signatures
- advanced sequence number schemes
  - sequence numbers with parallelism

Ethereum 2.0

This abstraction enables:

- UTXO-based token management
- Contract pays fee
  - miners can statically analyse that they will actually be paid
  - current POC pattern matches contract (checker code with 250k gas, then runner code)

Verification code can also check other stuff

- merkle proofs of receipts
- state of other accounts

Serenity

Transaction consist of

destination either the actual target or the account to send from

data

start gas maximal gas usage

init code initialisation code for new account

address = sha3(creator + initcode) % 2**160

=> account can still receive value prior to creation

=> this seems problematic (for identical contracts)

Metropolis

Some of those thing already proposed for Metropolis

Issue #86

Sending from 2^160-1 (instead of 0)

miners accept all tx <250k gas (DDOS?)

allow only specific code for larger tx

new contract address generation

Serenity

Separation of blocks, state and consensus layer

Consensus incentivization is done inside a contract

Consensus-level objects as transactions

makes it easier to swap out consensus algorithms

Serenity

Ethereum state moved into contract storage

account code at an immutable location in contract

receipts will be stored in a "log contract" (EIP issue 120)

blockhash as well (already in Metropolis)

greatly simplifies the implementation of the state object

=> state is an (address, key) -> value mapping (without shards)

Serenity

balances will be stored in a specialized “ether contract”

address 0x0 in EIP 101

ether is no longer part of a message

cheques used for transfer instead

manual gas payment (checker / runner patter match)

gas payments in tokens?

Ethereum 2.0

Overall the goal is to

reduce the necessary code of client implementations

by implementing as much as possible with contracts

using contract storage when possible

maybe even block contract that takes an entire block

=> makes bigger updates easier

=> should reduce the risk of consensus issues of clients

Ethereum 2.0

EIP104 - Unlimited storage key or value size

Changes the size of keys and values in store

from 32 bytes each to unlimited

gas cost scales with size of data

could also be part of Metropolis (issue #97)

used in EIP101 for storing contract code in storage

Ethereum 2.0

Parts proposed for Metropolis already

Serenity POC2 implements at least

EIP101

EIP105 (basic sharding, tx groups)

Ethereum 2.0

Possible OPCODE for zkSNARK

No EIP has been created yet

Working fork of parity made by cornell / zcash

"babyzoe", will also be presented at DEVCON-2

could bring transaction anonymity to ethereum

github.com/ahirner/ethereum