much justin

very riat

wow

Clash of Coins

Ethereum Vienna

Monero Austria

Dogecoin Austria

RIAT

RESEARCH INSTITUTE FOR ARTS AND TECHNOLOGY

Agenda

Ethereum Name Service (ENS)

Privacy with Monero

Origins of Dogecoin


DAS SCHÖNSTE AM SUCHEN
IST DAS FINDEN.
CLASH OF COINS
11.MAY.2017
RIAT, VIENNA.

RIAT is an institute for research, development, communication and education in the fields of crypto-economics, the blockchain and experimental artistic technology. We explore and actively stress-test the role of research and development in the age of zero-trust, through novel forms of presentation, discussion and publication. Examining the global crypto-economic condition and its effects on culture and society, we foster an open and interdisciplinary discourse to improve crypto-literacy for the society of tomorrow.


Bitcoincloud (2010)
Artistic Bokeh

Too Much Money (2014)
Artistic Bokeh & Societe Realiste

Blockchain Performance (2012)
Artistic Bokeh & Spacebank

Ai Weiwei Sunflower Seeds.
http://bit.ly/sunflowerweiwei

Tarasiewicz and Newman "Cryptocurrencies as Distributed Community Experiments" in: Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Academic Press; 1 edition (2014), ISBN-13: 978-0128021170, ISBN-10: 0128021179.

riat.ac.at
facebook.com/riat.ac.at
riat.academia.edu
https://riat.academia.edu/MatthiasTarasiewicz

Tarasiewicz, M. (2017). Forking as cultural practice: Institutional governance after the DAO. Proceedings of the 23nd International Symposium on Electronic Art ISEA2017 Manizales, Colombia.

+

Satoshi Nakamoto
Residency in MQ Vienna

ethereum

vienna

ENS
Ethereum Name Service

Ethereum **N**ame **S**ervice

maps names to resources

Ethereum **N**ame **S**ervice

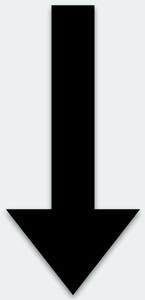
why do we need this?

Public Keys

0x0405bd548e783860a1abc0798fd23540ab0a38af3
8e8ad7e86b26cd0fe8f1ed355f8141d895d824805356
73346b8c3ff559d22737e23f2f785e5c7fade76ac8654

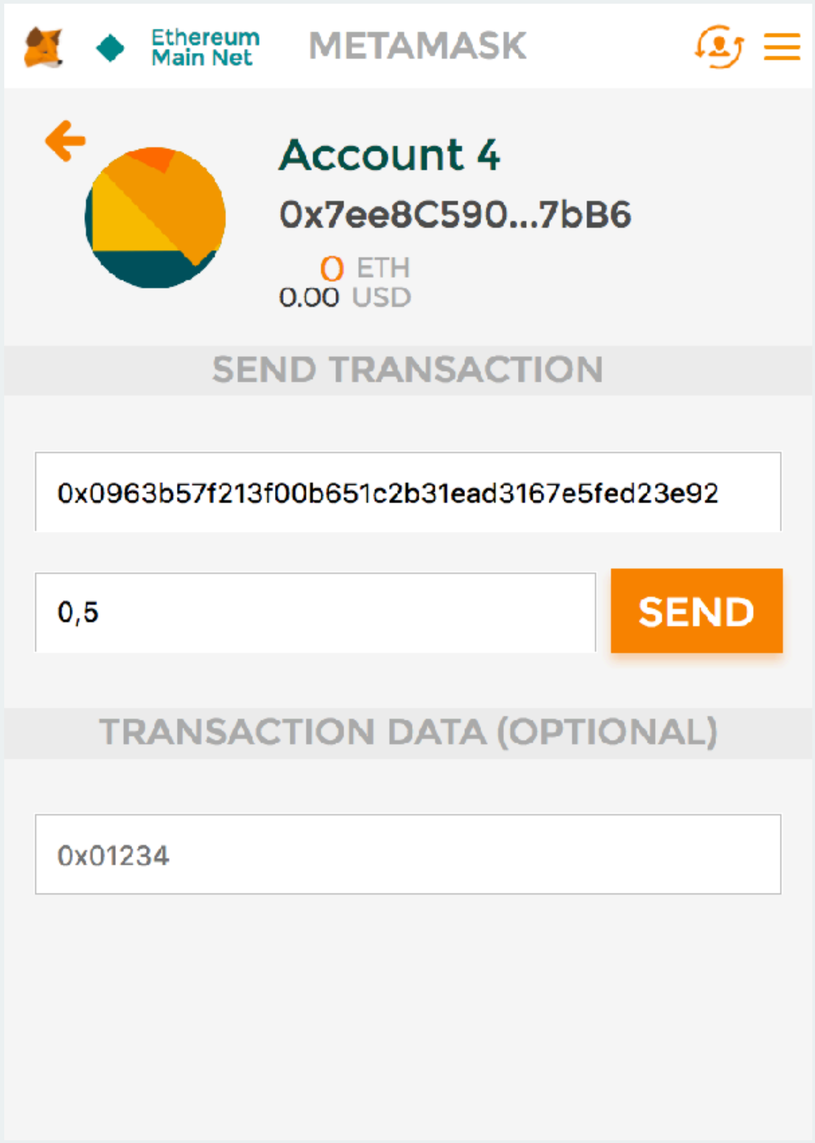
Swarm

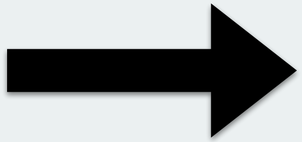
bzzr://
9e13b5c93f8cf80fb0139496813a6b96a5acc026d2e0ea7fbe7b53aeaac827f9

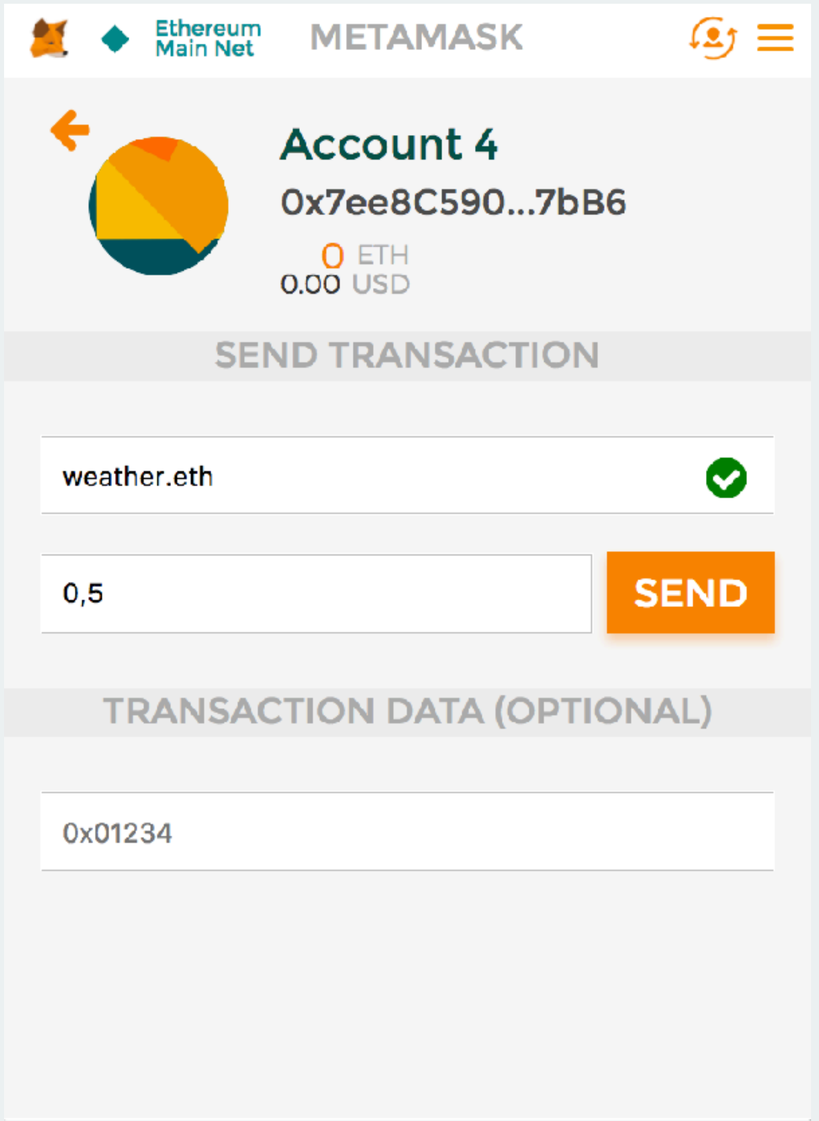


bzz://go-chat.eth

ETH Accounts







Architecture

owns name in ens

tracks ownership
maps name to resolver

maps name to resources

Register

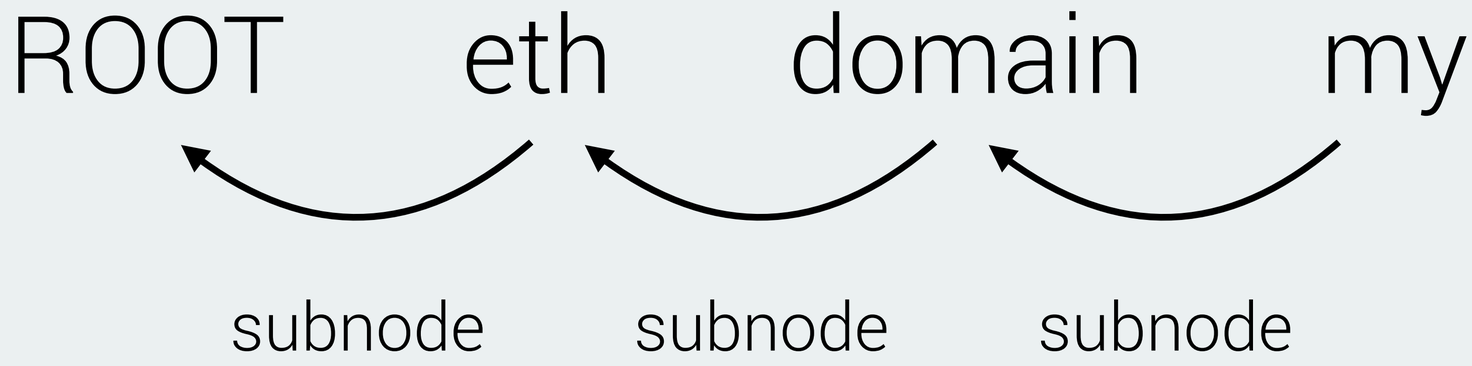
names in ens are stored only as hashes (=nodes)

for every node, ENS keeps track of

- the resolver
- a TTL
- the owner: can assign those two and subnode ownership

(e.g. domain.eth is a subnode of eth)

Hash: my.domain.eth



Hash: my.domain.eth

h(ROOT)	0x0000000000000000000000000000000000000000
h(eth)	SHA3(h(ROOT) + SHA3('eth'))
h(domain.eth)	SHA3(h('eth') + SHA3('domain'))
h(my.domain.eth)	SHA3(h('domain.eth') + SHA3('my'))

Registrar

Contract owning a node

Sell / Distribute ownership of subnodes

Example: eth-registrar (owns .eth)

ENS does not differentiate between registrars and regular owners.

Resolver

resolve nodes to resources like

Record type	Function(s)	Interface ID	Defined in
Ethereum address	*addr*	0x3b3b57de	EIP137
ENS Name	*name*	0x691f3431	EIP181
ABI specification	*ABI*	0x2203ab56	EIP205
Public key	*pubkey*	0xc8690233	EIP619

also "content" is the de-facto standard for swarm hashes

.eth Registrar

Registration takes place by sealed bid **Vickrey auction**

3 day bidding period

2 day reveal phase

Winner pays 2nd highest bid

Unrevealed / Invalid bids lose deposit

.eth Registration Process

Hash of the name revealed at the beginning of the auction

Bids cannot be attributed to a particular name until revealed

Registration DApp also starts 2 random fake auctions

Extra funds can be sent with bid to hide real value

.eth Registration Process

Registration for a minimum of 1 year

Afterwards registration can be released => deposit returned (minus fee)

Every losing bid gets the money back instantly (minus fee)

.eth Registrar

active for 2 years

then supposed to be replaced

only name of at least 7 characters allowed

slow start period of 8 weeks

root node of ENS owned by multisig

root node owners

Aron Fischer	Colony, Swarm
Dan Finlay	Metamask
Nick Johnson	ENS
Juan Benet	IPFS
Piper Merriam	Populus, Alarm Clock, EPM
Taylor Monahan	MyEtherWallet
Vlad Zamfir	Casper

Statistics

> 17600 auctions thus far

> 3000 bids revealed (of >7000 total)

> 500 names registered

> 100k ether locked up in bids

~ 700 ether locked up for names

highest revealed bid thus far: 14500 eth for freemarket.eth

highest deposit overall: 29500

cbsnews.eth, for 287 ETH

weather.eth for 250 ETH

gateway.eth for 210 ETH.

DApp for Registration:

https://registrar.ens.domains

(requires web3 support)

Supported by

Metamask

MyEtherWallet

Mist (planned)

github.com/ethereum-vienna-meetup