A gentle introduction to Blockchain

at the TechConnex Blockchain Peer Group

By Marc Lijour

February 28, 2019

BY SA

The Blockchain Peer Group is brought to you by

www.metameshgroup.com

Who am I?

https://www.linkedin.com/in/marclijour/

Team Experience

CONSENSYS	THE WORLD BANK	TOYOTA	NORTEL NETWORKS
Celestica	AMERICAN EXPRESS	NATO OTAN	BlueCross BlueShield
McDonald's	CISCO	NOKIA Bell Labs	SLA SINGAPORE LAND AUTHORITY
ETS Educational Testing Service	ies INSTITUTE OF EDUCATION SCIENCES	RioTinto	BirdLife SOUTH AFRICA Giving Conservation Wings

MetaMesh

Access these slides

https://bit.ly/2Tou0Jy

or find in the folder 2019 TechConnex - Blockchain Peer Group at

https://github.com/marclijour/presentations

MetaMesh

Table of Contents

1. What is Blockchain?
2. Hands-on Introduction to Crypto
3. ICOs, STOs, and other Token launches
4. Introduction to Smart Contracts

MetaMesh

The Trust Machine

Source of Trust

World Economic Forum: *What is Blockchain* Youtube Video

Key Cryptographic Primitives

Signing

Credit: FlippyFlink

Encrypting

Hashing

MetaMesh

Where do we need more trust?

- payments

MetaMesh

Where do we need more trust?

- payments
- national identity

MetaMesh

Where do we need more trust?

- payments
- national identity
- supply chain (e.g. food: Spanghero horse meat trial, Opioids, expensive cargos)

MetaMesh

Where do we need more trust?

- payments
- national identity
- supply chain (e.g. food: Spanghero horse meat trial, Opioids, expensive cargos)
- contracts

MetaMesh

Where do we need more trust?

- payments
- national identity
- supply chain (e.g. food: Spanghero horse meat trial, Opioids, expensive cargos)
- contracts
- *real* news & historical events (e.g. bombings)

MetaMesh

Where do we need more trust?

- payments
- national identity
- supply chain (e.g. food: Spanghero horse meat trial, Opioids, expensive cargos)
- contracts
- *real* news & historical events (e.g. bombings)
- collaborative data reporting
- ...

MetaMesh

Table of Contents

1. What is Blockchain?
2. Hands-on Introduction to Crypto
3. ICOs, STOs, and other Token launches
4. Introduction to Smart Contracts

MetaMesh

Let's try things out!

Install MetaMask

Follow step by step:

1. Install the Chrome/Chromium extension
2. Watch the intro on Youtube
3. Create an account
4. Switch to the Ropsten Testnet (top-right in MetaMask)
5. Fill your account with Ether from https://faucet.metamask.io

https://metamask.io

MetaMesh

Request Ether from the faucet (on the Ropsten network)

Do it several times; then donate 1 ether to the faucet

https://faucet.metamask.io

MetaMask Ether Faucet

faucet

address: 0x81b7e08f65bdf5648606c89998a9cc8164397647
balance: 4094302.54 ether

request 1 ether from faucet

user

address: 0x56e552eb5a9ab277d9eb841f92d473bf0cae7ebf
balance: 1.00 ether
donate to faucet:

1 ether | 10 ether | 100 ether

transactions

MetaMesh

Check the transaction on Metamask

Click on the transaction for a detailed view

MetaMesh

Check the transaction on Etherscan

ROPSTEN Etherscan The Ethereum Block Explorer

ROPSTEN (Revival) TESTNET | Search by Address / Txhash / Block / Token / Ens | GO | Language

HOME | BLOCKCHAIN | TOKEN | MISC

Transaction 0xa8a8f32539cb69bd3e506b6527fcc7d44c43cccead09b30b10a9891c99355a3d

Home / Transactions / Tx Info

Overview

Transaction Information

Tools & Utilities

[This is a Ropsten **Testnet** Transaction Only]

TxHash:	0xa8a8f32539cb69bd3e506b6527fcc7d44c43cccead09b30b10a9891c99355a3d
TxReceipt Status:	Success
Block Height:	4610407 (348 Block Confirmations)
TimeStamp:	1 hr 12 mins ago (Dec-12-2018 04:23:14 AM +UTC)
From:	0x56e552eb5a9ab277d9eb841f92d473bf0cae7ebf
To:	0x81b7e08f65bdf5648606c89998a9cc8164397647
Value:	1 Ether ($0.00)
Gas Limit:	21000
Gas Used By Transaction:	21000 (100%)
Gas Price:	0.000000005 Ether (5 Gwei)
Actual Tx Cost/Fee:	0.000105 Ether ($0.000000)
Nonce & {Position}:	0 | {6}
Input Data:	0x

MetaMesh

A note about gas price

https://ethgasstation.info

MetaMesh

Price of (real) ether: ETH

More information: https://www.tradingview.com/symbols/ETHUSD/

MetaMesh

Wallets

More information: https://blockgeeks.com/guides/cryptocurrency-wallet-guide/

Software	Hardware	Paper
Jaxx		
mycelium ad-hoc economy		
MyEtherWallet		

MetaMesh

Exchanges

1. Centralized Exchanges (Coinbase, Quadriga, ...)
2. Decentralized Exchanges

MetaMesh

ATMs

More information: https://coinatmradar.com/country/38/bitcoin-atm-canada/

MetaMesh

ATMs

More information: https://coinatmradar.com/country/38/bitcoin-atm-canada/

Other crypto-assets

More information:
https://www.tradingview.com/markets/cryptocurrencies/prices-all/

Overview | Performance | Oscillators | Trend-Following

USD BTC

NAME 301 matches	MKT CAP	FD MKT CAP	LAST	AVAIL COINS	TOTAL COINS	TRADED VOL	CHG %
Bitcoin	59.852B	72.158B	3436.1	17.419M	21M	4.712B	0.02%
XRP	12.167B	29.729B	0.29729	40.927B	100B	369.224M	0.17%
Ethereum	9.257B	9.257B	89.23	103.745M	103.745M	1.739B	0.10%
Stellar	2.165B	11.811B	0.11297826	19.165B	104.543B	197.41M	-0.34%
Tether	1.838B	2.554B	0.99000000	1.856B	2.58B	2.97B	-0.10%
Bitcoin Cash	1.729B	2.074B	98.760	17.506M	21M	71.709M	0.92%
EOS	1.692B	1.879B	1.8672	906.245M	1.006B	740.947M	0.44%
Bitcoin SV	1.548B	1.858B	88.45300000	17.505M	21M	59.813M	-2.60%
Litecoin	1.431B	2.02B	24.045	59.532M	84M	380.518M	1.14%
TRON	877.572M	1.314B	0.013247	66.247B	99.218B	72.465M	-0.88%
Cardano	772.388M	1.341B	0.029791	25.927B	45B	9.766M	-0.09%
Monero	722.858M	722.858M	43.445	16.638M	16.638M	11.502M	1.38%
NEM	642.663M	642.663M	0.07141	9B	9B	8.23M	-1.53%
Binance Coin	635.009M	926.299M	4.8548350	130.799M	190.799M	20.772M	-2.52%
IOTA	631.509M	631.509M	0.2272	2.78B	2.78B	4.203M	1.07%
Dash	554.925M	1.234B	65.28257000	8.5M	18.9M	160.684M	2.12%
Ethereum Classic	402.997M	402.997M	3.777	106.698M	106.698M	106.521M	0.68%
NEO	387.602M	596.31M	5.96	65M	100M	100.484M	1.51%

MetaMesh

Table of Contents

1. What is Blockchain?
2. Hands-on Introduction to Crypto
3. ICOs, STOs, and other Token launches
4. Introduction to Smart Contracts

MetaMesh

Ethereum, Alt-Coins, and ICOs

1. 94% of the top 100 tokens are built on top of Ethereum
2. $5.5 billion raised in 2017
3. $6.5 billion raised in the first quarter of 2018
4. Ethereum has the largest developer community
5. Close to 2,000 dapps (decentralized applications) counted on Ethereum

MetaMesh

Amount raised by ICOs

https://cointelegraph.com/news/
from-2-9-billion-in-a-month-to-hundreds-dead-trends-of-the-rollercoaster-ico-market-in-18-months

MetaMesh

ICOs fell down 90% in 2018

https://www.investinblockchain.com/invest-in-icos/

see also https://www.coindesk.com/dont-throw-the-crypto-tokens-out-with-the-bathwater

MetaMesh

Token Types

http://www.untitled-inc.com/

the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

MetaMesh

Token Types

http://www.untitled-inc.com/

the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

MAIN TOKEN TYPES PER DIMENSION

Technical Layer

Blockchain-Native Tokens

Description: A token that is implemented on the protocol-level of a blockchain

Characteristics:
- Critical to operate the blockchain
- Integral component of the blockchain's consensus mechanism
- Part of the blockchain's incentive mechanism for block validators/other nodes

Examples: BTC (Bitcoin, Bitcoin); ETH (Ether, Etherum), STEEM (Steem, Steem)

Non-native Protocol Tokens

Description: A token that is implemented in a cryptoeconomic protocol on top of a blockchain

Characteristics:
- Integral component of the protocol's consensus mechanism
- Part of the protocol's incentive mechanism for nodes
- Tracked on an underlying blockchain to which it is not integral (e.g. ERC20 Tokens on Ethereum)

Examples: REP (Decentralized Oracle Protocol, Augur)

(d)App Tokens

Description: A token that is implemented on the application-level on top of a blockchain (and potentially protocol)

Characteristics:
- Integrated within the application
- Part of the app's incentive mechanism for nodes and/or users
- Tracked on an underlying blockchain to which it is not integral (e.g. ERC20 Tokens on Ethereum)

Examples: WIZ (Wisdom, Gnosis), SAFE (Safecoin, SAFE Network)

Purpose

Cryptocurrencies

Description: A token that is intended to be a "pure" cryptocurrency

Characteristics:
- Intended as a global medium of exchange
- Functions as a store of value

Examples: BTC (Bitcoin), ZEC (Zcash), KIN (Kin, Kik)

Network Tokens

Description: A token that is primarily intended to be used within a specific system (e.g. network, application)

Characteristics:
- Token has functionality within the issuers system
- Not intended as a general cryptocurrency

Examples: GNO (Gnosis), STX (Stacks, Blockstack)

Investment Tokens

Description: A token that is primarily intended as a way to passively invest in the issuing entity or underlying asset

Characteristics:
- Promises owners a share of asset value or in (future) success of the issuing entity
- No or little significant functionality

Examples: Neufund Equity Tokens (Neufund), DGX (Digix Gold, DigixDAO)

Underlying Value

Asset-backed Tokens

Description: A token that functions as a claim on an underlying asset

Characteristics:
- Allows trading via IOUs without actually having to move the underlying asset
- The issuer is responsible to hold the underlying asset
- Introduces counterparty risk

Examples: USDT (Tether USD, Tether), GOLD (GOLD, GoldMint), Ripple IOUs (Ripple)

Network Value Tokens

Description: A token that is tied to the value and development of a network

Characteristics:
- Tied to the value generated and exchanged on the network (e.g. transaction fee volume)
- Closely intertwined with key interactions of network participants

Examples: ETH (Ether, Ethereum) STEEM (Steem)

Share-like Tokens

Description: A token with share-like properties

Characteristics:
- The issuer promises token owners a share in the success of the issuing entity (e.g. dividends, profit-shares)
- May or may not come with voting-rights
- Mostly on no/weak legal basis

Examples: DGD (DigixDAO), LKK (Lykke)

Likely to be classified as a security token

Utility

Usage Tokens

Description: A token that provides access to a digital service, similar to a paid API key

Characteristics:
- Grants holders access to exclusive functionality of the service

Examples: BTC (Bitcoin), STX (Stacks, Blockstack)

Work Tokens

Description: A token that provides the right to contribute to a system

Characteristics:
- Owning Tokens is the precondition for contributing to the system
- Contributions are either incentivized with a rewards system or holders get utility from the system/decentralized organization

Examples: REP (Reputation, Augur), MKR (Maker, Maker DAO)

Hybrid Tokens

Description: A token featuring traits of both usage and work tokens

Characteristics:
- Grants access to system functionalities
- Allows owners to contribute to the system

Examples: ETH (Ether, Ethereum, after Casper), DASH (Dash)

Legal Status*

Utility Tokens

Description: A token offering owners clearly defined utility within a network or (decentralized) application

Characteristics:
- Closely tied to the functionality of the issuing network or application
- Internal network/app currency but not necessarily attempting to be a currency
- Grants owners the right to actively contribute to the system vs. passive investor role
- Avoids security-like features

Examples: GNO (Gnosis), STEEM (Steem)

Security Tokens

Description: A token that behaves like a security

Characteristics:
- Showcases security-like features, e.g. voting on decisions regarding the issuing entity, dividends, or profit shares
- Holders are regarded as owners
- Little or insufficient utility

Examples: SPiCE (SPiCE VC), Bitwala (tba)

Cryptocurrencies

Description: A token that is a pure cryptocurrency

Characteristics:
- Acts as a store of value and medium of exchange
- Not emitted by a central authority against which owners have claims

In Germany (according to BaFin):
- currently not regarded as lawful, functional currency
- not regulated by e-money laws

Examples: BTC (Bitcoin), ZEC (Zcash), LTC (Litecoin)

Untitled INC

*details dependent on respective jurisdiction

MetaMesh

Crypto as seen by the Regulator (and the taxman)

1. Cryptocurrency
2. Utility Token
3. Security Token

MetaMesh

Create your own (ERC-20) token

1. Use the Token Factory Dapp at https://tokenfactory.surge.sh/#/factory
2. MetaMask will pop up (see picture above)
3. Submit the transaction (on the Ropsten Testnet)
4. Check your transaction on https://ropsten.etherscan.io

MetaMesh

Check your Smart Contract

1. Select the "Sent" tab
2. Check the orange Copy icon (Tx Hash)
3. Click on "Contract Published"
4. That should bring you to Etherscan (see next page)

MetaMesh

Verify the status of your transaction on Etherscan

ROPSTEN Etherscan
The Ethereum Block Explorer

ROPSTEN (Revival) TESTNET | Search by Address / Txhash / BlockNo | GO

HOME | BLOCKCHAIN | ACCOUNT | TOKEN | CHART | MISC

Transaction 0x75c37645d2ade85d200d5bf9cdbcb61bcd9787f36d24790e2f427594e8289b6d

Home / Transactions / Transaction Information

Overview

Transaction Information — Tools & Utilities

TxHash:	0x75c37645d2ade85d200d5bf9cdbcb61bcd9787f36d24790e2f427594e8289b6d
Block Height:	2358440 (15 block confirmations)
TimeStamp:	2 mins ago (Dec-29-2017 10:03:52 AM +UTC)
From:	0x51ae690685ea0e7bc68c3e939f9c00eaaa8e0524
To:	[Contract 0xc8f30ddeb584e2a8e922054204501f47316eb33c Created]
Value:	0 Ether ($0.00)
Gas Limit:	1000000
Gas Used By Txn:	681757
Gas Price:	0.00000002 Ether (20 Gwei)
Actual Tx Cost/Fee:	0.01363514 Ether ($0.000000)
Cumulative Gas Used:	2288703
TxReceipt Status:	Success
Nonce:	2
Input Data:	0x60a060405260046060527f48302e310000000000000000000000000000000000000000000000000000000000000000006080526006 805460008290527f48302e310000000000000000000000000000000000000000000000000000000882556100b5907ff652 222313e28459528d920b65115c16c04f3efc82aaedc97be59f3f377c0d3f602060026001841615610100026000190190 93 1692909204601f0191909104810190 5b808211156101795760008155600101610 0a1565b505060405161094b3803806109

Convert To Ascii

Transaction Information: note the "To" line with your contract address

MetaMesh

Watch your Token

1. Click on the "Add Token" button
2. Wait for the next window (picture on the right)
3. Copy your contract address (from Etherscan)
4. Go back to your Token Factory tab, which should show an UI to interact with your contract or go to the URL: https://tokenfactory.surge.sh/#/token/0x... (replace 0x... by your contract address)
5. Move coins around
6. In MetaMask, click on your token to check the tx on Etherscan

MetaMesh

Want to sell to token (ICO)?
Consult your lawyer now...

Table of Contents

1. What is Blockchain?
2. Hands-on Introduction to Crypto
3. ICOs, STOs, and other Token launches
4. Introduction to Smart Contracts

MetaMesh

Remember: Ethereum

Ethereum is a **decentralized platform that runs smart contracts**: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.
— https://ethereum.org

MetaMesh

Coding your first ERC-20 Smart Contract

1. Open the Remix IDE at https://remix.ethereum.org
2. Close the ballot file
3. Create a new file named TokenRecipient.sol
4. Copy the code from https://ethereum.org/token (second white box, under "The Code", starting with "pragma")
5. Switch to the "Run" tab (top-right bar, after Compile)

Reference:
ERC-20 Token Standard

MetaMesh

Compiling Successfully

1. Two green boxes should show on the right
2. TokenERC20 is the name of the contract (class)
3. tokenRecipient is the name of the interface
4. Switch to the "Run" tab (top right)

MetaMesh

Submitting the Smart Contract

1. Under the dropdown showing "TokenERC20", add a number (total amount of tokens to issue) and two strings (the latter is the token symbol)
2. Add enough gas (top right, try 30)
3. Click Create and check whether MetaMask needs confirmation

MetaMesh

Interacting with the contract

1. A new interface will pop up on the bottom right corner of the IDE

MetaMesh

Tools for Developers

Truffle Framework

http://truffleframework.com

YOUR ETHEREUM SWISS ARMY KNIFE

Truffle is the most popular development framework for Ethereum with a mission to make your life a whole lot easier.

Star 4,734 Fork 594 gitter join chat

INSTALL VIA NPM

```
$ npm install -g truffle
```

Requires NodeJS 5.0+. Works on Linux, macOS, or Windows.

DOCUMENTATION TUTORIALS

Don't know where to start? Get yourself a Truffle Box!

Infura

http://infura.io

MetaMesh

Mythril

https://github.com/ConsenSys/mythril

Mythril is a security analysis tool for smart contracts.
It comes as a Python package that requires a solidity compiler and a C++ compiler.

```
$ sudo apt install libssl-dev
$ sudo apt install gcc g++
$ sudo add-apt-repository ppa:ethereum/ethereum
$ sudo apt install solc
$ sudo pip3 install mythril
$ myth -x contracts/higherbidder.sol
```

See also https://hackernoon.com/introducing-mythril-a-framework-for-bug-hunting-on-the-ethereum-blockchain-9dc5588

MetaMesh

Big Data and Analytics on Ethereum

https://aleth.io

MetaMesh

Getting paid for your work: The Bounties Network

https://bounties.network

Gitcoin (depth-first) and Bounties Network (breadth-first) have integrated!

Gitcoin

https://gitcoin.co

Thank you!

Email: marc@metameshgroup.com
Twitter: @marclijour

www.metameshgroup.com

MetaMesh

References