universität innsbruck

Tracking Payment Flows in Ethereum

Michael Fröwis

Overview

Content:
This talk explains the differences of money-flow tracking between Bitcoin and Ethereum.

We outline challenges for forensic investigations in Ethereum.

What is Ethereum ?

- Second most relevant blockchain system by market valuation

What is Ethereum ?

- Second most relevant blockchain system by market valuation
- Built-in currency called Ether (ETH)

What is Ethereum ?

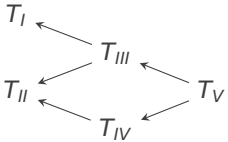
- Second most relevant blockchain system by market valuation
- Built-in currency called Ether (ETH)
- Online since July 30th, 2015

What is Ethereum ?

- Second most relevant blockchain system by market valuation
- Built-in currency called Ether (ETH)
- Online since July 30th, 2015
- $\approx$ 14 second block time

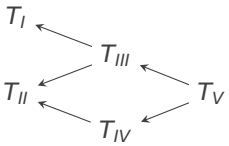
Tracking Payment Flows: From Bitcoin to Ethereum

Transaction graph

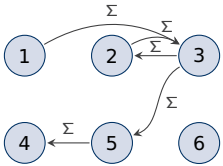


Tracking Payment Flows: From Bitcoin to Ethereum

Transaction graph

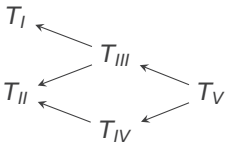


Address graph

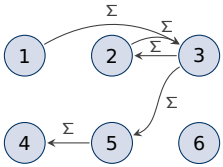


Tracking Payment Flows: From Bitcoin to Ethereum

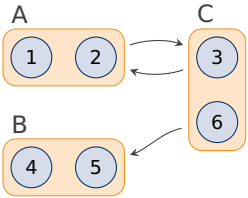
Transaction graph



Address graph



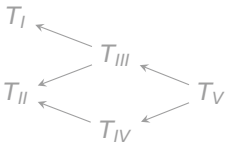
Entity graph



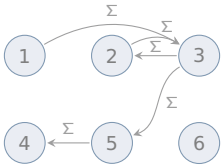
Tracking Payment Flows: From Bitcoin to Ethereum

usefulness

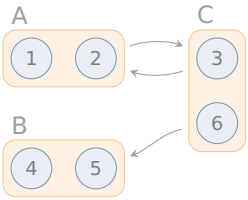
Transaction graph



Address graph



Entity graph

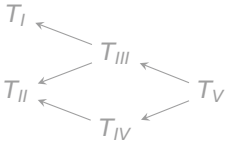


Tracking Payment Flows: From Bitcoin to Ethereum

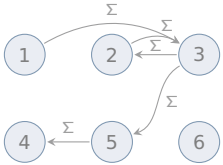
usefulness

Bitcoin

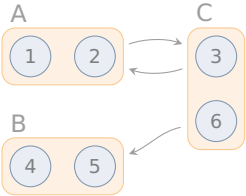
Transaction graph



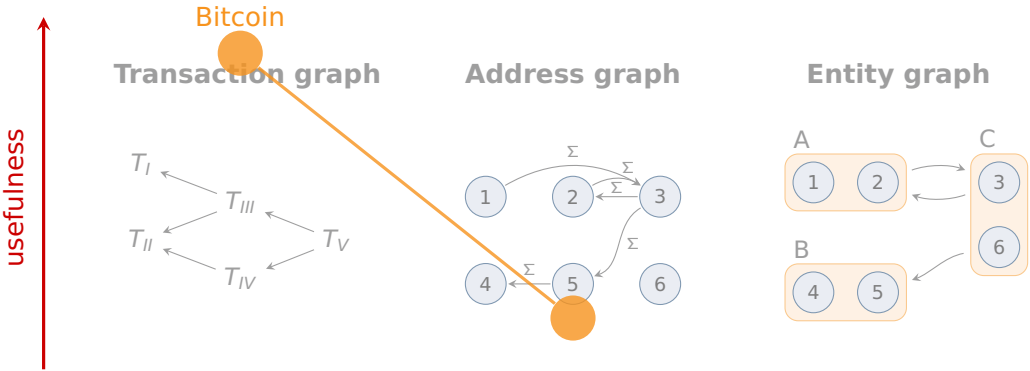
Address graph



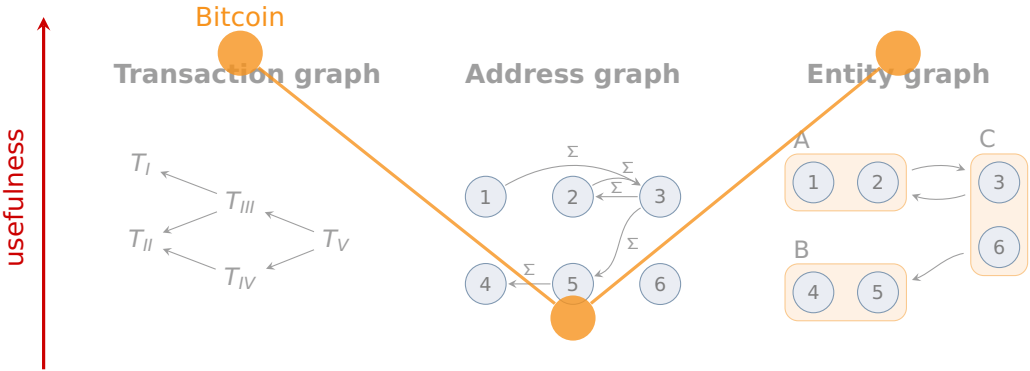
Entity graph



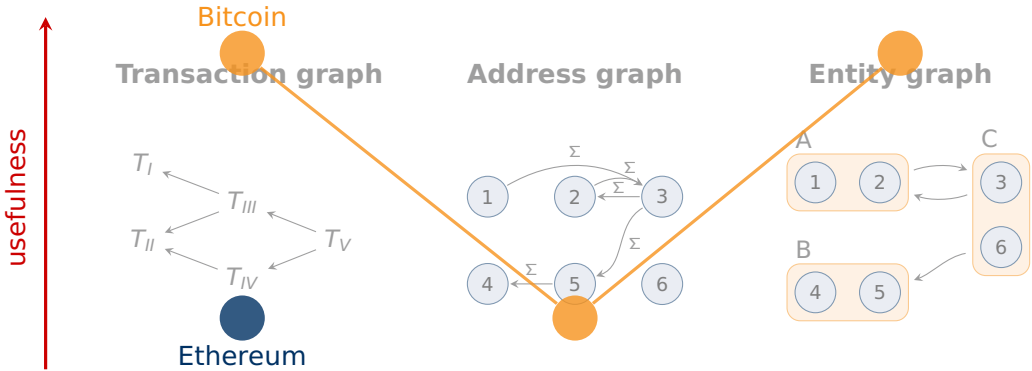
Tracking Payment Flows: From Bitcoin to Ethereum



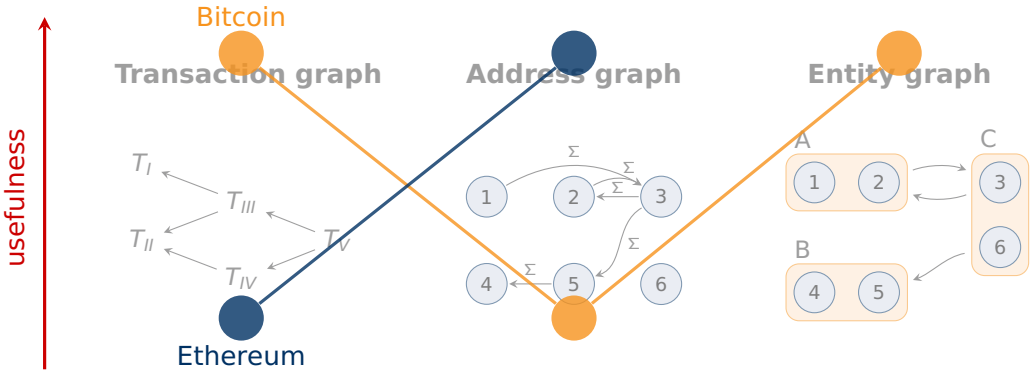
Tracking Payment Flows: From Bitcoin to Ethereum



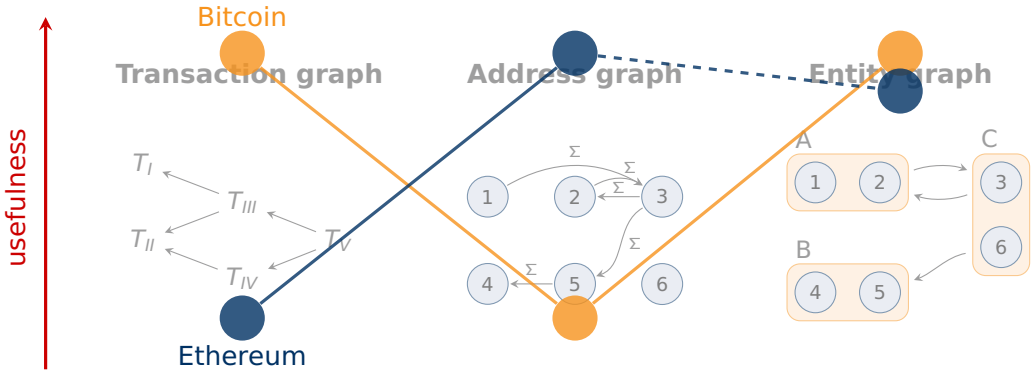
Tracking Payment Flows: From Bitcoin to Ethereum



Tracking Payment Flows: From Bitcoin to Ethereum



Tracking Payment Flows: From Bitcoin to Ethereum



Ethereum

Account model: Analogy std. bank transfer, accounts have balances

Externally Owned Account (EOA):

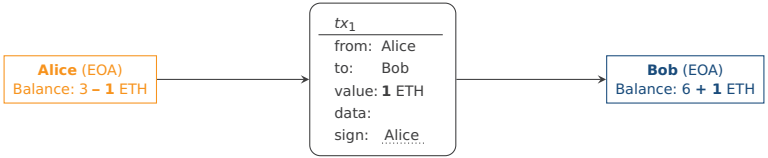
Alice (EOA)
Balance: 3 ETH

Bob (EOA)
Balance: 6 ETH

Ethereum

Account model: Analogy std. bank transfer, accounts have balances

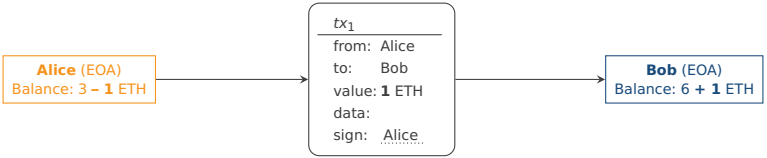
Externally Owned Account (EOA):



Ethereum

Account model: Analogy std. bank transfer, accounts have balances

Externally Owned Account (EOA):

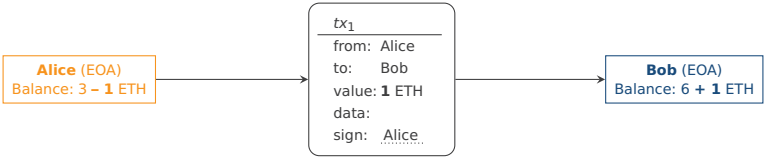


Code Account (*CA*) aka „Smart Contract“:

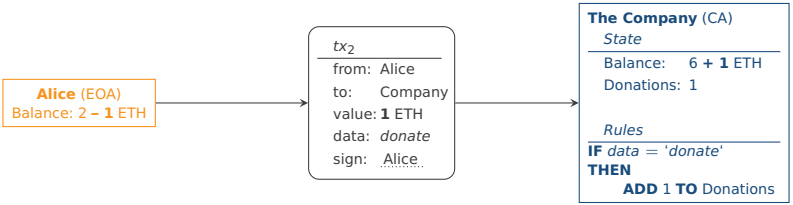
Ethereum

Account model: Analogy std. bank transfer, accounts have balances

Externally Owned Account (EOA):



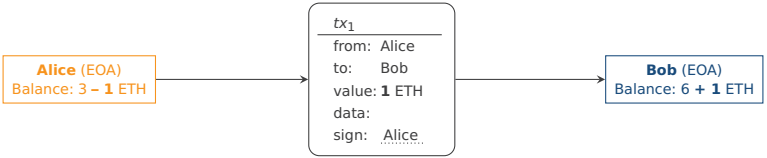
Code Account (*CA*) aka „Smart Contract“:



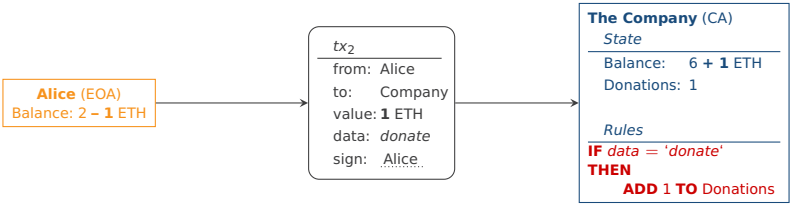
Ethereum

Account model: Analogy std. bank transfer, accounts have balances

Externally Owned Account (EOA):



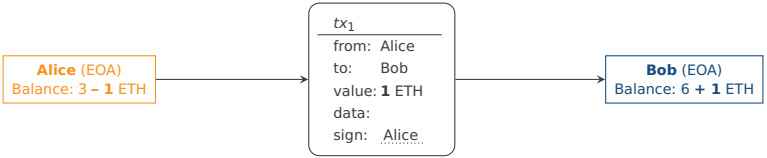
Code Account (*CA*) aka „Smart Contract“:



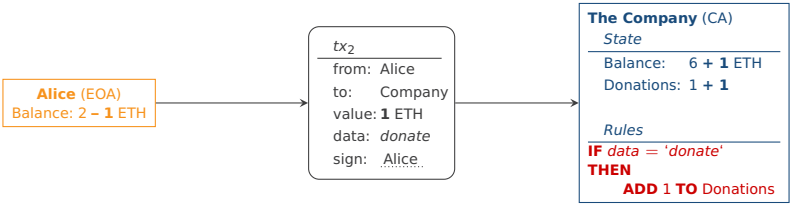
Ethereum

Account model: Analogy std. bank transfer, accounts have balances

Externally Owned Account (EOA):



Code Account (*CA*) aka „Smart Contract“:



What Can Code Accounts Do ?

- Activated on receipt of a transaction

What Can Code Accounts Do ?

- Activated on receipt of a transaction
- Store and modify local state

What Can Code Accounts Do ?

- Activated on receipt of a transaction
- Store and modify local state
- Arbitrary computations

What Can Code Accounts Do ?

- Activated on receipt of a transaction
- Store and modify local state
- Arbitrary computations
- Create transactions: communicate, transfer Ether

What Can Code Accounts Do ?

- Activated on receipt of a transaction
- Store and modify local state
- Arbitrary computations
- Create transactions: communicate, transfer Ether

Why is this useful ?

Gambling services, decentralized exchanges, prediction markets, wallets, state channels and payment channels, . . .

But most prominently token systems.

What Is a Token System?

Token: Jargon for exchangeable virtual asset, fungible or non-fungible.

What Is a Token System?

Token: Jargon for exchangeable virtual asset, fungible or non-fungible.

What Is a Token System?

Token: Jargon for exchangeable virtual asset, fungible or non-fungible.

Token system: *CA* keeping track of token ownership and transfers.

What Is a Token System?

Token: Jargon for exchangeable virtual asset, fungible or non-fungible.

Token system: *CA* keeping track of token ownership and transfers.

Use-cases: Sub-VCs, crowdfunding, shares, votes, reward systems, . . .

How Does a Token System Work ?

Alice (EOA)
Balance: 3 ETH

My Token (CA)

State

Balance:	0 ETH
Alice:	2
Bob:	0

Rules

IF *data* = '*send*';*to*;*val*
AND *from* $\geq$ *val*
THEN
  SUB *val* **FROM** *from*
  ADD *val* **TO** *to*

How Does a Token System Work ?

Alice (EOA)
Balance: 3 ETH

My Token (CA)

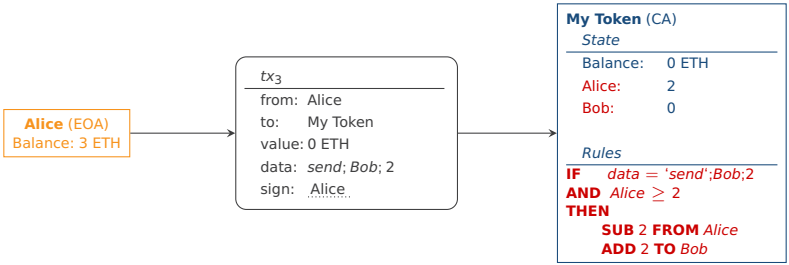
State

Balance:	0 ETH
Alice:	2
Bob:	0

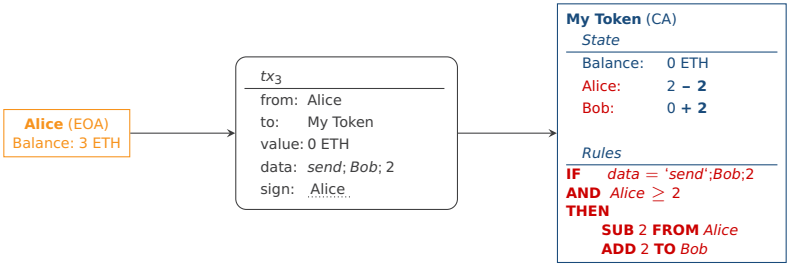
Rules

IF *data* = '*send*';*to*;*val*
AND *from* $\geq$ *val*
THEN
  SUB *val* **FROM** *from*
  ADD *val* **TO** *to*

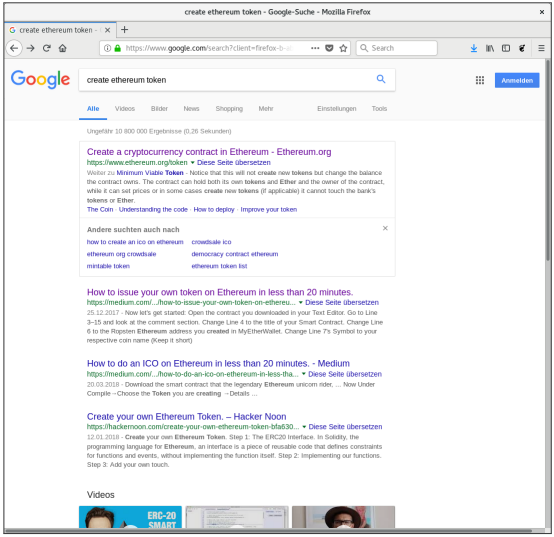
How Does a Token System Work ?



How Does a Token System Work ?



What Does It Take to Create a Token System ?



What Does It Take to Create a Token System ?

Create a cryptocurrency contract in Ethereum - Mozilla Firefox

Create a cryptocurrency

https://www.ethereum.org/token

ETHEREUM » Create your own crypto-currency

NEXT

The Coin

We are going to create a digital token. Tokens in the Ethereum ecosystem can represent any fungible tradable good: coins, loyalty points, gold certificates, IOUs, in-game items, etc. Since all tokens implement some basic features in a standard way, this also means that your token will be instantly compatible with the Ethereum wallet and any other client or contract that uses the same standards.

MINIMUM VIABLE TOKEN

The standard token contract can be quite complex. But in essence a very basic token boils down to this:

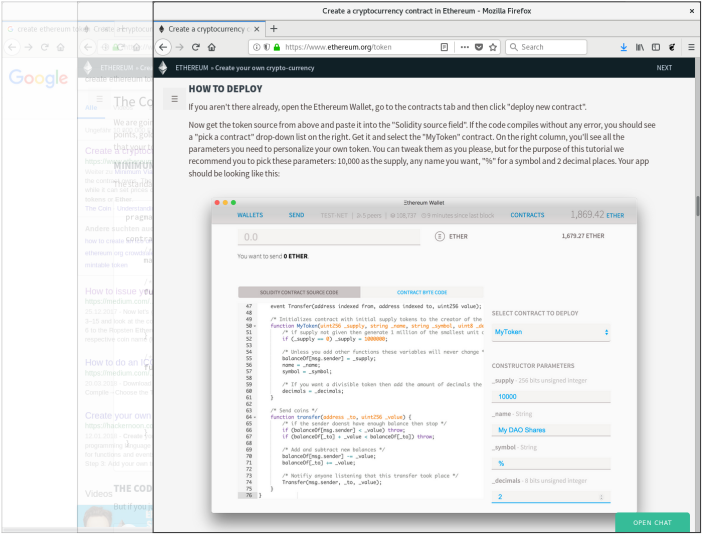
```
pragma solidity ^0.4.20;

contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) public {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) public returns (bool success) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
        return true;
    }
}
```

THE CODE

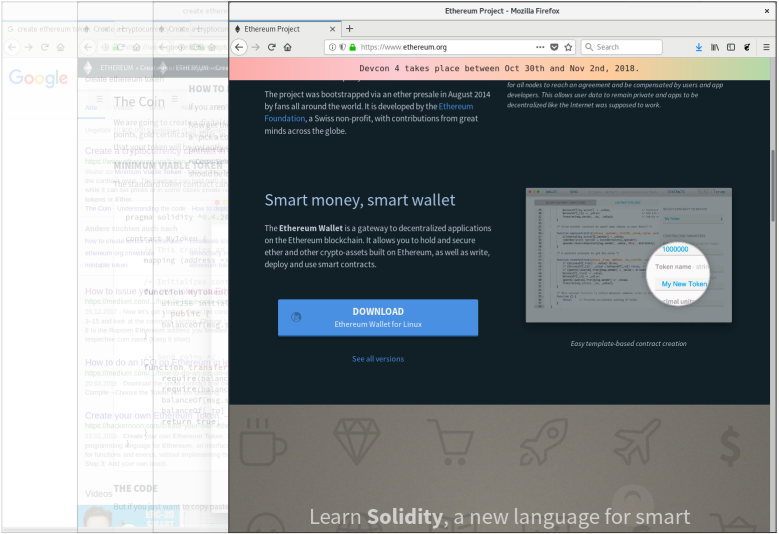
But if you just want to copy paste a more complete code, then use this:

OPEN CHAT

What Does It Take to Create a Token System ?



What Does It Take to Create a Token System ?



What Does It Take to Create a Token System ?

Create a cryptocurrency contract in Ethereum - Mozilla Firefox

Create a cryptocurrency

https://www.ethereum.org/token

Search

ETHEREUM » Create your own crypto-currency

NEXT

The Coin

We are going to create a digital token. Tokens in the Ethereum ecosystem can represent any fungible tradable good: coins, loyalty points, gold certificates, IOUs, in-game items, etc. Since all tokens implement some basic features in a standard way, this also means that your token will be instantly compatible with the Ethereum wallet and any other client or contract that uses the same standards.

MINIMUM VIABLE TOKEN

The standard token contract can be quite complex. But in essence a very basic token boils down to this:

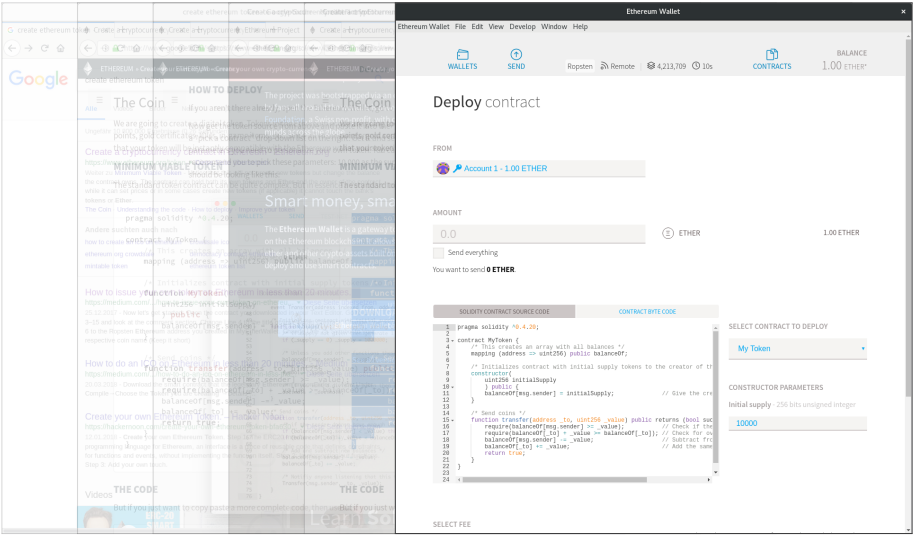
```
pragma solidity ^0.4.20;

contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) public {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) public returns (bool success) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
        return true;
    }
}
```

THE CODE

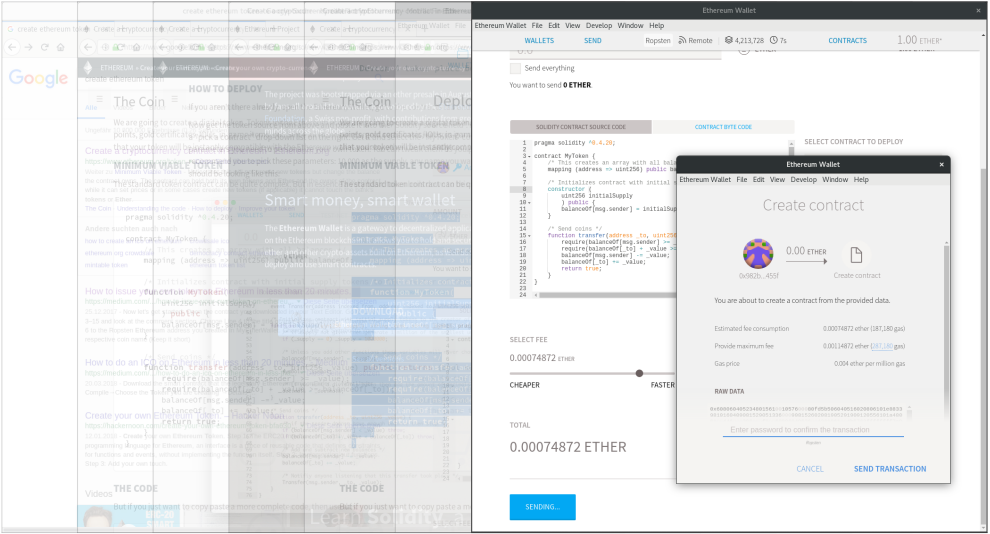
But if you just want to copy paste a more complete code, then use this:

OPEN CHAT

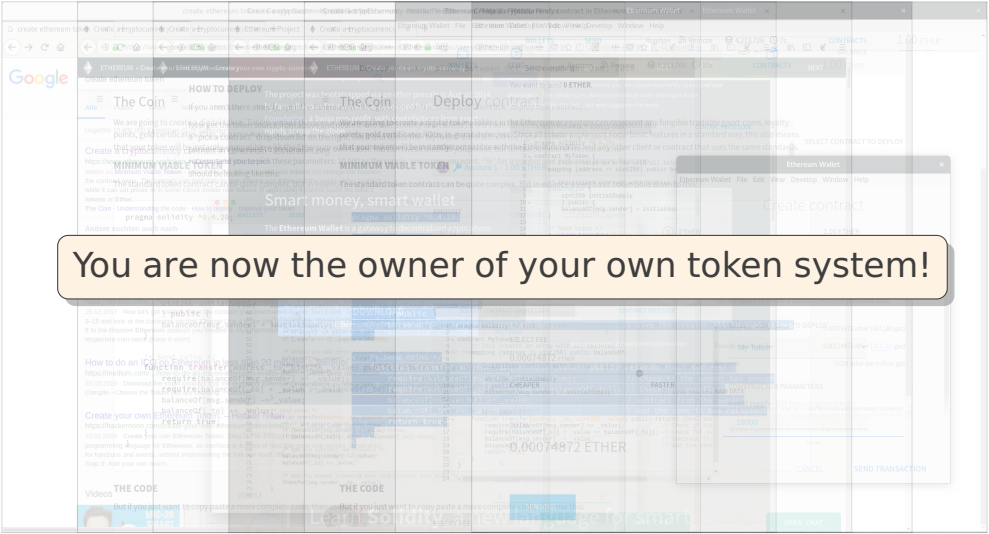
What Does It Take to Create a Token System ?



What Does It Take to Create a Token System ?

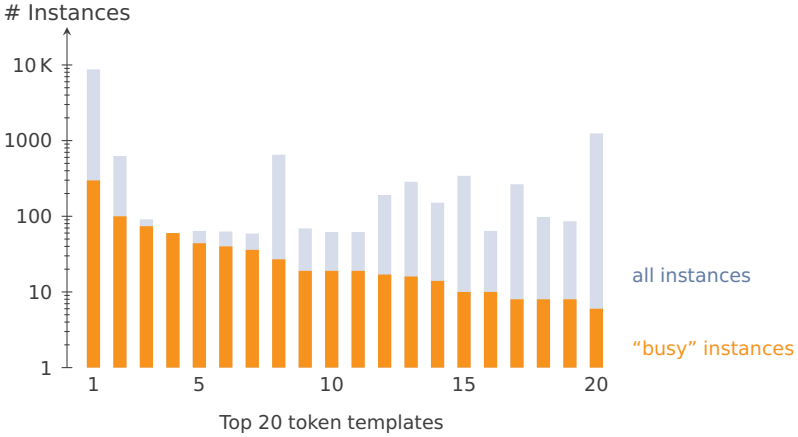


What Does It Take to Create a Token System ?



You are now the owner of your own token system!

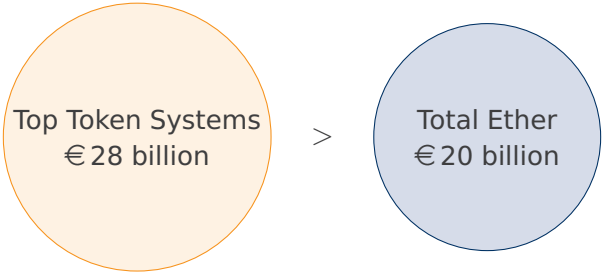
Code Reuse in Ethereum



Source: own research, data until May 30th, 2018

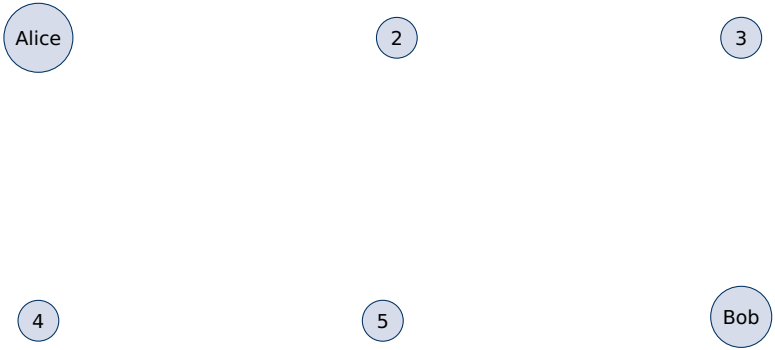
Why Are Token Systems Interesting ?

Market valuation:

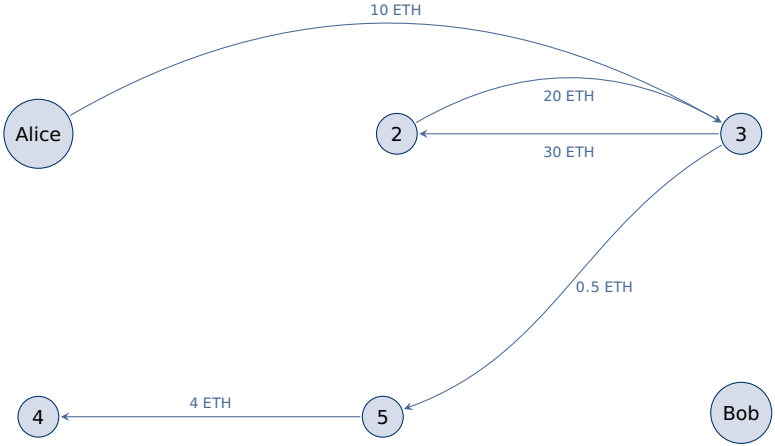


Sources: Etherscan, coinmarketcap.com, October 9th, 2018

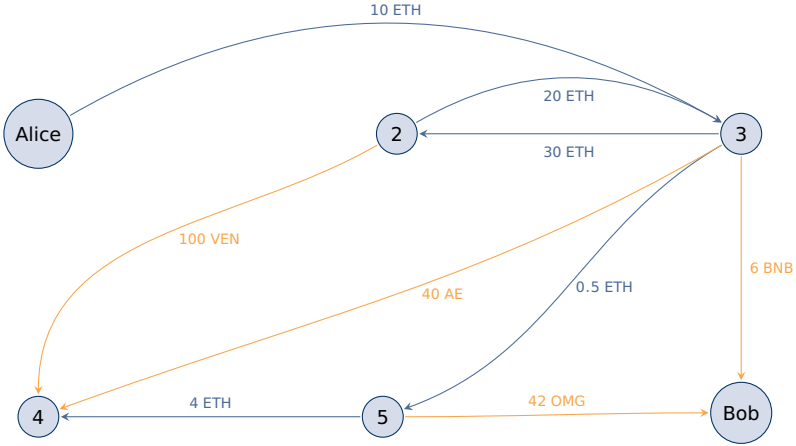
Why Are Token Systems Interesting?



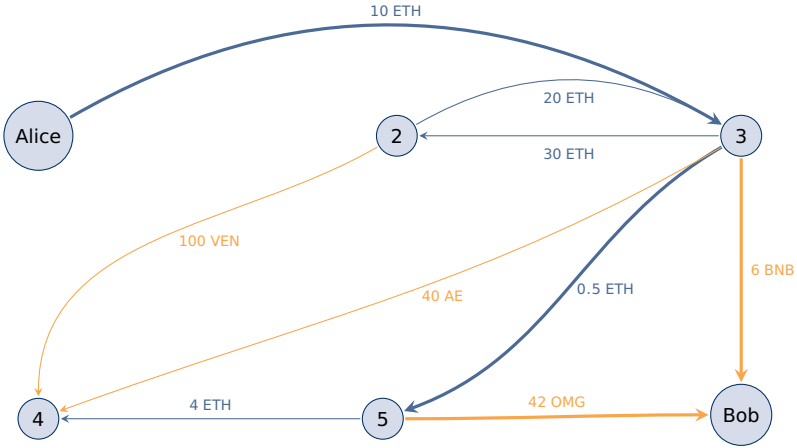
Why Are Token Systems Interesting?



Why Are Token Systems Interesting?



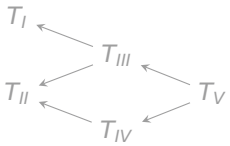
Why Are Token Systems Interesting?



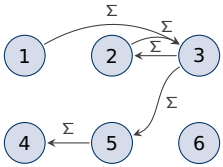
Tracking Payment Flows: From Bitcoin to Ethereum

usefulness

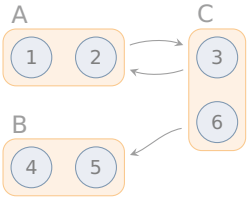
Transaction graph



Address graph



Entity graph



Challenges

Only considering Ether flows gives an incomplete picture.

Challenges

Only considering Ether flows gives an incomplete picture.

Upside:

- Many *CAs* follow standards to make them more observable.

Challenges

Only considering Ether flows gives an incomplete picture.

Upside:

- Many *CAs* follow standards to make them more observable.

Challenges:

- But there is no obligation for *CAs* to be transparent.

Challenges

Only considering Ether flows gives an incomplete picture.

Upside:

- Many *CAs* follow standards to make them more observable.

Challenges:

- But there is no obligation for *CAs* to be transparent.
- Automatic identification of the purpose of a system is a research topic.

Take Home Messages

Privacy was not a design goal of Ethereum

Take Home Messages

Privacy was not a design goal of Ethereum

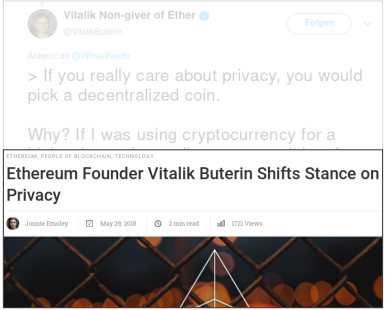
- Identifiers are more sticky than in Bitcoin.

Take Home Messages

Privacy was not a design goal of Ethereum

- Identifiers are more sticky than in Bitcoin.
- Ethereum wallets are built for one identifier per person.

Take Home Messages



Privacy was not a design goal of Ethereum

- Identifiers are more sticky than in Bitcoin.
- Ethereum wallets are built for one identifier per person.
- But there are efforts to improve privacy.

Take Home Messages (cont'd)

Tracking Ether is easy, but . . .

Take Home Messages (cont'd)

Tracking Ether is easy, but . . .

- incomplete.

Take Home Messages (cont'd)

Tracking Ether is easy, but . . .

- incomplete.
- tokens and other services must be considered.

Take Home Messages (cont'd)

Tracking Ether is easy, but . . .

- incomplete.
- tokens and other services must be considered.
- programmers of *CAs* decide what is easily observable.

Take Home Messages (cont'd)

Tracking Ether is easy, but . . .

- incomplete.
- tokens and other services must be considered.
- programmers of *CAs* decide what is easily observable.
- we lack adequate tools for investigations and monitoring.

Take Home Messages (cont'd)

Why should regulators care?

Ethereums is not criminals' first choice. But ...

Take Home Messages (cont'd)

Why should regulators care?

Ethereums is not criminals' first choice. But ...

- everyone can issue their own financial products. $\rightarrow$ Security regulation

Take Home Messages (cont'd)

Why should regulators care?

Ethereums is not criminals' first choice. But ...

- everyone can issue their own financial products. → Security regulation
- there are shady services and business practices. → Consumer protection

Take Home Messages (cont'd)

Why should regulators care?

Ethereums is not criminals' first choice. But ...

- everyone can issue their own financial products. → Security regulation
- there are shady services and business practices. → Consumer protection

Ethereum is relevant and different.

Regulators who take Bitcoin as a model may **miss** important aspects.

universität innsbruck

Tracking Payment Flows in Ethereum

Thank you for your attention

Michael Fröwis · michael.froewis@uibk.ac.at

Fungible vs. Non-fungible

Asset

Fungible

Non-fungible