Ethereum, Smart-contracts, Swarm, Web 3.0

Viktor Tron and Aron Fischer

September 1, 2016

Outline

What is ethereum?

What is ethereum?

Ethereum is a (simulated) global computer

What is ethereum?

Ethereum is a (simulated) global computer

- Anyone can access it

What is ethereum?

Ethereum is a (simulated) global computer

- Anyone can access it
- It is tamper proof

What is ethereum?

Ethereum is a (simulated) global computer

- Anyone can access it
- It is tamper proof
- No single entity can stop it, censor it, control it.

What are “smart contracts”?

What are "smart contracts"?

So-called "smart contracts" are programs running on the ethereum computer.

So why are they called smart contracts?

A toy example

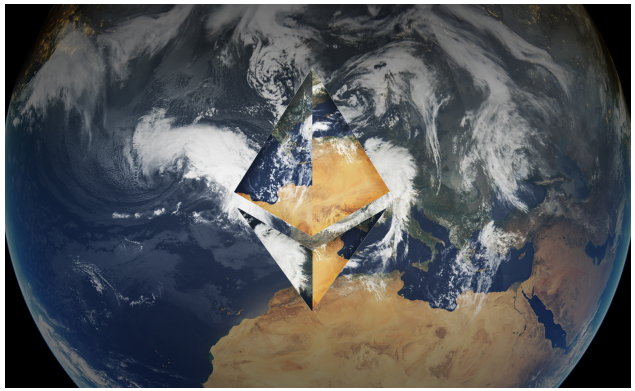
Let us pretend that the city of Amsterdam

A toy example

Let us pretend that the city of Amsterdam decides to move its land-registry database from the basement of city hall (I imagine)

A toy example

Let us pretend that the city of Amsterdam decides to move its land-registry database from the basement of city hall to the ethereum world computer.



A toy example

Let us pretend that the city of Amsterdam decides to move its land-registry database from the basement of city hall to the ethereum world computer.
I put money (Ether) in a smart contract that says the following:

A toy example

Let us pretend that the city of Amsterdam decides to move its land-registry database from the basement of city hall to the ethereum world computer.
I put money (Ether) in a smart contract that says the following: If the ownership of this **apartment is transferred to me** (i.e. the land registry updates to show it as mine),

A toy example

Let us pretend that the city of Amsterdam decides to move its land-registry database from the basement of city hall to the ethereum world computer.
I put money (Ether) in a smart contract that says the following: If the ownership of this apartment is transferred to me (i.e. the land registry updates to show it as mine), then **transfer all the money to you** (the previous owner).

So?

What's so special about that?

Why are smart contracts special?

The contract is self enforcing.

Why are smart contracts special?

The contract is self enforcing.
The money will be transferred if and only if the ownership of the apartment changes. In fact it is the transfer of ownership (as represented in the land registry) that releases the payment.

Why are smart contracts special?

The contract is self enforcing.
The money will be transferred if and only if the ownership of the apartment changes. In fact it is the transfer of ownership (as represented in the land registry) that releases the payment.
There is no need for a notary to hold on to the money (escrow) – the contract itself can act as the trusted third pary.

What else can we do?

For a start, anything that only really involves maintaining a database according to some rulues:

What else can we do?

For a start, anything that only really involves maintaining a database according to some rulues:

- Domain Name System

What else can we do?

For a start, anything that only really involves maintaining a database according to some rulues:

- Domain Name System
- Money and bank accounts

What else can we do?

For a start, anything that only really involves maintaining a database according to some rulues:

- Domain Name System
- Money and bank accounts
- Land registry
- ...

Also popular are interactions requiring only basic logic:

What else can we do?

For a start, anything that only really involves maintaining a database according to some rulues:

- Domain Name System
- Money and bank accounts
- Land registry
- ...

Also popular are interactions requiring only basic logic:

- Gambling and Betting

What else can we do?

For a start, anything that only really involves maintaining a database according to some rulues:

- Domain Name System
- Money and bank accounts
- Land registry
- ...

Also popular are interactions requiring only basic logic:

- Gambling and Betting
- Financial derivatives

What else can we do?

For a start, anything that only really involves maintaining a database according to some rulues:

- Domain Name System
- Money and bank accounts
- Land registry
- ...

Also popular are interactions requiring only basic logic:

- Gambling and Betting
- Financial derivatives
- "Fair" pyramid and Ponzi schemes

Outline

Intrade and Augur

The intrade / Augur story
the story of intrade (centralisation problem) the story of augur (decentralised oracle)

bylaws on-chain

We can imagine a company encoding all of its corporate bylaws into smart contracts.
For example the rules could say:

bylaws on-chain

We can imagine a company encoding all of its corporate bylaws into smart contracts.
For example the rules could say:

- only the **treasurer** can propose spending

bylaws on-chain

We can imagine a company encoding all of its corporate bylaws into smart contracts.
For example the rules could say:

- only the treasurer can propose spending
- the proposed spending **can only happen if** 3 board members agree...

bylaws on-chain

We can imagine a company encoding all of its corporate bylaws into smart contracts.
For example the rules could say:

- only the treasurer can propose spending
- the proposed spending can only happen if 3 board members agree...
- ...**unless** it is more than 1000 Ether, in which case two-thirds must agree.

bylaws on-chain

We can imagine a company encoding all of its corporate bylaws into smart contracts.
For example the rules could say:

- only the treasurer can propose spending
- the proposed spending can only happen if 3 board members agree...
- ...unless it is more than 1000 Ether, in which case two-thirds must agree.
- There will be an **election** for treasurer **every year** on 1st September.

bylaws on-chain

We can imagine a company encoding all of its corporate bylaws into smart contracts.
For example the rules could say:

- only the treasurer can propose spending
- the proposed spending can only happen if 3 board members agree...
- ...unless it is more than 1000 Ether, in which case two-thirds must agree.
- There will be an election for treasurer every year on 1st September.

...and so on. Can be arbitrarily complex. It's up to you.

Benefits:

When doing things this way, you are protected from some forms of corruption and you do not have to rely on weak legal systems to enforce the laws for you.

Benefits:

When doing things this way, you are protected from some forms of corruption and you do not have to rely on weak legal systems to enforce the laws for you.

Lesson:

smart contracts are stubborn.

Benefits:

When doing things this way, you are protected from some forms of corruption and you do not have to rely on weak legal systems to enforce the laws for you.

Lesson:

smart contracts are stubborn.

This means that they will execute as written.

Benefits:

When doing things this way, you are protected from some forms of corruption and you do not have to rely on weak legal systems to enforce the laws for you.

Lesson:

smart contracts are stubborn.

This means that they will execute as written. If you encode term limits, there will be term limits(*),

Benefits:

When doing things this way, you are protected from some forms of corruption and you do not have to rely on weak legal systems to enforce the laws for you.

Lesson:

smart contracts are stubborn.

This means that they will execute as written. If you encode term limits, there will be term limits(*), if you code for monthly elections there absolutely will be monthly elections.

Copyright the right way?

can the act of listening to music be paired with automatic payments to the correct people?
smart contract payment splits? yes. music on blockchain? no.

We need to look at how this all works under the hood.

Outline

Blockchain

Blockchain and POW

Ethereum is Turing complete

turing completeness – generic blockchain tech.

Swarm

swarm as a storage layer and as a CDN
data storage and distribution is (has to be) off-chain, but with close integration into blockchain we can use smart contracts to regulate what happens (eg SWINDLE litigation engine)

Outline

Web3

The Web3 Vision