

Ethereum, Smart-contracts, Swarm, Web 3.0

Viktor Tron and Aron Fischer

September 2, 2016

1 Introductory remarks

- What is ethereum?
- What are “smart contracts”?
- An example.
- What else is there?

2 Real-world examples

- The story of Intrade and Augur
- Corporate bylaws
- Crowdfunding
- A story about copyright and DRM

3 A brief tour of the technology

- The blockchain and proof-of-work
- Turing-completeness
- Swarm

4 The Web3 Vision

Outline

1 Introductory remarks

- What is ethereum?
- What are “smart contracts”?
- An example.
- What else is there?

2 Real-world examples

3 A brief tour of the technology

4 The Web3 Vision

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



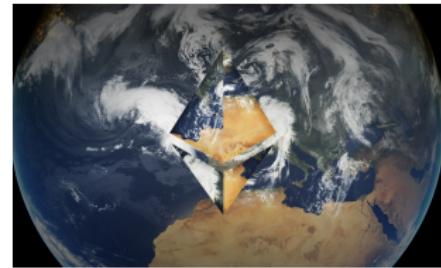
A toy example

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 party.

What else can we do?

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

What else can we do?

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

- Domain Name System

What else can we do?

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

- 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 rules:

- 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 rules:

- 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 rules:

- 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 rules:

- 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

1 Introductory remarks

2 Real-world examples

- The story of Intrade and Augur
- Corporate bylaws
- Crowdfunding
- A story about copyright and DRM

3 A brief tour of the technology

4 The Web3 Vision

Intrade and Augur

Let me tell you the story of Intrade and Augur

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.

Crowdfunding and so on...

This technology allows people to **cooperate** and **coordinate** without needing to trust each other. People can pool resources and work towards common goals.

- Crowdfunding
- Voting and collective decision making.
- Governance and resource management.

Because the *logic* and the *value* (currency) live on the same platform, incentives can be neatly modulated towards some goal.

Copyright the right way?

The story of micropayments.

Copyright the right way?

The story of micropayments.

Question

Can we combine the act of listening to music with automatic (micro-)payments to the correct people?

Copyright the right way?

The story of micropayments.

Question

Can we combine the act of listening to music with automatic (micro-)payments to the correct people?

- Payment-split: when paying for a song the money is channeled to *all* the right people?

Copyright the right way?

The story of micropayments.

Question

Can we combine the act of listening to music with automatic (micro-)payments to the correct people?

- Payment-split: when paying for a song the money is channeled to *all* the right people? **Yes.**

Copyright the right way?

The story of micropayments.

Question

Can we combine the act of listening to music with automatic (micro-)payments to the correct people?

- Payment-split: when paying for a song the money is channeled to *all* the right people? **Yes.**
- Paying for every single listen?

Copyright the right way?

The story of micropayments.

Question

Can we combine the act of listening to music with automatic (micro-)payments to the correct people?

- Payment-split: when paying for a song the money is channeled to *all* the right people? **Yes.**
- Paying for every single listen? **No.** Scalability issues.

Copyright the right way?

The story of micropayments.

Question

Can we combine the act of listening to music with automatic (micro-)payments to the correct people?

- Payment-split: when paying for a song the money is channeled to *all* the right people? **Yes.**
- Paying for every single listen? **No.** Scalability issues.
- Music file storage and distribution on ethereum blockchain?

Copyright the right way?

The story of micropayments.

Question

Can we combine the act of listening to music with automatic (micro-)payments to the correct people?

- Payment-split: when paying for a song the money is channeled to *all* the right people? **Yes.**
- Paying for every single listen? **No.** Scalability issues.
- Music file storage and distribution on ethereum blockchain? **No!** Ethereum may be a global computer, but it is slow and expensive. Good for smart contracts but not for data storage.

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

Outline

1 Introductory remarks

2 Real-world examples

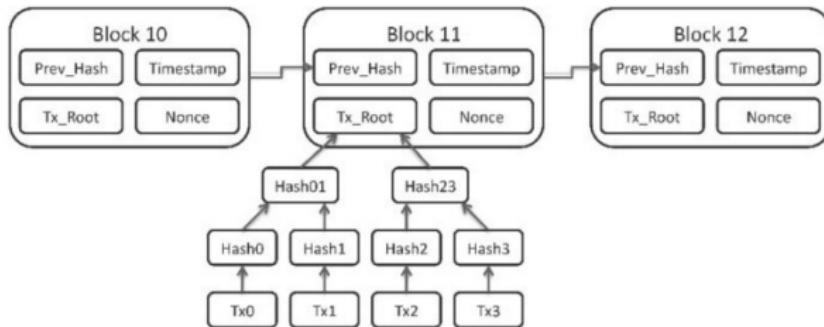
3 A brief tour of the technology

- The blockchain and proof-of-work
- Turing-completeness
- Swarm

4 The Web3 Vision

Blockchain and proof-of-work

Blockchain Diagram

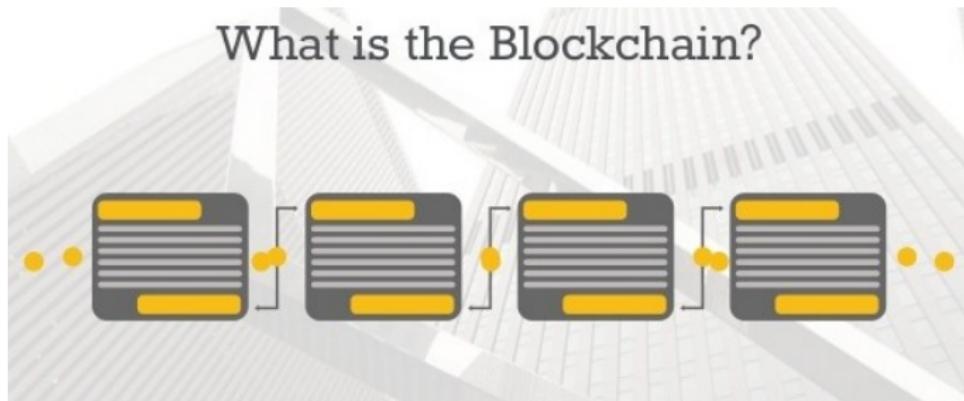


By Matthäus Wander (Own work) [CC-BY-SA-3.0 (<http://creativecommons.org/licenses/by-sa/3.0>)], via Wikimedia Commons

http://commons.wikimedia.org/wiki/File%3ABitcoin_Block_Data.svg

Blockchain and proof-of-work

What is the Blockchain?



Ethereum is Turing complete

Ethereum is *the* general purpose blockchain.

Q: What information is stored in the blockchain?

Bitcoin Account balances

Litecoin Account balances

Dogecoin Account balances

Ethereum Data of any complexity

Ethereum is Turing complete

Ethereum is *the* general purpose blockchain.

Q: What is contained in the transactions?

Bitcoin Transfer

Litecoin Transfer

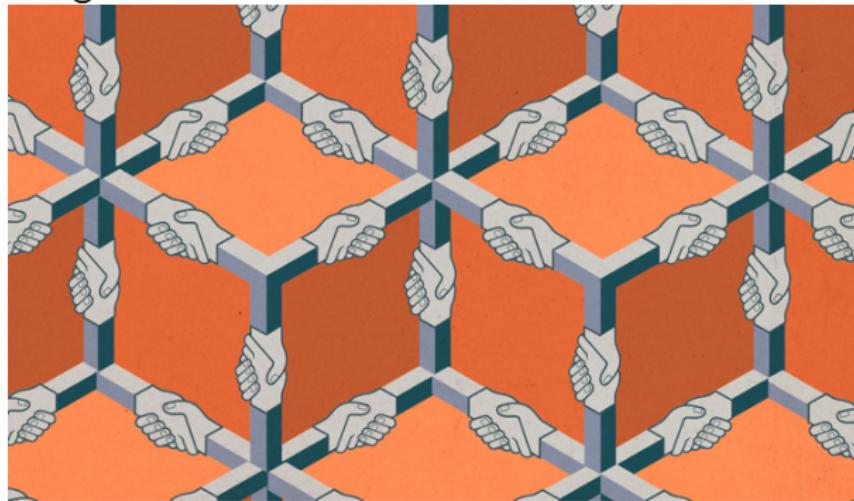
Dogecoin Transfer

Ethereum Computation of arbitrary(*) complexity

So what about movies? music? chat? email?

Swarm

Swarm is a peer-to-peer file storage and distribution network integrated with ethereum.



Outline

- 1 Introductory remarks
- 2 Real-world examples
- 3 A brief tour of the technology
- 4 The Web3 Vision

The ethereum ecosystem



ethereum



swarm



whisper

Web3

