

Smart contracts

A simple “smart contract”

AXA Is Using Ethereum's Blockchain for a New Flight Insurance Product

Sep 13, 2017 at 17:50 UTC by Stan Higgins

French insurance giant AXA has launched a new flight delay insurance product that uses the public ethereum blockchain to store and process payouts.

The product, called [Fizzy](#), is being pitched as a "smart insurance" tool that flyers can use to insure their trips if their flight is delayed by two hours or more. As such, the product makes notable use of smart contracts, self-executing piece of code that triggers once certain conditions are met on a blockchain.

According to AXA, ethereum's public blockchain plays two key roles here. It maintains an accessible record of the insurance contract itself within a [smart contract](#), and serves as a mechanism for triggering the payment to the client once the two-hour mark is passed.

AXA representative Jean-Baptiste Mounier told CoinDesk in an email:

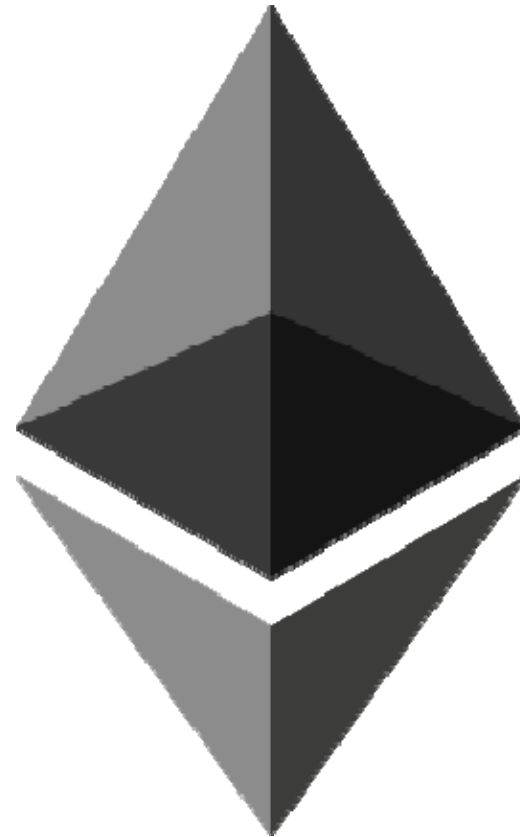
"The smart contract is the party that decides whether or not we should indemnify the policy holder and triggers a payment request to our system. The use of a smart contract to trigger claims will add trust in the insurer / policy holder relationship."

Vitalik Buterin and Ethereum



Ethereum

- Built as a “Turing complete” blockchain that can execute contingent instructions
 - Intended use: smart contracts
- Native Ether currency functions as “gas” to pay mining fees for contract execution
- Complex method for determining new supply, based on use and depletion of prior tokens, and limited to 18 million per year.
- Governance is nominally decentralized, but continues to be dominated by founder.
 - Transitioning to proof-of-state mining



Smart contracts: Szabo (1997)

<http://ojphi.org/ojs/index.php/fm/article/view/548/469>

- “The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive. . .”



Nick Szabo

Example:

Two ways to purchase a coke



or



The vending machine was introduced in London in 1883.

What can go wrong with the soda jerk?

- Adds cost
- Agency problems
 - May work too slowly
 - May put in too much ice
 - May make incorrect change
 - May steal from the cash register
 - Will want to be tipped
- Sabotage
 - May discriminate against certain customers
 - May pretend you did not pay
- Etc.



What problems can smart contracts solve?

- Guaranteeing specific performance
 - Is this always a good idea?
- Economizing on contracting costs
- Economizing on enforcement costs
- Deterring strategic behavior
- *Removing the need for trust*

Some important points

- Smart contracts have existed for many years
 - Often involving automated payments
- They do not require blockchains
- However, blockchains open up much more complex possibilities

Example: Recurring monthly mortgage payment



or

Transfers requested before 8:00 p.m. Eastern Time on a business day will be processed on the same day.

Step 1 of 3: Enter Information [Help](#)

From:

To:

* Amount: \$

* Date:

* How Often:

* Total Number of Transfers:

Example: If you select quarterly for How Often, and a total number of 4, the transfer will be made every quarter for the next year from the Transfer Date.

* Required Fields.

- One-Time
- Daily
- Weekly
- Every 14 Days
- Monthly
- Every 2 Months
- Quarterly
- Semi-Annually
- Annually

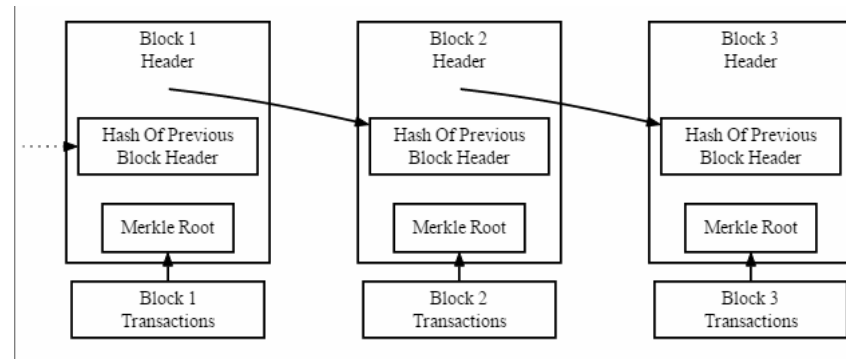
Problems solved by recurring payment

- Quicker / cheaper / more reliable
- Opting in by the customer indicates stable income, enabling bank to cut interest rate

Smart contracts in consumer finance: auto loans



Now



Future

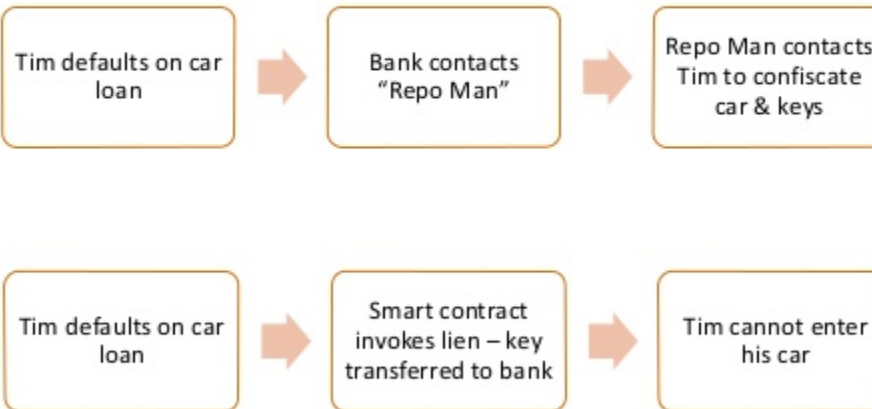
- Ownership and title will be tracked on a blockchain

<https://www.youtube.com/watch?v=IgNfoQQ5Reg>

<https://www.youtube.com/watch?v=2rLNbd6MQXg>

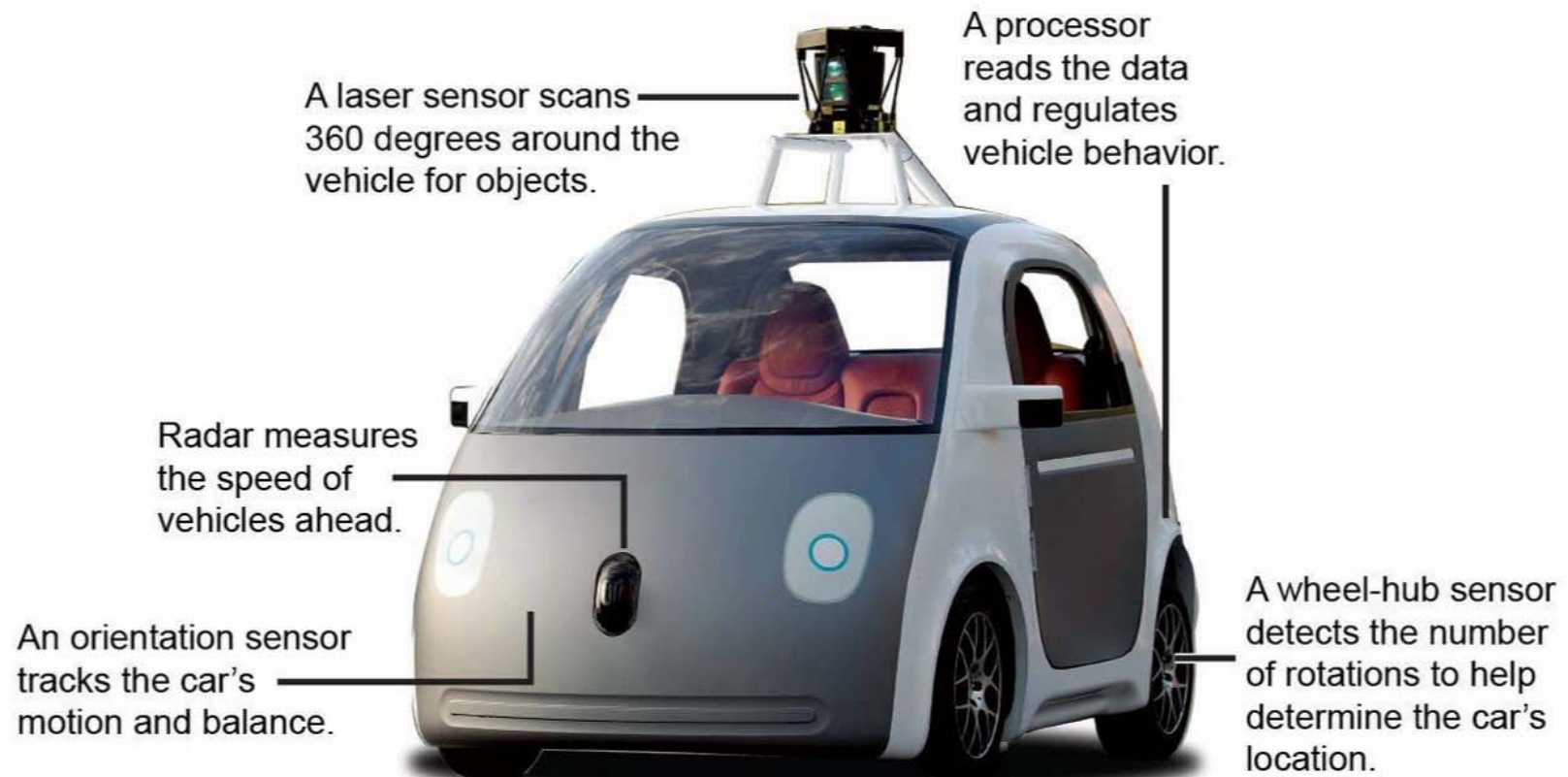
Smart contracts in consumer finance: auto loans

Smart Contracts on Car



<https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/>

Smart contracts in consumer finance: Internet of Things



Source: Google

Raoul Rañoa / @latimesgraphics

Smart contracts in consumer finance: Internet of Things



- Devices will provide real-time driver coaching and feedback
 - to law enforcement
 - to insurance company

Smart contracts in consumer finance: auto insurance



- Self-driving cars have 90% fewer accidents, so they probably need 90% less insurance.

Blockchain Insurance Industry Initiative



Some weaknesses of Ethereum

- No clear concept of “time.”
 - Time is measured in blocks
- Contracts might “run out of gas” while executing
- Need to consult an “oracle” for external data
 - The oracle might be vulnerable to hacking or operational failure

TheDAO

June 16, 2016

ETHEREUM DROPS 33% AS DAO DEBACLE CONTINUES

📅 June 17, 2016



Ethereum has lost more than a third of its value after it was reported earlier today that the DAO has suffered a \$50 Million hack attack.

Ethereum exchange Kraken has suspended payouts of Ethereum after an appeal of the Ethereum foundation, a Swiss organisation controlled by Ethereum founders.

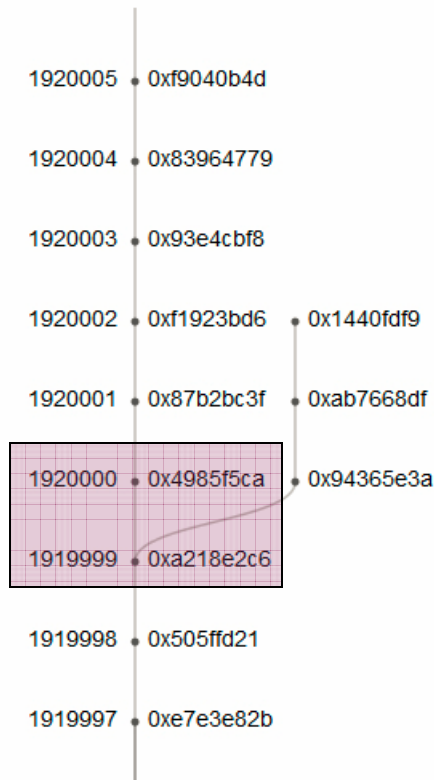
Possible action by the group controlling Ethereum has sparked a heated debate, as reported by Coindesk.

Key stakeholders behind the alternative blockchain platform ethereum are debating changes to the platform's code after millions of dollars in ether were diverted from a major project by an alleged attacker.

Full story: – <http://www.coindesk.com/will-ethereum-hard-fork/>

Ethereum's hard fork

July 20, 2016



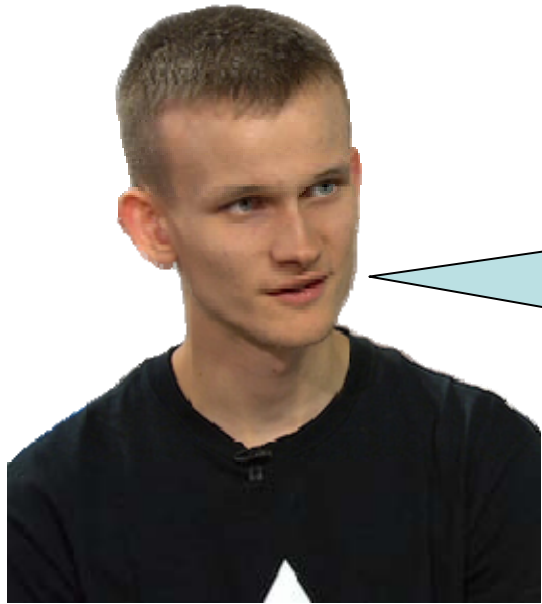
The “hard fork” re-started the Ethereum blockchain at block 1920000.

About 15% of miners refused to participate, continuing to work on the “Ethereum classic” blockchain.

A schism has now existed for almost one year

Intervention by a blockchain sponsor: a terrible precedent?

- Two “impossible” things have occurred
 - History rewritten on a blockchain
 - Smart contract pre-empted by human intervention
- Who has the authority to do this?
- What are the criteria?
- Should an entire platform stop for one bad contract?
- Are the victims eligible for compensation?
- What regulations or laws apply?



“Some bitcoin users see the hard fork as in some ways violating their most fundamental values. I personally think these fundamental values, pushed to such extremes, are silly.”



E. Gün Sirer
Whistleblower



Christoph Jentzsch
Programmer



0xF35e2cC8E6523d683eD44870f5B7cC785051a77D

Different views of TheDAO intruder

- A thief
who was ultimately outsmarted by Buterin
- A smart programmer who played by the rules and won big
and then became a victim of a theft via Buterin's hard fork
- A philosopher and provocateur, or
A public servant / whistleblower
who provided a much-needed object lesson