Smart Contracts

By Omid Malekan

What the Hell is a Smart Contract?

An agreement between different parties, executed in real time on a blockchain, in a manner that is guaranteed to satisfy all those who agreed to its terms.

-My definition

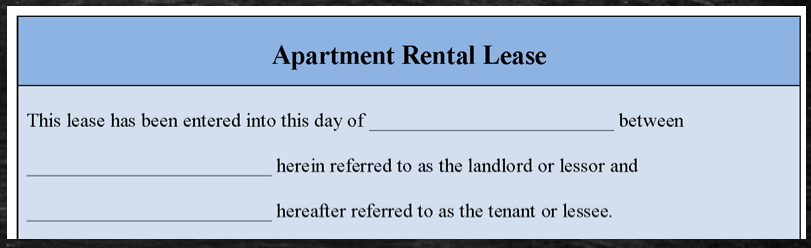
Traditional Contract

A written or spoken agreement, especially one concerning employment, sales, or tenancy, that is intended to be enforceable by law.

-Dictionary.com

Existing Contracts

- Lease on an apartment
- Purchase agreement
- Service agreement
- Insurance
- Bet on a sporting a event
- Peace treaty


Apartment Rental Lease

This lease has been entered into this day of _____ between

_____ herein referred to as the landlord or lessor and

_____ hereafter referred to as the tenant or lessee.


MGM GRAND

64305-EBFF-4E1B

$10.00 Straight Bet

ODDS TO WIN THE 2012 MASTERS

5851 L OOSTHUIZEN

100/1 MLB

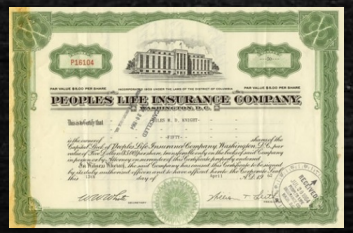
Event Date 4/8/12

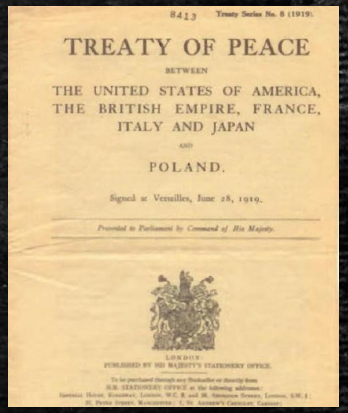
Win $1,000.00 to pay $1,010.00

Ticket Cost $10.00

0B02B WG08612 Book 140ct2011 11:57:03

64305-EBFF-4E1B


PEOPLES LIFE INSURANCE COMPANY


8413 Treaty Series No. 8 (1919).

TREATY OF PEACE

BETWEEN

THE UNITED STATES OF AMERICA, THE BRITISH EMPIRE, FRANCE, ITALY AND JAPAN

AND

POLAND.

Signed at Versailles, June 28, 1919.

Presented to Parliament by Command of His Majesty.

LONDON:

PUBLISHED BY HIS MAJESTY'S STATIONERY OFFICE.

Smart vs. Dumb

	Traditional Contract	Smart Contract
Language	Legalese	Computer code
Enforcement	After the fact	Real-time
Enforcer	Third-party	Blockchain
Nature	Centralized	Decentralized

Blockchain

- "A decentralized and distributed ledger of transactions "

  - *standard definition*

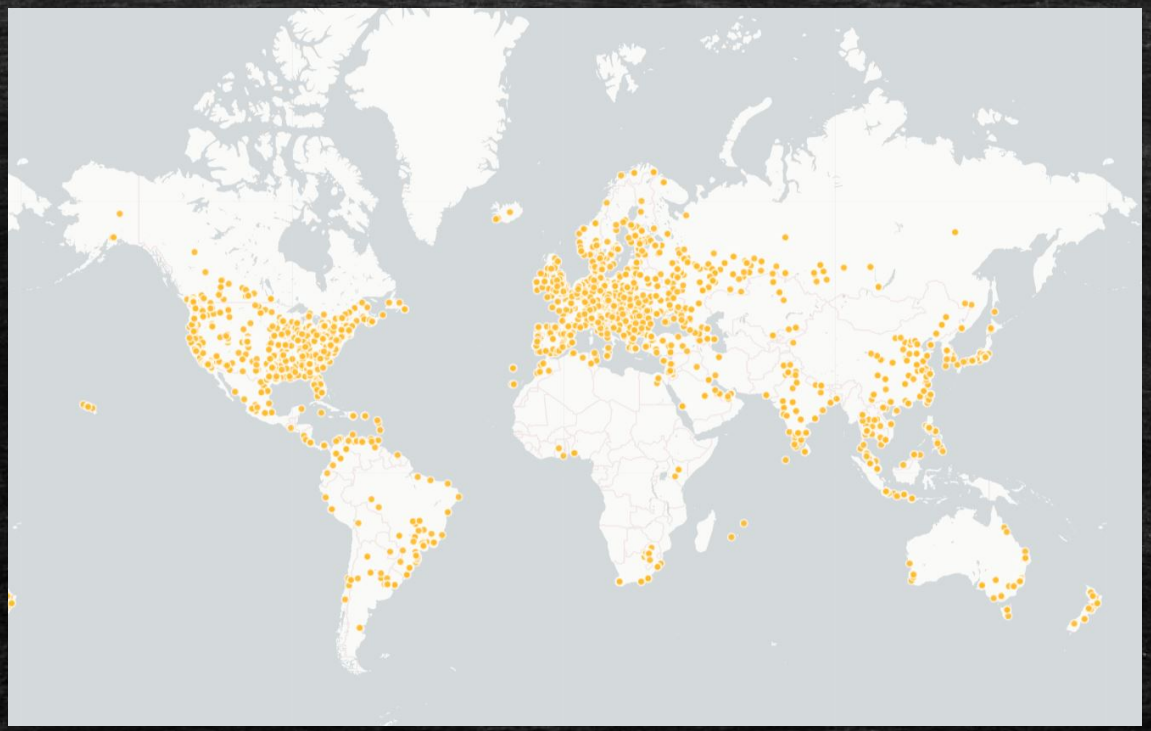
- "A technology that allows for a digital item to exist in only one place at any given moment in time"

  - my definition

- A global computer that nobody owns or controls

  - alternate definition

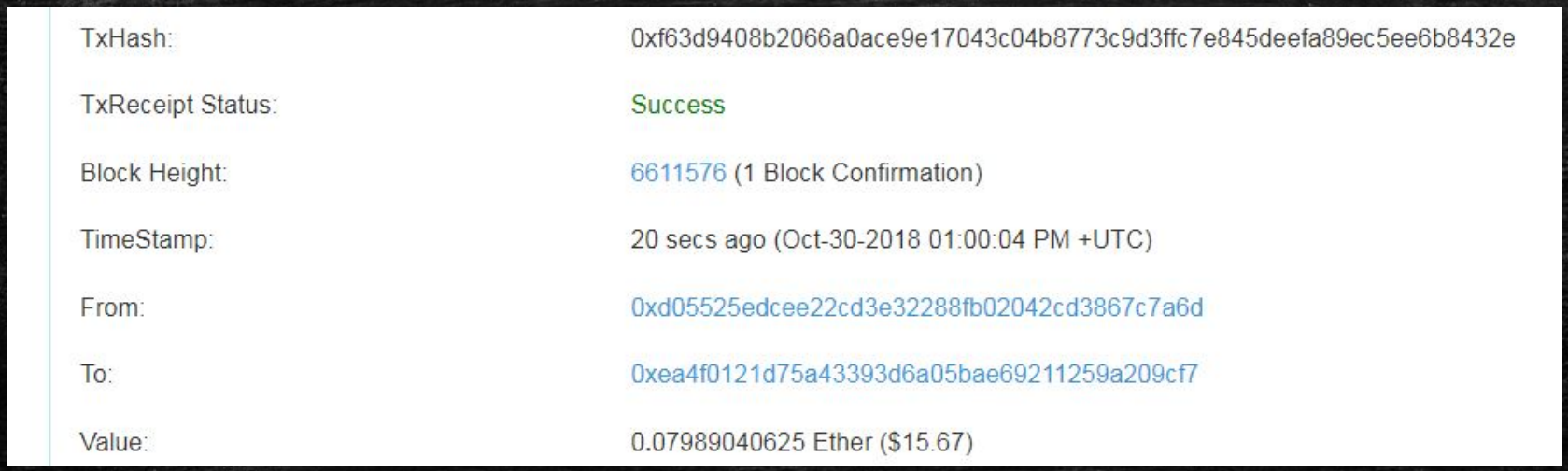
Ethereum



Simplest Use Case

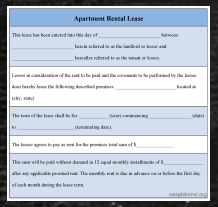
- Payments:

  " Laurel pays Sophie 1 Ether"



TxHash:	0xf63d9408b2066a0ace9e17043c04b8773c9d3ffc7e845deefa89ec5ee6b8432e
TxReceipt Status:	Success
Block Height:	6611576 (1 Block Confirmation)
TimeStamp:	20 secs ago (Oct-30-2018 01:00:04 PM +UTC)
From:	0xd05525edcee22cd3e32288fb02042cd3867c7a6d
To:	0xea4f0121d75a43393d6a05bae69211259a209cf7
Value:	0.07989040625 Ether ($15.67)

Contracts Result in Payments


Apartment Rental Lease

This lease has been entered into this day of _____ between _____ herein referred to as the landlord or lessor and _____ hereafter referred to as the tenant or lessee.

Tenant pays landlord $1000 on the 1st of each month


PEOPLES LIFE INSURANCE COMPANY

Insurance company pays client $5000 after hurricane


MGM GRAND
64305-EBFF-4E1B
$10.00 Straight Bet
ODDS TO WIN THE 2012 MASTERS
5851 L OOSTHUIZEN
100/1 MLB
Event Date 4/6/12
Win $1,000.00 To pay $1,010.00
Ticket Cost $10.00
14Oct2011 11:57:03
64305-EBFF-4E1B

Casino pays $50 to winner of a bet

Conditional Payments

1. Pay Sophie 1 Ether
2. Pay Sophie 1 Ether, on Tuesday
3. Pay Sophie 1 Ether, on Tuesday, if the Mets win.

A blockchain that can handle conditional payments turns dumb contracts into smart ones

Smart Contract

An agreement between different parties, executed in real time on a blockchain, in a manner that is guaranteed to satisfy all those who agreed to its terms.

-My definition

Current Setup

Downside of Centralization

- Expensive
- Inefficient
- Fragile
- Censorable

Blockchain

- "A technology that creates trust where it wouldn't otherwise exist, without the involvement of a central authority"

- *another definition*

Smart Contract

An agreement between different parties, executed in real time on a blockchain, in a manner that is guaranteed to satisfy all those who agreed to its terms.

-My definition

Justice

Justice

Ethereum Definition

"In a contract account, every time the contract account receives a message its code activates, allowing it to read and write to internal storage and send other messages or create contracts in turn.

Note that "contracts" in Ethereum should not be seen as something that should be "fulfilled" or "complied with"; rather, they are more like "autonomous agents" that live inside of the Ethereum execution environment, always executing a specific piece of code when "poked" by a message or transaction, and having direct control over their own ether balance and their own key/value store to keep track of persistent variables."

Example: Augur

augur

Political Forecasting

Turn political knowledge into predictive power by trading on the outcome of upcoming elections, potential policy decisions, and other political events.

Event Hedging

Hedge against catastrophic events like natural disasters, market crashes, and geopolitical upheaval by betting that the event will occur.

Weather Prediction

Harness the power of crowds to create a more accurate weather prediction tool for events like hurricane landfalls, heat waves, and daily temperature averages.

Company Forecasting

Companies can use Augur to guide decision making by forecasting vital information such as total product sales and project completion times.

Example: Augur

Which party will control the House after 2018 U.S. Midterm Election?

Activity

Volume: $808,826.05 **Open Interest:** $728,945.06 **Last Traded:** 21 minutes ago

Fee: 0.01% **Ends:** Dec 10, 2018 11:00 PM (UTC-0500)

Outcomes

Prediction:	Volume:	Qty:	Bid:	Ask:	Qty:	Last:
65% Democrats	$640,845.56	1	0.6	0.65	2.9	0.65
Prediction:	**Volume:**	**Qty:**	**Bid:**	**Ask:**	**Qty:**	**Last:**
38% Republicans	$164,461.20	2	0.36	0.38	18	0.38
Prediction:	**Volume:**	**Qty:**	**Bid:**	**Ask:**	**Qty:**	**Last:**
1% Tied	$3,519.29	5.214	0.01	0.04	1	0.01

Other Details

Resolution Source: None

Market Type: Categorical **Reporting State:** Pre-Reporting **Last Trade Block:** 6660198

Author: 0xc64e96319366da7d00ef4bc14b42e8b1f3a31f52

Created: Jul 15, 2018 3:54 PM (UTC-0400) **Creation Block:** 5970620

Designated Reporter: 0xc64e96319366da7d00ef4bc14b42e8b1f3a31f52

Designated Reporter Stake: 0.35 REP

Universe: 0xe991247b78f937d7b69cfc00f1a487a293557677

Creator Mailbox: 0x90a80c4cc0e86e285a9cba6fb2bc47f9e454cc3f

Creator Mailbox Owner: 0xc64e96319366da7d00ef4bc14b42e8b1f3a31f52

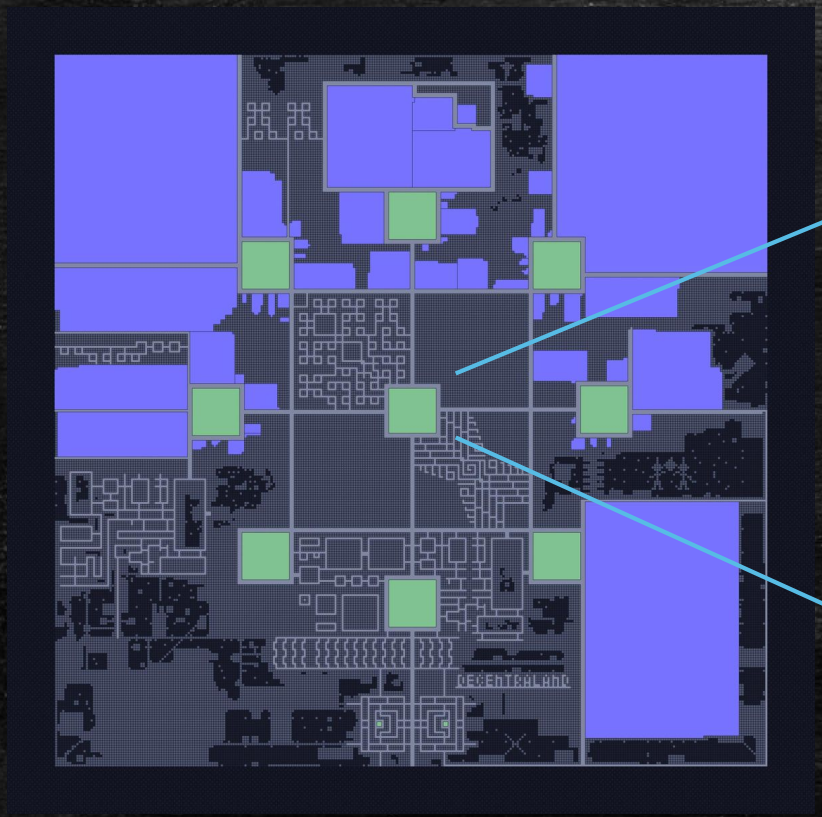
Market Contract: 0xbbbc0a8baa03535e0a680ee2f057162aaaafd570

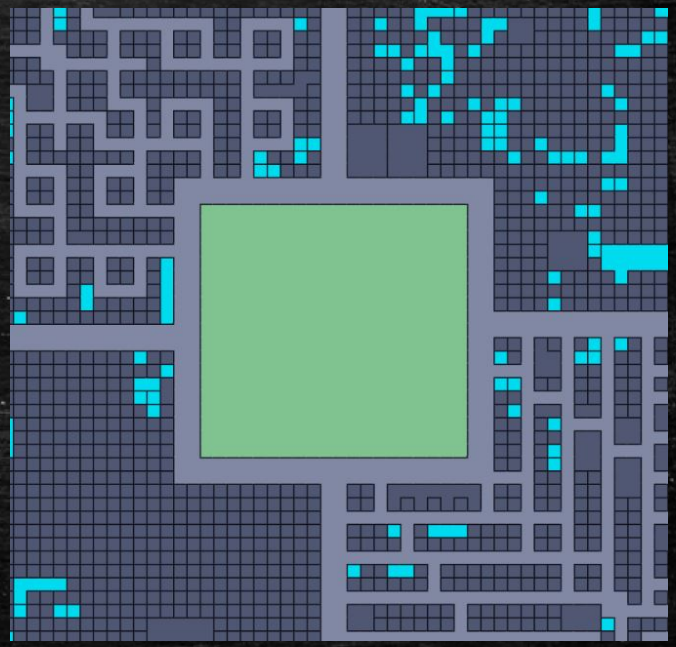
Blockchain

- "A technology that gives physical properties to digital items"

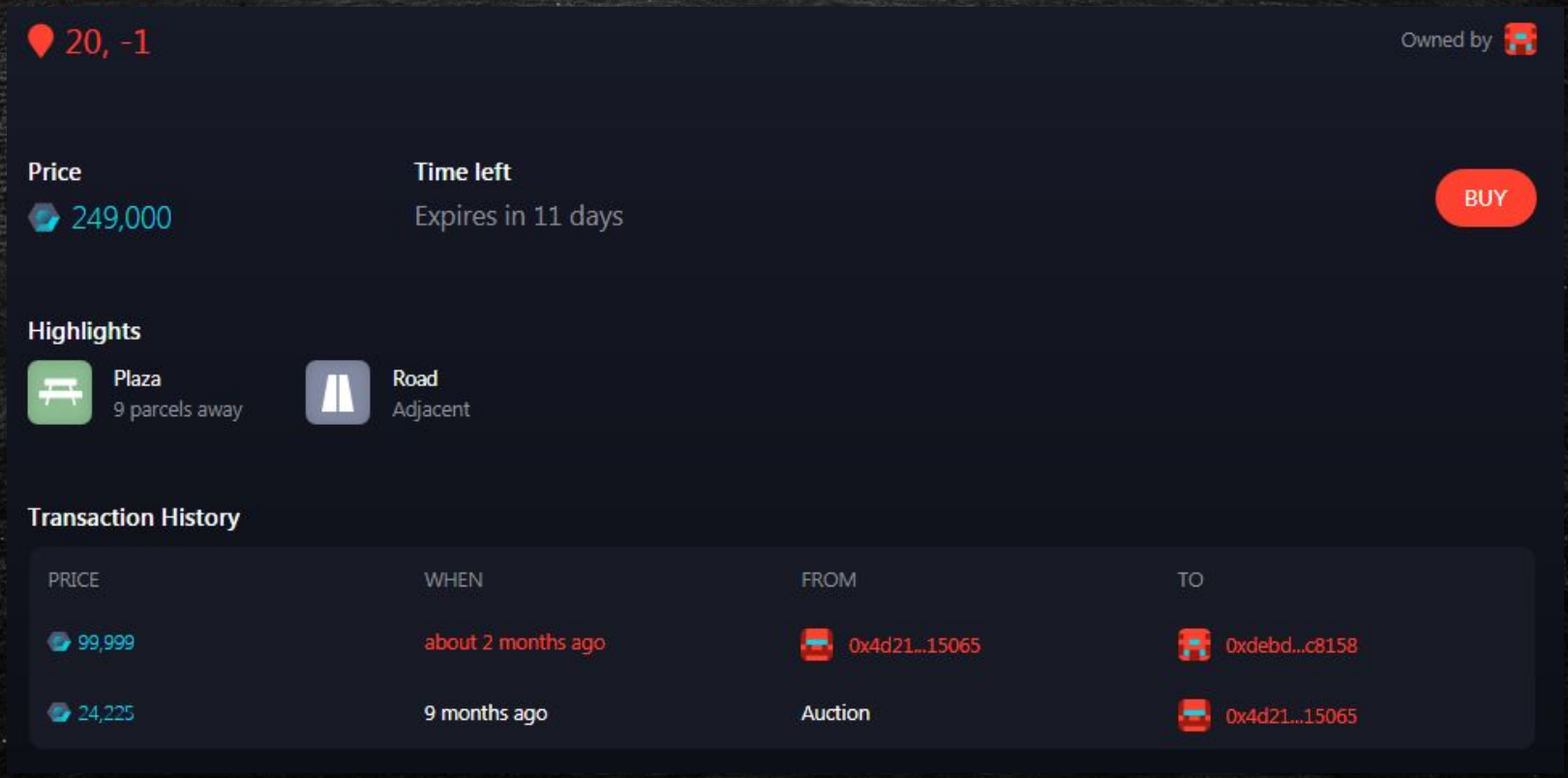
- *my definition*

Example: Decentraland





Example: Decentraland



Example: Decentraland