

# Blockchain and smart contract applications

## 区块链和智能合约应用

What is a blockchain?

区块链是什么？

The  
Economist

OCTOBER 31ST–NOVEMBER 6TH 2015

Economist.com

Our guide to America's best colleges

Myanmar's free-ish election

Those ever-creative accountants

America takes the fight to IS

Coywolves: the new superpredator

# The trust machine

How the technology behind bitcoin  
could change the world



So what is a blockchain, really?

区块链到底是什么？

## A blockchain is... 区块链是 ...

- Decentralized computer network  
去中心化的计算机网络
- Keeps track of and processes “transactions” sent by users  
追踪和处理用户发送的”交易”
- Consensus algorithm ensures that the network agrees on the order of the transactions and the result  
共识算法保证整个网络同意交易的顺序和结果
- Once the consensus algorithm confirms a transaction, it cannot be reverted  
共识算法敲定一个交易以后，不可能撤销它

## Benefits 好处

- Single database with rapid consensus - allows for extremely fast clearing and settlement (eg. 3-60 seconds, instead of 1-3 days)  
统一的数据库和快速的共识算法允许快速的清算和结算 (3-60 秒代替 1-3 天)
- Massively fault-tolerant (even if many nodes go offline or are hacked, the system continues to work)  
非常容错：即使很多节点离线或者被黑，系统继续运行
- Not dependent on any single administrator or organization  
不依靠与一个管理人员或公司

# Applications 应用

- Three major categories of applications:  
大概有三种应用
- Timestamping / data irrepudiability  
时间戳 / 数据不可否认性
- Digital assets (incl. cryptocurrencies, digitized fiat currencies, stocks, etc)  
数字资产（包括数字货币，数字化的法币，股票，等等）
- Smart contracts and complex business processes  
智能合约和复杂的业务流程

What are smart contracts?

智能合约是什么？



# Smart contracts 应用

- Concept originally invented by Nick Szabo in the 1990s  
概念 Nick Szabo 1990 年代发明的
- Computer code that directly controls digital assets or business processes  
代码直接控制数字资产或业务流程
- Like a vending machine, but for the digital world and essentially unbreakable  
类似与自动售货机，但是运行在数字世界和实质上牢不可破

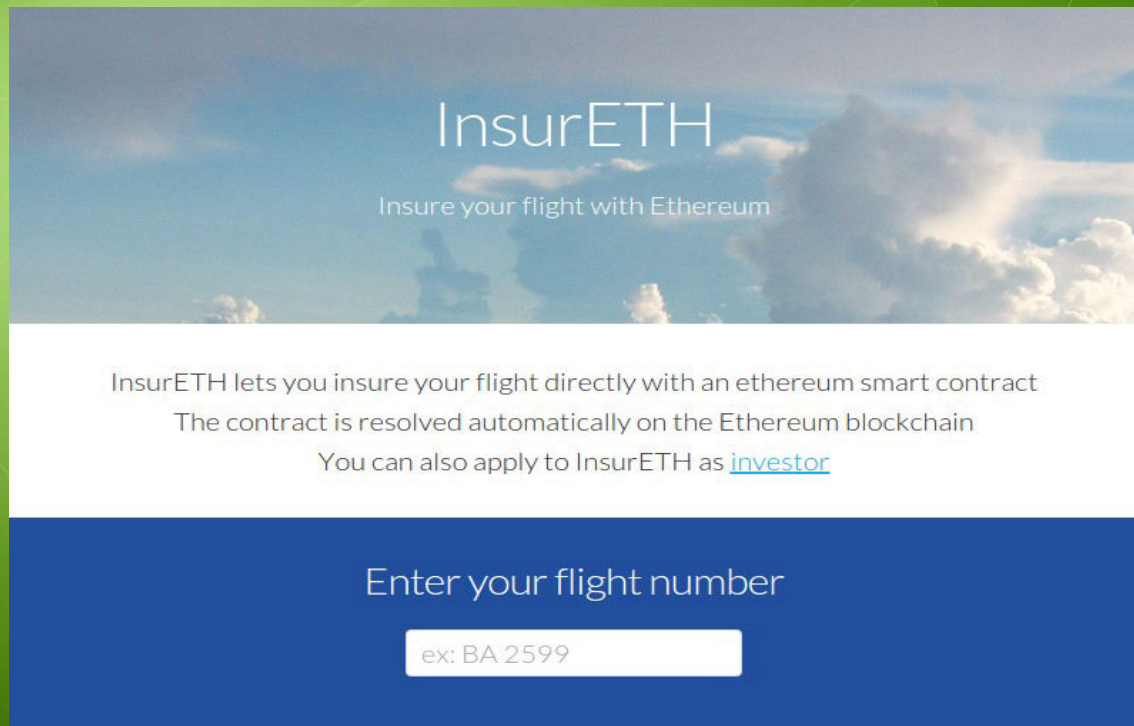


## Note 注释

- Smart contracts are not legal contracts  
智能合约不是法律合约
- Smart contracts are not “smart” in the sense that AI is smart  
智能合约的“智能”不是人工智能的“智能”
- They can encode complex rules and conditions, but do not understand their creators' intentions, unexpected conditions, etc  
他们可以包含复杂的规则和条件，但是他们不能了解他们制造者的意图，意外情况，等等

# Example: Smart contract based flight cancellation insurance

## 例子：基于智能合约航班取消的保险



The image shows a screenshot of the InsurETH website. The top section features a blue sky with white clouds background. The text 'InsurETH' is centered in a large, white, sans-serif font. Below it, the tagline 'Insure your flight with Ethereum' is written in a smaller, white, sans-serif font. The middle section has a white background with black text. It reads: 'InsurETH lets you insure your flight directly with an ethereum smart contract', 'The contract is resolved automatically on the Ethereum blockchain', and 'You can also apply to InsurETH as [investor](#)'. The bottom section has a solid blue background with white text. It says 'Enter your flight number' and below that, a white input field contains the text 'ex: BA 2599'.

InsurETH

Insure your flight with Ethereum

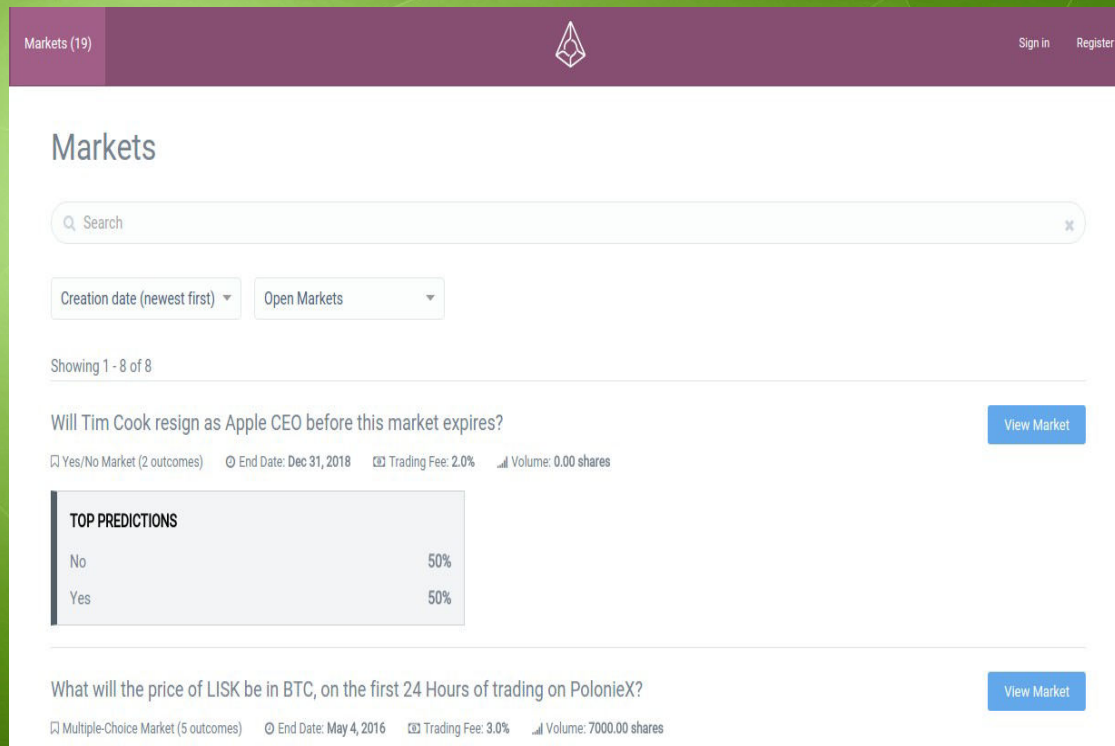
InsurETH lets you insure your flight directly with an ethereum smart contract  
The contract is resolved automatically on the Ethereum blockchain  
You can also apply to InsurETH as [investor](#)

Enter your flight number


ex: BA 2599

# Example: Prediction markets (Augur)

## 例子：预测市场 (Augur)



The screenshot displays the Augur prediction market interface. At the top, there is a purple header with 'Markets (19)' on the left, the Augur logo in the center, and 'Sign in' and 'Register' links on the right. Below the header, the main content area is titled 'Markets'. It features a search bar with a magnifying glass icon and a close button. Below the search bar are two dropdown menus: 'Creation date (newest first)' and 'Open Markets'. The interface shows 'Showing 1 - 8 of 8' markets. The first market listed is 'Will Tim Cook resign as Apple CEO before this market expires?' with a 'View Market' button. Below this market, there are statistics: 'Yes/No Market (2 outcomes)', 'End Date: Dec 31, 2018', 'Trading Fee: 2.0%', and 'Volume: 0.00 shares'. A 'TOP PREDICTIONS' section is highlighted with a dark background, showing a table with two rows: 'No' at 50% and 'Yes' at 50%. The second market listed is 'What will the price of LISK be in BTC, on the first 24 Hours of trading on PoloniEX?' with a 'View Market' button. Below this market, there are statistics: 'Multiple-Choice Market (5 outcomes)', 'End Date: May 4, 2016', 'Trading Fee: 3.0%', and 'Volume: 7000.00 shares'.

Markets (19)  Sign in Register

### Markets

Q Search ✕

Creation date (newest first) Open Markets

Showing 1 - 8 of 8

Will Tim Cook resign as Apple CEO before this market expires? [View Market](#)

Yes/No Market (2 outcomes)  End Date: Dec 31, 2018  Trading Fee: 2.0%  Volume: 0.00 shares

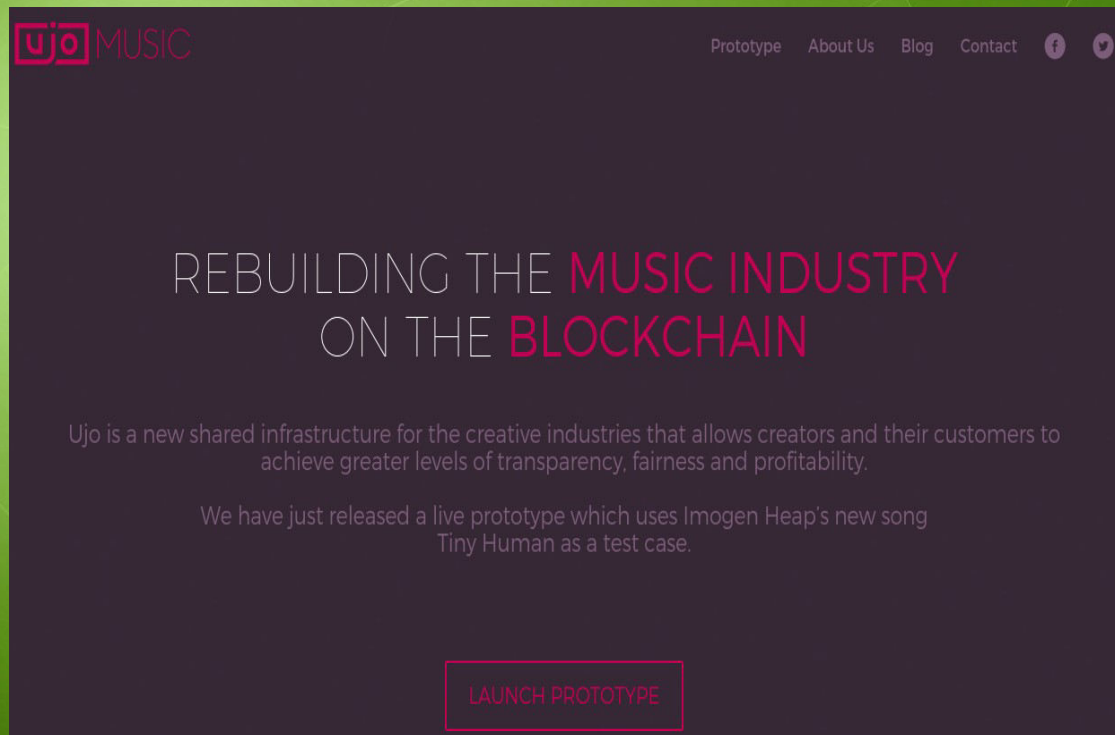
TOP PREDICTIONS	
No	50%
Yes	50%

What will the price of LISK be in BTC, on the first 24 Hours of trading on PoloniEX? [View Market](#)

Multiple-Choice Market (5 outcomes)  End Date: May 4, 2016  Trading Fee: 3.0%  Volume: 7000.00 shares

# Example: Music industry (Ujo)

## 例子：音乐行业（宇宙）



# Financial industry examples

## 金融行业的例子

- OTC financial derivatives trading  
场外金融衍生品的交易
- Equity crowdfunding  
股权众筹
- Insurance (incl mutual insurance, etc)  
保险（包括互助保险等等）

# Non-financial applications useful for smart contracts

## 非金融应用用于智能合约

- Identity verification  
身份验证
- Credit rating  
信用评级
- Smart contract data sources (“oracles”)  
智能合约的数据来源（“神谕”）

# Example: Estonian E-Residency verification on Ethereum

例子：基于以太坊爱沙尼亚的“电子居留”计划的验证

## Proof of Identity on Ethereum (or the “KYC problem”)

🕒 April 27, 2016   📁 Uncategorized   👤 bertani

It doesn't come as a surprise that the “*KYC problem*” is such a hot topic today when talking about interesting blockchain apps. **Everybody** keeps talking about it as the killer use case and for a good reason.

The “KYC” term, Know-Your-Customer, has an inherent reference to a centralized approach where a company needs to verify the identity of its customers. If we want to get rid of this



