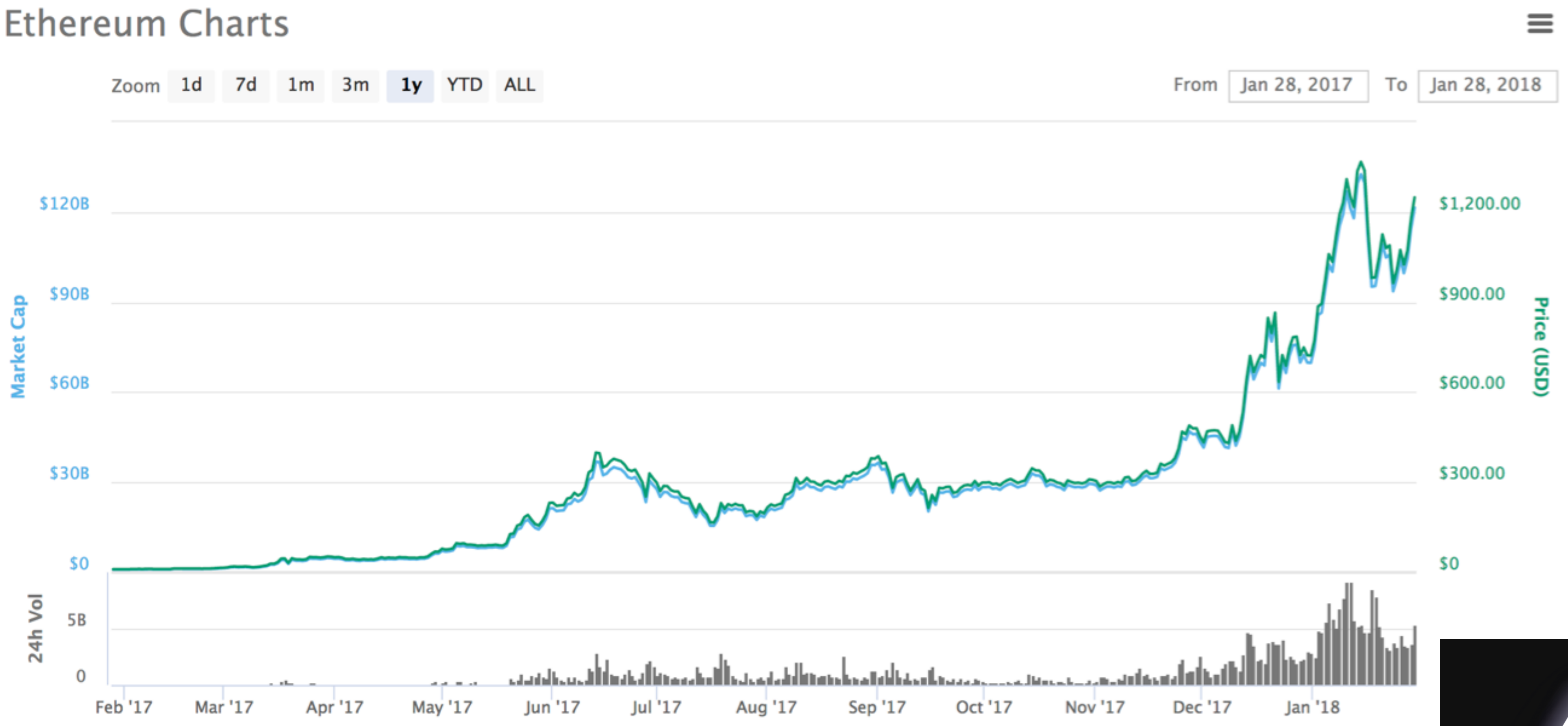
Smart Contracts

Raymond Cheng

Dawn Song

Berkeley EECS
ELECTRICAL ENGINEERING & COMPUTER SCIENCES

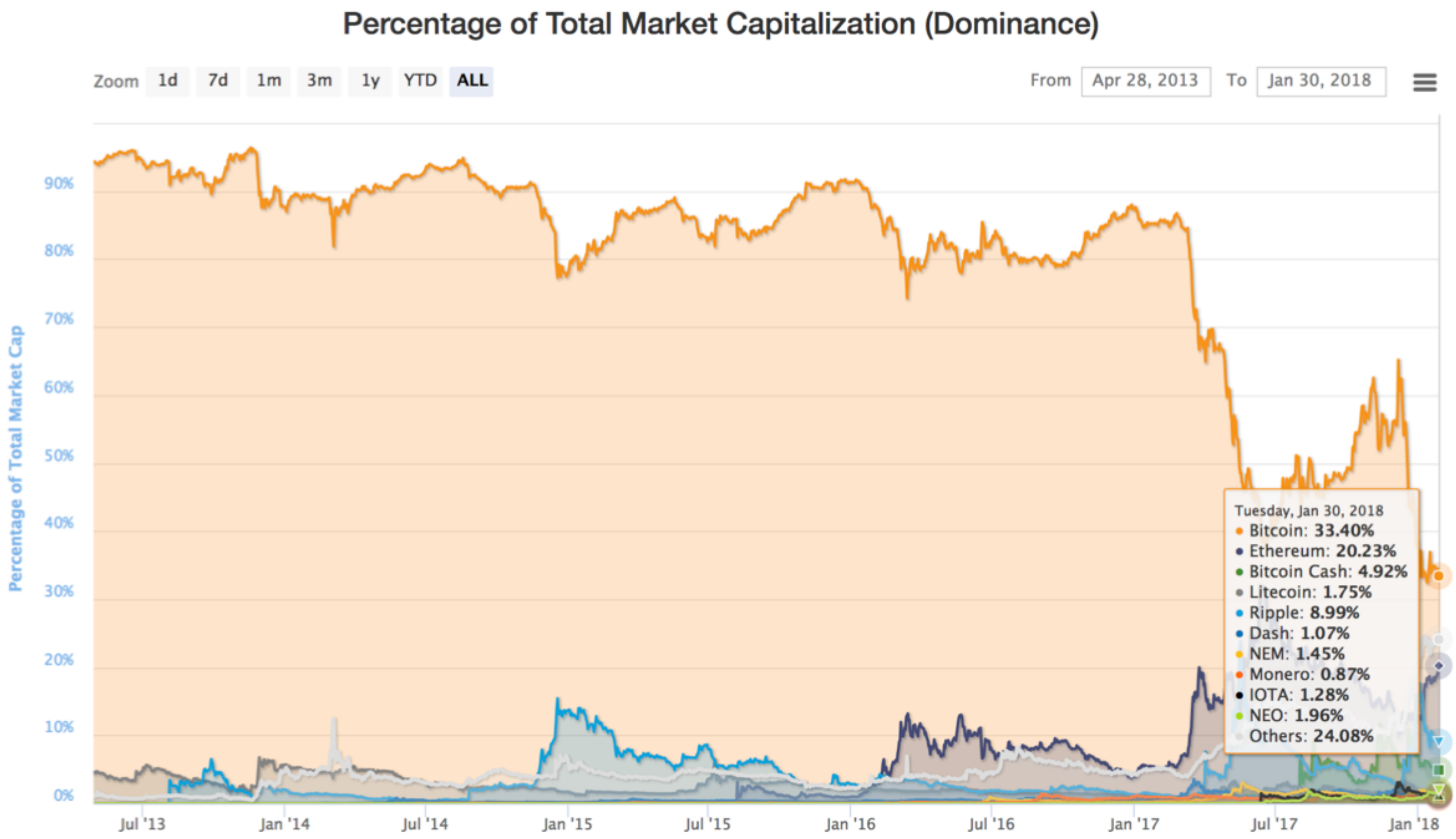
Slides credits: Andrew Miller & Ari Juels



- Currently #2 public cryptocurrency
- Many of the top cryptocurrencies are implemented as smart contracts on top of smart contract blockchains (e.g. Ethereum)

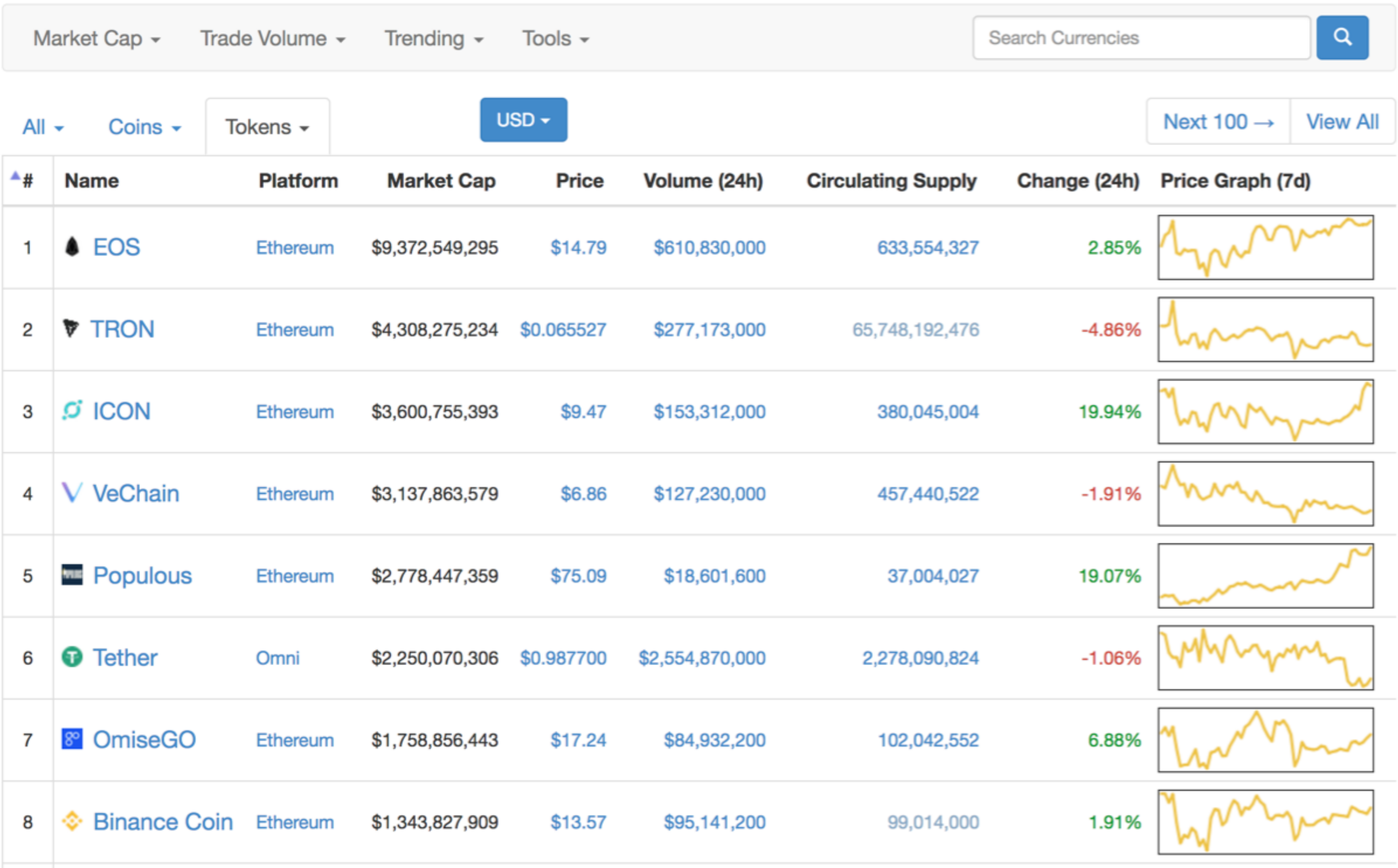
ethereum.org

Ethereum may overtake Bitcoin in market cap



Source: nmarketca

Cryptocurrency Market Capitalizations



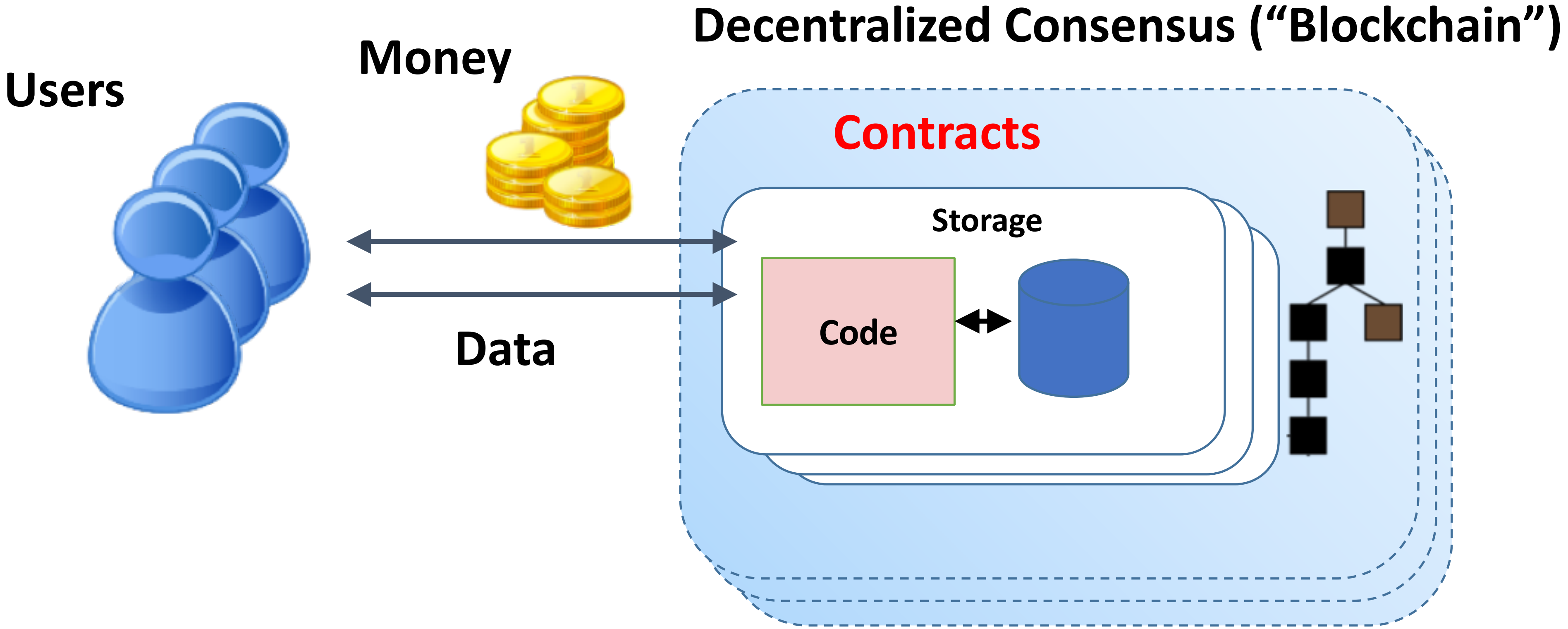
#	Name	Platform	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	EOS	Ethereum	$9,372,549,295	$14.79	$610,830,000	633,554,327	2.85%	
2	TRON	Ethereum	$4,308,275,234	$0.065527	$277,173,000	65,748,192,476	-4.86%	
3	ICON	Ethereum	$3,600,755,393	$9.47	$153,312,000	380,045,004	19.94%	
4	VeChain	Ethereum	$3,137,863,579	$6.86	$127,230,000	457,440,522	-1.91%	
5	Populous	Ethereum	$2,778,447,359	$75.09	$18,601,600	37,004,027	19.07%	
6	Tether	Omni	$2,250,070,306	$0.987700	$2,554,870,000	2,278,090,824	-1.06%	
7	OmiseGO	Ethereum	$1,758,856,443	$17.24	$84,932,200	102,042,552	6.88%	
8	Binance Coin	Ethereum	$1,343,827,909	$13.57	$95,141,200	99,014,000	1.91%	

What do we expect from contracts?

- Language to specify terms of the agreement
- A way to specify your identity and consent
- Enforcement and dispute resolution

What is a smart contract?

- **User-defined programs running on top of a blockchain**
- Smart contract simulates *trusted third party with shared state.*



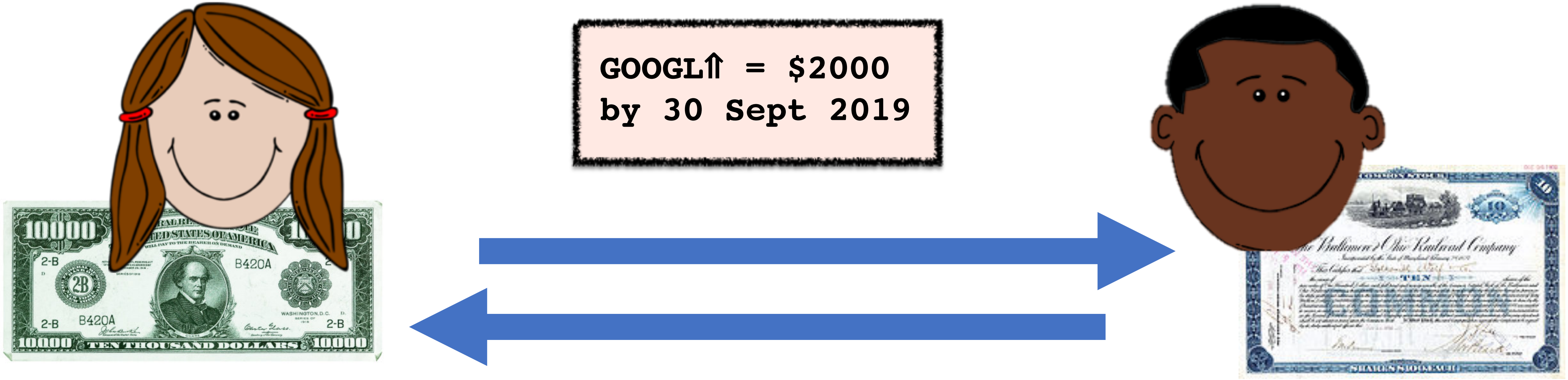
“Smart contracts” conceptualized by Szabo in 1994

A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.

-Nick Szabo “The Idea of Smart Contracts”

For example: Smart contract reassigns physical access to your car from you to your bank if you don’t make a payment

Suppose Alice and Bob strike a deal…



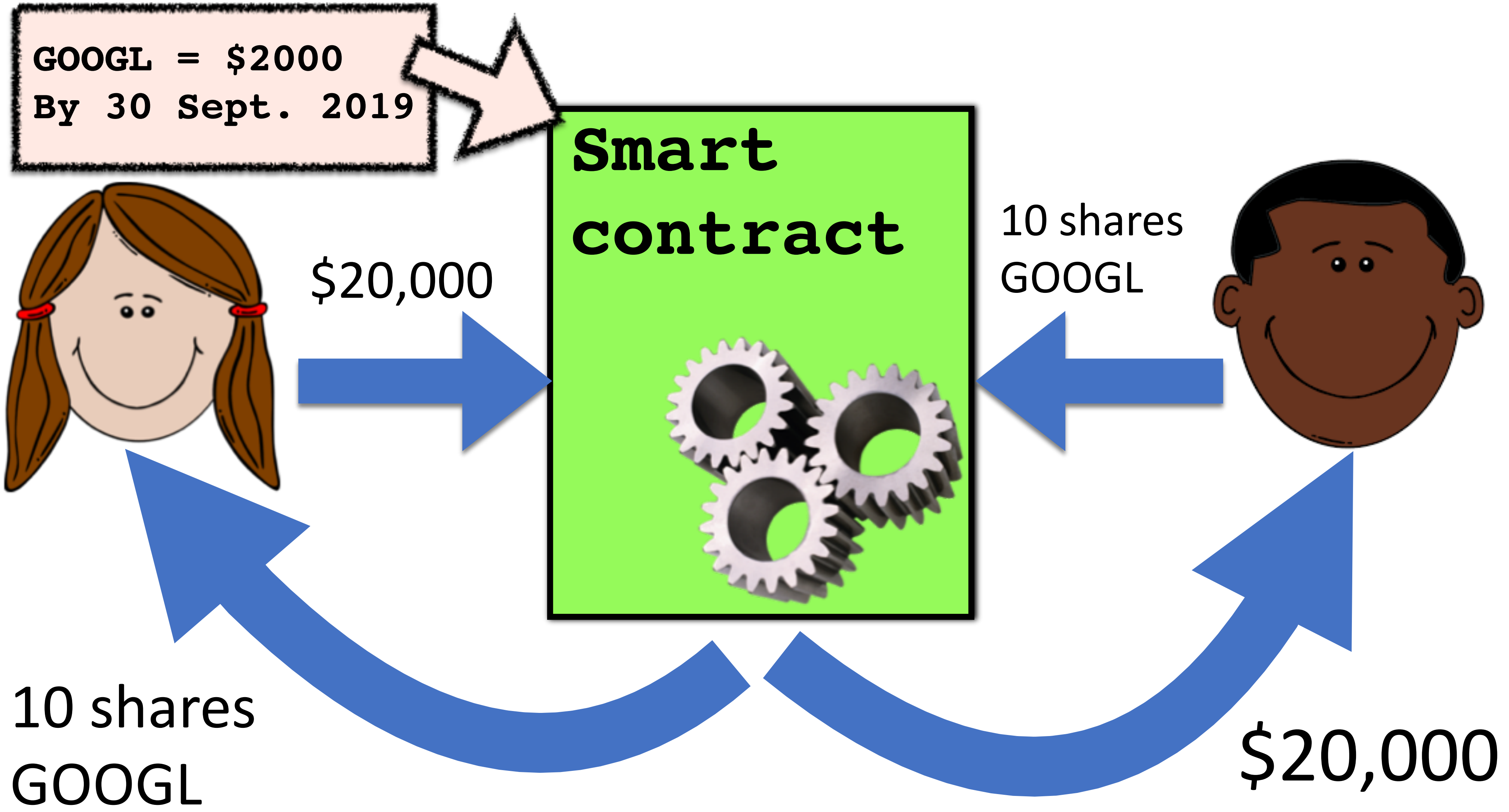
GOOGL⇑ = $2000
by 30 Sept 2019

$20,000

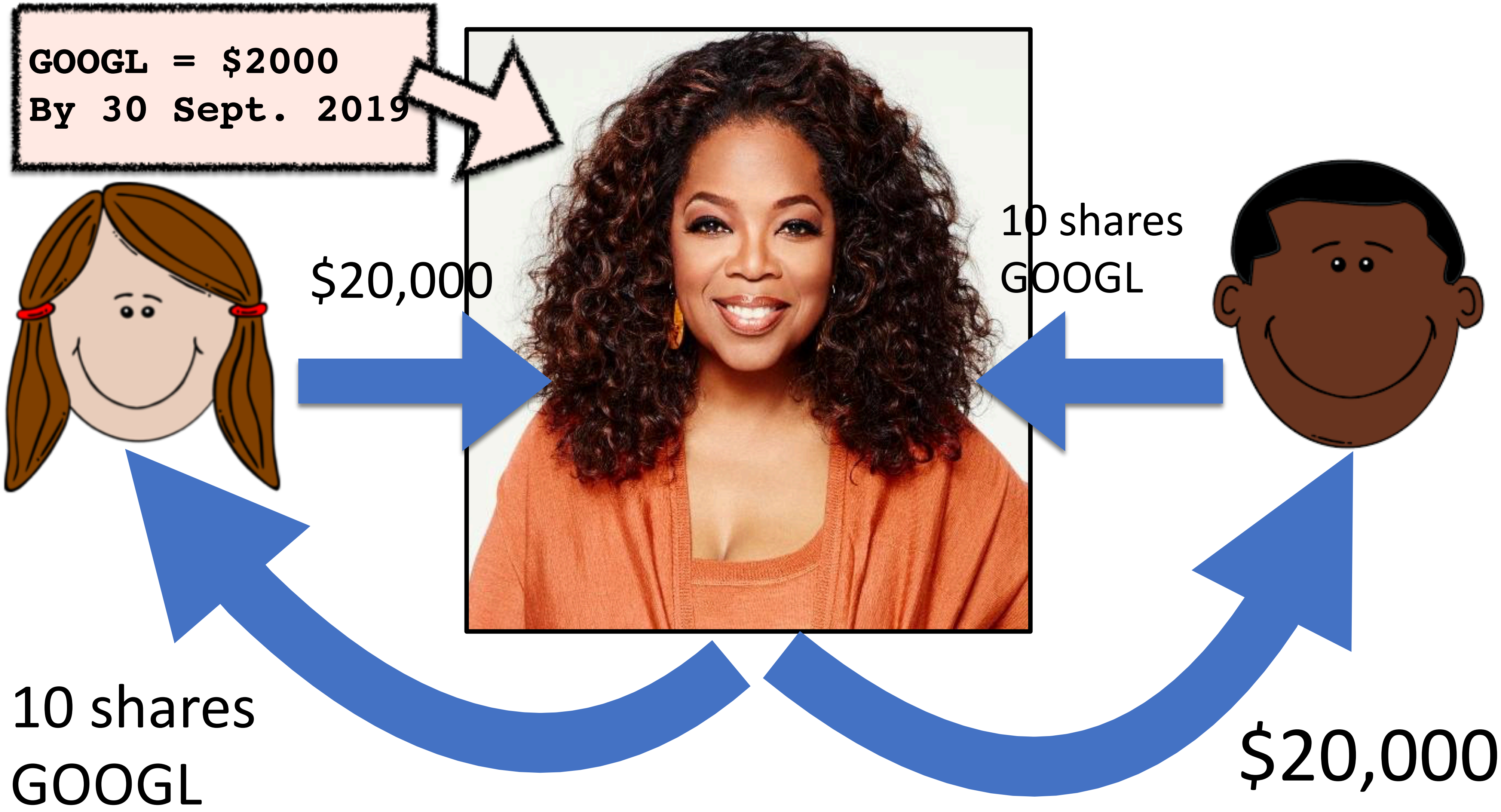
10 shares
GOOGL

Problem of *Fair Exchange*!

Virtual trusted third-party (with public state)



Virtual trusted third-party (with public state)



GOOGL = $2000
By 30 Sept. 2019

$20,000

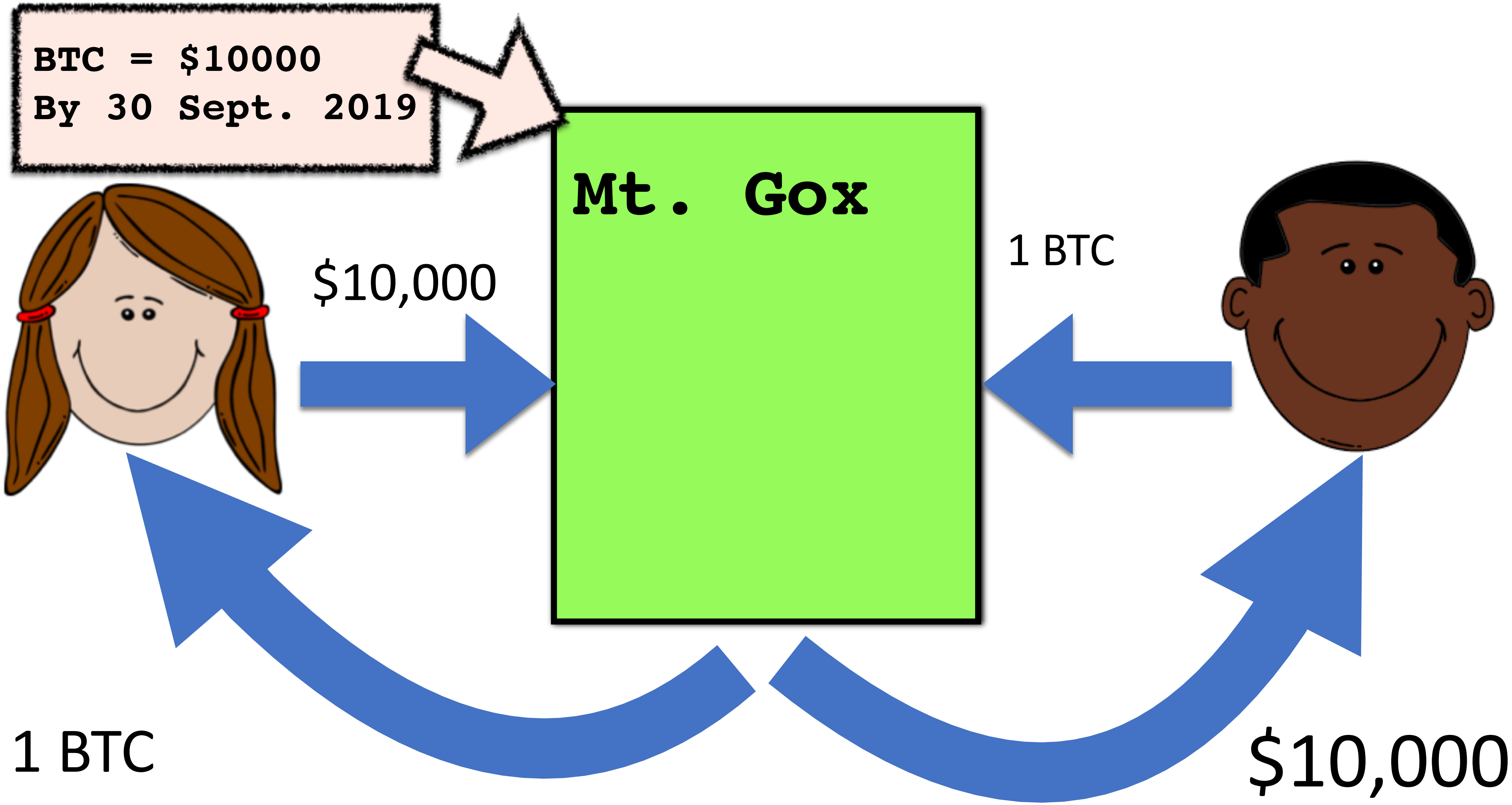
10 shares
GOOGL

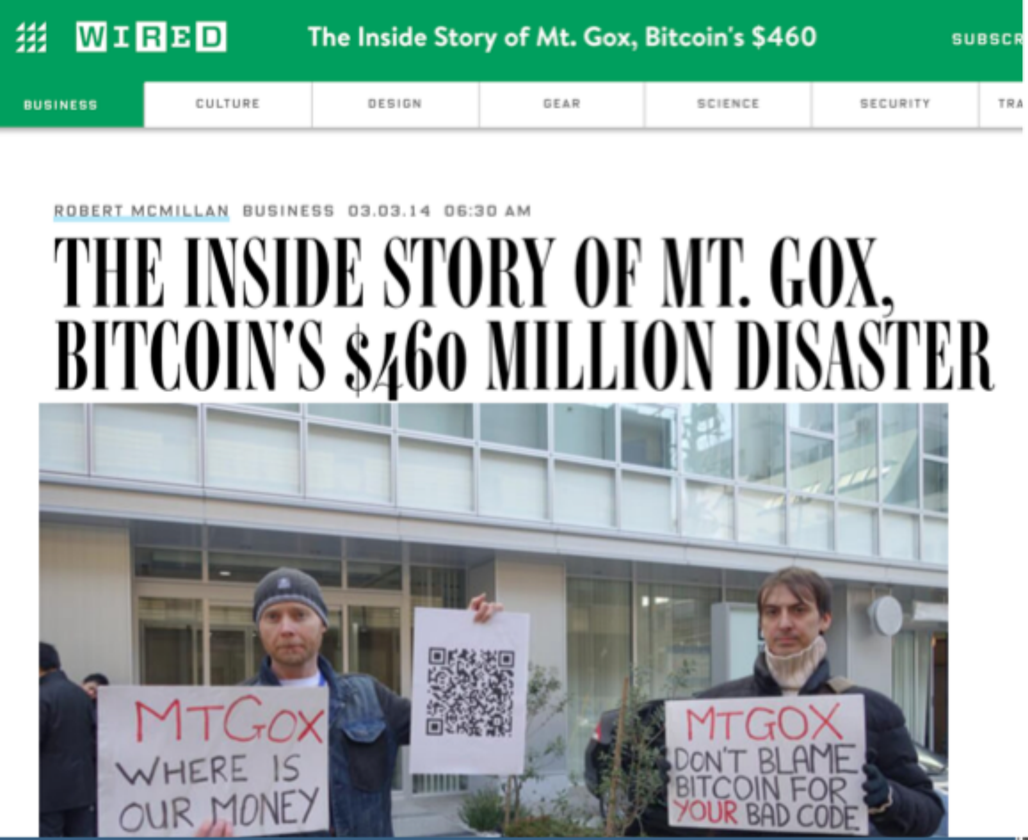
10 shares
GOOGL

$20,000

Okay great, we want smart contracts, but why on blockchain?

Cryptocurrency Exchanges



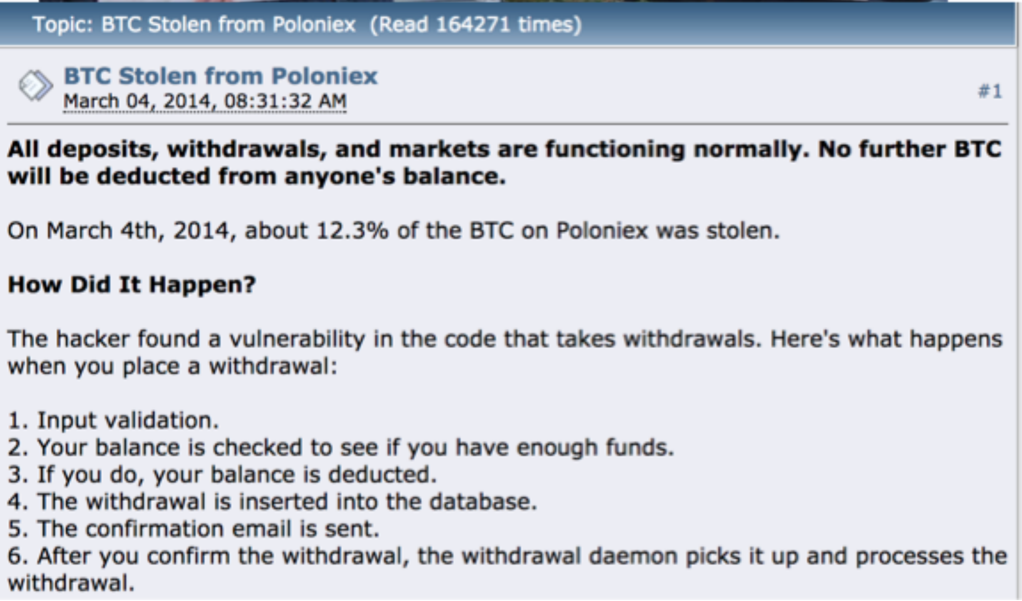


WIRED The Inside Story of Mt. Gox, Bitcoin's $460 SUBSCR

BUSINESS CULTURE DESIGN GEAR SCIENCE SECURITY TRA

ROBERT MCMILLAN BUSINESS 03.03.14 06:30 AM

THE INSIDE STORY OF MT. GOX, BITCOIN'S $460 MILLION DISASTER



Topic: BTC Stolen from Poloniex (Read 164271 times)

BTC Stolen from Poloniex
March 04, 2014, 08:31:32 AM #1

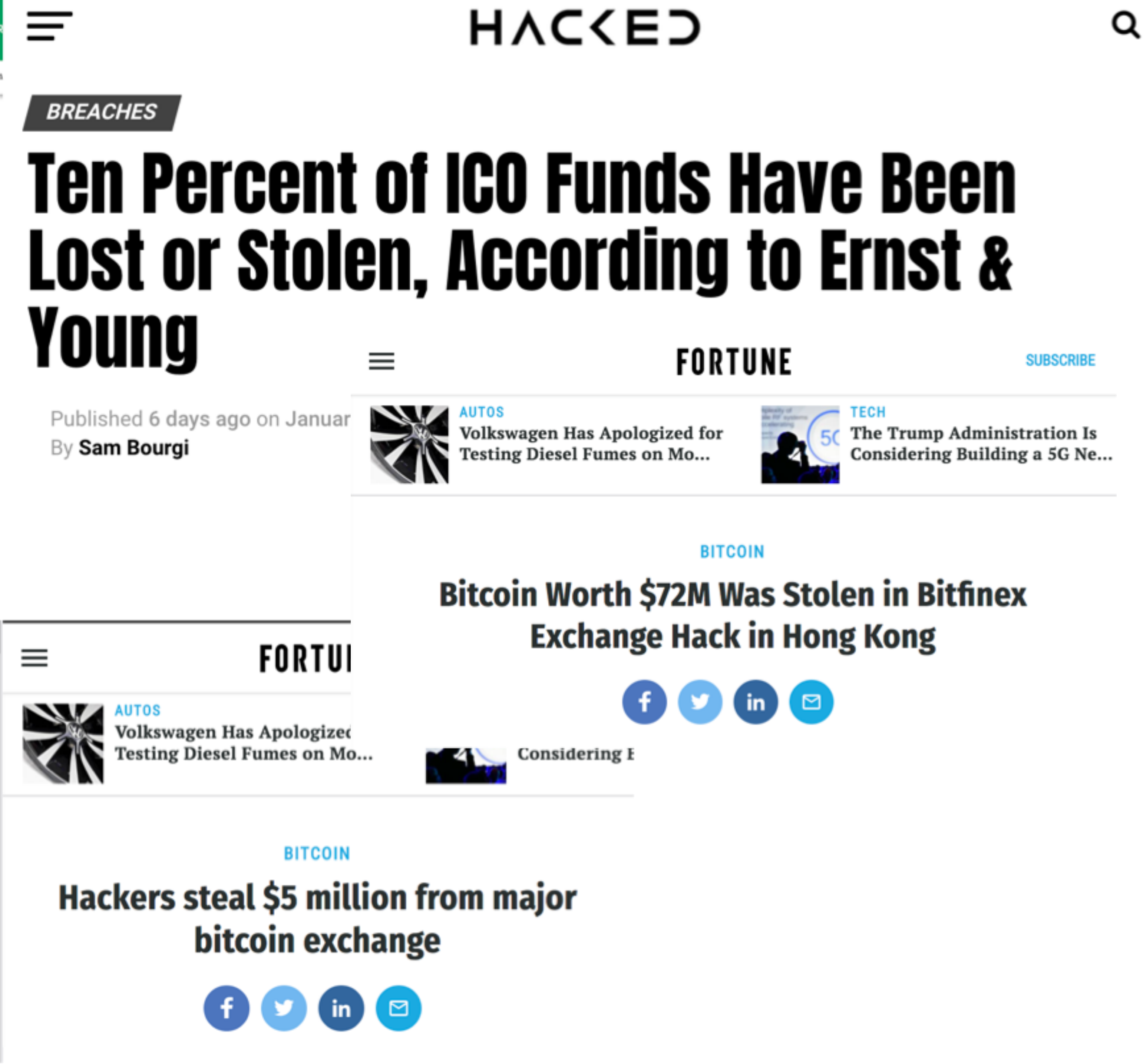
All deposits, withdrawals, and markets are functioning normally. No further BTC will be deducted from anyone's balance.

On March 4th, 2014, about 12.3% of the BTC on Poloniex was stolen.

How Did It Happen?

The hacker found a vulnerability in the code that takes withdrawals. Here's what happens when you place a withdrawal:

1. Input validation.
2. Your balance is checked to see if you have enough funds.
3. If you do, your balance is deducted.
4. The withdrawal is inserted into the database.
5. The confirmation email is sent.
6. After you confirm the withdrawal, the withdrawal daemon picks it up and processes the withdrawal.



HACKED

BREACHES

Ten Percent of ICO Funds Have Been Lost or Stolen, According to Ernst & Young

Published 6 days ago on Januar
By Sam Bourgi

FORTUNE SUBSCRIBE

AUTOS Volkswagen Has Apologized for Testing Diesel Fumes on Mo...

TECH The Trump Administration Is Considering Building a 5G Ne...

BITCOIN

Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong

FORTU

AUTOS Volkswagen Has Apologized Testing Diesel Fumes on Mo...

Considering I

BITCOIN

Hackers steal $5 million from major bitcoin exchange

#1: Smart contracts must enforce correct execution

Smart Contract Applications

- Tokens
- Lotteries
- Insurance
- Supply-chain management
- Marketplaces
- Cryptocurrency exchanges
- “Self-sovereign” identity management
- Covenants
- Sharing economy
- And many more!

Token Smart Contracts

```
Init:
 balance[creator] = 1,000,000

Transfer($amt, from, to):
  Assert balance[from] ≥ $amt
  balance[from] := balance[from] – $amt
  balance[to] := balance[to] + $amt
```

Contract stores everyone’s balance

Transfer moves tokens from one account to another

#2: Transactions to smart contracts must be all-or-nothing

Lottery Smart Contract

```
Init:
  $\mathcal{T}_{end}$ := 7 June 2018,
  $ticket := 1 ,
  pool := {},
  pot := 0

TicketPurchase($amt, P):
  On receive $amt from party P:
    Assert $amt = $ticket, balance[P] ≥ $amt
    balance[P] := balance[P] – $ticket
    pot := pot + $ticket
    pool := pool ∪ P

Timer:
   If T > $\mathcal{T}_{end}$ then
    W $\in_R$ pool
    balance[W] := balance[W] + pot
```

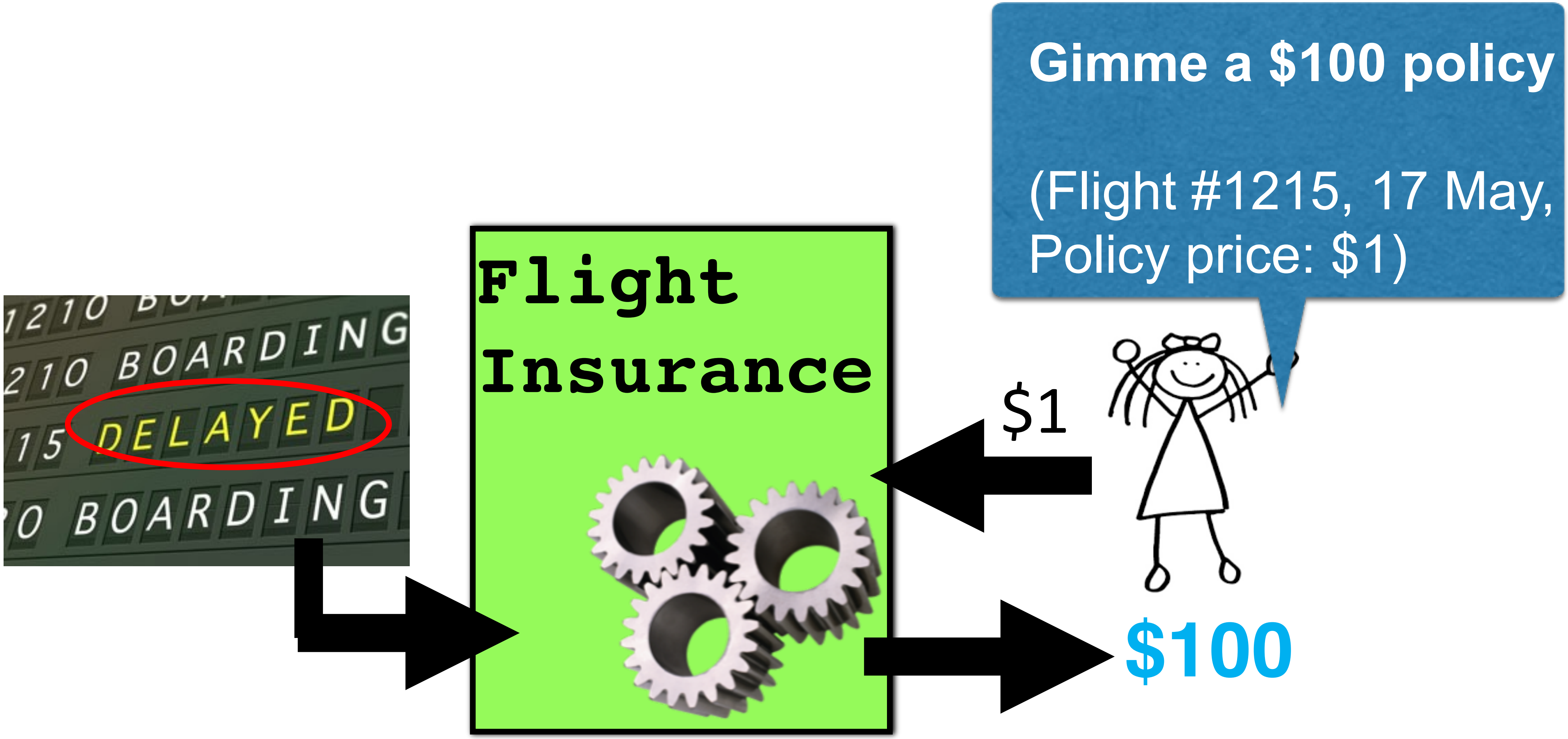
Contract stores the end time, ticket cost, current pool, and pot

If the party has enough money, add them to the pool and their money to the pot

At the end, select a winner

#3: Contracts are enforced by the blockchain

Automated Insurance Contracts



Gimme a $100 policy

(Flight #1215, 17 May, Policy price: $1)

Flight Insurance

$1

$100

#4: Contracts have an auditable history

Smart contract properties

- Guaranteed to execute correctly
  - Malicious miner cannot cheat
- Transactions are all-or-nothing
- Autonomous: Enforced by network
  - Cannot be changed or stopped, even by its creator
- All data is stored on the blockchain
  - Auditable history

- Intuition: Smart contract simulates *trusted third party with public state.*

Traditional contracts vs. smart contracts

	Traditional	**Smart**
Specification	Natural language + “legalese”	Code
Identity & consent	Signatures	Digital signatures
Dispute resolution	Judges, arbitrators	Decentralized platform
Nullification	By judges	????
Payment	As specified	built-in
Escrow	Trusted third party	built-in