• Currently #2 public cryptocurrency
• Many of the top cryptocurrencies are implemented as smart contracts on top of smart contract blockchains (e.g. Ethereum)
Ethereum may overtake Bitcoin in market cap

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

$20,000

GOOGL\uparrow = $2000 by 30 Sept 2019

10 shares GOOGL

Problem of *Fair Exchange*!
Virtual trusted third-party (with public state)

GOOGL = $2000
By 30 Sept. 2019

Smart contract

$20,000

10 shares GOOGL

$20,000

10 shares GOOGL
Virtual trusted third-party (with public state)

GOOGL = $2000
By 30 Sept. 2019

10 shares GOOGL
$20,000

10 shares GOOGL
$20,000
Okay great, we want smart contracts, but why on blockchain?
Cryptocurrency Exchanges

BTC = $10000
By 30 Sept. 2019

Mt. Gox

$10,000

1 BTC

$10,000

1 BTC
Okay great, we want smart contracts, but why on blockchain?
#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:
  \( \text{balance[creator]} = 1,000,000 \)

Transfer(\( \text{amt, from, to} \)):
  Assert \( \text{balance[from]} \geq \text{amt} \)
  \( \text{balance[from]} := \text{balance[from]} - \text{amt} \)
  \( \text{balance[to]} := \text{balance[to]} + \text{amt} \)

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:
$T_{\text{end}} := 7 \text{ June 2018}$, 
$\$\text{ticket} := 1$, 
$\text{pool} := \{\}$, 
$\text{pot} := 0$

TicketPurchase($\$\text{amt}, P)$:
On receive $\$\text{amt}$ from party $P$:
Assert $\$\text{amt} = \$\text{ticket}$, $\text{balance}[P] \geq \$\text{amt}$
$\text{balance}[P] := \text{balance}[P] - \$\text{ticket}$
$\text{pot} := \text{pot} + \$\text{ticket}$
$\text{pool} := \text{pool} \cup P$

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

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

Flight Insurance

Gimme a $100 policy
(Flight #1215, 17 May, Policy price: $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

<table>
<thead>
<tr>
<th></th>
<th>Traditional</th>
<th>Smart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification</td>
<td>Natural language + “legalese”</td>
<td>Code</td>
</tr>
<tr>
<td>Identity &amp; consent</td>
<td>Signatures</td>
<td>Digital signatures</td>
</tr>
<tr>
<td>Dispute resolution</td>
<td>Judges, arbitrators</td>
<td>Decentralized platform</td>
</tr>
<tr>
<td>Nullification</td>
<td>By judges</td>
<td>????</td>
</tr>
<tr>
<td>Payment</td>
<td>As specified</td>
<td>built-in</td>
</tr>
<tr>
<td>Escrow</td>
<td>Trusted third party</td>
<td>built-in</td>
</tr>
</tbody>
</table>