The power of Blockchain: Smart Contracts

Foteini Baldimtsi
The Blockchain at the heart of a cryptocurrency

Alice sends 2💰 to Bob
John sends 1💰 to Eve
Dave sends 5💰 to Alice

Bob sends 1💰 to Dave
Eve sends 4💰 to Bob

...
The Blockchain at the heart of a cryptocurrency

Alice sends 2 📈 to Bob
John sends 1 📈 to Eve
Dave sends 5 📈 to Alice

Bob sends 1 📈 to Dave
Eve sends 4 📈 to Bob

...
Abstracting the notion of Blockchain

- Immutable data collection
  - Data added in an “append-only” manner
  - Nobody can modify an old transaction

- Controlled in a decentralized manner by multiple parties running a consensus protocol
  - Byzantine agreement
  - Proof-of-work
  - Proof-of-space
Where is Blockchain used?

Cryptocurrencies
Where is Blockchain used?

Cryptocurrencies
Why is Blockchain useful?

1. As a distributed, tamper-proof, **data structure**
   - No central trusted authority exists
   - Participating parties do not trust each other

2. As a mechanism for execution of **smart contracts**
   - Enforce the negotiation or performance of a contract
   - Allows for fair-exchange (blockchain is the mediator)
   - No direct interaction between parties
Smart Contracts

Introduced by Nick Szabo in 1994

Help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

1. An option contract between parties is written as code into the blockchain. The individuals involved are anonymous, but the contract is the public ledger.

2. A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3. Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors’ positions.
Smart Contract for Fair Exchange
Smart Contract for Fair Exchange
Smart Contract for Fair Exchange

Impossible without the use of a trusted third party!

Needs to be an atomic operation!
Smart Contract for Fair Exchange
Smart Contract for Fair Exchange
Smart Contract for Fair Exchange
Smart Contract for Fair Exchange

1. Pick a secret key $K$
2. Encrypt document into $\text{Enc}_K(D)$
Smart Contract for Fair Exchange

1. Pick a secret key $K$
2. Encrypt document into $\text{Enc}_K(D)$
Smart Contract for Fair Exchange

1. Pick a secret key $K$
2. Encrypt document into $\text{Enc}_K(D)$

1. Prepare contract
   $C = \text{"1 Bitcoin for the secret key } K\text{"}$
1. Pick a secret key $K$
2. Encrypt document into $\text{Enc}_K(D)$

1. Prepare contract
   $C = " 1 \text{ Bitcoin} \) for the secret key $K$"
1. Pick a secret key $K$
2. Encrypt document into $\text{Enc}_K(D)$

1. Prepare contract $C = "1 \text{ Bitcoin} for the secret key } K"$
Smart Contract for Fair Exchange

1. Pick a secret key $K$
2. Encrypt document into $\text{Enc}_K(D)$

Q: How can the buyer know that the seller has encrypted the correct document?

1. Prepare contract $C = "1 \text{ Bitcoin} for the secret key } K"$
Smart Contract for Fair Exchange

1. Pick a secret key $K$
2. Encrypt document into $\text{Enc}_K(D)$

Q: How can the buyer know that the seller has encrypted the correct document?
A: Break $D = D_1 \ldots D_n$, encrypt and post all shares and reveal some random ones before selling.
1. Pick a secret key $K$
2. Encrypt document into $\text{Enc}_K(D)$

1. Prepare contract $C = "1 \text{ Bitcoin} for the secret key } K"$

Q: What if the seller never reveals $K$? What happens to the buyers coin?
1. Pick a secret key K
2. Encrypt document into $\text{Enc}_K(D)$

Q: What if the seller never reveals $K$? What happens to the buyers coin?
A: Timelocked transactions: funds are returned after a specific time window.
Bitcoin Smart Contracts

C = “1 $\text{ Bitcoin}$ for the secret key $K$ for $tw=10$ hours”

Such a contract cannot be implemented in Bitcoin!

Bitcoin has been designed to only check two conditions:
- Verification of an ECDSA signature (under specific parameters)
- Preimage of a hash function output

Post: $\text{Enc}_K(D)$, $\text{Hash}(K)$ and ZK proof that the hashed key is the correct one

C = “1 $\text{ Bitcoin}$ for the preimage of $\text{Hash}(K)$ for $tw=10$ hours”

After verifying the proof, post
Ethereum smart contracts

Provides a “Turing-complete” scripting language: supports a broader set of computational instructions.
- Contracts can use data outside of the blockchain (i.e. weather, stock prices etc)
- We can build chains of contracts (the 2nd settles on information from the output of the 1st contract)

Smart contracts run on the **Ethereum Virtual Machine** (works at a level too low to be convenient to directly program).
**Solidity** is the most popular language for writing contracts (JavaScript-like)
Smart contracts interacting with each other
Ethereum smart contracts need gas to run

<table>
<thead>
<tr>
<th>Task</th>
<th>Gas Required</th>
<th>Cost (ETH)</th>
<th>Cost (USD)</th>
<th>Ops per ETH</th>
<th>Ops per USD</th>
<th>Ops per Block</th>
<th>Blocks to complete Op</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or subtract two integers</td>
<td>3</td>
<td>0.00000009</td>
<td>0.00002655</td>
<td>11111111.11</td>
<td>37664.78343</td>
<td>1566666.667</td>
<td>0.0000006382978723</td>
</tr>
<tr>
<td>Add or subtract two integers 1 million times</td>
<td>3000000</td>
<td>0.09</td>
<td>26.55</td>
<td>11.11111111</td>
<td>0.03766478343</td>
<td>1.566666667</td>
<td>0.6382978723</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>Gas Required</th>
<th>Cost (ETH)</th>
<th>Cost (USD)</th>
<th>Ops per ETH</th>
<th>Ops per USD</th>
<th>Ops per Block</th>
<th>Blocks to complete Op</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save a 256-bit word to storage</td>
<td>20000</td>
<td>0.0006</td>
<td>0.177</td>
<td>1666.666667</td>
<td>5.649717514</td>
<td>235</td>
<td>0.004255319149</td>
</tr>
<tr>
<td>Save 1 MB to storage (31250 256-bit words)</td>
<td>6250000000</td>
<td>18.75</td>
<td>5531.25</td>
<td>0.05333333333</td>
<td>0.000180790960</td>
<td>0.00752</td>
<td>132.9787234</td>
</tr>
<tr>
<td>Save 1 GB to storage (1000 MB)</td>
<td>625000000000</td>
<td>18750</td>
<td>5531250</td>
<td>0.0000533333333</td>
<td>0.000000180790</td>
<td>0.00000752</td>
<td>132978.7234</td>
</tr>
</tbody>
</table>

There is a need for efficient smart contract protocols!

https://hackernoon.com/ether-purchase-power-df40a38c5a2f
A note on privacy

The blockchain is **public** and all posted data:

- **Code** of the contract
- **PKs** of the participants
- **Data** send to the contract
- **Payments** (amounts and PKs)

- Generic smart contract anonymity compilers for ethereum [Hawk]
- Specialized tools for Bitcoin contracts anonymity [Tumblebit]
Advantages of smart contracts

Applications: Government: e-voting, e-IDs (decentralized PKIs), Auctions, Real estate, Healthcare, Supply chain

- Autonomy: no need for trusted third party
- Trust: data stored in a shared ledger (cannot be lost)
- Backup: data duplication
- Speed: automating various processes
thank you!

foteini@gmu.edu