Blockchain Engineering

Hackathon

Dr. Lars Brünjes

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Ostbayerische Technische Hochschule
Amberg-Weiden

OTH
REGENSBURG

MIND
MODULARES INNOVATIVES
NETZWERK FÜR DURCHLÄSSIGKEIT

AUFSTIEG DURCH
BILDUNG
OFFENE HOCHSCHULEN

23. November 2019

- Auktionen bieten sich für die Implementierung als Smart-Contract geradezu an, um “digitale Güter” wie zum Beispiel Non-Fungible Tokens zu versteigern.
- Wie bei allen Smart-Contracts ist die Idee, Regeln, für deren Einhaltung normalerweise das Rechtssystem verantwortlich ist, automatisch durchzusetzen.
- Aufgrund der speziellen Bedingungen auf der Blockchain sind dazu einige Änderungen im Vergleich zu “normalen” Auktionen nötig. Zum Beispiel können Gebote dadurch verbindlich gemacht werden, dass ein Bieter sein Gebot zunächst in den Smart-Contract einzahlt und dann später zurückforden kann, falls er überboten wird.

- Laut Wikipedia gibt es sechs gängigen Auktions-Varianten, die wir im folgenden kurz vorstellen.
- In unserem heutigen Hackathon wollen wir eine oder mehrere Varianten solcher Auktionen als Smart-Contract in Solidity implementieren. Sie können dazu alleine oder in kleinen Gruppen arbeiten.
- Bitte suchen Sie sich eine oder mehrere Varianten aus (außer der “Englischen”!) und versuchen Sie, Sie in Solidity zu implementieren.
- Denken Sie möglichst auch an besondere Fälle und stellen Sie sicher, dass weder das zu versteigernde Gut noch Gebote für immer im Vertrag “eingeschlossen” bleiben!

- Die Englische Auktion (English Auction) ist die “übliche” Auktion, bei der Käufer solange Gebote abgeben können, bis niemand mehr bereit ist, höher zu bieten. Der Käufer mit dem höchsten Gebot erhält den Zuschlag, der Preis ist das höchste Gebot.
- Im letzten Vorlesungsblock haben wir gesehen, wie man eine Englische Auktion als Solidity-Contract implementieren kann.

- Bei der Holländischen Auktion (Dutch Auction) wird mit einem hohen Gebot gestartet, welches dann mit der Zeit systematisch gesenkt wird, bis ein Käufer bereit ist, den Preis zu bezahlen.

- In einer First-Price Sealed Bid Auktion geben alle Käufer nur ein einziges, geheimes Gebot ab. Der Käufer mit dem höchsten Gebot gewinnt und bezahlt sein Gebot als Preis.
- Falls Sie sich für diese Variante entscheiden, besteht die Hauptschwierigkeit darin, die Gebote geheim zu machen, denn alle Vorgänge auf der Blockchain sind bekanntlich öffentlich.
- Eine Möglichkeit wäre, ein Commitment Scheme zu verwenden, wie wir es in der Vorlesung über Hashing diskutiert haben:
  - Alle Käufer machen zunächst einen Einsatz, der höher als der zu erwartende Kaufpreis sein muss.
  - Ihrem Einsatz fügen Sie ein Commitment über ihr tatsächliches Gebot bei, was nicht höher als der Einsatz sein darf.
  - In der zweiten Runde legen alle Käufer ihr Commitment offen, und der Sieger wird bestimmt.
  - Weigert sich ein Käufer, sein Gebot zu veröffentlichen, so verliert er seinen Einsatz.
  - Alle anderen Käufer (außer dem Sieger) erhalten ihren Einsatz zurück.

- Die Vickrey Auktion verläuft zunächst wie eine First-Price Sealed Bid Auction.
- Der Unterschied ist, dass zwar der Käufer mit dem höchsten Gebot gewinnt, er aber nur das zweithöchste Gebot bezahlen muss.
- Diese Variante verhindert “strategische” Gebote, weil man beweisen kann, dass die beste Strategie für Käufer darin besteht, zu bieten, was ihnen das versteigerte Gut tatsächlich wert ist.

- Bei der Umgekehrten Auktion (Reverse Auction) sind die Rollen von Käufer und Verkäufer vertauscht: Mehrere Verkäufer bieten, bis der Käufer bei einem von ihnen kauft.
- In der Praxis werden umgekehrte Auktionen beispielsweise benutzt, um einen Bauunternehmer für ein geplantes Bauprojekt auszuwählen.
- Wenn Sie sich für diese Variante entscheiden, könnten Sie zum Beispiel den Fall betrachten, in dem der Käufer ein Fungible Token erwerben will, und mehrere Besitzer des Tokens darum bieten, es ihm zu verkaufen.
- Die Schwierigkeit ist, sicherzustellen, dass die Verkäufer ihr Token dem Vertrag zur Verfügung stellen, bevor sie ein Angebot abgeben. Eine Möglichkeit ist es, für jeden Verkäufer einen persönlichen “Treuhandvertrag” einzurichten, in dem er sein Token deponieren kann.

- In einer Cent Auktion (Bidding Fee Auction, Penny Auction) müssen Käufer für jedes Gebot eine feste Gebühr bezahlen, und Gebote steigen jeweils um einen niedrigen festen Wert (z.B. einen Cent) an.
- Der Vorteil für den Verkäufer ist, dass sein Gewinn oft um ein Vielfaches höher als das höchste Gebot ist, da er die Gebühr aus jedem Gebot ebenfalls erhält.
- Ansonsten verläuft die Auktion wie eine Englische Auktion: Gebote starten bei einem Mindestgebot, und der Käufer mit dem höchsten Gebot gewinnt und bezahlt sein Gebot als Preis.

Beispiel

Bei einem Mindestgebot von 10€, einer schrittweisen Erhöhung um 1 Cent, einer Gebühr von 10 Cent und einem Höchstgebot von 15€ sind 500 Gebote nötig, d.h. der Verkäufer erhält $500 \times 0.1€ + 15€ = 65€$.

Hinweis

Diese Publikation wurde im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Bund- Länder- Wettbewerbs “Aufstieg durch Bildung: offene Hochschulen” erstellt. Die in dieser Publikation dargelegten Ergebnisse und Interpretationen liegen in der alleinigen Verantwortung der Autor/innen.