Blockchain Engineering

Incentives (Anreize)

Dr. Lars Brünjes

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

MODULARES INNOVATIVES
NETZWERK FÜR DURCHLÄSSIGKEIT

AUFSTIEG DURCH
BILDUNG
OFFENE HOCHSCHULEN

19. Oktober 2019

- Incentives (Anreize) im Kontext einer Kryptowährung dienen dazu, Menschen zu ermutigen, die Infrastruktur für die Blockchain zur Verfügung zu stellen und das Protokoll zu unterstützen.

- Incentives (Anreize) im Kontext einer Kryptowährung dienen dazu, Menschen zu ermutigen, die Infrastruktur für die Blockchain zur Verfügung zu stellen und das Protokoll zu unterstützen.
- Im Falle von Bitcoin oder Ethereum bedeutet dies zum Beispiel, Knoten zu unterhalten, neue Blöcke zu schürfen und möglichst viele gültige Transaktionen in diese Blöcke einzubauen.

- Incentives (Anreize) im Kontext einer Kryptowährung dienen dazu, Menschen zu ermutigen, die Infrastruktur für die Blockchain zur Verfügung zu stellen und das Protokoll zu unterstützen.
- Im Falle von Bitcoin oder Ethereum bedeutet dies zum Beispiel, Knoten zu unterhalten, neue Blöcke zu schürfen und möglichst viele gültige Transaktionen in diese Blöcke einzubauen.
- Im Falle von Cardano bedeutet es, sich an den Slot-Leader-Wahlen zu beteiligen und einen Block zu erstellen, wenn man gewählt wurde.

- Incentives (Anreize) im Kontext einer Kryptowährung dienen dazu, Menschen zu ermutigen, die Infrastruktur für die Blockchain zur Verfügung zu stellen und das Protokoll zu unterstützen.
- Im Falle von Bitcoin oder Ethereum bedeutet dies zum Beispiel, Knoten zu unterhalten, neue Blöcke zu schürfen und möglichst viele gültige Transaktionen in diese Blöcke einzubauen.
- Im Falle von Cardano bedeutet es, sich an den Slot-Leader-Wahlen zu beteiligen und einen Block zu erstellen, wenn man gewählt wurde.
- Ein Proof-of-Stake System wie Cardano erfordert wesentlich weniger Energie als ein Proof-of-Work System, aber es ist trotzdem wichtig für Sicherheit und Effizienz, dass Teilnehmer motiviert werden, zu gegebener Zeit online zu sein und ihre Arbeit zu tun.

- Wenn wir von Anreizen sprechen, meinen wir in dieser Vorlesung in erster Linie finanzielle Anreize.
- Als Ausgleich für ihre Kosten und Mühen bekommen Teilnehmer am Protokoll Zahlungen in Form der Kryptowährung.

- Trotzdem ist es wichtig, daran zu denken, dass finanzielle Anreize nicht die einzigen und vielleicht nicht einmal die wichtigsten sind.
- Andere Anreize sind Idealismus, Moral und allgemein der Wunsch, “das Richtige zu tun”.

- Trotzdem ist es wichtig, daran zu denken, dass finanzielle Anreize nicht die einzigen und vielleicht nicht einmal die wichtigsten sind.
- Andere Anreize sind Idealismus, Moral und allgemein der Wunsch, “das Richtige zu tun”.
- Als zum Beispiel der Bitcoin Mining Pool GHash.io 2014 51% der Hash-Rate auf sich vereinigte, verpflichtete er sich freiwillig dazu, in Zukunft 40% nicht zu überschreiten.

- Trotzdem ist es wichtig, daran zu denken, dass finanzielle Anreize nicht die einzigen und vielleicht nicht einmal die wichtigsten sind.
- Andere Anreize sind Idealismus, Moral und allgemein der Wunsch, “das Richtige zu tun”.
- Als zum Beispiel der Bitcoin Mining Pool GHash.io 2014 51% der Hash-Rate auf sich vereinigte, verpflichtete er sich freiwillig dazu, in Zukunft 40% nicht zu überschreiten.
- GHash.io nahm finanzielle Verluste in Kauf, um das Richtige zu tun und das Ideal einer dezentralisierten Währung nicht zu verraten.

- Trotzdem ist es wichtig, daran zu denken, dass finanzielle Anreize nicht die einzigen und vielleicht nicht einmal die wichtigsten sind.
- Andere Anreize sind Idealismus, Moral und allgemein der Wunsch, “das Richtige zu tun”.
- Als zum Beispiel der Bitcoin Mining Pool GHash.io 2014 51% der Hash-Rate auf sich vereinigte, verpflichtete er sich freiwillig dazu, in Zukunft 40% nicht zu überschreiten.
- GHash.io nahm finanzielle Verluste in Kauf, um das Richtige zu tun und das Ideal einer dezentralisierten Währung nicht zu verraten.

Ideal

Moralische und finanzielle Anreize sollten sich nicht widersprechen.

- Das Beispiel von GHash.io zeigt, dass zumindest im Fall von Bitcoin das Ideal nicht erreicht wird.
- Finanzielle und moralische Anreize können zueinander im Widerspruch stehen und Menschen zwingen, sich für das eine oder das andere zu entscheiden.

- Das Beispiel von GHash.io zeigt, dass zumindest im Fall von Bitcoin das Ideal nicht erreicht wird.
- Finanzielle und moralische Anreize können zueinander im Widerspruch stehen und Menschen zwingen, sich für das eine oder das andere zu entscheiden.
- Ziele des Incentives-Designs von Cardano war es, die finanziellen Anreize so zu gestalten, dass sie automatisch zu Verhalten führen, dass gut für das System ist.

Silvio Micali, der Erfinder des Proof-of-Stake Systems Algorand, hat sich bewusst gegen ein System von Anreizen für Algorand ausgesprochen. Seiner Meinung nach ist der Betrieb von Algorand billig genug, um ohne Anreize auszukommen, deren korrektes Design seiner Meinung nach sowieso zu kompliziert und schwierig sei.

- Bei Bitcoin stammen die finanziellen Anreize aus zwei Quellen, Transaktionsgebühren und Coinbase Transaktionen.
- Der Miner, der ein Krypto-Puzzle löst und einen Block erzeugt, erhält zur Belohnung alle Transaktionsgebühren aus allen im Block enthaltenen Transaktionen.
- Außerdem darf er eine spezielle “Coinbase Transaktion” in den Block einfügen, die im Gegensatz zu gewöhnlichen Transaktionen keine Inputs hat und ihm eine bestimmte Menge an Bitcoin (z.Zt. 12.5 ฿) gutschreibt.
- Durch Coinbase Transaktionen werden neue Bitcoin erzeugt. Die Belohnung wird alle 210.000 Blöcke halbiert, so dass die Gesamtmenge von Bitcoin endlich ist.

- Es ist für Bitcoin-Miner aufgrund des Designs der Bitcoin-Anreize finanziell vorteilhaft, sich in Mining-Pools zusammenzuschließen:
  - Kosten können durch Synergie-Effekte gesenkt werden.
  - Die Varianz des erwarteten Einkommens sinkt, so dass finanzielle Planung einfacher wird.
- Allerdings läuft die Konzentrierung in Mining-Pools dem Ideal einer dezentralisierten Währung zuwider.
- Dies ist ein Beispiel eines Incentive-Designs, dass finanzielle Anreize bietet, die nicht perfekt auf das Wohl des Systems ausgerichtet sind.

- Da die Belohnungen bei Bitcoin aus zwei Quellen stammen, den Transaktionsgebühren und den Coinbase-Transaktionen, müssen Bitcoin-Miner zwei Dinge optimieren:
  - Einerseits natürlich ihre Hash-Rate, damit sie möglichst oft Blöcke erzeugen und dann dafür belohnt werden.
  - Andererseits die Summe der in ihren Blöcken enthaltenen Transaktionsgebühren.

- Da die Belohnungen bei Bitcoin aus zwei Quellen stammen, den Transaktionsgebühren und den Coinbase-Transaktionen, müssen Bitcoin-Miner zwei Dinge optimieren:
  - Einerseits natürlich ihre Hash-Rate, damit sie möglichst oft Blöcke erzeugen und dann dafür belohnt werden.
  - Andererseits die Summe der in ihren Blöcken enthaltenen Transaktionsgebühren.
- Letzteres ist ein interessantes mathematisches Problem: Wie wähle ich Transaktionen derart aus meinem Mempool aus, dass diese
  - alle untereinander und mit der Blockchain konsistent sind (denn sonst wäre der Block ja ungültig) und
  - andererseits die Summe der enthaltenen Transaktionsgebühren maximal ist?

- Nicht jeder hat Lust, Zeit und technisches Know-How, Blöcke in einer Kryptowährung zu schürfen — dies gilt für Cardano genauso wie für Bitcoin und Ethereum.
- Daher ist es auch in Cardano für “Power-User” möglich, sogenannte Stake-Pools zu gründen, an die andere Benutzer dann ihren Stake delegieren können.
- Dabei ist es wichtig, zu beachten, dass in einem Proof-of-Stake-System wie Cardano Geld eine Doppelrolle hat.
  - Es dient wie in anderen Kryptowährungen auch als Zahlungsmittel.
  - Sein Besitz ist aber auch an die Chancen bei der Wahl zum Slot-Leader geknüpft: Je mehr Geld man hat, desto höher die Chance, Slot-Leader zu werden und einen Block erzeugen zu dürfen.
- Beim Delegieren wird nur die *zweite* Funktion delegiert, nicht die erste. Auch wer an einen Stake-Pool delegiert kann sein Geld weiterhin frei als Zahlungsmittel benutzen. Er tritt lediglich sein Recht ab, an Slot-Leader-Wahlen teilzunehmen.

- In Cardano ist unser Ziel, die Anreize so zu gestalten, dass sich “automatisch” eine bestimmte, vorgegebene Zahl k von Stake-Pools bildet (k wird wahrscheinlich 1000 sein).
- Diese Pools sollten alle in etwa dieselbe Größe haben.
- Im Gegensatz zu Bitcoin sollen sich dieses gewünschte Ergebnis und die finanziellen Interessen der Teilnehmer nicht widersprechen.

- Die Grundidee ist, dass die Anreize wie bei Bitcoin aus zwei Quellen stammen, Transaktionsgebühren und “neues Geld”.
- Im Gegensatz zu Bitcoin werden Belohnungen aber nicht pro Block, sondern pro Epoche bezahlt: Alle Transaktionsgebühren aus allen Blöcken einer Epoche werden gesammelt, “neues Geld” wird hinzugefügt, und diese Summe wird dann zunächst unter den Stake-Pools verteilt, die das Geld dann weiter unter ihren Mitgliedern aufteilen.
- All dies sollte möglichst fair sein, d.h. die Grundidee wäre, die Stake-Pools proportional zu ihrer Größe zu belohnen.
- Außerdem sollten die Betreiber der Stake-Pools einen etwas höheren Anteil des Gewinns des Pools bekommen, um sie für ihre Kosten zu entlohnen, d.h. sie dürfen sich einen gewissen Anteil vom Gewinn nehmen, bevore dieser unter allen Mitgliedern aufgeteilt wird.

- Wie kann man prüfen, ob ein gegebenes System von Anreizen zu einem gewünschten Ergebnis führt?
- Einen Ansatz dazu bietet die mathematische Disziplin der Spieltheorie.
- Für Mathematiker wird ein Spiel für einen oder mehrere Spieler durch eine Menge von Strategien für jeden Spieler und eine Payoff Matrix (Auszahlungsmatrix) definiert, die angibt wieviel (Geld, Punkte,...) jeder Spieler bekommt, wenn sich jeder Spieler für eine seiner Strategier entschieden hat.

- Wie kann man prüfen, ob ein gegebenes System von Anreizen zu einem gewünschten Ergebnis führt?
- Einen Ansatz dazu bietet die mathematische Disziplin der Spieltheorie.
- Für Mathematiker wird ein Spiel für einen oder mehrere Spieler durch eine Menge von Strategien für jeden Spieler und eine Payoff Matrix (Auszahlungsmatrix) definiert, die angibt wieviel (Geld, Punkte,...) jeder Spieler bekommt, wenn sich jeder Spieler für eine seiner Strategier entschieden hat.

Bemerkung

Bei vielen Spielen haben alle Spieler dieselben Strategien zur Auswahl, aber das muss nicht so sein. (Denken Sie z.B. an das Gesellschaftsspiel “Wolf und Schafe”, bei dem die beiden Spieler völlig unterschiedliche Züge zur Verfügung haben, je nachdem, ob sie Wolf oder Schaf spielen!)

Zwei Spieler A und B haben je zwei Strategier, “schweigen” und “verraten” mit der folgenden Auszahlungsmatrix:

	B schweigt	B verrät
A schweigt	-1/-1	-3/0
A verrät	0/-3	-2/-2

Wenn also z.B. A schweigt und B verrät, dann beträgt A’s Auszahlung -3, und B’s Auszahlung beträgt 0.

- Eines der wichtigsten Konzepte in der Spieltheorie ist das des Nash-Equilibriums, benannt nach dem berühmten Mathematiker John Forbes Nash Jr. (Nobelpreis für Öknonmie 1994).
- Ein Nash-Equilibrium besteht wird durch eine Wahl einer Strategie für jeden Spieler gegeben, welche die Eigenschaft hat, dass kein Spieler seine Auszahlung durch Wahl einer anderen Strategie verbessern kann, sofern alle anderen Spieler ihre Strategie beibehalten.
- Jedes “gutartige” Spiel hat mindestens ein Nash-Equilibrium.
- Wenn ein Spiel von rationalen Spielern gespielt wird, tendiert es dazu, in einem Nash-Equilibrium zu enden.
- Daher ist es wichtig, die Nash-Equilibria eines Spiels zu verstehen, wenn man das Spiel verstehen will.

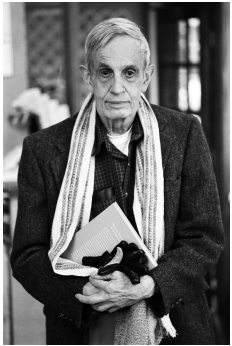

Abb.: John Nash. Von Peter Badge / Typos1 — OTRS submission by way of Jimmy Wales, CC BY-SA 3.0

Beispiel: Nash-Equilibrium im Gefangenendilemma

	B schweigt	B verrät
A schweigt	-1/-1	-3/0
A verrät	0/-3	-2/-2

	B schweigt	B verrät
A schweigt	-1/-1	-3/0
A verrät	0/-3	-2/-2

- Wenn einer der Spieler schweigt, kann er immer eine höhere Auszahlung erhalten, wenn er stattdessen verrät.

	B schweigt	B verrät
A schweigt	-1/-1	-3/0
A verrät	0/-3	-2/-2

- Wenn einer der Spieler schweigt, kann er immer eine höhere Auszahlung erhalten, wenn er stattdessen verrät.
- Wenn beide verraten, hat keiner einen Anreiz, einseitig zur Strategie “schweigen” zu wechseln.

	B schweigt	B verrät
A schweigt	-1/-1	-3/0
A verrät	0/-3	-2/-2

- Wenn einer der Spieler schweigt, kann er immer eine höhere Auszahlung erhalten, wenn er stattdessen verrät.
- Wenn beide verraten, hat keiner einen Anreiz, einseitig zur Strategie “schweigen” zu wechseln.
- Dies bedeutet, dass die Wahl “verraten” für beide das einzige Nash-Equilibriums dieses Spiels ist.

Finden Sie das eindeutige Nash-Equilibrium des folgenden Nullsummenspiels (was bedeutet, dass die Zahlen in der Auszahlungsmatrix die Auszahlungen des *ersten* Spielers (der eine Reihe wählt) sind und dass die des zweiten Spielers (der eine Spalte wählt) das jeweils Negative sind):

	1	2	3	4	5
1	0	1	8	-9	1
2	4	3	5	5	2
3	-5	-6	6	2	-1
4	0	4	-3	1	-5
5	9	-9	8	8	0

- Wie kann man all dies auf das Design der Anreize bei Cardano anwenden?
- Wir modellieren Staking als Spiel, wobei jeder Spieler zwei Arten von Strategien hat:
  - Ein Spieler kann einen Stake-Pool eröffnen und seine Gewinnmarge wählen (wie viel er vom Gewinn des Pools nehmen darf, bevor der Rest gerecht verteilt wird).
  - Ein Spieler kann an einen oder mehrere Pools delegieren.
- Nun können wir Spieltheorie benutzen, um zu untersuchen, ob die von uns gewünschte Konstellation (also k etwa gleich große Pools) ein Nash-Equilibrium dieses Spiels ist.

- Angenommen, die Strategien, die alle Spieler wählen, führen zu der von uns gewünschten Konstellation.
- Dann hätte ein Spieler, der an einen Pool delegiert hat, einen Anreiz, an einen größeren Pool zu delegieren, da dort die Kosten auf mehr Schultern verteilt werden und der Gewinn pro Spieler damit höher ist.
- Dies Zeit, dass die von uns gewünschte Konstellation kein Nash-Equilibriums ist.
- Wir müssen die Belohnungen daher anders aufteilen!

- Angenommen, die Strategien, die alle Spieler wählen, führen zu der von uns gewünschten Konstellation.
- Dann hätte ein Spieler, der an einen Pool delegiert hat, einen Anreiz, an einen größeren Pool zu delegieren, da dort die Kosten auf mehr Schultern verteilt werden und der Gewinn pro Spieler damit höher ist.
- Dies Zeit, dass die von uns gewünschte Konstellation kein Nash-Equilibriums ist.
- Wir müssen die Belohnungen daher anders aufteilen!
- Wir haben die Aufteilung der Belohnungen so modifiziert, dass Pools ihren fairen Anteil bekommen, solange sie nicht größer als $1/k$ sind. Ab einer Größe von $1/k$ wachsen die Belohnungen für den Pool nicht weiter.

- Ein weiteres Problem sind sogenannte Sybil Attacken: Bei einem solchen Angriff erzeugt ein Spieler eine sehr große Anzahl von Pools und macht diese (durch geringe Kosten) sehr attraktiv, wodurch er womöglich mehr als 50% des Stakes dazu bewegen kann, an einen dieser Pools zu delegieren. Damit hätte er ohne großen eigenen Stake die Kontrolle über die Blockchain.
- Wir mitigieren dieses Problem, indem wir die Belohnungen eines Pools leicht erhöhen, wenn der Pool-Betreiber mehr eigenen Stake in seinen Pool einbringt.
- Dies macht eine Sybil-Attacke unrealistisch, weil der Angreifer seinen Stake auf so viele Pools aufteilen müsste, dass diese dann geringere Belohnungen als “ehrliche” Pools zahlen würden.
- Andererseits führt dies zu einer Bevorzugung der “Reichen” — man muss also zwischen Fairness und Schutz vor Sybil-Attacken awägen, wenn man den Einfluss des Stakes des Pool-Betreibers auf die Pool-Belohnungen justiert.

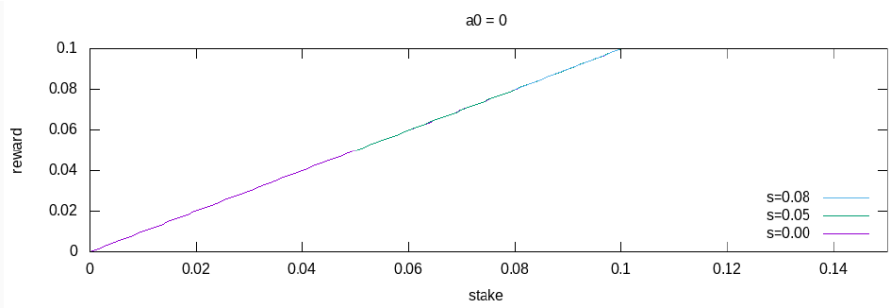

Abb.: Grafische Darstellung der Pool-Belohnungen abhängig von Pool-Größe und Stake des Pool-Betreibers.

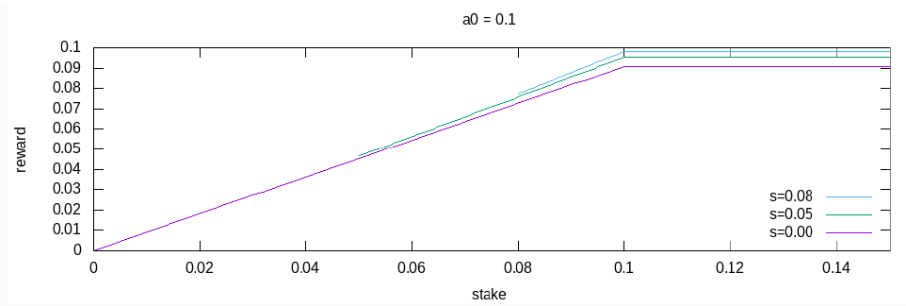

Abb.: Grafische Darstellung der Pool-Belohnungen abhängig von Pool-Größe und Stake des Pool-Betreibers.

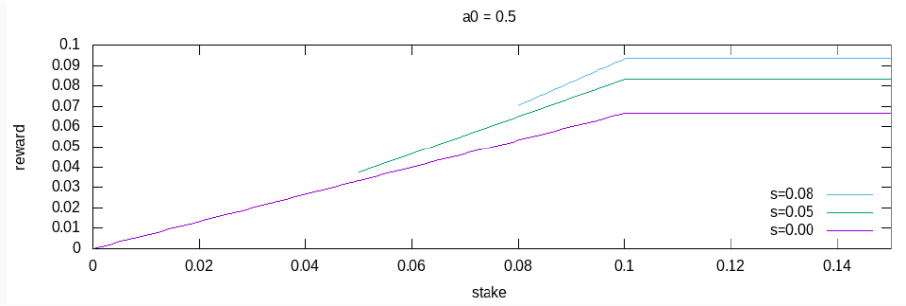

Abb.: Grafische Darstellung der Pool-Belohnungen abhängig von Pool-Größe und Stake des Pool-Betreibers.

Man kann beweisen, dass diese Verfeinerungen der Grundidee tatsächlich dazu führen, dass alle Nash-Equilibria des Spiels die gewünschte Form haben: k Pools von der Größe $1/k$.

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.