Orakel und Smart Contracts

meetup.123-altcoin.de

190311

Orakel

von Delphi?

Orakel von Delphi

Wikipedia:
“Das Orakel von Delphi war eine Weissagungsstätte des antiken Griechenlands.”

Orakel von Delphi

https://www.kinderzeitmaschine.de/antike/griechen/lucys-wissensbox/goetter-und-sagen/was-war-das-orakel-von-delphi/

“Standen bei den Griechen wichtige Entscheidungen an, so befragten sie das Orakel von Delphi. Wahrscheinlich waren die Griechen nicht so entscheidungsfreudig und benötigten da einfach Hilfe.”

“Das Orakel von Delphi war dem Gott Apollon geweiht und es war auch das wichtigste Orakel der antiken Welt. “

“Der Spruch des Orakels wurde von der Pythia verkündet. Sie war auch die einzige Frau, die den Apollontempel betreten durfte, ansonsten waren da nämlich nur Männer zugelassen. Wissenschaftler vermuten, dass sie in der Nähe einer Erdspalte saß, aus der besondere Gase hervortraten. Durch diese Gase war die Dame wohl immer etwas benebelt und redete recht wirr daher. “

Orakel von Delphi

https://www.kinderzeitmaschine.de/antike/griechen/lucys-wissensbox/goetter-und-sagen/was-war-das-orakel-von-delphi/

“Ihre ziemlich undeutlich gestammelten und oft auch unverständlichen Worte wurden dann von den Priestern des Apollon irgendwie "übersetzt", denn der Orakelspruch war ja nie so ganz eindeutig.

Das sollte er allerdings auch gar nicht sein. Ging ein Wunsch oder ein Orakelspruch nicht so in Erfüllung, wie es sich der Fragesteller erhoffte, konnte man ja immer noch sagen, es sei ganz anders gemeint gewesen. “

Zusammengefasst: Orakel von Delphi

- **Wurde bei (wichtigen) Entscheidungen befragt**
- **Orakelspruch war nicht eindeutig und bedurfte Übersetzern**
- **Orakelspruch betraf die Zukunft**

Blockchain Institut

Orakel im Blockchain-Kontext

- **Wird bei (wichtigen) Entscheidungen befragt (durch Smart Contracts, die blind für alles außerhalb ihrer Blockchain sind)**
- **Orakelspruch soll immer eindeutig sein**
- **Orakelspruch betrifft (vollendete) Gegenwart (grammatikalische Zeitform: Perfekt)**

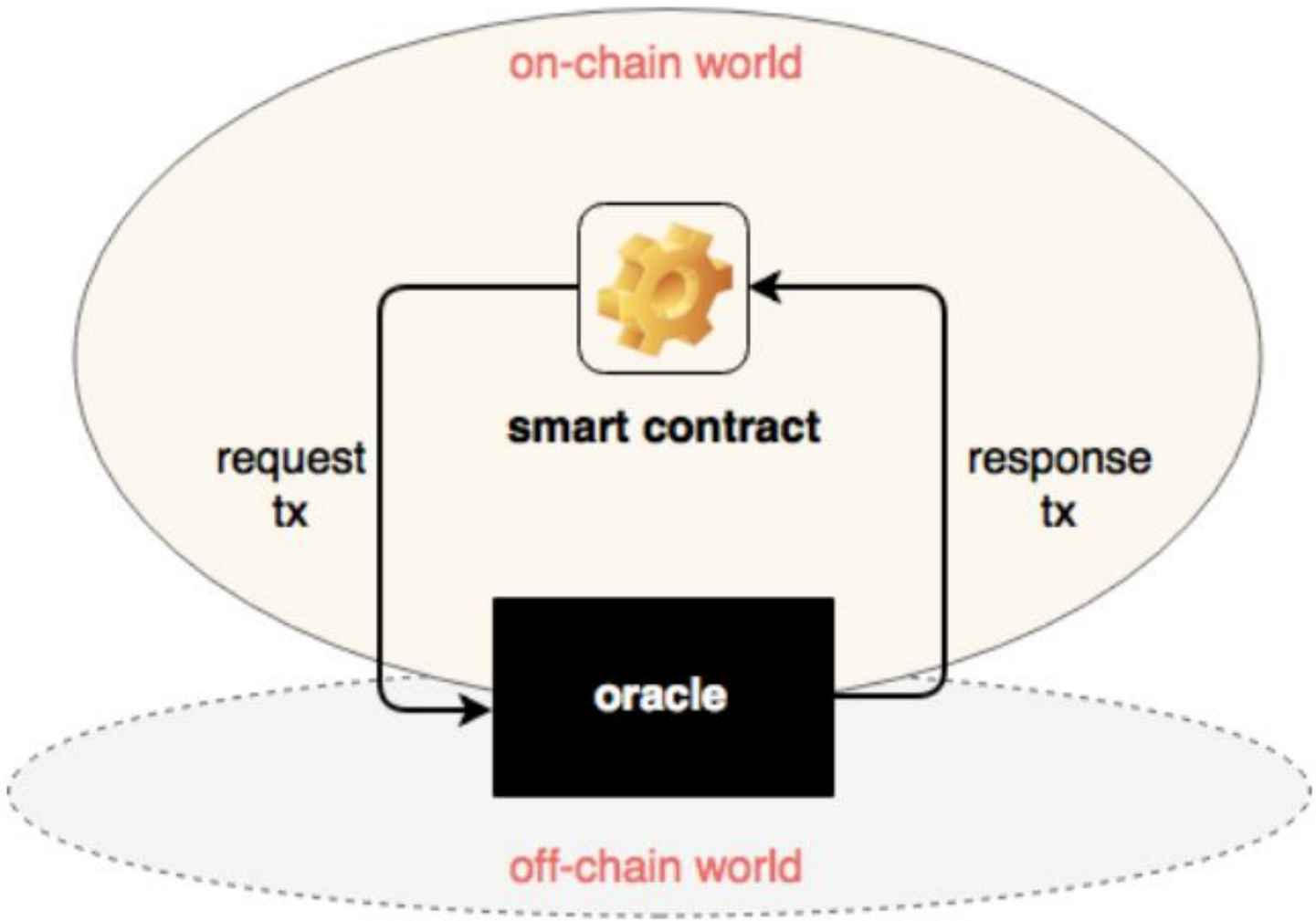
- **Aber: Kann man einem Orakel vertrauen?**

Blockchain Institut

Wie unterscheiden sich BC-Orakel?

Orakelklassen

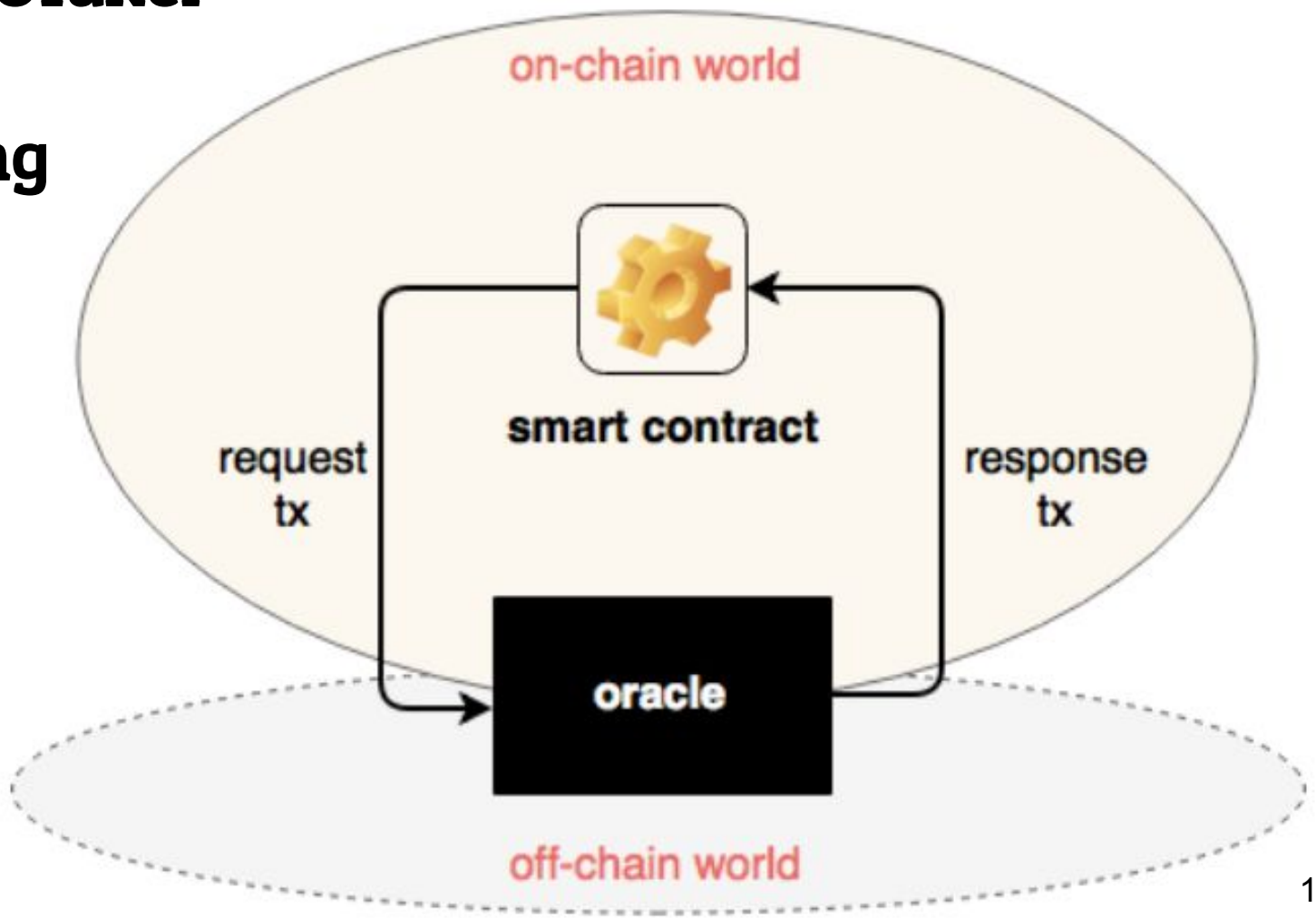
- **Maschinengetrieben**
- **Sozialgetrieben**



Orakeltypen

- **Software-Orakel (Datenfeeds)**
- **Hardware-Orakel (Sensoren)**
- **Menschliche Orakel**

- **Incentivierung der Leistung**
- **Anfragen pro Zeiteinheit**



Wie kann man BC-Orakeln vertrauen?

Vertrauen von Fremden als Blinder

Wir erinnern uns an die Lösung des Problems der byzantinischen Generäle durch Satoshi Nakamoto.

PROBLEM:

- **SmartContracts können nicht auf externe Daten zugreifen.**
- **Sie benötigen einen Sehenden, der außerhalb der Blockchain auch schauen kann.**

Bei der Befragung von Orakeln:

1. **Aus den Fehlern der Griechen lernen, denn ihr Imperium ging unter**
2. **Mehrere Orakel befragen**
3. **Mehrheitsquorum (notw. Stimmenzahl zur Gültigkeit einer Abstimmung)**

Wahrheit des Orakelspruchs

Wahrheit der Daten:

- **Schwierig bei Software-Orakeln (Datenströmen)**
- **Hart bei Hardware-Orakeln (Sensordaten), wenn ohne “Trusted Environment”**
- **Unmöglich bei menschlichen Orakeln**

=> Orakel mit Reputation in der Realwelt z.B. Bloomberg, Reuters

=> Orakel-Pools

- **Incentivierung der beteiligten Orakel steigert Kosten**
- **Aussortieren der Orakel mit falschen Antworten, ggf. monetäre Bestrafung durch Pfandverlust**

Blockchain Institut

Wahrheit des Orakelspruchs

Wahrheit der Daten:

- **Schwierig bei Software-Orakeln (Datenströmen)**
- **Hart bei Hardware-Orakeln (Sensordaten), wenn kein “Trusted Enviroment”**
- **Unmöglich bei menschlichen Orakeln**

=> Orakel mit Reputation in der Realwelt z.B. Bloomberg, Reuters

=> Orakel-Pools

- **Incentivierung beteiligter Orakel erhöht Kosten**
- **Aussortieren der Orakel mit falschen Antworten, ggf. monetäre Bestrafung durch Pfandverlust**

Blockchain Institut

Orakeldienste

- **Orakel bei eigenem Knotenrechner**
- **Fremde Orakelservices**
- **Orakel-Clouds**

- **Notar- und Reputationsdienste für Orakeldaten**

- **Orakel-Marktplätze:**
  - **Dezentrale Prognosemärkte (wie Augur, Gnosis, Bitcoin Hivemind, OpenBazaar) könnten Orakeldienste durch automatisierte Smart Contracts sicherer, kostengünstiger und transparenter machen.**
  - **IOTA-Marktplatz für Sensordaten**

Blockchain Institut

Thor Alexander

+49 171 120 0 121

meetup@bc-i.org