

Byzantinische Fehler

Matthias Reumann

9. April 2020

Inhaltsverzeichnis

1	Byzantinische Fehler	3
1.1	Definition	3
1.2	Anwendungen	3
2	Problem der byzantinischen Generäle	3
2.1	Beispiel mit drei Generälen	4
2.2	Mögliche Lösungen	5

1 Byzantinische Fehler

1.1 Definition

Byzantinische Fehler treten in verteilten Systemen auf, wenn fehlerhafte Nachrichten von einem Knoten versendet werden, die von der Struktur und vom Inhalt nicht von fehlerfreien unterscheidet werden können. [2]

Den Namen hat diese Fehlerklasse im Jahr 1982 von Lamport et. al. im Papier *The Byzantine Generals Problem* erhalten.[1] In diesem werden Byzantinische Fehler durch das abstrakte Beispiel der Byzantinischen Generäle näher erklärt.

1.2 Anwendungen

Da Fehlentscheidungen katastrophale Folgen hätten, wird in Boeing Flugzeugsystemen Byzantinischen Fehlern eine hohe Bedeutung zugewiesen. Das Raumfahrtunternehmen SpaceX beachtet byzantinische Fehler in ihren Dragon Raumschiffen, welche Astronauten zur ISS transportieren sollen. Um die Integrität der Blockchain zu gewährleisten, ist die Implementierung von Bitcoin Byzantinische Fehler Tolerant (BFT).

2 Problem der byzantinischen Generäle

Mehrere Generäle und ihre Truppen umzingeln eine feindliche Stadt. Da diese voneinander räumlich getrennt sind können sie nur über Boten miteinander kommunizieren. Jeder General beobachtet den gemeinsamen Feind und schlussendlich muss eine gemeinsame Entscheidung getroffen werden um den Feind zu besiegen. Jedoch könnten unter den Generälen Verräter sein, deren Ziel es ist eine gemeinsame Entscheidung der loyalen Generäle zu verhindern.

Die Generäle müssen einen Algorithmus finden der garantiert, dass

- (a) Alle loyalen Generäle die gleiche Entscheidung treffen
- (b) Eine geringe Anzahl an Verrätern die loyalen Generäle nicht zu einer Fehlentscheidung führt

Eine Entscheidung unter den Generälen wird gefällt indem jeder General seine Informationen an die anderen Generäle weitergibt. Die Nachricht gesendet vom i .ten General wird als $v(i)$ bezeichnet. Jeder General erhält die Nachrichten $v(1)$ bis $v(n)$, wobei n die Anzahl der Generäle darstellt.

Die finale Entscheidung wird durch die absolute Mehrheit der Werte dieser Nachrichten bestimmt. In diesem konkreten Beispiel können die Werte entweder *ANGRIFF* oder *RÜCKZUG* sein.

Allerdings könnte es sein, dass ein Verräter unterschiedliche Werte zu unterschiedlichen Generälen sendet, was wiederum bedeutet, dass loyale Generäle unterschiedliche $v(i)$ Werte besitzen.

Deshalb müssen sogenannte *interactive consistency conditions* gelten. Ein führender General, auch Commander genannt, sendet einen Befehl an seine $n - 1$ Leutnant Generäle so, dass:

- IC1 Alle loyalen Leutnants den gleichen Befehl ausführen
- IC2 Wenn der Commander loyal ist, dann befolgt jeder loyale Leutnant seinen Befehl

2.1 Beispiel mit drei Generälen

In diesem Abschnitt wird eine Situation beschrieben in der drei Generäle miteinander kommunizieren. Wichtig dabei ist, dass niemand der loyalen Generäle weiß wer der Verräter ist.

In Abbildung 1 ist Leutnant 2 (L2) der Verräter. Der loyale Commander sendet den Befehl *ANGRIFF* an beide Leutnants L1 und L2. Zur Verifizierung sendet L2 L1 die Nachricht, er habe den Befehl *RÜCKZUG* erhalten. L1 hat nun die Nachrichten *ANGRIFF* und *RÜCKZUG* und kann auf Grund dessen keine eindeutige Entscheidung treffen.

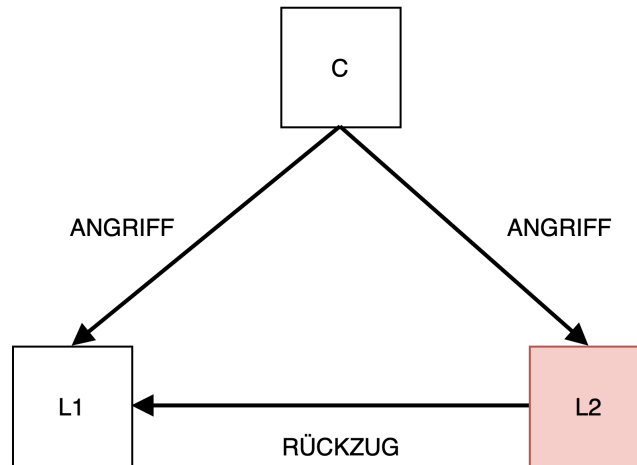


Abbildung 1: L2 ist der Verräter. L1 muss den Befehl des Commanders ausführen um die IC2 einzuhalten.

Im nächsten Szenario (Abbildung 2) ist der Commander der Verräter. Dieser sendet unterschiedliche Befehle an L1 und L2. Für L1 ist es die exakt selbe Situation wie in Abbildung 1. L2 steht vor dem selben Problem.

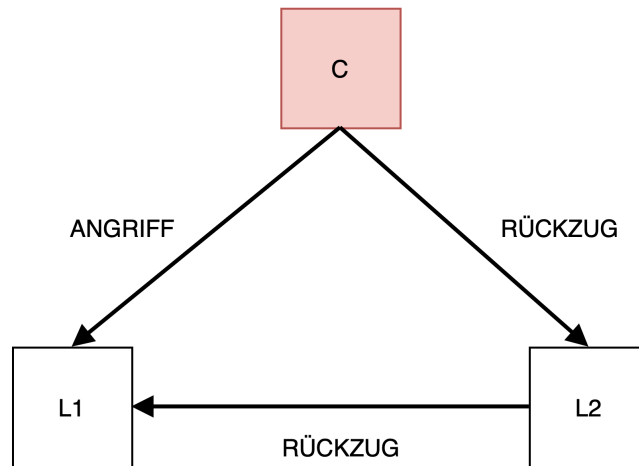


Abbildung 2: Der Commander ist der Verräter. Für L1 ist es die selbe Situation wie in Abbildung 1.

Wie aus diesem Beispiel hervorgeht, existiert keine Lösung für drei Generäle mit einem Verräter. Um einen byzantinischen Fehler zu erkennen muss daher folgende Eigenschaft gelten: $n \geq 3m + 1$, wobei n die Anzahl der Generäle und m die Anzahl der Verräter in diesem System ist. Mit anderen Worten, mehr als zwei Drittel müssen loyal sein, um einen byzantinischen Fehler zu erkennen.

2.2 Mögliche Lösungen

Eine mögliche Lösung des Problems ist das Hinzufügen eines weiteren Generals. Dadurch kann, wenn jeder Leutnant seine erhaltene Nachricht an die anderen Leutnants sendet, genau ein byzantinischer Fehler erkannt werden.

Literatur

- [1] Lamport et. al. *The Byzantine Generals Problem*. URL: <https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf>. (Zugegriffen am: 06.04.2020).
- [2] Esra Unal. *Seminararbeit Byzantinische Fehler*. URL: http://www.mi.fu-berlin.de/inf/groups/ag-tech/teaching/2010_SS/S_19510b_Proseminar_Technische_Informatik/esra-uenal-report.pdf. (Zugegriffen am: 06.04.2020).