

Blockchain Queries

Studiengang: BSc in Informatik | Vertiefungen: Mobile Computing / IT-Security

Betreuer: Dr. Kai Brännler

Experte: Dr. Stéphane Barbey (Paranor Engineering AG)

Blockchain Queries ist eine Software um die Bitcoin Blockchain in eine Relationale Datenbank zu transformieren. Das flexible und detaillierte Datenbankmodell erlaubt es dem Nutzer beliebige Daten abzufragen. Auf diese Weise lassen sich Informationen aus der Blockchain extrahieren und neue Erkenntnisse zum Stand der Kryptowährung gewinnen.

Problemstellung

Blockchain ist die Technologie hinter Bitcoin, welche die Kryptowährung überhaupt erst ermöglicht. In dieser öffentlichen Aufzeichnung aller Transaktionen finden sich viele Daten (zurzeit ca. 70 GB binäre Rohdaten). Diese Daten zu extrahieren und zu analysieren ist aber nicht ganz einfach. Bereits vor einem Jahr konnten wir im Rahmen unserer Projekt-1-Arbeit aufzeigen, dass das Binärformat, in welchem die Blockchain abgelegt wird, zwar eine effiziente Speicherung erlaubt, zum Durchsuchen aber ungeeignet ist.

Bestehende Systeme

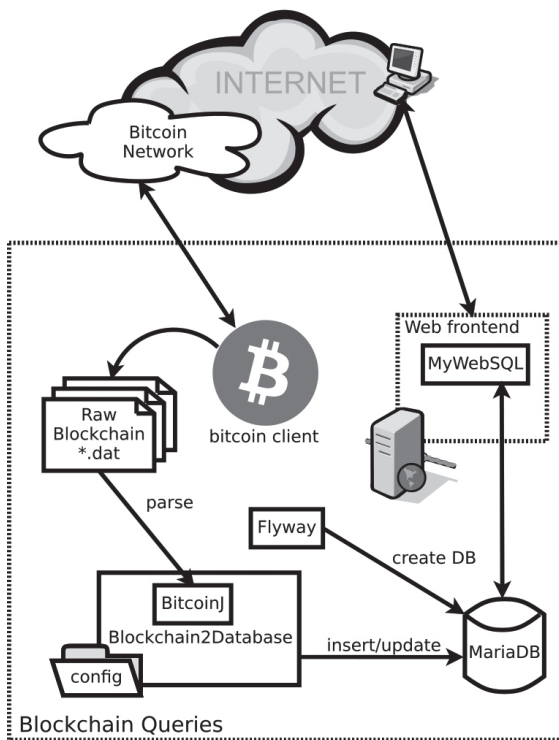
Es gibt eine Vielzahl bereits bestehender Lösungen um den Inhalt der Blockchain zu durchsuchen, die jedoch auf bestimmte Usecases ausgelegt sind. Herkömmliche Blockchainexplorer erlauben es Blöcke, Transaktionen und Adressen abzufragen. Diese werden mit zusätzlichen Informationen aufbereitet und dem Nutzer dargestellt. Damit können aber nur schwer Zusammenhänge untersucht werden.

Insbesondere ist aber die Art von Informationen nach denen sich Blockchainexplorer durchsuchen lassen beschränkt auf einige vorgegebene Werte. Auch bei den angezeigten Informationen und bereitgestellten Statistiken verhält es sich so. Zumeist sind diese Programme auf die finanziellen Aspekte von Bitcoin ausgelegt. Wer Informationen ausserhalb dieses Bereiches sucht, ist all zu oft auf sich allein gestellt.

Unsere Implementation

Mit unserer Arbeit wollen wir aufzeigen, dass sich mit relationalen Datenbanken auch ganzheitliche Lösungen für das Problem umsetzen lassen. Zu diesem Zweck haben wir eine neue Abbildung der Blockchain als ein relationales Datenmodell erstellt. Das daraus resultierende Datenbank Schema bildet die Blockchain umfassend ab und erlaubt das effiziente Durchsuchen nach einem breiten Spektrum an Informationen. Anhand ausgewählter Beispiele haben wir Abfragen erstellt, die zeigen wie sich das System flexibel einsetzen lässt. So lassen sich etwa Entwicklungen und Trends über die Zeit verfolgen, der Fluss von Geld aufzeigen und zusammenhängende Transaktionen finden.

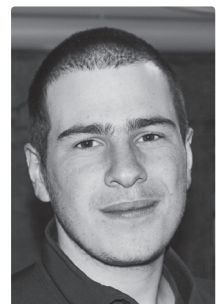
Damit das System trotz seiner Komplexität und der schier Menge an Daten gute Performance liefert, setzen wir auf eine schnelle In-Memory Datenbank und die bewährte Bitcoinj Bibliothek. Wenn die Daten der produktiven Bitcoin Blockchain komplett eingelesen sind beträgt die Grösse der Datenbank zurzeit etwa 400 GB.



Systemarchitektur



Stefan Jacob Andonie
stefan_andonie@gmx.ch



Niklaus Manuel Hofer