EOS
dezentralisierte Anwendungen

Entwicklung dezentraler Applikationen

Autor-Team: europe@eosbros.eu

Die verkürzte Bezeichnung "App" hat sich auf mobilen Geräten für Anwendungen durchgesetzt. Über das Internet werden mit dem Entwickler Daten ausgetauscht. Einzelne Anbieter (Monopole) können jederzeit unbemerkt Funktionen von mobilen Anwendung verändern, ohne dass Anwender dies bemerken.

Fortschrittliche dezentrale Anwendungen (dApps) werden nicht von einem einzelnen Anbieter betrieben, gewartet oder weiterentwickelt sondern in einem Netzwerk durch diverse Anbieter betrieben. Anwendungen werden im Netzwerk nicht nur als ausführbare Programme bereitgestellt, sondern zusätzlich können Netzwerk-Teilnehmer den Quelltext einsehen, um softwarebedingte Prozesse auf Sicherheit und Transparenz kontrollieren zu können.

Eine dApp-Software erfüllt vier Kriterien: Open-Source, basiert auf einer Blockchain, bietet kryptografisch verschlüsselte Token an und verfügt über einen Mechanismus, der diese Token erzeugt.

Open-Source bedeutet, dass der Software-Code frei

zugänglich und als geschriebener Text besteht.
Wird im Quelltext etwas geändert, verändern sich die Funktionen des Computerprogramms. Ein frei zugänglicher Quelltext kann, abgesehen von den Entwicklern der Software, von Dritten eingesehen, umprogrammiert und frei verwendet werden. Zudem muss dieser Quelltext autonom operieren. Es gibt keine zentrale Instanz, wie einen Systemadministratoren, der alleine darüber entscheidet, wie die zukünftige Entwicklung der dApp aussehen soll. Vielmehr muss sich das Protokoll, wodurch der Quellcode festgehalten wird, an Veränderungs-vorschläge für die zukünftige Entwicklung oder aber auch an Marktreaktionen anpassen. Alle Entwicklungen innerhalb des Quellcodes müssen außerdem durch einen Konsens der Entwickler entschieden werden.

Alle dApps müssen, um die Definition zu erfüllen, Daten, Berichte und den Quellcode auf einer dezentralisierten Blockchain speichern. Eine Blockchain (dtsch. Block-Kette) ist eine Software, die auf vielen, miteinander vernetzten Computern betrieben wird. Anders als bei Apps, wo die Funktion durch ein zentrales Rechenzentrum betrieben wird, funktionieren DApps dezentralisiert. Das hat den Vorteil, dass sie nicht gehackt werden können. Wird das gesamte Rechenzentrum von App-Firma gehackt, funktioniert App nicht mehr, Daten können gestohlen werden und im schlimmsten Fall missbraucht werden. Um eine dApp zu hacken, müssten Angreifer jeden einzelnen Computer des Netzwerkes gleichzeitig angreifen, die kryptografische Verschlüsselung der Blockchain knacken und dann den Quellcode der dApp ändern. Das ist nahezu unmöglich, weshalb die Wahrscheinlichkeit, eine dApp zu hacken, gegen null geht.

Die Speicherung des Quellcodes auf einer dezentralen, aber dennoch öffentlich einsehbaren, Blockchain verringert Angriffsflächen. Der Quellcode einer Software wird gezielt ausgewählten Entwicklern zur Verfügung gestellt, welche über sogenannte Tokens verfügen und damit den Quellcode ändern dürfen.

Kryptografisch verschlüsselte Token sind beispielsweise Teil einer kryptografisch verschlüsselten Blockchain. Was genau ein Token ist, ist nicht ganz so einfach zu verstehen. Wenn jemand in einem Satz das Wort „Hund“ verwendet, kann dieser Begriff unterschiedliche Bedeutungen haben. In dem Satz „Das ist mein Hund Botox.“, bezeichnet der Begriff tatsächlich einen echten Hund. In dem Satz „Du Hund!“, wird der Begriff als Beleidigung verwendet. Und in dem Satz „Was ist das für ein Hundewetter.“, meint der Begriff beispielsweise ein stürmisches, regnerisches Wetter. Es ist erkennbar, dass der Begriff von der Grundbedeutung her ein Säugetier mit Fell, mit vier Beinen, einem Schwanz, einer feuchten Nase, was bellen kann bezeichnet. In den unterschiedlichen Satzkontexten jedoch bekommt der Begriff eine andere Bedeutung. Die Grundbedeutung des Begriffes „Hund“ bleibt jedoch dieselbe. Sie bezeichnet in der eigenen Vorstellung immer das Säugetier. Die Grundbedeutung des Begriffes kann auch als Typ bezeichnet werden. Je nachdem in welchen Kontexten der Begriff nun verwendet wird, ändert sich diese Bedeutung. Die tatsächliche Verwendung des Begriffes „Hund“ wird „Token“ genannt. Ein Token ist eine definite Verwendung eines Begriffes in einem festgelegten Kontext. Kryptografisch verschlüsselte Token sind digitale Einheiten, welche eine Kopie eines sensiblen Datensatzes auf einer Blockchain darstellen.

Wenn im Bitcoin-Universum eine Identität mit Token operiert, also mit Bitcoin Handel betreibt (Bitcoins sind die Token der Bitcoin-Blockchain), wird mit einer Kopie eines Datensatzes der Bitcoin-Blockchain gehandelt. Das hat den Zweck, dass sie einerseits für das Mining, also die Erzeugung von Bitcoin durch die Lösung von Hashfunktionen, belohnt werden und andererseits die Blockchain nicht hacken können. Jedes Token bleibt solange ein Token, bis mehrere Miner, durch ein Peer-to-Peer-Netzwerk, eine Transaktion über die Blockchain bestätigt haben. Auf eine einfache Ebene runtergebrochen, kann Pauline dem Harald einen Bitcoin senden. Pauline sendet den Bitcoin direkt an die Wallet-Adresse von Harald. Der Bitcoin, beziehungsweise das Token, wird nun gemeinsam mit den Sender- und Empfänger-Adressen auf der Blockchain verzeichnet. In einem nächsten Schritt überprüfen Miner die Transaktionsbedingungen. Wenn mehrere Miner zum selben Ergebnis kommen, hat die Transaktion stattgefunden. Das hat den Zweck, dass keine zentrale Instanz notwendig ist, um eine Transaktion durchführen zu können. Weiterhin kann Pauline auf diese Weise Token, also den Betrag den sie in Bitcoin versendet, nicht beliebig umprogrammieren. Pauline könnte ihre Token einfach so umprogrammieren, dass sie auf einmal zwei Bitcoin an Harald sendet, obwohl sie nur einen besitzt. Genau dafür sind Token da. Sie verändern die Information, wer wie viel an wen gesendet hat, nicht direkt auf der Blockchain, sondern stellen eine verschlüsselte Datenkopie dar, welche von mehreren Minern überprüft wird, bevor sie endgültig in die Blockchain integriert wird. Auf diese Weise können Miner belohnt werden und falsche Transaktionen beziehungsweise Angriffe auf die Blockchain können sehr effizient abgewehrt werden.

dApps müssen einen Mechanismus verwenden, um kryptografisch verschlüsselte Token generieren zu können, damit Miner eine Belohnung bekommen können. Bitcoin verwendet den SHA-256-Algorithmus, den sogenannten Proof-of-Work-Algorithmus, um Bitcoins zu schürfen. Miner können sich einfach eine Bitcoin-Software herunterladen und Rechenleistung zur Verfügung stellen, um über eine Hashfunktion Transaktionsdaten miteinander zu verrechnen, damit diese verschlüsselt in der Bitcoin-Blockchain gespeichert werden können. Miner bilden das Rückgrat des Bitcoin-Netzwerkes. Ohne sie würde das Netzwerk nicht funktionieren. Diese vier Kriterien müssen erfüllt sein, damit eine App als dApp bezeichnet werden kann. Weiterhin gibt es drei Klassentypen von dApps: dApps die eine eigene Blockchain betreiben, dApps die eine Blockchain von Typ 1 verwenden und dApps die das Protokoll von Typ 2 verwenden. Die drei Klassen bauen logisch aufeinander auf. Als Beispiel sei die Kryptowährung Ethereum angeführt. Ethereum erfüllt die vier Kriterien einer dApp. Das Protokoll von Ethereum ist Open-Source, Ethereum verfügt über eine eigene Blockchain, verwendet kryptografisch verschlüsselte Token und verfügt über einen Token-Erzeugungs-Mechanismus. Ethereum bietet sogenannte Smart-Contracts an. Das sind digitale Verträge, welche zu festen Bedingungen programmiert werden und bei Erfüllung dieser Bedingung automatisch die vereinbarten Vertragsbedingungen erfüllt. Das hat beispielsweise den Vorteil, dass menschliche Fehler, beim Abschluss eines Vertrages, vollständig ausgeschlossen werden können. Über die Smart Contracts wird es möglich eigene dApps anbieten zu können. dApps die auf der Ethereum-Blockchain basieren sind beispielsweise R3, ein Blockchain-Konsortium, GNOSIS, eine Anwendung für dezentrale Prognosemärkte oder Microsoft Azure, ein Blockchain as a

Serivice (SaaS). Diese drei Beispiele sind in den Typ 2 einzuordnen, weil sie die Blockchain von Ethereum verwenden, also Typ 1. Eine Applikation die nun die Infrastruktur der Microsoft Azure Cloud nutzt, kann in den Typ 3 eingeordnet werden. Ein Beispiel dafür ist Heineken, Real Madrid oder Absolut, die alle auf Basis von Microsoft Azure eine App betreiben. Über die Smart-Contracts wird es möglich eigene dApps anbieten zu können.

dApp-Technologie sollte besonders effizient, kostengünstig und sicher sein.

Rethinking ideas, implementing them in a planned manner and benefiting.

Düsseldorf / D & Zug, CH // 2018.07 // EOSBROS-STAFF