Über das KILT Protocol

Jeden Monat lesen wir von Datenskandalen. Große Plattformen werden von Hackern angegriffen, die Millionen von Passwörtern stehlen und damit erheblichen Schaden anrichten. Manchmal sind es sogar die Plattformen selbst, die Daten verkaufen und die Konsequenzen verantworten.

Als Lösungsansatz wird Nutzern immer wieder empfohlen, viele unterschiedliche und möglichst komplizierte Passwörter zu verwenden. Das ändert aber nichts daran, dass die Passwörter in zentralen Silos von meist amerikanischen Internetplattformen gesammelt werden. Diese Silos bieten aufgrund ihrer Größe einen enormen Anreiz für Hacker und führen gleichzeitig zu monopolistischen Strukturen im Internet: Hat eine Internet-Plattform erst einmal Millionen von Benutzern, so ist Wettbewerb kaum noch möglich. Gute Ideen werden nicht finanziert, da Investoren die Marktmacht des Monopolisten scheuen; Innovation wird verhindert.

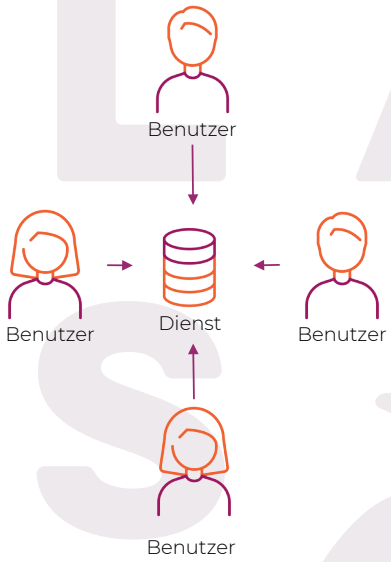

Abbildung 1: Viele Benutzer speichern ihre Benutzernamen und Passwörter bei einem zentralen Dienst.

Das Berliner Unternehmen BOTLabs packt dieses Problem bei der Wurzel, indem es Mechanismen für das Internet bereitstellt, die Benutzernamen und Passwörter generell unnötig und so deren zentrale Speicherung überflüssig macht. Die Grundidee ist so einfach wie bestechend: In der analogen Welt haben wir keine Benutzernamen und Passwörter, sondern Dokumente, mit denen wir uns ausweisen. Das von BOTLabs entwickelte KILT Protocol ermöglicht das Ausstellen und Vorzeigen von Dokumenten nun auch im Internet.

Das Verfahren funktioniert wie folgt: Ein Aussteller („Attester“) stellt Benutzern („Claimer“) auf Verlangen ein Dokument über eine bestimmte Eigenschaft aus, das von diesem Aussteller elektronisch signiert ist. Das Dokument wird nicht zentral beim Aussteller, sondern direkt beim Benutzer gespeichert, so als hätte man seinen Ausweis in die Brieftasche gesteckt.

Das KILT Protocol speichert eine Prüfsumme des signierten Dokuments auf der KILT Blockchain. Die Blockchain-Technologie ermöglicht es dem Benutzer, jederzeit die Echtheit seines Dokuments zu beweisen und sorgt gleichzeitig dafür, dass niemals personenbezogene Daten öffentlich verfügbar gemacht werden.

Möchte der Benutzer sich nun bezüglich einer bestimmten Eigenschaft ausweisen, sendet er anstelle eines Logins oder Passworts sein signiertes Dokument. Falls der Empfänger („Verifier“) auch der Aussteller des Dokuments war, kann er seine eigene Unterschrift überprüfen und den Benutzer hereinlassen. Ist der Empfänger ein anderer Dienst, der aber dem Aussteller generell vertraut, kann er auf der Blockchain die Gültigkeit des Dokuments überprüfen.

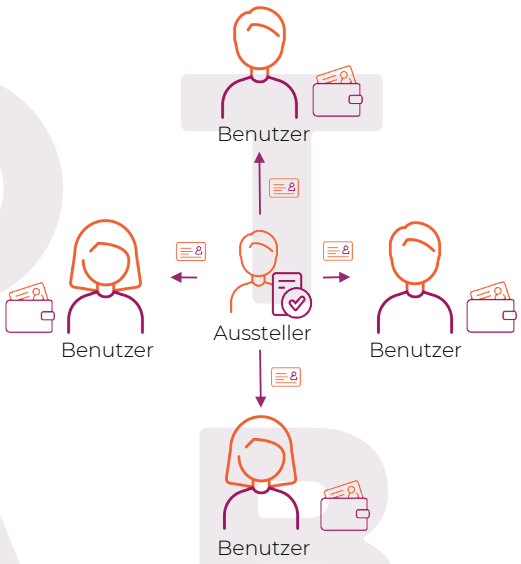

Abbildung 2: Jeder Benutzer bekommt ein individuelles, signiertes Dokument und legt es in seiner digitalen Brieftasche ab.

Genau wie bei Dokumenten aus der analogen Welt kann der Benutzer unterschiedliche Dokumente in seiner digitalen Brieftasche sammeln und diese je nach Bedarf einsetzen. Beispielsweise könnten mehrere verschiedene Dienste ein Dokument von einer

Abbildung 3: Abbildung 3: Eine Prüfsumme (Hash-Wert) des signierten Dokuments wird auf der KILT Blockchain abgelegt.

besonders vertrauenswürdigen Institution akzeptieren, so wie das in der analogen Welt beim Personalausweis der Fall ist. Der Benutzer behält dabei immer die volle Kontrolle über seine Daten: Er entscheidet, wem er welches Dokument zugänglich macht und sogar welcher Teil der Information auf dem Dokument sichtbar sein soll. Er hat vollständige Datensouveränität.

Durch das KILT Protocol wird der Vorgang der Dokumentenprüfung vom Aussteller entkoppelt: Derjenige, dem das Dokument gezeigt wird, entscheidet nur mit Hilfe der Blockchain darüber, ob er das Dokument akzeptiert. Der Aussteller selbst ist nicht mehr involviert. Dies entspricht ebenfalls dem Prozess in der analogen Welt, in der beispielsweise der Aussteller eines Personalausweises keine Information darüber erhält, dass der Benutzer den Ausweis bei einer Bank vorgelegt hat. Diese Entkoppelung als wichtige Eigenschaft des KILT Protocols schützt die Privatsphäre der Benutzer und schafft gleichzeitig eine enorme Skalierbarkeit des Systems, da eine beliebig hohe Anzahl von gleichzeitigen Überprüfungen stattfinden kann, ohne dass jedes Mal der Aussteller aktiv werden muss.

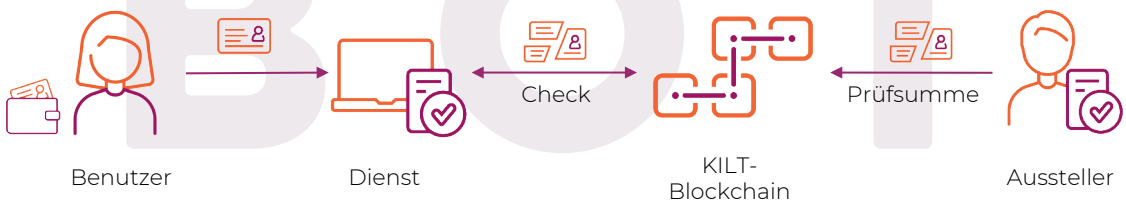

Abbildung 4: Der Benutzer meldet sich mit seinem Dokument bei einem Dienst an.

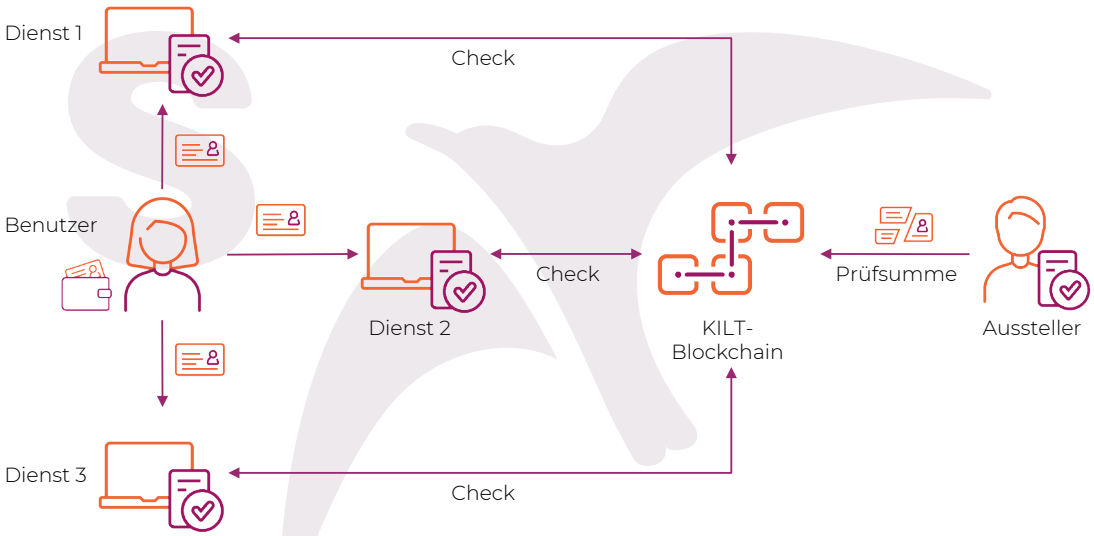

Abbildung 5: Ein Benutzer verwendet sein Dokument bei mehreren Diensten. Diese überprüfen auf der Blockchain die Gültigkeit des Dokuments.

Über BOTLabs

Die BOTLabs GmbH wurde im Januar 2018 vom Informatiker und ehemaligen Burda CTO Ingo Rübe gemeinsam mit Hubert Burda Media gegründet. Im Oktober 2018 beteiligte sich zusätzlich die Ringier AG an BOTLabs.

Ziel des Unternehmens ist es, die Blockchain-Technologie für eine breite Öffentlichkeit zugänglich und sinnvoll nutzbar zu machen. BOTLabs entwickelt dazu Basistechnologien, die von Unternehmen und öffentlicher Verwaltung genutzt werden können, um neue Geschäftsmodelle zu entwickeln und bestehende Prozesse zu verbessern.

BOTLabs stellt am 14.05.2019 in Berlin das KILT Protocol vor, mit dem eines der wichtigsten und drängendsten Probleme im heutigen Internet gelöst werden kann: Der Verlust von Vertrauen.

Über Ingo Rübe

Ingo Rübe ist Gründer und CEO der BOTLabs GmbH.

Von 2012 bis 2017 war Rübe CTO des deutschen Verlags Hubert Burda Media. Dort initiierte und verantwortete er unter anderem das Open Source CMS-System „Thunder“. Zuvor war der Berliner Informatiker über sechs Jahre als Project Director bei der Axel Springer SE beschäftigt.

Bereits 1995 gründete er mit „Network Department“ sein erstes Start-up im Bereich der Medizininformatik, welches im Jahre 2000 mit der IT-Abteilung der Fresenius AG zur heutigen Fresenius Netcare GmbH fusionierte.

Ingo Rübe ist Gründungsmitglied der internationalen Blockchain-Organisation INATBA (www.inatba.org) sowie Vorstandsmitglied der Drupal Association (www.drupal.org).