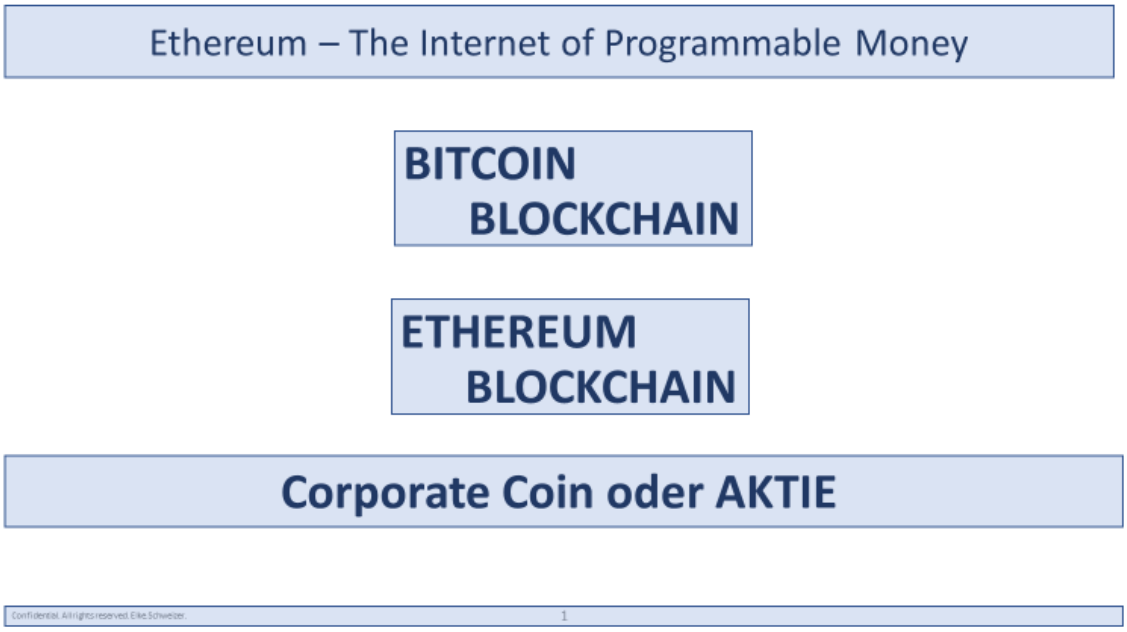
Ethereum
The Internet of Programmable Money

FinTech: Securing, Accounting and Fundraising with Blockchain Technologies

SPEAKER

Elke Schweizer started her professional life as a Software Developer for CHiLL based Mobile Switches at Alcatel in 1994. In parallel she wrote her dissertation in the field of solid state physics at the Max Planck Institute in Stuttgart. In 1998 she switched over to the development of Hybrid Fiber Coax Networks and worked as a customer project leader for the French customer Lyonnaise Cable. In 2004 she joined the Bosch Corporate IT and managed a global agile Team for Java, iOS and Android platforms focusing on the Security Architecture. Her team developed an App PKI Infrastructure which was used to securely integrate the IBM Connections Platform on iOS and Android smartphones. Elke Schweizer enabled the Bosch Engineering Group (BEG) to secure IoT-Functions on embedded devices by using PKI related IT Technologies and the global team developed a prototype for a BoschSecure based asynchronous Theft Prevention System for vehicle (TPS), which does not prevent the Theft, but the selling of the stolen car. Elke Schweizer filed three Patents (2015/2016) for Bosch related to the BoschSecure technology. She continued with crypto and security based R&D efforts on Blockchain Technologies like Bitcoin and Ethereum to be able to provide secure, banking system independent and resilient accounting microservices for IoT based business models.

Slide 1: Ethereum – The Internet of Programmable Money



Was ist der Unterschied zwischen der Bitcoin Blockchain und der Ethereum Blockchain? Bitcoin könnte ein Ethereum Smart-Contract sein. Einzige Funktion des Contracts: Die Übergabe eines Betrages von der eigenen Adresse zu einer definierten Zieladresse. Klar, dass der Code des Smart-Contracts sicherstellt, dass man nicht mehr Geld übertragen kann, als man auf dieser Adresse besitzt. Tatsächlich ist aber Bitcoin keine Ethereum Implementierung, sondern eher umgekehrt. Dieser Ansatz ist wesentlich schlauer. Erst gab es Bitcoins und als sich der Erfolg und die Sicherheit der Kryptowährung in der Praxis gezeigt hat, hatte Vitalik Buterin die Idee, aus der Bitcoin-Architektur eine Infrastruktur zu bauen, mit der neue Kryptowährungen und vielleicht noch viel mehr Produkte oder Services umsetzbar sind. Das ist ein seltener, aber vielversprechender Ansatz, der leider in der Geschichte der Infrastrukturen und Plattformen nicht oft gewählt wurde. Im Folgenden werde ich die Technologien erläutern und einen Einsatzbereich für Ethereum vorstellen.

Slide 2: Die Bitcoin Blockchain

Zuerst müssen wir die Funktionsweise und den Sinn von Bitcoins verstehen:

https://www.youtube.com/watch?v=l9jOJk30eQs

Slide 3: Die Bitcoin Blockchain

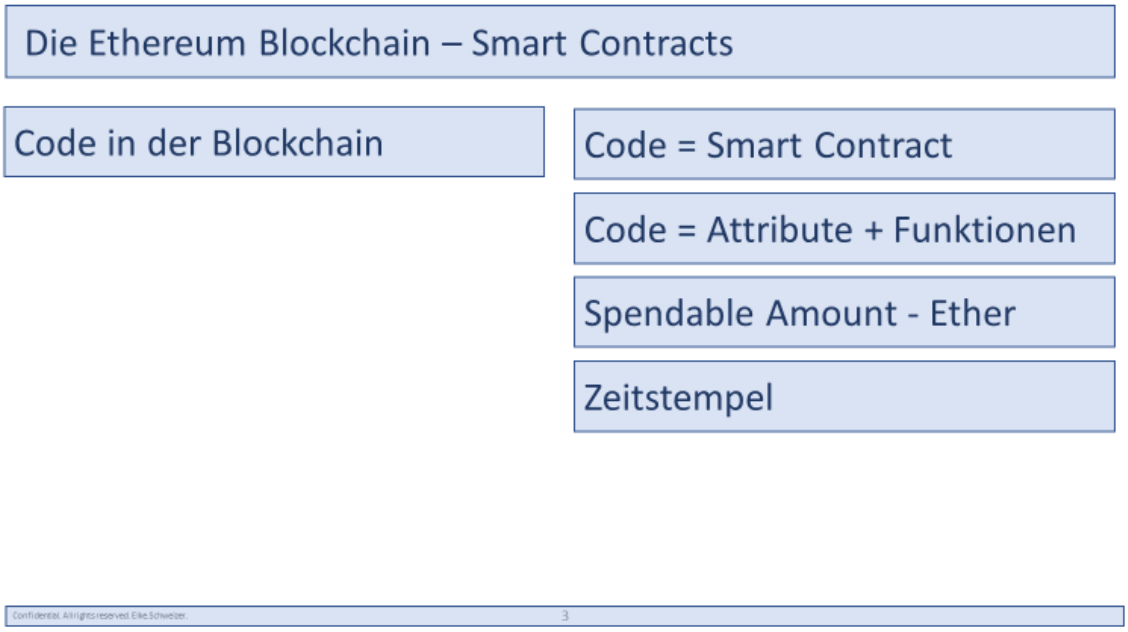
Ich fasse nochmal die wichtigsten Punkte der Architektur zusammen. Bei Bitcoin kann man sagen: „*Be your own Bank*“. Das bedeutet, dass jeder Teilnehmer auf seinem Computer ein Stück Software inklusive Datenbank installiert, das einen Knoten darstellt. Die Software sorgt dafür, dass alle Buchungen auf allen Knoten identisch sind. Das nennt sich dann distributed Ledger, also verteiltes Hauptbuch. Distributed ist in diesem Kontext als redundant zu verstehen. Also: Das gesamte Hauptbuch ist auf jedem Knoten repliziert. Damit wäre Bitcoin erst dann tot, wenn der letzte Knoten, also Computer, aus dem Netzwerk genommen wird. Bitcoin ist dezentral und nicht von einem oder mehreren zentralen Servern abhängig, die zum Beispiel von Regierungen abgeschaltet oder von Hackern lahmgelegt werden könnten. Man muss keinen Knoten betreiben, um Bitcoins zu besitzen. Es gibt Service Provider, die das für die Kunden tun, die sich die Installation der Software auf ihrem Rechner nicht zutrauen. Ein Konto ist eine ID, auf die ein Betrag gutgeschrieben wurde. Man spricht von einem „*spendable Amount*“, dem Betrag den man ausgeben, also auf eine andere ID übertragen kann. Die ID ist ein „*Public Key*“. Die Software, die auf den Knoten läuft, sorgt dafür, dass man nur wenn man den dazugehörigen Private Key besitzt, den Betrag auf ein anderes Konto übertragen kann. Es reicht also aus, eine Sicherung der sogenannten „*private/public Keypairs*“ seiner Konten zu besitzen, notfalls als Ausdruck auf einem Stück Papier, um zu einem späteren Zeitpunkt wieder über die Bitcoins zu verfügen. In dem Fall würde man von einem „*Paper-Wallet*“ sprechen. Also einer Papier-Brieftasche. Typischerweise würde man nicht alle Bitcoins in einer Adresse halten, sondern mehrere anlegen. Jetzt ist noch die Frage offen, wie die Bitcoins in das System kommen und was das mit der Blockchain zu tun hat. In dem Film haben wir gesehen, dass die Blockchain eine chronologische Kette von Blöcken ist. Die Blöcke enthalten Buchungen auf die öffentlichen Adressen, also die Public Keys. Wenn jemand eine Buchung versucht, dann überprüfen die sogenannten Miner die offenen Transaktionen und bestätigen diese. Die Miner sammeln dazu alle Transaktionen, die noch nicht in einen Block zusammengefasst wurden ein und erzeugen so einen neuen Block zu dem die Software des Miners eine vordefinierte Anzahl Bitcoins auf dessen Adresse gutschreibt. Dann kann der Block an die Blockchain gehängt werden. Damit sind die Transaktionen unabänderlich mit Zeitstempel bzw. Reihenfolge dokumentiert.

Doch was hat es mit dem ominösen Rätsel auf sich, das die Miner lösen müssen? Ich finde den Begriff etwas unglücklich gewählt, da es nicht wirklich ein Rätsel zu lösen gibt. Bitcoins haben wie alle Währungen zwei Eigenschaften. Sie sollen leicht teilbar und austauschbar sein, um Käufe von Waren und Dienstleistungen zu ermöglichen und eine Buchung sollte möglichst schnell und kostengünstig sein. Eine weitere wichtige Eigenschaft von Geld ist die Aufbewahrung eines Wertes. Man sollte Geld sparen können. Das geht aber nur, wenn die Geldmenge nicht ständig erhöht wird. Deshalb gibt es eine mathematische Obergrenze bei der Bitcoin-Schöpfung. Diese Grenze sollte nicht zu schnell erreicht werden, sondern erst um das Jahr 2140. Eine Obergrenze wird mathematisch ganz einfach realisiert: Zum Start von Bitcoin am 03.01.2009 war die sogenannte „*Block Reward*“ 50 Bitcoins. Die Block-Reward bringt die Bitcoins quasi als Belohnung für die Buchungsbestätigungen ins System. Der Algorithmus schreibt vor, dass immer wenn 210.000 Blöcke generiert wurde, die Block-Reward halbiert wird. Die erste Halbierung war am 28.11.2012 und die zweite am 09.07.2016 [Controlled-Money-Sypply].

Dass sich durch dieses Vorgehen die Menge der Bitcoins asymptotisch einer Obergrenze [21-Millionen-Bitcoins, 64-Bit-Floating-Point-Number] annähert, kann man sich so vorstellen: Wenn man eine Schüssel Suppe hat und jeder nimmt sich die Hälfte heraus, dann kann man das im Prinzip endlos lange fortsetzen, ohne dass die Schüssel jemals ganz leer wird. Das erklärt aber noch immer nicht, warum ein Rätsel gelöst werden muss. Dass kommt daher, dass der Algorithmus ebenfalls sicherstellen möchte, dass nur etwa alle 10 Minuten ein gültiger Block gemined wird - damit die Obergrenze nicht zu früh erreicht wird. Wenn jetzt aber viele Miner ständig Blöcke bestätigen, dann lässt sich dieser Takt nicht einhalten. Daher wird in den Header jedes potenziellen Blocks eine Zufallszahl eingetragen. Diese Zufallszahl wird manchmal auch „*Salt*“, also Salz, genannt. Dann wird ein Hash-Wert aus dem Block mit dem zufälligen Salt berechnet. Hashing ist eine Art mathematische Einwegfunktion, die aus einem beliebig langen String einen immer gleich langen Ergebnisstring erzeugt. Gültig ist ein Block nur, wenn die Zufallszahl zu einem Hash-Wert führt, der mit einigen führenden Nullen beginnt. Wenn nun zu viele Miner oder zu viel „*Hashing-Power*“ im System ist, dann wird einfach die Anzahl der geforderten führenden Nullen erhöht, die notwendig sind, um einen gültigen Block zu generieren. Das Rätsel ist also die „*Brute-Force-Suche*“ nach einer Zufallszahl, die einen Block mit den notwendigen führenden Nullen seines Hash-Wertes ergibt. Der hohe Strom- und damit Energieverbrauch, der Bitcoins immer wieder zur Last gelegt wird, kommt aus der Popularität des Bitcoin-Minings. Nur weil so viele Miner Bitcoins schürfen wird die Anzahl der Nullen durch den Algorithmus ständig erhöht und damit müssen die Rechner so viel Salt, also Zufallszahlen, durchprobieren, bis ein gültiger Block entsteht und der Miner damit die Block-Reward einstreichen kann.

Man kann die Architektur der Bitcoin Blockchain also ganz einfach zusammenfassen: Die Blockchain ist eine auf allen beteiligten Knoten replizierte, im Sinne der Integrität sichere Datenbank, die die Buchungen mit Zeitstempel sowie die Kontostände der einzelnen Adressen enthält. Die Open-Source-Implementierung der Software, die auf den Computern, die die Knoten darstellen, läuft, sorgt dafür, dass die Buchungen nicht manipuliert werden können und dass die Gesamtmenge der möglichen Bitcoins mathematisch begrenzt ist.

Slide 4: Was ist Ethereum?



Die Ethereum Blockchain ist eine Blockchain, die als Nutzdaten zu einer Adresse nicht nur eine Reihe von Betragsbuchungen mit Zeitstempel, sondern optional auch ausführbaren Code und weitere programmierbare Attribute, also weitere Daten enthalten kann. Der ausführbare Code besteht aus einer Reihe von Attributen und Funktionen. Der Code, auch Smart-Contract genannt, bestimmt, welche User die Funktionen ausführen dürfen, und ob die Ausführung für die Nutzer des Smart Contracts etwas kostet.

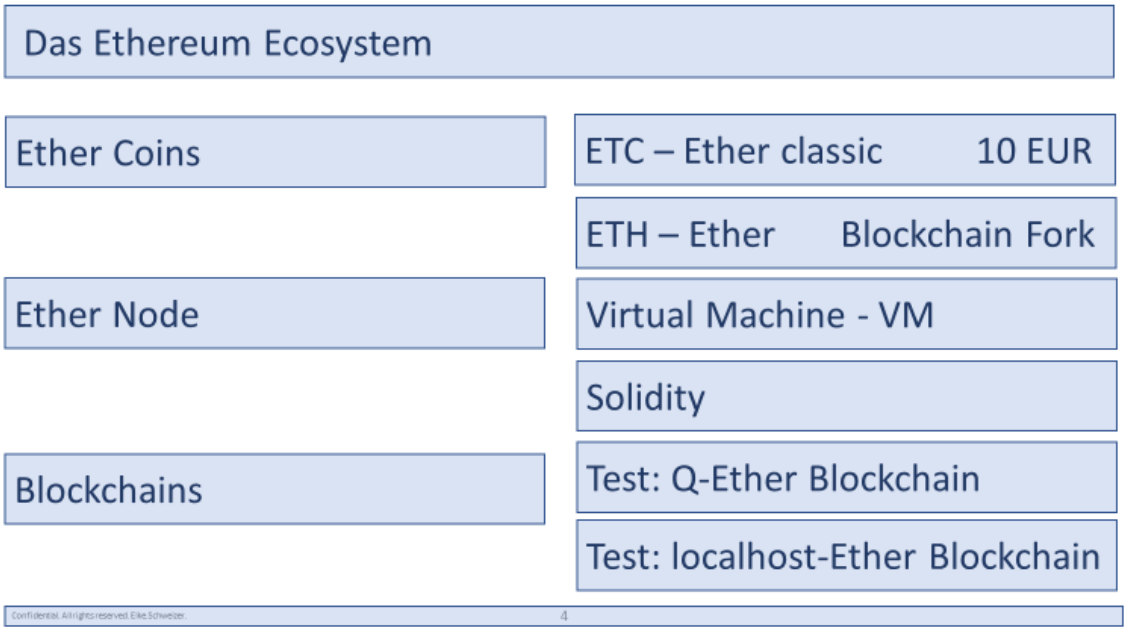
Bei Ethereum spricht man von Smart-Contracts, weil man durch die Ablage von Code in der Blockchain, Verträge automatisch ausführen kann. Der Code besteht aus einer Baumstruktur von Attributen und einer Reihe von Funktionen. Die Funktionen können die im Smart-Contract gespeicherten Daten, also die Attribute abändern und ggf. Buchungen auf Ethereum Adressen durchführen. Sie können leider keine Informationen aus dem Internet einlesen. Ein Ethereum Account wird wie bei der Bitcoin-Blockchain durch einen Public Key identifiziert. Der Besitzer des Accounts ist der User, der über den Private Key verfügt. Ein User kann in seinen Ethereum-Account Bytecode deployen, also ablegen, und damit zum Anbieter eines Smart-Contracts werden. Er kann damit die Funktionen für sein Vertragsangebot programmieren. Kunden können dann durch Aufrufen einer der Smart-Contract-Funktionen den Vertrag parametrisiert abschließen. Typischerweise würde der Anbieter des Smart-Contracts eine Webanwendung oder eine App bereitstellen, durch die Ether-Coin Besitzer die typischerweise kostenpflichtigen Funktionen des Smart-Contracts aufrufen können. Die Vertragsdaten, also z.B. welcher User, mit welchen Parametern den Vertrag abgeschlossen hat, werden unter der Adresse des Contract-Anbieters in einer Baumartigen Datenstruktur abgelegt. Die Adresse des Kunden enthält wie bei den Bitcoins auch nur den spendable-Amount. Das Mining dient bei Ethereum der Bestätigung der Blockchain-Änderungen, also der Buchungen der Ether-Coins oder des Deployments der SmartContracts. Wie bei Bitcoins, werden dem erfolgreichen Miner Ether-Coins

gutgeschrieben. Allerdings ist es im Moment noch nicht klar, ob die Menge an generierbaren Ethers genauso wie bei Bitoins limitiert wird.

Vertragsänderungen werden als neuer Vertrag unter einer neuen Adresse deployed. Dann können die Kunden zum Beispiel mit einer aktualisierten App den neuen Vertrag abschließen. Genauso wirken sich auch Bugfixes aus. Sie können nicht in einen bestehenden Vertrag deployed werden. Entwickler von SmartContracts umgehen dieses Problem, indem sie Proxy-Contracts verwenden. Mit diesem Kniff kann dann aber auch der Contract auf den der ProxyContract verweist, geändert werden, ohne dass der Nutzer das zwingend bemerkt. Deployments von Bytecode in die Ether-Blockchain sind kostenpflichtig. Auch die Ausführung von Funktionen kosten in Abhängigkeit der durchgeführten Rechenschritte Ether-Coins, besser gesagt Bruchteile davon, die auf dem Account des Contracts verfügbar sein müssen.

Ethereum Smart Contracts erhalten eine eigene Adresse, also einen anonymen Key, der keine Rückschlüsse über den Anbieter des Contracts ermöglicht. Der "Anbieter" oder „Owner“ muss bei Bedarf explizit im Smart Contract Code als Attribut festgehalten werden, ansonsten ist er nur über die Transaktion ermittelbar, die den Smart Contract angelegt hat. Den Owner eines SmartContracts kann man z.B. mit Etherscan herausbekommen.

Slide 5: Das Ethereum Ecosystem



Ethereum ist nicht wie Bitcoin nur eine Währung, sondern ein ganzes Ecosystem. Zu Ethereum gehört die produktive Ethereum Blockchain, in der Ether-Coins den Besitzer wechseln. Bei der Ether Blockchain gibt es inzwischen einen „*Fork*“, so dass man sich zwischen ETCs (ETher Classic) und ETH (ETHer) entscheiden muss. Ein ETC ist im Moment so etwa 10 Euro wert. Um den Bytecode der Smart-Contracts ausführen zu können, läuft in jedem Ether-Node eine Virtual Machine. Zur Entwicklung des Bytecodes gibt es eigene Programmiersprachen, die bekannteste heißt Solidity, mit jeweiligen Entwicklungsumgebungen zur Unterstützung der Programmierung und des Deployments. Zum Testen gibt es eine Q-Ether-Blockchain sowie die Möglichkeit lokalhost-Blockchain-Instanzen zu starten. Testtools erlauben den lesenden Zugriff auf die Blockchains.

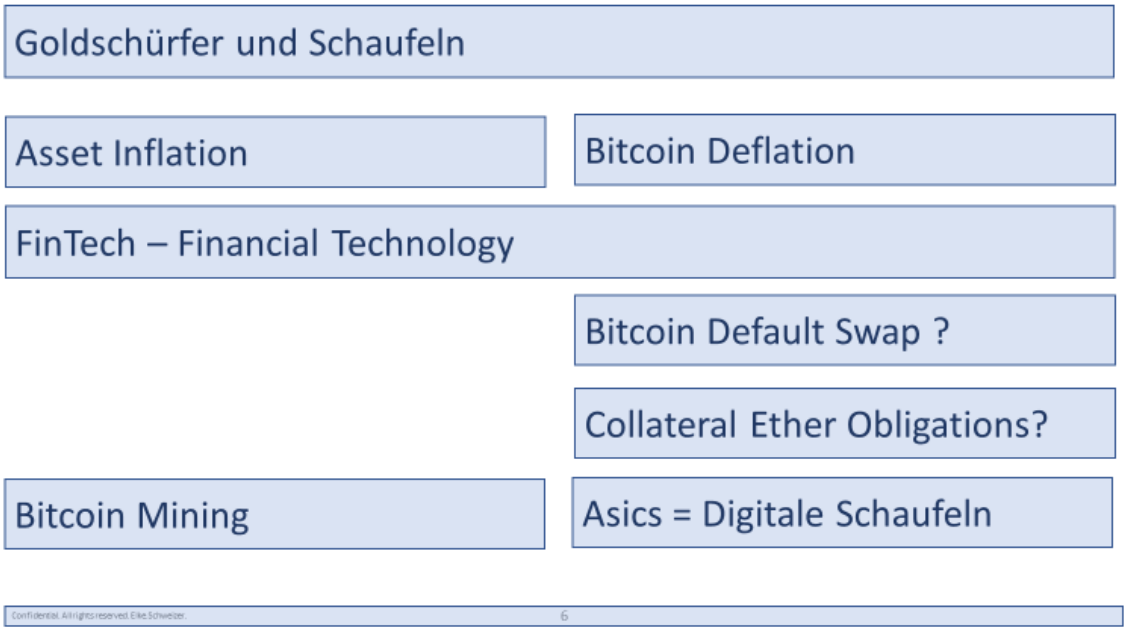
Die Ethereum Blockchain ist also eine auf allen Knoten replizierte Datenbank mit auf allen Knoten replizierten Funktionen, die im Falle eines Aufrufs auf allen Knoten mit Hilfe der integrierten VM ablaufen. Bei Oracle-Datenbanken heißen solche Funktionen „*Stored Procedures*“ und laufen natürlich immer nur einmal auf der zentralen Datenbank ab. Um kurz bei dem Oracle-Vergleich zu bleiben, würde das bedeuten, dass jeder Smart-Contract eine Reihe von Key-Value-Tabellen inklusive stored-Procedures enthält. Nicht vergessen darf man, dass der Großteil der User auf seinen Adressen nur den Ether-Kontostand in die BlockChain abspeichert. Nur die Smart-Contract-Provider halten in ihren Adressen zusätzlich zu ihrem Ether-Kontostand noch eine Mini-Datenbank mit stored-Procedures.

Slide 6: Den Ethereum Killer-Contract…

… gibt es leider nicht [Adam B. Levine on Epicenter Bitcoin]. Mit Ethereum könnte man relativ einfach eigene Krypto-Währungen implementieren. Meines Wissens sind aber alle Altcoins nicht mit Ethereum implementiert worden, sondern vermutlich einfach dadurch, dass entweder nur die Architektur oder gleich die OpenSource Implementierung von Bitcoin geklont und marginal abgeändert wurde. Die Ethereum Hauptfunktionalität bliebe dabei sowieso ungenutzt. Außerdem ist Ethereum wesentlich unsicherer als Bitcoin – einfach, weil es bislang außer bei Hackathons praktisch keine Angriffe auf Ethereum gab.

Es gibt ein paar produktive Smart-Contracts, die Wetten aller Art implementieren. Man könnte zum Beispiel auf das Wetter morgen an einem bestimmten Ort wetten. Ist das Wetter dann tatsächlich so, bekommt man den Gewinn auf seinem Account gutgeschrieben. Ist es anders, dann bleiben die eingesetzten Ethers auf der Adresse des Contract-Providers. Allerdings würde schon bei dieser einfachen Wette, das Herzstück des Vertrags, also die Prüfung des Wetters das Ethereum Ökosystem verlassen und man müsste einen Wetterdienst nutzen. Da die SmartContracts aber nicht auf das Internet zugreifen können, kommen hier sogenannte „*Oracles*“ ins Spiel, die Zustandsänderungen von außen in den Smart Contract bringen. Bei dem Beispiel stellt sich die Frage, warum der Contract wirklich in jedem Knoten laufen muss. Da täte es vermutlich auch ein einfacher Server, dem der User mittels App Bitcoins schickt und der nach der Prüfung des Wetters dem User den Gewinn gutschreibt. Und wenn der User checken möchte, ob alles mit rechten Dingen zugeht, müsste er nur seine Buchungen prüfen, statt den gesamten Sourcecode für alle möglichen Wetten, die der Server anbietet zu checken, das Ganze mit proprietären Tools zu kompilieren, den Bytecode hashen und dann vielleicht festzustellen, dass der Hash Wert nicht dem in der Ethereum-Chain abgelegten Hash Wert entspricht. Den Vorteil, dass der Bytecode auf jedem Knoten repliziert ist, kann ich für die gesamte Use-Case Gruppe Wetten und Versicherungen nicht erkennen.

Slide 7: Goldschürfer und Schaufeln



Das Ganze erinnert ein wenig an das Goldschürfen. Dass Bitcoin und Ethereum Meisterleistungen der Software-Architektur sind, ist sofort erkennbar. Bitcoins haben disruptive Einsatzgebiete, wie zum Beispiel den Angriff auf das weltweite Finanzsystem mit der Geldschöpfung durch Banken – *„out-of-thin-air*“. Seit 2011 werden die Währungen aller Länder bis auf Kuba, Iran und Nordkorea privat geschöpft und sind inflationär angelegt. In dem Moment, in dem sich Zentralbanken – meistens auf Druck von Regierungen – entscheiden, die Geldmenge zu erhöhen, entsteht eine sogenannte Asset-Inflation, die all diejenigen schleichend enteignet, die ihr Geld sparen möchten. Mit den deflationär angelegten Bitcoins hingegen kann der Bürger mit den Füßen abstimmen. Den finanzielle Kollaps den wir damit auslösen könnten, will ich mir gar nicht vorstellen, damit ich kein schlechtes Gewissen kriege. Den privaten Besitzern der amerikanischen FED das weltweite durch den Handel mit Öl gestützte Geldschöpfungsmonopol wegzunehmen hat trotzdem was.

Bei Ethereum liegt der Fall nicht ganz so klar. Wie bereits erläutert werfen die Geschäftsmodelle mit oft illegalen Wetten oder Versicherungen mehr Probleme als Lösungen auf. Interessanterweise sind gerade die Banken und Versicherungen ganz heiß auf Blockchain, vielleicht einfach deshalb, weil ihre Kunden sich nicht länger melken lassen wollen und FinTech hört sich ja irgendwie so an, als ob man als Bank oder Versicherung etwas damit verdienen könnte. Vielleicht lassen sich ja lustige SWAP-Pakete auch in irgendwelchen Kontrakten zusammenpacken, die man dann wieder am Kapitalmarkt verkaufen kann...

Aber zurück zum Goldschürfen. Ich war nie Bitcoin Miner, weil ich zu spät eingestiegen bin. Da hätte man schon ASICs gebraucht. Zu diesem Zeitpunkt waren so viele Miner auf dem Plan, dass der Erlös des Minings ähnlich war, als wenn man statt Mining-Equipment gleich Bitcoins gekauft hätte. So funktioniert eben der Markt, wenn ihn keiner manipuliert oder besser: manipulieren kann. Wirklich

eine goldene Nase haben sich nur die Hersteller des Equipments verdient. Genau wie früher bei dem Goldrausch. Da haben auch die Verkäufer von Schaufeln und Hacken den größten Reibach gemacht. Bei Ethereum ist das auch ein bisschen so. Der Ether-Kurs steigt ständig, obwohl noch keiner damit Geld verdient. Eigentlich beobachtet man das in der Software-Branche schon länger. Statt mit großem Aufwand Anwendungen oder Apps zu entwickeln, die dann am Markt vielleicht gar nicht erfolgreich sind, haben sich viele Software-Konzerne auf die Entwicklung von Werkzeugen verlegt. Die Beispiele haben wir auf dieser Konferenz gerade um uns. Leider sind einige der Werkzeuge und Plattformen nur auf den ersten Blick hilfreich und manchmal sogar so lieblos implementiert, dass für einige der abfällige Spruch „*Architects Dream – Developers Nightmare*“ wahr werden kann.

Bei Ethereum ist der Fall anders gelagert. Klar hat Ethereum auch seine Bugs oder ist an der einen oder anderen Stelle noch nicht ganz fertig. Aber Ethereum ist eine OpenSource Implementierung und kann notfalls durch die Nutzer selbst weiterentwickelt werden. Daher glaube ich, dass man die Vorteile dieser disruptiven Technologie gefahrlos nutzen kann.

Slide 8: Ethereum Use Case - Corporate Coin statt Aktie

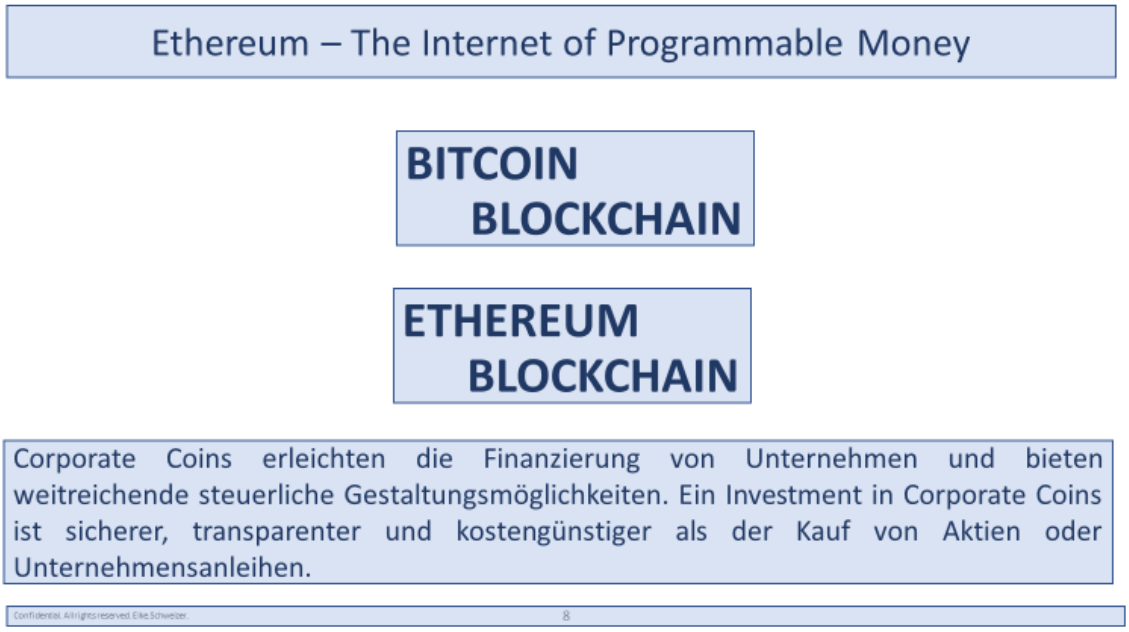
Jetzt habe ich gerade ganz lange erklärt, warum Ethereum zwar großartig ist, es aber keinen Killer-Contract gibt, also keine disruptive Anwendung auf dieser Plattform – um mir jetzt selbst zu widersprechen und eine Nutzung von Ethereum vorzustellen, die nicht nur technischen Innovationen einen enormen Drive geben kann: Die Implementierung einer proprietären Coin. Mit Ethereum ist es wie ich schon erklärt habe, ganz einfach, eine neue Coin, also Währung zu implementieren. Das ist so eine halbe Seite Sourcecode, die als Smart-Contract in die Ethereum Blockchain deployed wird. Damit kann man dann eine App schreiben, mit der die Coins der Währung sicher von einem User zum Anderen gebucht werden können. Wichtig ist anzumerken, dass man damit natürlich kein Mining der neuen „*Corporate-Coin*“ hat. Mit dem Begriff Corporate-Coin habe ich die Anwendung schon vorweggenommen. Es ist also eine Art eigene Firmenwährung, die man damit aufsetzt. Man könnte das Ganze natürlich auch als Produktwährung anlegen. Richtig neu ist die Idee nicht. Bei Finanzexperten werden Dinge wie Rabattmarken oder Flugmeilen auch als Währung bezeichnet. Bitcoin wird übrigens in den meisten Ländern gesetzlich wie eine Währung betrachtet. Es gelten also andere Fristen beispielsweise für Spekulationsgewinne mit Währungen, also auch mit Bitcoins, als mit anderen Wertgegenständen wie z.B. Rohstoffen oder Immobilien. Deswegen redet man von FinTech, also Financial Technologies. Immer wenn etwas digitalisiert wird, fallen durch Technik an irgendeiner Stelle große Aufwände weg. Damit erübrigen sich oft auch ganze Berufsgruppen oder Branchen.

Corporate-Coin oder Aktien

Im Folgenden möchte ich zeigen, wie man mit einer Corporate Coin für eine Firma einiges an Bankern und Steuerberatern einsparen und sehr kosten- und steuergünstig ein für Klein- und Großanleger lukratives Investment anbieten kann, ohne wie bei dem Verkauf von Aktien Stimmrechte abgeben zu müssen. Man kann sich auch einen teuren Börsengang sparen und die Coins praktisch von Anfang an

über Altcoin-Plattformen handeln lassen. Anders als bei Aktien, kann die Coin aber auch unabhängig von einem Handelsplatz direkt von Investor zu Investor weiterverkauft oder weitergegeben werden. Damit wird die Coin zur Devise und steuerliche Aspekte aller Art werden für die Weitergabe der Coin obsolet, solange man die Spekulationsfristen für den Devisenhandel einhält. Jetzt muss man es nur noch schaffen, dass ein Bezug der Coin zu dem Erfolg des Unternehmens hergestellt wird. Das ergibt sich aber von alleine, wie man bei Ethereum sieht. Ich habe vor einiger Zeit bei unserem Bitcoin-Stammtisch eine Bankerin kennengelernt, die etwas genervt war, dass man Ether nur über den Umweg von Bitcoins kaufen kann. Sie war eine klassische Chartistin und hat sich nur die Charts, also den Werteverlauf von verschiedenen Investments angeschaut. Bei Ethereum hat sie sich rudimentär über die Technik informiert, ohne das wirklich zu verstehen, aber der Verlauf des Charts und die Begeisterung der Ethereum Nutzer hat sie sofort überzeugt. Klar, dass es bei den Crypto-Coins keinerlei Regulierungen gibt. Daher hat ein Startup auch die Möglichkeit, den Investoren den Einstieg in das Investment etwas leichter zu machen. Wenn man z.B. ein Corporate-Coin für einen Einstiegskurs von einem Euro verkauft, dann kann man dem Investor für eine gewisse Zeit eine Rücknahme der Coin für 50 Cent garantieren. Damit kann man in dieser Zeit eben nur die Hälfte des eingenommenen Kapitals verwenden, hat aber für den Investor das Risiko eingeschränkt. Oder man bietet das Produkt auch gegen Coins an. Wenn also ein Service oder das Produkt 10 Euro kosten soll, dann kostet es auch maximal 10 Coins. Rabatte gibt es natürlich immer in Coins oder auch Prämien für das Werben neuer Kunden und ähnliches. Selbst die Mitarbeiter können einen Teil ihres Gehalts in Coins bekommen. Wenn beispielsweise der Kurs der Coin unter einen Euro fallen würde, Leistungen aber in Coins zu einem Kurs von 1:1 bezahlt werden können, dann würden die Kunden Coins kaufen, um das Produkt günstiger zu kriegen. Damit würde eine Nachfrage nach der neu geschaffenen Währung entstehen und der Kurs dadurch automatisch steigen. Im umgekehrten Fall, also wenn der Kurs zu stark steigt, kann der Herausgeber – also das Startup – die Geldmenge erhöhen und neu geschaffene Coins verkaufen. Es wäre sicherlich schlau, darauf zu achten, dass die Coin auf lange Sicht eine gewisse moderate Wertsteigerung erfährt.

Slide 9: Fazit



Ethereum erlaubt es nicht nur Startups mit minimalem Aufwand eine Corporate-Coin zu erstellen, die zu einem Baustein des Ethereum Ökosystems wird und dadurch direkt bei der Einführung den Wert des Unternehmens repräsentiert. Durch vertragliche Verpflichtungen gegenüber Kunden und Investoren wird diese Bindung gefestigt. Die Corporate-Coin ist als Crypto-Währung ohne Börsengang für jeden handelbar und kann gleichzeitig als Crowdfunding-Instrument dienen. Auch wenn das Unternehmen selbst vielleicht eine Aktiengesellschaft ist, kommen Wertsteigerungen in erster Linie dem Unternehmen und den Mitarbeitern zugute.