:get know howww
UBIT Steiermark

BlockchainHub Graz

Das Internet der Werte – Blockchain Technologie & Kryptowährungen als Basis einer neuen Wirtschaft

Kapitel 2: Was sind Altcoins und was kann man damit machen?

Darstellung der Vielfalt der gelisteten Coins auf http://com-http.us/

Von DI Thomas Zeinzinger

BlockchainHub Graz (https://blockchainhub.net/graz/)

Meetup jeden letzten Montag im Monat
http://www.meetup.com/de-DE/BlockchainHub-Graz/

Inhaltsverzeichnis

Was versteht man unter dem Begriff „Altcoin“? 1
Wie finden die ersten Coins ihren Besitzer? 3
Mining 3
Minting 3
Airdrop 4
ICO – Initial Coin Offering 5
Der Handel mit Altcoins 8
Wechselbörsen 8
36 Regeln für Kryptomärkte von Markus M. Bohl 11
Achtung Betrug! – Finger weg von Scamcoins 14
Ausgewählte Altcoins und ihre Eigenschaften 16
Die eigene Währung für Jedermann ☺ 23

Was versteht man unter dem Begriff „Altcoin“?

Das Wort Altcoin besteht aus den Begriffen „alt“ als Kurzform für alternate bzw. im Deutschen alternativ und „coin“ für Münze bzw. Währung. Unter diesem Begriff versteht man all die Kryptowährungen, die angeregt vom Erfolg von Bitcoin entwickelt wurden.

Davon gibt es Hunderte, laufend entstehen neue, andere anfänglich hochgelobte Währungen sind nach wenigen Monaten praktisch wieder vom Markt verschwunden bzw. haben den ursprünglichen Wert komplett verloren.

Die meisten Coins sind mehr oder minder eine Kopie von Bitcoin, mit Variationen, bspw. hinsichtlich Blockgröße, Konsensmechanismus bzw. Anonymität, einige der Coins wie bspw. Ether oder IOTA dienen als Zahlungsmittel für die Transaktionen auf Plattformen, die für mehr als den reinen Zahlungsverkehr gedacht sind. Ethereum bietet mit den SMART Contracts eine Möglichkeit Verträge zu automatisieren, IOTA sieht sich als Plattform für das Internet of Things. Neben der eigentlichen Funktion dieser Kryptowährung auf der jeweiligen Plattform, werden diese Währungen wie Bitcoin und andere Altcoins auch auf dem Sekundärmarkt gehandelt. Und wie der Wert von Bitcoin und anderen Altcoins auch vom Verbreitungsgrad und der Einsetzbarkeit im tagtäglichen Leben beeinflusst wird, hängt der Wert dieser Kryptowährungen vom Bekanntheitsgrad und der Einsatzmöglichkeiten der jeweiligen Plattform ab.

Die Schwerpunkte der unterschiedlichen Plattformen und wie diese die Welt von morgen möglicherweise beeinflussen könnten, stehen im Mittelpunkt unseres nächsten Kapitels. Im Folgenden möchte ich Ihnen zeigen, wie die einzelnen Kryptowährungen entstehen und welche Möglichkeiten es gibt, dass die Coins ihre ersten Besitzer finden. Besonders interessant in diesem Kontext ist, dass sich dadurch auch eine neue Möglichkeit entwickelt hat, die Finanzierung des Unternehmensaufbaus zu garantieren, ohne dass dafür wie ansonsten im Angel Investor oder Venture Capital Bereich üblich Unternehmensanteile abgegeben werden müssen.

Außerdem finden Sie eine kurze Einführung in den Handel von Kryptowährungen, was aktuell einen großen Teil der täglichen Transaktionen in der Kryptowelt ausmacht, denn die Hoffnung durch Kursgewinne eine hohe Verzinsung realisieren zu können, ist sehr groß. Teilweise entsteht aus der Hoffnung auch Gier, die gepaart mit Unwissenheit und Ignoranz dazu führt, dass auch fragwürdige Angebote auf dem Markt reißenden Absatz finden, etwas für die die Namen Scamcoins oder Shitcoins verwendet werden.

Weiters werde ich Ihnen die Altcoins mit der höchsten Markt Kapitalsierung mit ihren Besonderheiten vorstellen wie auch auf ein paar Coins mit besonderen Eigenschaften eingehen. Und als Abschluss zeige ich Ihnen, wie Sie es Staaten gleichtun können und ihre eigene Währung generieren können. Viel Spaß!

Wie finden die ersten Coins ihren Besitzer?

Viele Kryptowährungen benutzen den Code einer anderen Kryptowährung wie Bitcoin als Basis und entwickeln diesen weiter bzw. adaptieren diesen auf die spezifischen Anforderungen der jeweiligen Währung. Man spricht hier von einem Fork, was übersetzt Gabelung bedeutet. Andere wiederum werden von Grund auf bspw. mit Java oder C++ programmiert, um die gewünschten Eigenschaften realisieren zu können.

Ähnlich wie beim Entstehungsprozess gibt es auch unterschiedliche Ansätze, die Kryptowährung unter die Leute zu bringen bzw. die Menge zu erhöhen.

Mining

Der klassische Weg ist das Mining, wie es bei Bitcoin gemacht wurde. Nach dem Generieren des ersten Blocks, des sogenannten Genesis Blocks rechnen die sogenannten Miner um die Wette. Wer als erstes das kryptografische Rätsel löst und den Block generiert erhält als Belohnung eine bestimmte Menge der neuen Kryptowährung.

Dieser Prozess nimmt natürlich Zeit in Anspruch und die Geldmenge nimmt erst schrittweise zu. Ein möglicher Nachteil liegt auch darin, dass die Miner nicht notwendigerweise Interesse an der spezifischen Kryptowährung und deren speziellen Eigenschaften haben, sondern das Mining der Belohnung wegen betreiben, viele von ihnen müssen nicht nur die Stromkosten damit decken, sondern auch die spezielle auf den Miningprozess optimierte Hardware refinanzieren. Daher werden die frisch geminten Coins nicht lange gehalten, sondern direkt wieder auf dem Sekundärmarkt verkauft, wodurch durch das große Angebot der Preis für den Coin auf den Handelsbörsen bei gleichzeitig geringer Nachfrage in den Keller fallen kann.

Die Entwickler des Altcoins oder solche, die eventuell planen, auf Basis des neuen Altcoins Anwendungen zu programmieren – also Personen, für die der Coin intrinsisch einen Wert hat, haben auf der anderen Seite bei der professionellen Mining-Konkurrenz Schwierigkeiten, selbst Coins zu minen.

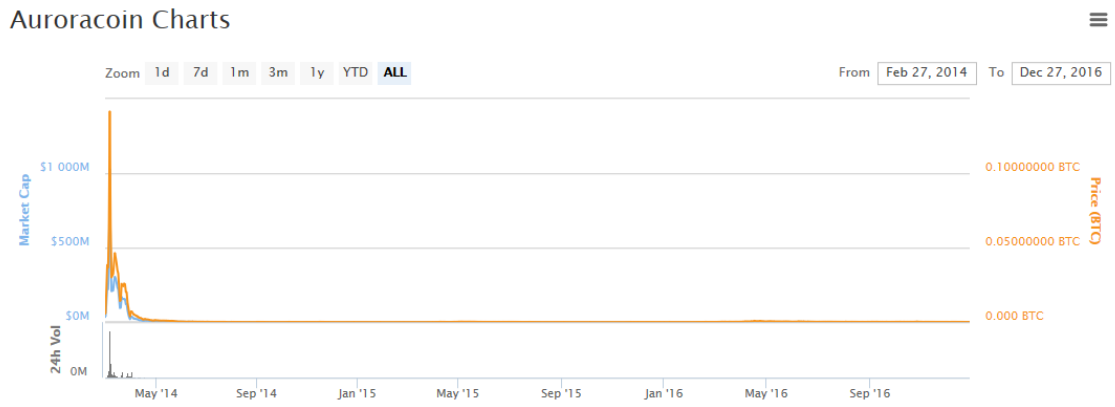
Minting

Eine Abhilfe gegen diesen Effekt ist, eine gewisse oder die gesamte Altcoin-Menge vorab zu generieren und diese Münzen dann entweder kostenlos zu verteilen oder in einem sogenannten ICO, einem Initial Coin Offering zu verkaufen.

Airdrop

Beim Airdrop werden die vorab generierten Kryptocoins kostenlos ausgegeben, üblicherweise muss man sich vorab dafür anmelden, die Verteilung erfolgt dann nach bestimmten Kriterien.

Ein Beispiel dafür ist AuroraCoin, der 2014 als isländische Alternative zu Bitcoin und der isländischen Krone auf den Markt kam, in der Hoffnung, für die nach der Finanzkrise erschütterte isländischen Krone eine Alternative zu bieten. "One of the most important power in society is the power over money. That is why the government monopolizes the Icelandic currency." Dies sagte der Gründer Óðinsson in einem Interview und genau diese Macht über das Geld wollte er den Bürgern wieder zurückgeben. Um die Währung rasch zu verbreiten und als Zahlungsmittel interessant zu machen, wurden 50 Prozent der möglichen Menge bereits gemintet und an Personen mit isländischer Staatsbürgerschaft in drei Tranchen verteilt. Die Folge beim AuroraCoin war jedoch, dass die „Beschenkten“ die Währung großteils nicht hielten, um die Währung als Zahlungsmittel zu verwenden, sondern sofort versuchten, die geschenkten Coins an einer Börse zu Geld zu machen, was nicht limitiert wurde. Der anfängliche Wert der ursprünglich 31,8 Auroracoins pro Person entsprach ungefähr einem Gegenwert von 385 $. Ein Wertverfall war die Folge – was sich auch in der Kursentwicklung der Währung sehen lässt, dieser Versuch, eine alternative Währung in einem Land einzuführen, war so also nicht gelungen.



Quelle: https://coinmarketcap.com/currencies/auroracoin/

Die Coins gleichmäßig zu verteilen, ist auch das Ziel des New Economy Movements NEM. Die gesamte Coin-Anzahl über 8.999.999.999 XEM wurde direkt im ersten Block generiert und dann an anfänglich ca. 1.500 Personen verteilt, die sich dafür registrieren konnten und jeweils eine Million XEM erhielten, der andere Teil wurde zurückgehalten, um zukünftige Entwicklungen entlohnen zu können. NEM versucht durch innovative Ansätze, Probleme anderer

Währungssysteme zu lösen, beispielsweise die ungleiche Verteilung, dass wenige Personen einen Großteil des Vermögens halten. Ein Weg dazu ist der Proof of Importance Mechanismus, um die Transaktionen zu bestätigen. Ungleich dem Proof of Work Mechanismus von Bitcoin, bei dem um die Wette gerechnet wird, zählen hier die Menge an XEM, die gehalten werden in Kombination mit der Anzahl der eigenen Transaktionen und dem für das Netzwerk erbrachten Nutzen.

Insofern darf man gespannt sein, welche Entwicklungen aus dieser Bewegung heraus entstehen und inwiefern es gelingt, die Währung in ihrem Nutzen und ihren Anwendungsmöglichkeiten und so in ihrem Wert steigen zu lassen. Dass die Bedeutung der Währung nach dem Airdrop im Gegensatz zu Auroracoin nicht auf Null gesunken ist, sieht man an der Kursentwicklung.

Quelle : https://coinmarketcap.com/currencies/nem/

ICO – Initial Coin Offering

Anstatt Coins einfach zu verteilen, wird auch die Möglichkeit genutzt, eine gewisse Menge vorab zu generieren und diese wiederum im Rahmen eines Crowdsales, auch ICO oder Initial Coin Offering genannt, zu verkaufen.

Diese Variante ist zu einem beliebten Finanzierungsmodell avanciert und ist im Kryptobereich eine beliebte Alternative zu Investments auf Beteiligungsbasis. Oft verwendet wird diese Variante für unterschiedlichste Plattformen, die mehr im Sinn haben, als eine reine Zahlungsfunktion zu erfüllen.

Als Basis für den ICO gibt es meist ein Whitepaper, in dem die Entwickler das geplante Projekt, die Einsatzmöglichkeiten, die technischen Grundlagen und den geplanten Entwicklungsverlauf beschreiben. Auch der Ausblick auf die zukünftigen Einsatzmöglichkeiten und wie individuelle Entwickler von der Plattform profitieren können, indem sie eigene Projekte starten, wird beschrieben. Die im Crowdsale angebotene Kryptowährung ist üblicherweise die, die auf der Plattform als Transaktionsgebühr genutzt werden wird.

Interessante Projekte stoßen so einerseits auf das Interesse von Investoren, die sich bei Erfolg der Plattform eine Wertsteigerung der Währung erhoffen, die dann beim Verkauf der Währung am Sekundärmarkt realisiert werden kann – ungeachtet dessen, ob die Investoren das technische Konzept verstehen. Andererseits wird das Interesse von Entwicklern geweckt, die selbst mit der Plattform experimentieren wollen und dafür die angebotene Währung in ihren eigenen Projekten nutzen möchten.

Die Entwicklung der Plattform beginnt, sobald ausreichend Geld eingesammelt wurde. Diese Vorgehensweise bringt einige Vorteile. Die Gründer haben ausreichend Geld zur Verfügung, um talentierte Entwickler angemessen zu entlohnen. Sie müssen jedoch keinerlei Unternehmensanteile im Gegenzug zum Investment abgeben, was die Finanzierung von Open Source und nicht auf unmittelbaren Gewinn ausgelegte Projekten erleichtert.

Das Plattformprojekt an sich zieht bereits zu Anfang großes Interesse auf sich, ähnlich wie bei Kickstarter ergibt sich ein hoher Bekanntheitsgrad in der Community. Ob das Projekt finanziert wird, hängt stark davon ab, inwiefern es gelingt, auch die Entwickler anzusprechen, insofern ist der ICO ein Test am Markt, wie groß das Interesse an der Plattformidee ist. Wenn es erfolgreich ist, warten bereits Entwickler darauf, weitere Anwendungen auf Basis der Plattform entwickeln zu können.

Die generierten Kryptowährungen bleiben länger bestehen und halten eher den Wert, wenn die erhaltenen Gelder im Projekt sinnvoll genutzt werden. Denn die Währung wird in den auf der Plattform laufenden Anwendungen genutzt. Und für die Initiatoren der Projekte erhöhen sich im Erfolgsfall auch die Chancen, für auf die Plattform aufbauende kommerzielle Projekte Venture Capital gegen Beteiligung zu erhalten.

Durch diese Vorteile nimmt der Beliebtheitsgrad für ICOs zu – was wiederum zu Problemen führt. Denn mittlerweile verliert diese Form der Finanzierung an Reiz, zu viele solcher Projekte wurden in zu kurzer Zeit angeboten. So ist es mittlerweile auch bei guten Ideen nicht garantiert, ausreichend Interesse und Vertrauen generieren zu können. Denn neben den

seriösen Projekten gibt es auch in diesem Bereich Betrugsfälle, wo der Launch einer neuen Kryptowährung versprochen wird, nach erfolgreicher Finanzierung jedoch nichts passiert. Und selbst seriöse Projekte können scheitern, wie es beispielsweise bei „The DAO“ passierte, wo das Geld als Investmentfond für unterschiedlichste Blockchainprojekte verwendet werden sollte. Eine Attacke jedoch, bei der eine große Menge an DAO-Token (also der Werteinheiten und damit verbundenen Stimmrechte) gestohlen wurden, führte dazu, dass einerseits die dahinterliegende Ethereum-Blockchain auf den vorhergehenden Zustand manuell zurückgesetzt wurde, eine Entscheidung, die in der Community nicht von jedem unterstützt wurde, und die Gelder wieder an die Investoren zurückgegeben wurden.

Auch Regulierungsfragen sind zu einem großen Teil noch ungeklärt, wie der Gesetzgeber also mit ICOs in Zukunft hinsichtlich rechtlicher und steuerlicher Fragen umgehen wird, ist noch weitgehend unklar.

Dass die bei ICOs generierten Investmentsummen nicht vernachlässigbar sind und durchaus mit größeren Venture Capital Investitionssummen mithalten können, zeigen folgende Beispiele.

Die oben genannte „The DAO“ sammelte rund 150 Millionen Dollar von mehr als 11.000 Investoren ein – eine Summe, die die Initiatoren bei weitem nicht erwartet hatten, Ethereum erhielt für die Entwicklung der Plattform rund 18 Millionen Dollar, Madesafecoin 7 Mio. $ und Lisk rund 6 Mio. $.

Eine Liste der aktuellen ICOs findet sich bei Smith and Crown unter https://www.smithandcrown.com/icos/. Wer sich dafür interessiert, welche Projekte es bereits gab und wie diese vom Markt angenommen wurden, findet jede Menge Infos unter https://www.smithandcrown.com/past-icos/.

Der Handel mit Altcoins

Wie Bitcoin werden auch die unterschiedlichen Altcoins auf den unterschiedlichen Börsen für Kryptowährungen gehandelt, der Wert ergibt sich auf Basis des Angebots und der Nachfrage. Auf Wertsteigerungen zu spekulieren ist ein riskantes Geschäft, die Wahrscheinlichkeit alles zu verlieren, ist hoch. Mein persönliches Interesse an der Blockchain-Technologie liegt nicht darin, wie es gelingt, mit Geld Geld zu machen. Vielmehr finde ich die möglichen gesellschaftlichen und technologischen Implikationen der Blockchain und der Kryptowährungen spannend.

Nichtsdestotrotz sind ein Großteil der Transaktionen von Kryptowährungen Spekulation, dies erfüllt durchaus auch eine wichtige Funktion, denn die möglichen Währungsgewinne sind eines der Motive für Investoren, im Rahmen von ICOs in technologisch spannende, jedoch möglicherweise nicht unmittelbar wirtschaftlich interessante Projekte zu investieren.

Darum auch hier ein paar Quellen und Infos, die für den am Altcoin-Trading interessierten Leser von Wert sein könnten.

Wechselbörsen

Wie ja auch schon aufgezeigt kann man Bitcoin selbst „minen“, aber das ist in der Regel mit einem Verlust verbunden und die Miner müssen darauf spekulieren, dass es zu einer entsprechenden Wertsteigerung kommt. Wer sich mehr mit der gesamten Materie des Minings auseinandersetzen möchte, braucht neben den technischen Fähigkeiten in den üblichen Linux Umgebungen auch ein Verständnis zur besten Hardware und den verwendeten Hash-Algorithmen. Einen ersten Einblick finden Sie unter http://www.coindesk.com/information/how-to-mine-litecoin/ und die Berechnung der jeweiligen Einkünfte bei verschiedenen Kryptowährungen kann unter anderem auf http://www.coinwarz.com/cryptocurrency durchgeführt werden.

Wie schon im 1. Kapitel ausgeführt, kann man sich die ersten Bitcoins einfach von der Firma Coinfinity aus Graz holen. Wer aber mit verschiedenen Kryptowährungen spekulieren möchte ist auf entsprechend darauf eingestellte Handelsbörsen angewiesen. Einen Überblick über die jeweils auf den Börsen gehandelten Digitalen Währungen & Assets findet man auf https://coinmarketcap.com/exchanges/volume/24-hour/

Damit der Einstieg etwas leichter fällt, will ich hier nur einige der bekannteren und für verschiedene Kryptowährungen verwendeten Börsen aufzählen. Weiters will ich hier auf die

Gefahr des Diebstahls hinweisen. So wie es laufend auch im bekannten Banksystem zu Raubzügen[1] kommt, ist auch eine Wechselbörse, die selbst die Werte hält, nicht vor Diebstahl oder Betrug gefeit. Wenn der Diebstahl nicht aufgeklärt wird und die veruntreuten Gelder sichergestellt werden können, dann gibt es auch keine Kompensation der Geschädigten. Der bisher größte Schadensfall war die Insolvenz von Mt. Gox, eine Wechselbörse in Tokyo, die im Februar 2014 um 350 Mill. $ bestohlen wurde.

1. Poloniex – www.poloniex.com, Delaware, USA

Poloniex wurde im Jänner 2014 gegründet und ist eine der größten und aktivsten Handelsbörsen. Neben dem Wechsel zwischen Fiat Währungen und Kryptowährungen kann man hier auch Margin Trading betreiben und Bitcoin verleihen oder leihen. Der bisher einzig bekannte Diebstahl von 97 Bitcoin (damals ca. 50.000 $)[2] [3] im März 2014 wurde komplett vom Eigentümer an die Geschädigten zurückerstattet.

2. Bitfinex – www.bitfinex.com, Hong Kong, China

Die Plattform bietet sowohl finanzierte als auch unfinanzierte Transaktionen von Digitalen Werten. Damit lassen sich deutlich riskantere Spekulationsgeschäfte abbilden und man kann auch anderen Spekulanten gegen Zinsen die eigenen Bitcoins leihen. Bitfinex hat am 3. August 2016 die Medien informiert, dass sie um 119.756 Bitcoins bestohlen wurden – was einem Gegenwert von ca. 58 Mill. €[4] entsprach und damit der zweitgrößte Diebstahl nach Mt. Gox ist. Der Diebstahl wurde durch einen 36% “Haircut” im Austausch gegen eigene BFX Token für alle Einlagen egalisiert.

[1] Reuters, 12. Dec. 2016: SWIFT confirms new cyber thefts, hacking tactics. http://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT
[2] Truong, Alice (6 March 2014). *"Another Bitcoin exchange, another heist"*. Fast Company. *Retrieved 7 March 2014*.
[3] Poloniex, 2. July 2014. https://poloniex.com/press-releases/2014.07.02-Poloniex-Repays-97-Stolen-Bitcoins-to-Customers-from-March-Exploit
[4] Heise, 3. Aug. 2016. https://www.heise.de/newsticker/meldung/Bitfinex-Hack-58-Millionen-Euro-gestohlen-Bitcoin-Kurs-eingebrochen-3286784.html

3. Kraken – www.kraken.com, San Francisco, USA

Kraken ist eine vor allem in Europa beliebte Wechsel- und Handelsbörse, die seit der Gründung im Juli 2011 auch durch viele Zukäufe massiv an Profil gewonnen hat. Der Gründer und CEO Jesse Powell ist, nachdem er im Rahmen einer Untersuchung des Mt. Gox Desasters deren schlechte Umsetzung gesehen hat, mit diesem Handelsplatz durchgestartet. Kraken verwaltet die Ansprüche der bei Mt. Gox geschädigten Gläubiger vor Gericht und wurde bisher noch nie bestohlen.

4. Coinbase – www.coinbase.com, San Francisco, USA

Das Unternehmen wurde 2012 gegründet und hat nach eigenen Angaben ca. 5 Mio. Nutzer. Es wurden bereits über 100 Mio. $ an Investitionskapital eingesammelt und die professionell strukturierte Handelsplattform von Coinbase nennt sich Global Digital Asset Exchange (GDAX) - https://www.gdax.com. Bei Coinbase oder GDAX sind bisher keine Diebstähle gemeldet worden.

5. Bittrex – www.bittrex.com, Las Vegas, USA

Diese Handelsplattform wurde 2014 gegründet und bietet den Handel mit über 190 Kryptowährungen an. Wenn man bei den anderen Börsen nicht fündig wird, dann ist die Wahrscheinlichkeit hoch, dass der gesuchte Coin hier gehandelt wird. Der Gründer, Bill Shihara war zuvor bei BlackBerry und Microsoft für Security-Analysen zuständig. Es gibt keinen bekannten Diebstahl von Bittrex.

36 Regeln für Kryptomärkte von Markus M. Bohl

Der Handel mit Altcoins ist riskant. Um über neue und laufende Projekte informiert zu sein, ist es empfehlenswert, sich Informationen aus unterschiedlichsten Quellen zu suchen. Als erster Einstieg eignet sich ein gut geschriebener und interessanter deutschsprachiger Blog mit Infos rund um das Thema – der Altcoinspekulant von Markus M. Bohl (https://altcoinspekulant.wordpress.com/).

Kürzlich hat er einen Beitrag mit 36 prägnant formulierten, in willkürlicher Reihenfolge genannten Regeln für Kryptomärkte veröffentlicht, die einen ersten guten Einblick in die Welt des Altcoin-Handels geben. Viel Spaß beim Lesen dieser Expertentipps.

Kryptoregel 1: Die beste Performance bei Altcoins ist üblicherweise innerhalb eines Jahres nach der Veröffentlichung. 90% werden danach fallen und irgendwann verschwinden.

Kryptoregel 2: Als Kryptoinvestor benötigt man lediglich zwei Coinbörsen: Poloniex und Bittrex.

Kryptoregel 3: Wenn man bei Poloniex Bitcoin verleiht, sollte man Zinssätze von über 0.1% pro Tag für Bitcoin für 60 Tage einloggen. Sind die Zinsen tiefer, nur 2 Tage.

Kryptoregel 4: Möglichst bei Airdrops , Giveaways und Signaturkampagnen teilnehmen: Gratis Kapital für wenig Aufwand.

Kryptoregel 5: Niemals ausserhalb einer Exchange kaufen, wenn kein Escrow vorhanden ist. Das Risiko ist zu gross.

Kryptoregel 6: Manche ICOs bieten interessante Pre-ICO-Investitionsmöglichkeiten, welche höhere Rabatte ermöglichen als zum Start des ICOs.

Kryptoregel 7: Mache nicht den Fehler Dich in Deine Coins zu verlieben: Vermutlich musst Du innerhalb weniger Monate verkaufen müssen um finanziellen Erfolg zu haben.

Kryptoregel 8: Wer nicht viel Zeit hat am Tag sollte Twitter benutzen um den Kryptomärkten folgen zu können.

Kryptoregel 9: (Cloud)-Mining ist zwar spannend, aber die Zeiten sind vorbei um hier profitabel zu sein. Die Chance Geld zu verlieren ist sehr hoch.

Kryptoregel 10: Vermeide Hype-ICOs welche regelrecht mit tausenden Bitcoin geflutet werden in Verbindung mit viel Medien-Interesse.

Kryptoregel 11: Investiere nur was Du bereit bist zu verlieren. Selbst bei guten Projekten können unvorhergesehene Ereignisse das Aus bedeuten.

Kryptoregel 12: Bereits kurz nach dem Investment sollte man eine Verkaufsstrategie entwickeln. Am Besten schriftlich verfassen.

Kryptoregel 13: Es ist besser in lediglich 3-4 gute ICOs pro Jahr zu investieren, als seine Bitcoin bei schlechteren Projekten aufs Spiel zu setzen.

Kryptoregel 14: Die besten Deals werden hinter den Kulissen gemacht. Versuche entsprechende Kontakte in der Kryptoszene zu knüpfen um Zugang zu erhalten.

Kryptoregel 15: Teile Dein Wissen mit der Community. Du wirst im Gegenzug auf Hilfe hoffen können, wenn Du sie benötigst.

Kryptoregel 16: Es gibt bei Kryptos mehr Informationen täglich, als man selbst verarbeiten kann. Fokussierung auf das Wichtige, ist deshalb das Zauberwort.

Kryptoregel 17: Die besten Coinreturns gibt es nicht durch das Trading sondern durch ICOs (siehe auch IOTA, Nxt oder Ethereum).

Kryptoregel 18: Immer die Passwörter ändern und zudem möglichst verschiedene E-Mail-Adressen verwenden im Kryptoland.

Kryptoregel 19: Mein Passwortmanager für all die verschiedenen Accounts und Wallets: Kugelschreiber + Papier.

Kryptoregel 20: Immer etwas freie Bitcoin als Liquidität bereit halten: Manche Investitionschancen verstreichen innerhalb von Minuten.

Kryptoregel 21: Das beste Marketing bringt langfristig nichts ohne gute Technologie. Hüte Dich vor Projekten von Schaumschlägern.

Kryptoregel 22: Die Sicherheit Deines Computers ist sehr wichtig: Sichere Dein System mit einer guten Firewall und vermeide Smartphone-Logins.

Kryptoregel 23: Nach einer Investition in ein Kryptoprojekt muss man regelmässig seine Hausaufgaben machen und mindestens zweimal wöchentlich den Status überprüfen.

Kryptoregel 24: Gute Projekte mit neuer Technologie brauchen Zeit nach dem ICO. Investiere nicht wenn Du zu wenig Geduld hast und nicht ein Jahr oder länger warten kannst.

Kryptoregel 25: Wenn Du Dir unsicher bist über ein Investment, investiere einfach nicht. Es gibt nahezu täglich neue Chancen im Kryptoland.

Kryptoregel 26: Du wirst zeitlich nicht dazu in der Lage sein, mehr als eine Handvoll Projekte abzudecken. Wähle weise aus und ersetze die schlechten Projekte emotionslos.

Kryptoregel 27: Es gibt einige ICOs, bei denen Investoren nur einen kleinen Teil (<50%) erwerben können. Diese ICOs bitte meiden.

Kryptoregel 28: Die Krpytomärkte sind volatil genug. Investiere nicht in Hebelkontrakte wie Futures oder Margintrading. Du wirst höchstwahrscheinlich verlieren.

Kryptoregel 29: Investiere nicht in ICOs, wenn Du den höchstmöglichen Start-Bonus nicht mehr erhalten kannst. Wenn Du zu spät bist, ist es das Risiko meistens nicht wert.

Kryptoregel 30: Auch Shitcoins können problemlos eine Marktkapitalisierung von über 50 Millionen erreichen. Aber nur kurzfristig, längerfristig wird Qualität benötigt.

Kryptoregel 31: Ist eine Kryptowährung in Kombination mit einem Multi-Level-Marketing-System, handelt es sich um einen Scam und Du wirst alles verlieren.

Kryptoregel 32: Höhere Bitcoin-Preise beeinflussen die Altcoinmärkte nur kurzfristig negativ. Längerfristig steigen Altcoins immer stärker als der BTC in einem Bullenmarkt.

Kryptoregel 33: To survive in cryptoland you need at least good English reading skills.

Kryptoregel 34: Investiere nicht in bereits gehypte Coins nach mehreren hundert Prozent Kursanstieg. Du wirst höchstwahrscheinlich als sogenannter Bagholder enden.

Kryptoregel 35: Besorge Dir für größere Bitcoinbestände unbedingt ein Hardwarewallet wie den Trezor oder arbeite mit Paperwallets.

Kryptoregel 36: Es ist völlig normal 100% Verluste zu erleiden. Diese werden aber durch einige 1000% Gewinne mehr als ausgeglichen wenn man seine Hausaufgaben macht.

Quelle: https://altcoinspekulant.wordpress.com/2016/11/15/36-regeln-fuer-die-kryptomaerkte/

Achtung Betrug! – Finger weg von Scamcoins

110 % am ersten Tag, 120 % in der ersten Woche. Das sind typische Versprechungen von Schneeballsystemen, die nach sehr ähnlichen Mustern ablaufen und den Leuten das Geld aus der Tasche ziehen. Oft kommt gleich am Anfang schon die erste Rückzahlung und man wiegt sich in Sicherheit, aber in erster Linie machen diese Systeme die Initiatoren reich und alle anderen schauen durch die Finger. Anstatt Betrüger reich zu machen, sollten Sie Ihr überschüssiges Geld dann doch lieber spenden.

Hinweise auf derartige Betrügereien sind:

- Multi-Level-Marketing (MLM) Vertrieb
- Keine Listung auf www.coinmarketcap.com
- Software ist nicht als Open-Source frei verfügbar
- Verwendung der Wertsteigerung von Bitcoin als Referenz
- Reines Spekulationsgut – keine weitere Verwendung
- Hinweise darauf, dass bei kritischen Artikeln und Aussagen den Autoren mit rechtlichen Mitteln wie Abmahnungen gedroht wird

Betrugsbeispiele hierfür sind (mit an Sicherheit grenzender Wahrscheinlichkeit): OneCoin, Bitclub Netzwerk, MyCoin, usw. Die Betrüger gehen sehr aggressiv gegen Kritiker vor, überhäufen die Internet-Suchmaschinen mit positiven Meldungen und bauen Empfehlungsnetzwerke in massiver Größe auf. Damit man eine Vorstellung hat, wovon wir hier reden und dass hier weltweit im großen Stil agiert wird – der Schaden wird bei MyCoin auf ca. 387 Mill. USD[5] geschätzt.

Eine wesentlich umfangreichere Liste, die leider nie komplett sein kann, finden Sie unter: http://www.badbitcoin.org/thebadlist/index.htm.

Die Menge an dort gelisteten Coins zu sehen, ist eindrucksvoll.

[5] Business Insider, Malaysia, 9. Feb. 2015. http://www.businessinsider.my/mycoin-ponzi-scheme-allegations-losses-2015-2/#uYAzWHuHeGHIo1OH.97

Und einen interessanten Artikel dazu finden Sie auch beim Altcoinspekulant. Neben dem, dass hier viele Menschen getrieben durch Gier, Ignoranz und Unwissenheit Gefahr laufen, ihr gesamtes Erspartes zu verlieren, besteht natürlich auch die Sorge, dass solche Konstrukte, wenn sie irgendwann zusammenbrechen, zu Regulierungen von Seiten der Gesetzgeber führen werden, die auch seriöse Projekt beeinflussen.

Da es sich bei diesen Projekten um international agierende Betrugsnetzwerke handelt, die professionell agieren und bei denen oft bereits in anderen Betrugszusammenhang aufgefallene Spieler agieren, ist aus meiner Sicht die Aufklärung und Information der Bürger in Kombination mit der rechtlichen Verfolgung der Vertriebsnetzwerke am sinnvollsten.

Ausgewählte Altcoins und ihre Eigenschaften

Ein wichtiger Anhaltspunkt für die Aktivität rund um einzelne Altcoins finden Sie auf www.coinmarketcap.com und sollten Sie einen vermeidlichen Geheimtipp für ein spannendes Investment dort nicht finden, dann seien Sie – wie bereits gesagt – vorsichtig, es könnte sich um eines der vielen Betrugsnetzwerke handeln.

ACHTUNG: Selbst die auf Coinmarketcap aufgeführten und auf verschiedenen Börsen gehandelten Kryptowährungen (wie auch die dort angeführten Beteiligungen) sind in der Regel nicht reguliert und mit einem Totalverlust ohne jeglichen rechtlichen Schutz muss gerechnet werden. Altcoin-Spekulanten sind in der Regel Spielernaturen und wenn man sollte sich auf keinem Fall von der Gier nach dem schnellen Geld lenken lassen.

Hier ein Überblick der zehn Kryptowährungen mit der höchsten Marktkapitalisierung.

All | Currencies | Assets | EUR | Next 100 → | View All

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	€12 675 598 477	€789.49	16,055,400 BTC	€122 887 233	3.47%	
2	Ethereum	€651 708 841	€7.48	87,135,150 ETH	€6 805 700	1.13%	
3	Ripple	€221 692 085	€0.006193	35,794,578,423 XRP *	€1 720 606	-0.68%	
4	Litecoin	€172 944 123	€3.53	48,975,329 LTC	€2 276 467	0.72%	
5	Monero	€111 488 115	€8.20	13,592,149 XMR	€1 843 299	-0.53%	
6	Ethereum Classic	€93 596 716	€1.07	87,074,179 ETC	€2 305 711	-5.90%	
7	Dash	€66 932 958	€9.60	6,968,659 DASH	€2 129 679	-3.26%	
8	NEM	€30 638 966	€0.003404	8,999,999,999 XEM *	€57 794	-5.70%	
9	Steem	€29 505 303	€0.128831	229,022,984 STEEM	€128 600	-11.75%	
10	Factom	€23 025 013	€2.63	8,753,219 FCT *	€4 529 685	-16.67%	

Quelle: http://coinmarketcap.com/currencies/

Wie man an der obigen Liste leicht erkennen kann ist die Marktkapitalisierung massiv von Bitcoin dominiert. Trotz allem Erfolg von Bitcoin muss klar sein, dass auf globaler Ebene die Marktkapitalisierung der Kryptowährungen noch keine besondere Rolle spielt. Andererseits darf man das Potential auch nicht unterschätzen – denn bei vielen nationale Währungen sind

zirkulierenden Scheine und Münzen weniger wert als Bitcoin. Da es ja bei Bitcoin kein Giralgeld – also von Banken geschöpftes Geld – gibt, ist dieser Vergleich auch durchaus angebracht.

Ich möchte Ihnen hier eine kurze Einführung in die Altcoins aus der oben gezeigten Top Ten Liste geben, wie auch noch ein paar Projekte vorstellen, die aus unterschiedlichen Aspekten heraus interessant sind.

ETHEREUM ETH	Ethereum ist eine eigene Blockchain Lösung mit einer Kryptowährung – dem Ether. Mittels der dafür entwickelten Programmiersprache Solitity ist es möglich, frei definierbare Smart Contracts – also kleine Softwareprogramme – in die Blockchain zu speichern und mit einer eigenen Virtuellen Maschine auszuführen. Ethereum ist deshalb interessant für weitreichende dezentrale Automatisierungen.	Startdatum: 30.07.2015 Blockchain Art: Öffentlich Ursprung: Neuentwicklung Geldschöpfung: Mining Geldmenge: nicht beschränkt Konsens: PoW / PoS Hash-Algorithmus: Ethash Blockzeit: ca. 15 Sek. Homepage: www.ethereum.org Das Whitepaper find sich hier.
  XRP	Ripple ist ein Zahlungsnetzwerk und bietet eine Blockchain, über die Banken miteinander verbunden werden und den Wertaustausch durchführen. Es ist nicht auf eine bestimmte Währung beschränkt und so können USD, Euro, Bitcoin oder jede Währung, für die Gateaways existieren, ausgetauscht werden. Die eigene Währung XRP wird für die Bezahlung von Transaktionen verwendet und danach vernichtet.	Startdatum: Sept. 2012 Blockchain Art: Privat Ursprung: Neuentwicklung Geldschöpfung: Generiert Geldmenge: 100 Mrd. XRP Konsens: Consesus Hash-Algorithmus: SHA-256 Blockzeit: ca. 2-5 Sek. Homepage: www.ripple.com Das Consensus-Whitepaper find sich hier.
  LTC	Litecoin ist eine Weiterentwicklung von Bitcoin und unterscheidet sich hauptsächlich durch den verwendeten Hash-Algorithmus, der die Verwendung von Prozessoren (CPU's) und Grafikkarten (GPU's) bevorzugt. Trotzdem wurde 2014 die erste spezielle ASIC Mining-Hardware vorgestellt. Die Integration in Bitcoin Software ist leicht zu bewerkstelligen, und für gewisse Zeit war Litecoin für Investoren eine sehr spannende Alternative zu Bitcoin.	Startdatum: 7.10.2011 Blockchain Art: Öffentlich Ursprung: Bitcoin Geldschöpfung: Mining Geldmenge: 84 Mill. LTC Konsens: PoW Hash-Algorithmus: scrypt Blockzeit: ca. 2,5 Min. Homepage: www.litecoin.com Das Scrypt-Paper findet sich hier.

 XMR	Monero wurde von Bytecoin abgeleitet und hat einen Fokus auf deutlich verbesserte Privatsphäre bei Zahlungen im Vergleich zu Bitcoin. Der Proof-of-Work Algorithmus verwendet „Ring-Signaturen“, um die Rückverfolgung einer Person zu verschleiern. Deshalb wird diese Währung auch gerne mit den Internet-Schwarzmärkten in Verbindung gebracht.	Startdatum: 18.04.2014 Blockchain Art: Öffentlich Ursprung: Bytecoin Geldschöpfung: Mining Geldmenge: 18,4 Mill. XMR Konsens: PoW Hash-Algorithmus: CryptoNight Blockzeit: ca. 120 Sek. Homepage: www.getmonero.org Das CryptoNote-Whitepaper findet sich hier.
 ETC	Ethereum Classic ist im Prinzip äquivalent mit Ethereum. Entstanden ist es aus einem Disput in der Community, ob es gerechtfertigt werden kann, die in Blockchains gespeicherte Information manuell zurückzusetzen. Am 17. Juni 2016 wurde die „The DAO“ gehackt und 50 Mill. € in ein Depot eines Hackers abgezweigt – damals hat die Ethereum Foundation schlussendlich ein Update zur Verfügung gestellt, die diesen Diebstahl wieder zurückgesetzt hat. Ein Schritt, der nicht von allen gutgeheißen wurde – Gegner dieser Korrektur blieben bei der „alten“ Blockchain, der Ethereum Classic.	Startdatum: 20.07.2016 Blockchain Art: Öffentlich Ursprung: Ethereum Geldschöpfung: Mining Geldmenge: nicht beschränkt Konsens: PoW / PoS Hash-Algorithmus: Ethash Blockzeit: ca. 15 Sek. Homepage: www.ethereumclassic.org Whitepaper: siehe Ethereum

DASH	Dash ist eine Weiterentwicklung von Litecoin und bietet erhöhte Privatsphäre und verbesserte Resistenz gegen Spezialhardware. Überweisungen gehen durch einen Coin-Mixer, der mehrere gleichartige Transaktionen kombiniert und dann wieder aufgeteilt an die eigentlichen Empfänger weiterleitet. Neben den Minern gibt es noch sogenannte Masternodes zur Schnellüberweisung in 4 Sekunden.	Startdatum: 18.01.2014 Blockchain Art: Öffentlich Ursprung: Litecoin Geldschöpfung: Mining Geldmenge: ca. 18,9 Mill. DASH Konsens: PoW Hash-Algorithmus: X11 Blockzeit: ca. 2,5 Min. Homepage: www.dash.org Das Whitepaper findet sich hier.
XEM	NEM steht für New Economy Movement und wird gerade intensiv von der Firma Tech Bureau Corp. weiterentwickelt. Eine private Version dieses Blockchain Systems namens Mijin wird bei Finanzinstituten in Japan eingesetzt. Das System besteht aus Open-Source Clients (NCC) und Closed-Source Servern (NIS). Neben standardmäßig eingebauter Multi-Signatur Technologie werden Knoten (Nodes) durch das Eigentrust++ Reputationssystem bewertet.	Startdatum: 31.03.2015 Blockchain Art: Öffentlich Ursprung: Eigenentwicklung Geldschöpfung: Generiert Geldmenge: 9 Mrd. XEM Konsens: Proof-of-Importance Hash-Algorithmus: 512 bit SHA3 Blockzeit: ca. 2,5 Min. Homepage: www.dash.org Das NEM-Whitepaper findet sich hier.
STEEM	Steemit.com ist ein Soziales Netzwerk im Stil von Reddit mit Belohnungen für Beiträge und „Upvotes“. Die Logik ist, dass beliebte Beiträge auch wertvoll sind gelesen zu werden und die Ersteller entsprechend daran verdienen sollten. Aktuell werden die neu geschaffenen Coins zu 75% an die Autoren und Content-Schaffenden, zu 10% an Leser und Miner und zu 15% an Steem Power Besitzer (mehr dazu hier) ausgeschüttet.	Startdatum: 24.03.2016 Blockchain Art: Öffentlich Ursprung: Neuentwicklung Geldschöpfung: Mining Geldmenge: + 9,5 % pro Jahr Konsens: PoW / DPoS Hash-Algorithmus: SHA256 Blockzeit: 2 Sek. Homepage: www.steem.io Die Beschreibung des Distributed Proof-of-Stake (DPoS) Konsens-Algorithmus findet sich hier.

 FCT	Factom ist eine Plattform, bei der Skripte und Programme gegen Bezahlung einer Gebühr abgespeichert werden können und der Status dieser Blockchain alle 10 Minuten in der Bitcoin Blockchain dokumentiert wird. Bekannt wurde Factom vor allem über die Falschmeldung, dass Honduras sein Grundbuch mittels Factom abbilden möchte.	Startdatum: 01.09.2015 Blockchain Art: Privat Ursprung: Neuentwicklung Geldschöpfung: Generiert Geldmenge: nicht Bekannt Konsens: Details hier Hash-Algorithmus: Details hier Blockzeit: keine, bzw. 10 Min. Homepage: www.factom.org Das Factom-Whitepaper findet sich hier.

Einige weitere interessante Altcoins sind:

 ZEC	ZCash ist eine auf Privatsphäre ausgelegte Kryptowährung. Wenn gewünscht, kann man den Absender, die Geldmenge und den Empfänger komplett verbergen. Die dafür benötigten Hardware-Anforderungen sind hoch, werden aber über die Zeit sicher keine Rolle mehr spielen. Es ist die erste Währung die „Zero-Knowledge-Proof“ standardmäßig verwendet. Man kann gespannt sein, wie sich die versprochene Funktionalität im Erfolg wiederspiegelt.	Startdatum: 28.10.2016 Blockchain Art: Öffentlich Ursprung: Bitcoin Geldschöpfung: Mining Geldmenge: 21 Mill. ZEC Konsens: Proof-of-Work Hash-Algorithmus: Equihash Blockzeit: 2,5 Min. Homepage: www.z.cash Wie „Zero-Knowledge-Proof“ funktioniert wird im zk-SNARK Whitepaper erläutert.

CureCoin **CURE**	CureCoin werden als Belohnung verteilt, wenn jemand die persönliche Rechnerleistung zum Falten von Proteinen bereitstellt. Damit verbraucht man den Strom für die Rechenleistung nicht um „sinnlose“ Rätsel zu lösen, sondern hilft bei der medizinischen Forschung. Weitere Details werden in dem folgenden Youtube Video erklärt: https://www.youtube.com/watch?v=u-WM7iPBodI	Startdatum: 16.11.2013 Blockchain Art: Öffentlich Ursprung: Litecoin Geldschöpfung: Mining / Minting Geldmenge: 27.069.500 CURE Konsens: Hybrid PoW / PoS Hash-Algorithmus: SHA-256 Blockzeit: 1 Min. (Mining) Homepage: www.curecoin.net
FLDC **realisiert über** Counterparty **XCP**	Die eigene Rechnerleistung kann man auch bei Foldingcoin.net einsetzen und wird dafür mit einer auf Counterparty realisierten eigenen Währung belohnt. So wie auch bei CureCoin ist der bereitgestellte Gegenwert in etwa so groß, wie der verbrauchte Strom wert ist, und so machen es die Teilnehmer eher aus ideologischen Gründen. Der Sinn ergibt sich dadurch, dass die ohnehin vorhandene Grafik-Hardware für den guten Zweck eingesetzt werden und von den Forschern nicht extra beschafft werden muss.	Details zu Counterparty Startdatum: 02.01.2014 Es handelt sich um eine Erweiterung der Bitcoin Blockchain um Smart Contract Funktionalitäten und der Schaffung eigener, handelbarer Assets (z.B. FLDC). Die eigene Währung XCP wurde durch „verbrennen“ von Bitcoins geschöpft und die gesamte dabei erzeugte Geldmenge war 2.621.086 XCP. Homepage: www.counterparty.io Das Foldingcoin-Whitepaper findet sich hier.

Weitere Kryptowährungen und die jeweiligen Beschreibungen finden Sie unter:

http://cryptocoin.cc/

Die eigene Währung für Jedermann ☺

Die freie Verfügbarkeit der Software für das Bitcoin-Protokoll hat dazu geführt, dass sich jeder mittlerweile einfach seine eigene Kryptowährung erstellen kann. Deshalb gibt es neben den Weiterentwicklungen von Bitcoin (z.B. Litecoin) auch eine riesige Auswahl an einfachen Bitcoin-Derivaten, wo einzelne Parameter anders eingestellt wurden.

Wer sich also gerne seinen eigenen Kryptocoin erstellen möchte kann das auf der folgenden Seite ohne jegliche Programmierkenntnisse und fortgeschrittenem technischen Verständnis machen: https://cryptonotestarter.org/inner.html

Für alle die auch in die Programmierung einsteigen wollen findet sich der Einstieg zu Bitcoin unter https://github.com/bitcoin, zu Litecoin unter https://github.com/litecoin-project/litecoin und zu Ethereum unter https://github.com/ethereum/.

Wenn Sie eine eigene, globale Kryptowährung mit einer eigenen Blockchain aufbauen wollen, dann sollte klar sein, was der Einsatzzweck ist und wie man sich am Anfang vor Hackern schützen will. Der Erfolg einer Kryptowährung hängt von vielen Faktoren ab, eine Währung erfolgreich zu machen, ist ein höchst komplexes Unterfangen. Weiters sollte klar sein, dass es mögliche rechtliche Implikationen gibt und dies der wahrscheinlichste Grund ist, warum bis heute nicht bekannt ist, wer Satoshi Nakamoto ist.

Aber neben dem Einsatz als Kryptowährung könnten Krypto-Token auch für immaterielle Werte stehen – beispielsweise könnten damit Wahlentscheidungen oder ein Maß für Wertschätzung symbolisiert werden. Darum ist es nicht unwahrscheinlich, dass wir in Zukunft unterschiedlichste Krypto-Token für unterschiedlichste Einsatzmöglichkeiten neben der Funktion als Geld kennen lernen werden. Deshalb möchte ich Ihnen jetzt schon viel Vergnügen in dieser voraussichtlich bunten Kryptowelt von morgen wünschen.