Ten Things to Know About Bitcoin and Other Cryptocurrencies

Colorado Bar Association Real Estate Section

November 1, 2018

Donald D. Allen, Esq.
Markus Williams & Young LLC
(303) 318-0131 dallen@markuswilliams.com

In many ways, virtual currencies might just give existing currencies and monetary policy a run for their money.

Christine Lagarde, Managing Director of the IMF

---

1. What is bitcoin?

A type of digital currency (Cryptocurrency) in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds operating independently of a central bank (or any bank). Capital "B" Bitcoin is the protocol, the network and the community.

Bitcoin is generated and protected by blockchain technology (see below) which prevents the "double-spending" problem. Any transaction must be verified by a majority of computers ("nodes") before a block can be added to the chain.

There are more than 200 cryptocurrencies (some may only be tokens, see below) in circulation today with a combined market cap of over $202 Billion.

2. What is Blockchain?

A distributed, digital, immutable ledger in which transactions made are recorded chronologically and publicly. This is a decentralized system which means it is not controlled by any single governing entity.

A block is a new page of the ledger that cannot be changed.

The blockchain nodes (computers verifying transactions) are distributed across the globe.

The blockchain for bitcoin is open for all to download. (Currently 185 Gigabytes in size).

3. What is an Exchange[1].

Exchanges allows consumers to buy, sell and trade cryptocurrencies, whether through fiat currencies like dollars, euros or yen or other cryptocurrencies, e.g. exchanging bitcoin for Ether (see below). Not every exchange supports every cryptocurrency and users may use more than one exchange. Less common cryptocurrencies, called "altcoins" cannot be purchased directly with fiat currency and often must be traded against bitcoin.

American exchanges are subject to state by state regulations as well as federal guidelines. New York State implemented "BitLicense" regulations in 2015.

There are more than 200 cryptocurrency exchanges that support active trading. The combined 24 hour trade volume is more than $6.5 billion.

Exchanges charge fees of between .10% and 5.50% of each transaction.

Coinbase is one of the more popular exchanges, especially for beginners. As of December 2017, the company held more than $10 billion in digital assets. (Bloomberg Business Week, December 25, 2017). See attached 2018 Fortune Magazine 40 under 40 listing Brian Armstrong CEO and cofounder of Coinbase.

4. What is an ICO? What are Tokens?

"The term "ICO" is often used to describe Ethereum token launches. But coins and tokens are two very different things…

ICO—Initial Coin Offering—is a term created to describe the many bitcoin clones and other "coin" clones that erupted over the years. Bitcoin is basically a distributed ledger that performs best as digital money—a simple example of the power of decentralization. Satoshi Nakamoto's consensus process is revolutionary! But you can't build much with it. Ethereum can do what Bitcoin does. It can be digital money too, but unlike Bitcoin, Ethereum is highly programmable—it's designed to accommodate the construction of complex applications. Bitcoin produces "coins". Ethereum generates "tokens". A "Token Launch" is an Ethereum thing. An "ICO" is a bitcoin/altcoin thing.

Coins really only have one utility—to act as simple stores of value with limited-to-no other functionality. By "simple" value, I mean value not represented or manifested through a variety of dynamic functions. Tokens are a completely different breed all together. They can store complex, multi-faceted levels of value. Forget everything you know about bitcoin and pre-mined coins and that entire ilk of tech, Ethereum tokens are generated by a Smart Contract System (SCS), are highly programmable and have multi-

[1] Material in this section is from Forbes.com, June 20, 2018, Guide to Top Cryptocurrency Exchanges, Sarah Hansen.

functionality because of it. They transcend being just a coin, and through their array of functions become something much more—"tokens". Technically, they are not "offered", they are "generated". Probably the most accurate phrase of what's going on during an Ethereum token launch is to describe it as a "Token Generation Event", but I'm not sure TGE has the same flare as ICO. Nevertheless, a coin does one thing, and a token can do many things."

Medium. Com, What is the Difference between an ICO and a Token Launch, By Zach LeBeau, CEO of SingularDTV (May 11, 2017).

5. What is Ethereum?

Ethereum is a blockchain based platform that goes beyond bitcoin. Ethereum has a cryptocurrency called "Ether" which can transact value between actors, like bitcoin. Users need to use "Ether" to buy "gas" on Ethereum. Gas is the computational power needed to verify blocks.

Ethereum has expanded the underlying technology to a broader general purpose blockchain. Developers can use the Ethereum platform to design decentralized apps. It has been reported that as of August 2018, there were 867 such apps. Such apps include Provenance which aims to assist consumers by tracing the origins and histories of products. Another app is Ethlance, a freelance platform to exchange work for Ether rather than other currencies.

On June 14, 2018, William Hinman, director of SEC's division of corporation finance said "Putting aside the fundraising that accompanied the creation of Ether, based on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions."

See attached 2018 Fortune Magazine "40 under 40" listing Vitalik Buterin, creator of Ethereum and stating that Ethereum has a market capitalization of $48 billion.

6. What is a Public Key?

"Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption." Techtarget.com posted by Margaret Rouse.

The public key is comparable to a mailbox address or a username.

A hash of the public key, called an address, in the one displayed on the blockchain. For you to receive bitcoin it is enough for the sender to know your address. The public key is derived from the private key (see below) which you need to send bitcoin to another address.

7. What is a Private Key?

"A private key is a sophisticated form of cryptography that allows a user to access his or her cryptocurrency. A private key is an integral aspect of bitcoin and altcoins, and its security make up helps to protect a user from theft and unauthorized access to funds." www.investopedia.com.

"A private key is a secret, alphanumeric password/number used to spend/send your bitcoins to another Bitcoin address. It is a 256-bit long number which is picked randomly as soon as you make a wallet. The degree of randomness and uniqueness is well defined by cryptographic functions for security purposes. This is how the Bitcoin private key looks (it always starts with 5):

5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF"

Coinsutra, Bitcoin Private Keys: Everything you Need to Know by Sudhir Khatwani, Last Updated June 13, 2018.

8. What is a Digital Wallet?

A digital wallet is where you store your coins. More technically, a wallet is software used to store the public and private keys, enabling you to receive or spend the cryptocurrency and to monitor your balance. A "hot wallet" is the opposite of "cold storage". A strong form of cold storage is storage on a USB Drive, locked in a safe deposit box with no connection to the internet. Coinbase asserts that it stores USB Drives and paper backups of 98% of customer digital currencies in safe deposit boxes, with only 2% kept on line (e.g. hot wallets).

9. What is the Governor's Council for the Advancement of Blockchain Technology Use?

On May 2, 2018, Governor Hickenlooper signed Executive Order B 2018 002 creating the Council for the Advancement of Blockchain Technology Use ("Council").

A. Background and Scope.

The Background Statement in the Executive Order says that "Blockchain technology can be implemented in a variety of public and private settings such as elections, land use and health care… As more users adopt blockchain technology, it has the potential to change the landscape of virtually every recorded transaction."

The scope of the Council shall be to recommend a comprehensive legal framework to support blockchain technology that considers potential applications and boundaries of the technology and protections for consumers. The council shall make recommendations to the Governor and the General Assembly by December 15, 2018.

B. Working Groups.

The Council formed the following working groups

i. Definition of Tokens
ii. Securities
iii. Taxation
iv. Exchanges
v. Banking Money Transmitting
vi. Trust/Custody
vii. Incorporation
viii. Smart Contracts
ix. Digital Identity
x. Government Use of Blockchain
xi. General Regulatory Environment
xii. Debt Payments

C. Uniform Law Commission.

Beyond the Council, other legislative bodies are drafting legislation to address use of cryptocurrencies.

The Uniform Law Commissioners have forwarded to the states the "Uniform Regulation of Virtual-Currency Business Act". The Colorado Commission on Uniform Laws intends to present the act to the Colorado legislature at the next session.

The Act consists of 50 pages and contains a number of defined terms, including the following:

"Legal Tender" means a medium of exchange or unit of value, including the coin or paper money of the United States, **issued by the United States or by another government**.

"Virtual currency":

(A) means a digital representation of value that:

(i) is used as a medium of exchange, unit of account, or store of value; and

(ii) **is not legal tender**, whether or not denominated in legal tender; and

(B) does not include:

(i) a transaction in which a merchant grants, as part of an affinity or rewards program, value that cannot be taken from or exchanged with the merchant for legal tender, bank credit, or virtual currency; or

(ii) a digital representation of value issued by or on behalf of a publisher and used solely within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform.

Note the distinction between virtual currencies and affinity rewards programs or online gaming units of value.

10. How Does the Blockchain Community Think the Technology Will affect Formation and Performance under Contracts?

A number of commenters believe that blockchain and use of smart contracts will change the practice of transactional law. See below.

What Really Is Blockchain and Why Does It Matter to Lawyers?
www.artificiallawyer.com | March 2018 | By David Fisher

"Blockchain and Legal Contracts

Consider the ubiquitous case of contracts. All parties to a contract keep copies of the contract, and between the multiple parties, multiple employees, multiple law firms, multiple attorneys, and multiple enterprise backup systems, there could literally be hundreds of copies of the contract, none of which can be independently confirmed to be authentic.

Nobody can be trusted to hold the single copy of a contract, and so the remedy is massively redundant systems. Blockchain solves this problem of authenticity and uniqueness of contracts just as it does for Bitcoin, using a distributed ledger. The existence of a unique contract is confirmed by the blockchain network, rather than any one party.

And once you can confirm the digital uniqueness and authenticity of the contract, you can progress to the next level of functionality – computable contracts, more commonly known as smart contracts. Smart contracts are computer programs that are authenticated on a blockchain and that can perform operations on that blockchain without human intervention. For example, **consider the case of a real estate property purchase**.

Currently, this would be performed via a signed contract in multiple counterparts, a wire of funds from one bank to the bank of an escrow agent, the manual transfer of title, and finally the release of funds to another bank, with the whole process taking hours or days. In the future, a smart contract would be coded to automatically and instantly transfer title upon transfer of digital currency to the smart contract – no duplicate contracts, no escrow agent, no banks, no delays, and minimal transaction costs.

Following that general pattern, blockchain technology looks set to impact every aspect of the legal industry, from corporate, to criminal, to intellectual property, to real estate, and beyond. And where AI has been applied "top down" to use sophisticated applications to try to make sense of often chaotic and unstructured data, blockchain is applied "bottom up" to bring structure and integrity to data."

Query: Who will draft this "Smart" contract?

Is it time to go back to school? Another commentator has proposed that the hot new degree combination will be a combined Law/Computer Science degree.

11. Bonus Spinal Tap Question: How can you lose Bitcoin?

See attached "Say Bye to Your Bitcoin." Bloomberg Business Week, June 28, 2018.

20. BRIAN ARMSTRONG 35

CEO and cofounder
Coinbase

▸ LIST DEBUT: 2017

Armstrong is building Coinbase, the biggest U.S. Bitcoin exchange, into what his team hopes will become "the Google of crypto"—as relevant to the next wave of the web as Google was to the last. While it has a way to go, it's on the right track: During this winter's investment mania, Coinbase catapulted into the mainstream, eclipsing Charles Schwab in total accounts. Now the company is investing in upstarts and making acquisitions—including one that secured it a path to several tantalizing financial licenses.

22. VITALIK BUTERIN 24

Creator
Ethereum

▸ LIST DEBUT: 2016

Buterin describes his open-source blockchain platform Ethereum as a "world computer." The skinny visionary's experiment, which began as a white paper, now has a market valuation of $48 billion, making it the second-most-valuable crypto network next to Bitcoin. Ethereum caught a lucky break this year when the SEC said it would not regulate Ether, the network's native coin, as a security. Rumor has it Google recently tried to hire Buterin to lead its own whispered crypto endeavors, but he declined.

SAY BYE TO YOUR BITCOIN

There are lots of opportunities for cryptocurrency to go missing—some inherent to buying internet money, some involving crime. Below, a few common ways of going virtually broke

By Lily Katz and Andre Tartar
Illustrations by Nichole Shinn

NOT REALLY YOUR FAULT

Phone Porting

Pretty basic: Scammers hijack people's mobile accounts by calling their carriers and impersonating them. The thieves get their victims' numbers transferred to new devices and ultimately gain access to crypto accounts.

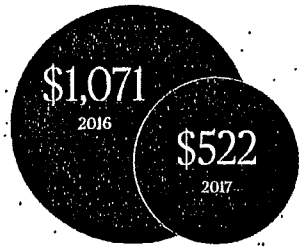
51 Percent Attack

This hasn't happened yet, but it's every crypto enthusiast's greatest fear. If a nefarious syndicate were to gain control of more than half of the Bitcoin network's computing power, it could tamper with the process of verifying transactions and potentially spend the same Bitcoins twice.

Ransom Demands

Everyone from local officials to large corporations has fallen victim to ransomware attacks, which often involve hackers holding computer files hostage until the victim pays a fee in crypto. In June 2017 a South Korean web provider paid hackers $1 million in Bitcoin. Although many payments aren't publicized, it's the largest ransomware demand known to have been paid.

Average ransomware demand

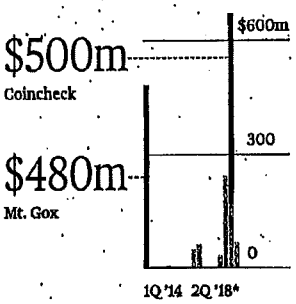


SORTA YOUR FAULT

Exchange Issues

It seems as if every week another cryptocurrency exchange says it's been breached by hackers who've run off with customer funds. Investors can also lose money on exchanges because of technology glitches or account holds that freeze funds and prevent buying or selling during significant market movements.

Losses from exchange hacks



Fraudulent ICOs

Investors have poured billions of dollars into initial coin offerings, only to find their savings drained. In April two founders of an ICO promoted by boxer Floyd Mayweather were brought up on federal charges of raising more than $25 million for a planned digital currency without registering the offering. (Mayweather wasn't accused of wrongdoing.)

Overhyped Stocks

Dozens of struggling businesses used the buzz around crypto to boost their stock market value in late 2017 and early 2018. (Long Island Iced Tea Corp. changed its name to Long Blockchain Corp., but it couldn't raise the capital to mine crypto.) Traditional investors looking for exposure to the nascent industry bought in, but the gains didn't last, and some companies got in trouble with regulators.

TOTALLY YOUR FAULT

Wrong Addresses

Unlike credit card transactions, Bitcoin payments are irreversible. If you send digital tokens somewhere you didn't mean to, you're out of luck unless the other party agrees to return your funds.

Twitter Scams

Fraudsters on social media have devised a new twist on an age-old con: If you send them one Ether coin, they'll send you 100 back! Sound too good to be true? It is. Still, scammers have tried to fool people's followers by making fake accounts (with real names and photos) to lure victims into thinking that they were being offered a great deal from a reputable source.

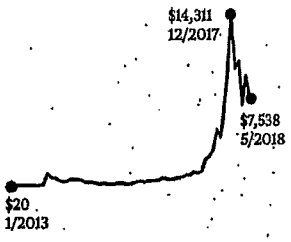
$225m
Losses from Ether-related cybercrimes through August 2017

51%
Share of those losses from phishing attacks

Lost Keys

There might be no worse self-inflicted crypto wound than buying Bitcoin low (say, in 2013) and trying to sell high (say, at the end of 2017), then realizing that you lost your private key. D'oh!

Price of Bitcoin at month's end



THROUGH JUNE 26. DATA: CHAINALYSIS, COINDESK, TECHCRUNCH, SYMANTEC, BLOOMBERG

There were more than 4,000 victims of virtual-currency-related crimes worldwide in 2017, with losses of more than $58 million, according to the FBI, up from 392 victims and less than $2 million in 2014.