

BLOCKCHAIN & BITCOIN

What Every In-House Counsel
Needs to Know

June 2018

Ethical Requirement

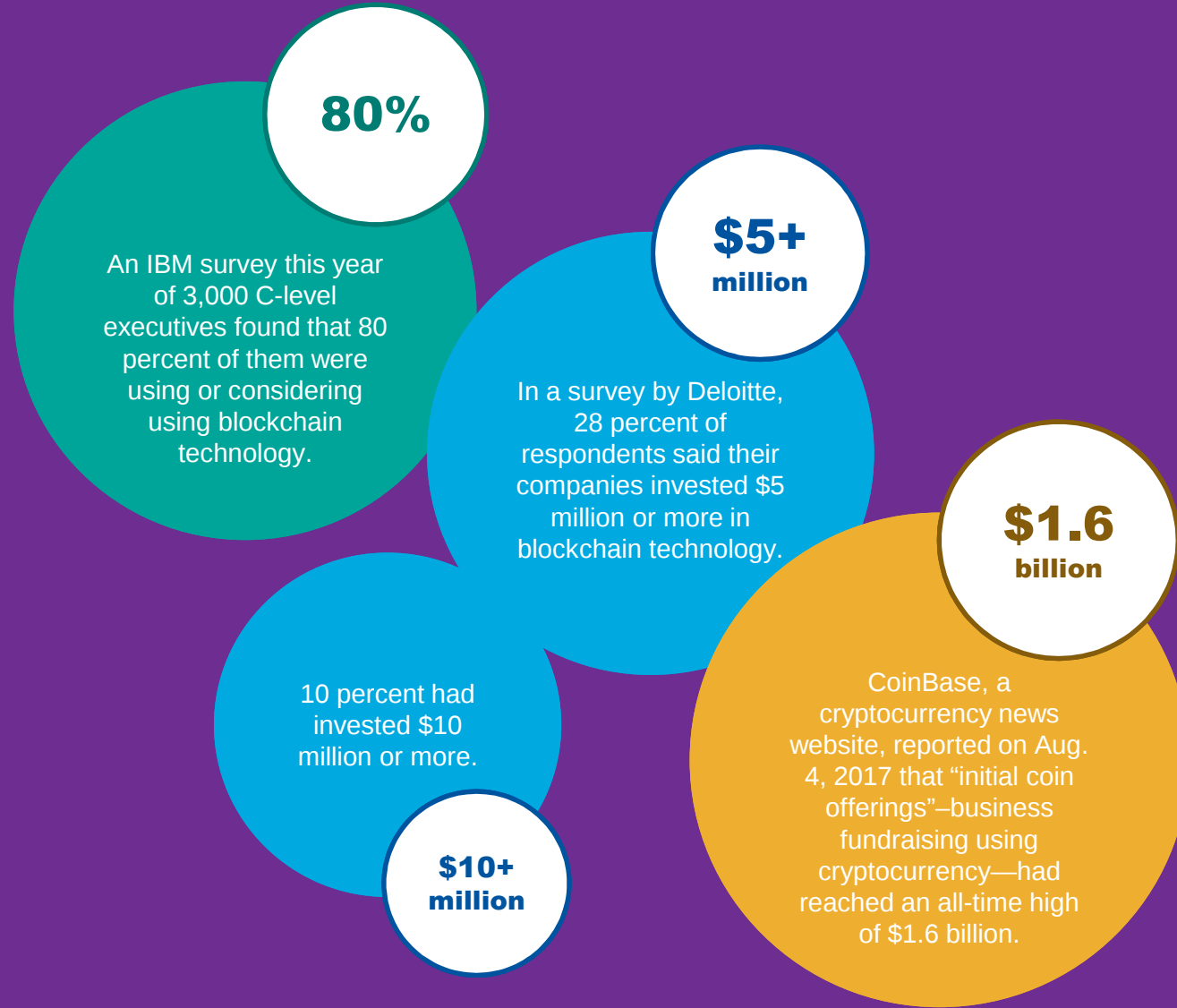
Lawyers have an ethical duty to be competent.

Comment 8 to Rule 1.1 of the Model Rules of Professional Conduct specifically refers to technological competence as part of this general duty.

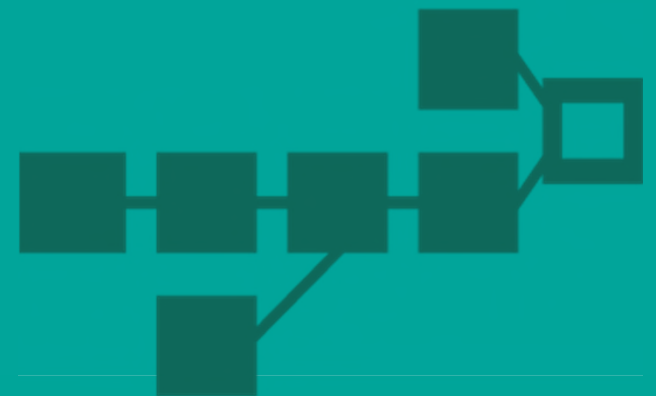
Comment 8:

“To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”

Business Duty



BLOCKCHAIN BASICS



What is Blockchain?

A shared, permissioned ledger, that cannot be altered, for recording the history of transactions

Peer-to-Peer Network that sits on top of the Internet

Like a public bulletin board, or database

Ledgers can be public, private, or hybrid; IBM, Oracle involved in creating blockchain programs for companies

Not a new concept: ledger system is the original system of accounting





Luca Pacioli, aka "Friar Luca"

Wrote first accounting treatise c. 1494
discussing ledgers

Leonardo Da Vinci
= student



We all have used the ledger system



- Blockchain technology is like your checkbook ledger on steroids - ideal for tracking lots of parties, many different items, sprawling distances.

Burglar alarm example

- A blockchain involves recording ownership of an asset and then “broadcasting” the registered owner of that asset using an anonymous key to a group of parties in a network.
- Any change in asset ownership by any member in the anonymous network is recorded and broadcast across the network, including an authorization key that verifies the legitimacy of the transfer.
- Because the entire record of transactions is recorded by many different parties across the network, a blockchain reduces the risk of fraud, and the risk of simple errors in transactions that are typically corrected through reconciliation in traditional bookkeeping.



Google Docs Example

- Think of Google Docs: one person creates a document, anyone with internet access to whom it is sent can type and add to it, and document is updated that way, with a master copy being stored and updated with Google.
- With blockchain technology, updates to such a "document" are broadcast to all nodes in the blockchain, who record the updates.
- Everyone who is part of the blockchain receives the updates and can access the ledger; no single entity like Google holds the master copy of the ledger; rather, the blockchain group collectively holds the ledger, and adds to the ledger. The ledger is decentralized.
- Upon joining the network, each connected computer receives a copy of the blockchain, which has records, and stands as proof of, every transaction ever executed. It can thus provide insight about facts like how much value belonged to a particular address at any point in the past. [Blockchain.info](https://blockchain.info) provides access to the entire Bitcoin blockchain.



Advantages

Blockchain ledgers unify multiple ledger systems so there is one accounting system that all participants share in

eliminates the need for multiple ledgers, which can lead to multiple versions of "the truth"

helps eliminate error, fraud, and inefficiencies

helps eliminate reliance on intermediaries

helps eliminate delays while multiple systems are reconciled

How is this done? Often through MINING

What is Mining?

-Mining is the process by which transactions are verified and added to the blockchain ledger (i.e. a ledger using blockchain technology), and also the means through which new cryptocurrencies, like bitcoin, are released. Anyone with access to the Internet and suitable hardware can participate in mining.

-The mining process uses a software application to compile recent transactions into "blocks" and solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both payment of the transaction fees associated with the transactions compiled in the block as well as newly released cryptocurrency, like bitcoin.



MINING

- Like gold miners expending resources to add gold to general circulation
- In the case of certain cryptocurrencies, eventually there will be nothing left to mine, because the total outstanding supply is limited
- E.g., rate of bitcoins issued declines by half every four years, and the number of bitcoins approaches but never reaches total supply of 21 million
- Incentive to mine will then be transaction fees



Examples of Blockchain Technology At Work

Tracking Diamonds from Mine to Final Customer

Problems:

- Diamond smuggling
- Fraud
- Counterfeit diamonds
- Unethically mined stones



With Blockchain technology, you can digitally:

Keep a record of
high-resolution
photos of
diamonds at every
point of its journey

Track real-time
records of every
payment
transaction

Hold certificates
of authenticity

Maintain product
details like serial
numbers, cut,
clarity, carat, color

Everledger

- Everledger, a global digital registry for diamonds, uses blockchain technology and is already tracking one million diamonds
 - Entries on the digital ledger (i.e. certificate number etc.) are inscribed by laser on the stone, creating a digital twin
 - Enables diamond suppliers, intermediaries like border agents, and purchasers to replace a paper certification process with a blockchain ledger that can track the provenance of a diamond

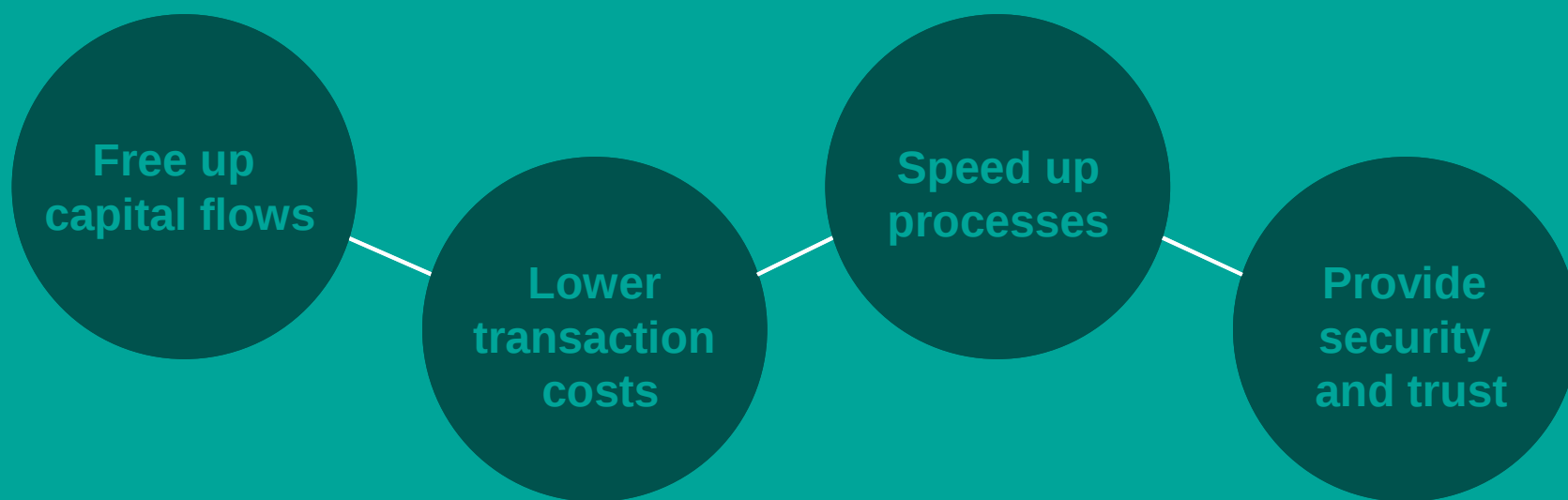


Everledger

- Everledger is adding other luxury goods to its blockchain, including wine (hidden codes are added to the bottle to see where the bottle originated and how it was distributed)
 - Useful for auction houses who have been sued for selling fake wines, i.e. allegedly belonging to Thomas Jefferson
<https://www.cbsnews.com/news/billionaire-spends-35m-to-investigate-400k-wine-fraud/>
 - Why important? Recent WSJ article explains ("Would You Know A Fake Wine If You Tasted It?"), sometimes the fake wines taste better than the real ones - fooling even the experts
 - If can't trust the experts to ferret out fakes, whom can you really trust?
 - Same technology being applied to fine art



Obvious business benefits?



Blockchain technology great for many industries:

Any industry with a supply chain



In 2016 **Walmart** partnered with IBM and Tsinghua University in Beijing to digitally track the movement of pork in China on a blockchain for transparency and food safety purposes



in 2017 **Maersk** partnered with IBM to enhance the management of shipping containers globally and facilitate payments to customs officials



Govt. of Singapore: building blockchain tool to digitally track shipments of various commodities

Blockchain is Changing the World



- **Fintech** (i.e. mobile-only stock trading apps, peer-to-peer lending sights, all-in-one money management tools), etc.
 - NASDAQ recently announced a new initiative to try and use blockchain to speed the securities clearing process.



- **Healthcare** (i.e. to track medical records, clinical trials, and prescription drug monitoring);
 - In 2016 Chronicled launched Cryptoseal, a tamper-evident seal that records the identity of its registrant and packaging metadata to the blockchain. Great for fighting counterfeit drug problem.
 - In 2017 US FDA and IBM entered into agreement to explore the use of blockchain technology to securely share patient data.



- **Intellectual property/Music industry:** PeerTracks, Bittunes, Ujo Music: companies using blockchain to register royalty payments and music and artists' intellectual property rights; tracks when songs are sold, assures correct revenue splits; allows for digital sale of music without intermediaries.



- **Real-estate (tracking title):** emerging countries that have no efficient, reliable, or corruption-free public land registry are starting them through blockchain.
 - Bitland: NGO in Ghana proposing block-chain based registry for property.



- **Government:** ideal for tracking birth and death certificates, citizenships, tax payments, voting, service-of-process, etc.

BLOCKCHAIN RISKS



Great way to fund illegal activity

- Avoids centralized banking and government repositories
- Often accept payment through cryptocurrencies like bitcoin, which can be hard to track
- Use can easily lead to other crimes: tax evasion, human trafficking, drug crimes, money laundering
- Prime target for hackers



Requires a phenomenal amount of energy

Blockchain technology is not run by any centralized entity, but by a network of users deploying algorithms that expend large amounts of computing power, and thus energy, building the "blockchain" through transactions.



Blockchain technology relies on “miners” powered by algorithms. Miners have to perform a phenomenally large number of computer calculations to track and verify transactions and solve complex puzzles. As blockchains become larger, the puzzles miners face grow more difficult, and therefore the demand for high-powered computer processing grows as well. That means more energy usage.

Blockchain technology is often slow - blockchain transactions are often far slower than credit card transactions

***problem** = most of the world gets its energy from fossil fuels (coal, natural gas, etc.) that require burning and cause pollution and environmental damage.



Hardware-hosting service for cryptocurrency miners



Legal issues abound!

- DATA PRIVACY ISSUES - HOW TO MANAGE BORDERLESS TECHNOLOGY?
- Blockchains can be comprised of blocks containing personal information from subjects resident in a multitude of jurisdictions. Which data privacy laws will apply?
 - The EU-US Privacy Shield may provide some protection for cross-border transfers of personal information from the EU to the US, but Privacy Shield is limited to EU-US data transfers and participating companies.
 - What about the EU General Data Protection Regulation (GDPR) that becomes effective in May 2018? The GDPR is a comprehensive regulation designed to protect the privacy of personal information of EU citizens for transactions taking place among (and with) EU member states.
 - Although pseudonymization of personal information is part of the GDPR requirements (something that is already implemented within BLT), the requirement that data subjects be able to request deletion of their personal information directly contradicts the immutability of information in records contained within the blockchain.
 - Failure to comply with GDPR requirements can result in hefty fines, so the answers to these questions are not only complicated, but carry significant potential risk.
 - Work around? CONSENT - Google parent Alphabet's method of choice
<https://www.wsj.com/articles/alphabets-earnings-soar-as-sales-continue-to-climb-1524514801>

Dispute resolution issues abound!

Whose law governs?

What jurisdiction are you in on a borderless, decentralized ledger?

Will want to draft user agreements to require consent to a specific jurisdiction as part of the “terms of use” for the technology. But what if such terms are not present? Even if such terms are present, will they be deemed enforceable? What about governing law and venue — what tribunal would (or should) address the dispute?

Serious thought should also be given to the type of award that may be given under any terms of use as well. For example, arbitration clauses are common in online terms of use; however, the enforceability of such clauses should be carefully evaluated when overseas transactions are involved.



* Be prepared when your CEO asks for cost reductions by applying blockchain technology and smart contracts.

“What the internet did for communications, blockchain will do for trusted transactions.”



Ginni Rometty
CEO of IBM

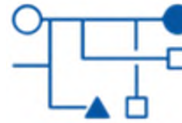
SMART CONTRACTS



Say what?



Smart contracts are computer programs that can automatically execute the terms of a contract. They are agreements whose execution is automated by software.



Programmed code allows contract to occur, i.e. monthly escrow payment will be made on the last day of the month and payment withdrawn from account.

If/then computer code triggers events

Super Bowl bet: Say you want to bet \$500 that the Packers will beat the Bears in their next match up. Step one is for you and your friend to place your bitcoin in a neutral account controlled by the smart contract. When the game is over and the smart contract is able to verify via ESPN that the Packers beat the Bears, the smart contract would automatically deposit your bet and your winnings from your friend back into your account.

Because smart contracts are computer programs, easy add more complex betting elements like odds and score differentials into the mix.

While there are services out there today that might handle this sort of transaction, they all charge a fee. The key difference with smart contracts is that they are a decentralized system accessible to anyone, don't require any intermediary party.





- **Online shopping.** Maybe you've ordered from overseas and been burned. Now you don't want to pay a merchant until you've received delivery of the item. You could set up a contract that looks for FedEx tracking data saying that the package you ordered has been delivered to your address before releasing payment.
- **Amazon:** Now using smart contracts to offer in-home and in-car delivery. Partnering with General Motors and Volvo. The system, which "includes a so-called smart lock for the door and a security camera, currently costs about \$220." Customers download the Amazon Key app with a connected car service, and a delivery driver unlocks the car through the wireless connection.





- **Mortgage payments:** although you got your mortgage through a bank, that bank won't generally hold onto it for the entire 30-year loan; it will be sold to an investor. But you keep making payments to the bank, not the investor that owns your mortgage. The bank just becomes a processor for your monthly payments, sending a chunk to the investor, a slice to taxes, and a bit for homeowner's insurance.
 - The bank will often take a quarter to a half percent per year to service that mortgage, i.e. to manage the operational headache of receiving payments and redirecting them. But a smart contract could theoretically administer this task very easily.
 - If mortgage payments were handled by smart contracts, mortgage processing fees could be eliminated and that savings passed on to consumers. The result would be lowered cost of home ownership.



Renting a vacation house: Configure locks so they are Internet-enabled and have network connections. When a bitcoin transaction is made for the rental, the smart contract automatically unlocks the house. You enter using keys stored on your smartphone.

A smart contract would also allow you to set up dates when those digital keys would automatically expire. Like Airbnb without the need for Airbnb.

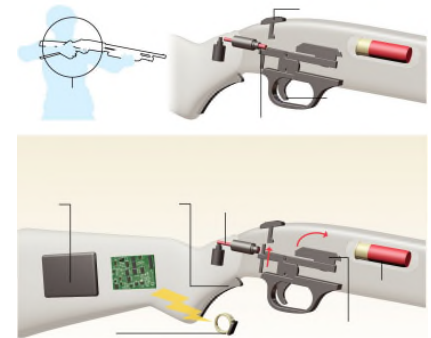
-Airbnb is desirable because it obviates the need for the host and the guest to trust each other—they both only need to trust Airbnb. If the guest doesn't pay up, or the host doesn't leave the keys, either of them can take it up with Airbnb.

Doing the same sublet with a smart contract would supplant a business model like Airbnb's. The homeowner and renter still don't need to trust each other—they just need to trust the smart contract. Smart contracts decentralize the model of who needs to be trusted. And cut out hefty fees by brokering services like Airbnb.

Could They Solve the 2nd Amendment Dilemma?

- "Smart" guns: supposed to allow only their owner to use
- "'The gun industry is not fond of [the smart gun] because it's change, and Silicon Valley isn't fond of it because it's guns,' said Jonathan Mossberg, former executive at shotgun maker O.F. Mossberg & Sons whose effort to put a smart gun into production has stalled."
- "might stop murderers like [Sandy Hook shooter] Adam Lanza who used guns purchased and stored by his mother, and to a greater degree prevent accidental shootings and suicides."

<https://www.wsj.com/articles/why-no-one-wants-to-back-the-gun-of-the-future-1523707203>



Say Goodbye To Lawyers And Banks?

In a lot of routine financial transactions, what lawyers and banks do is repetitively process mundane tasks. And yet huge fees go towards paying for lawyers to go through wills or for banks to process our mortgage payments.

Smart contracts could automate many of these processes, so that ordinary people can save time and money.



Smart contracts can also complement existing models of doing business. Imagine embedding smart contracts in physical objects. Think of a car loan: if you miss a car payment, the smart contract could automatically revoke your digital keys to operate the car.

In theory, financial institutions should be more willing to take risks on people who might not otherwise get loans. Because if someone can't pay up, easy for the bank to take back the asset.

Although the law in theory treats everyone equally, you generally need money to take someone to court over a breach of contract. Maybe no longer true with smart contracts?

Smart Contracts Raise Interesting Legal Issues

- Lawyers will always be necessary to draft appropriate smart contracts.
- Debate over whether and in what context the drafting of smart contracts constitutes computer programming, **the practice of law**, or the **unauthorized practice of law** under ABA Model Rule of Professional Conduct 5.5.
- What if no contract is drafted, just smart contract computer programming? Which forum governs the smart contract? Where is venue? How are disputes resolved? If the technology fails, are those issues governed by tort law, contract law, cybersecurity law, fraud, or all of the above?
- Can and will there be insurance coverage for smart contracts?
- How to securitize smart contracts?
- Lots of patent and IP issues surrounding smart contracts, blockchain technology

CRYPTOCURRENCES



Cryptocurrencies Offer Confidence



The circulation
of confidence
is better than
the circulation
of money.

James Madison

Virginia Convention, June 20, 1788

Cryptocurrencies

Brief History of Money

1. Physical trading of commodities and services
2. Use of certain commodities (precious metals or other valuable items) to represent and exchange value from one person to another.
3. Coins and paper money, backed by precious metals (i.e. gold, silver), made it easier to transfer value back and forth among users. Problem: money supply was limited by Mother Nature - only so much gold in the world.
4. Fiat currency, money that is not backed by precious metals—but only by the promise of the issuing government, enabling central authorities to control monetary supplies. Works well IF trust the issuing government.
5. Digitalization of currency. The world-changing creation of the blockchain ledger has eliminated the need for a central authority to back or issue currency.

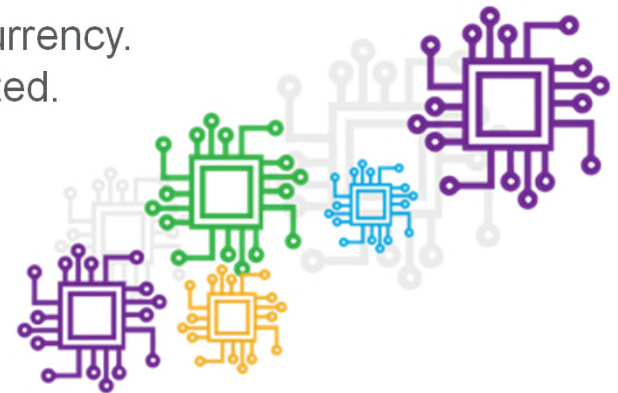
Bitcoin & Other Cryptocurrencies

What are cryptocurrencies?

A cryptocurrency is a **digital asset** designed to work as a **medium of exchange** that uses **cryptography** (computer codes) to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.

Cryptocurrencies use decentralized control as opposed to centralized **electronic money** and **central banking** systems. The decentralized control of each cryptocurrency works through a **blockchain**, which is a public transaction database, functioning as a distributed **ledger**.

Bitcoin, created in 2009, was the first **decentralized** cryptocurrency. Since then, numerous other cryptocurrencies have been created. These are frequently called altcoins (*alternative coins*).



Cryptocurrency Advantages

- Hard for most mainstream Americans to appreciate how valuable it is to eliminate need for government-back currencies
 - Our currency is backed by a stable government, is one of the leading world currencies
 - In economies where the government is unstable, or untrustworthy, ability to rely on banking system that is not tied to the government is priceless
 - Reason why China is banning bitcoin, ICOs, and other cryptocurrencies — not so much because are unsafe (the stated reason), but because investment in cryptocurrencies takes money away from People's Bank of China, government control
- Venezuela: suffering from U.S. sanctions, now offering Petro: a government-run oil-based Bitcoin-type money. Venezuela has significant oil reserves. What the country badly needs is cash in the form of dollars or other convertible currency, and Petro is the latest money-raising vehicle dreamed up by the Venezuelan government.
 - **But Americans will likely run afoul of U.S. sanctions laws if you buy!**



You, Too, Can Launch A Cryptocurrency!

- Russian farmer recently profiled in WSJ for launching his own cryptocurrency
- Saw it as best way to revive ailing economy in his small town, way to cut financial ties with Moscow and Russian banking system
- "Slowly becoming a 'tender of choice' ... for transactions from milk to tractors"
- Citizens want to pay one another for services each perform, but hampered by poverty and inability to get loans (due to high interest rates) from Russian banks
- Russia is weighing whether to embrace or ban cryptocurrencies

<https://www.wsj.com/articles/russian-farmer-alters-rural-economy-with-virtual-currency-as-moscow-watches-warily-1524398400>



Typical Cryptocurrency Marketing



<https://www.blockchain.com/>

Cryptocurrency Advantages

- Eliminates need for things like armored cars, high transportation costs
- Eliminates need for Automated Clearing House (ACH) system (electronic network of U.S. financial institutions)
- Eliminates need for money-moving services like Western Union, MoneyGram and their associated fees
- Offer "pseudonymity" - or do they? Usually have to use on exchanges, which can be subpoenaed



Over 1300 cryptocurrencies exist

Some of the most common:



Bitcoin

- largest cryptocurrency by value
- Originally described by its founder as a "peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."
- Runs on the "Blockchain" (capital "B")



Ether

- used on the blockchain Ethereum
- Aimed for use with Smart Contracts
- A consortium called the **Enterprise Ethereum Alliance**, which includes companies like Microsoft and JPMorgan and ~135 banks, is developing uses for the Ethereum blockchain.



- **Bitcoin Cash**

Bitcoin cash was created in 2017 by splitting **bitcoin through what is known as a "hard fork."** A section of the bitcoin community had forced the Blockchain (the digital ledger which records every bitcoin transaction) to **split into two separate chains for speed purposes (Bitcoin is slow).**



Ripple

- Markets itself as a cross-border payment solution for large financial institutions based on blockchain technology.
- Purports to solve the problem of high-volume/low value transactions, which are a headache for banks. The start-up has been conducting **trials with a number of financial institutions**, including **American Express** and Santander.



Litecoin

- Markets itself as very similar to bitcoin, but allegedly 4x as many coins and 4x faster.



To use Bitcoin, you have to sign up for a **Bitcoin Wallet app online** or download a Bitcoin Wallet app to your smartphone (**iOS** or **Android**).

Your **"Wallet"** acts as a **virtual bank account** of sorts that allows you to send or receive bitcoins.

You can buy bitcoins using your traditional bank account through a **Bitcoin Exchange**.

Then you can spend bitcoins by locating businesses that accept it.

Bitcoin Marketing





Bitcoin and other cryptocurrency balances are kept using public and private “keys,” which are long strings of numbers and letters linked through the mathematical encryption algorithm that was used to create them.

The public key (comparable to a bank account number) serves as the address which is published to the world and to which others may send bitcoins.

The private key (comparable to an ATM PIN) is meant to be a guarded secret, and only used to authorize Bitcoin transmissions.

Big problem

**YOU CAN'T LOSE YOUR PRIVATE KEY—
NOWHERE TO GO TO FIND IT!**

**Good News! You Are a Bitcoin Millionaire. Bad News!
You Forgot Your Password**
— Wall Street Journal Dec. 19, 2017.

Distraught investors go to extreme lengths to recover their lost cryptocurrency, including hypnosis and 'brute force' attacks with a supercomputer
<https://www.wsj.com/articles/good-news-you-are-a-bitcoin-millionaire-bad-news-you-forgot-your-password-1513701480>

"The private key is cumbersome and looks something like this:

E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262.
Protecting the private key is paramount—anyone who accesses it can transfer or spend the bitcoin, and transactions can't be reversed or stopped."



"Jason Miller, a hypnotist in Greenville, S.C., recently began offering to help people recall forgotten passwords or find misplaced storage devices. He charges one bitcoin plus 5% of the amount recovered, although he says that's negotiable."

Why should your company care?

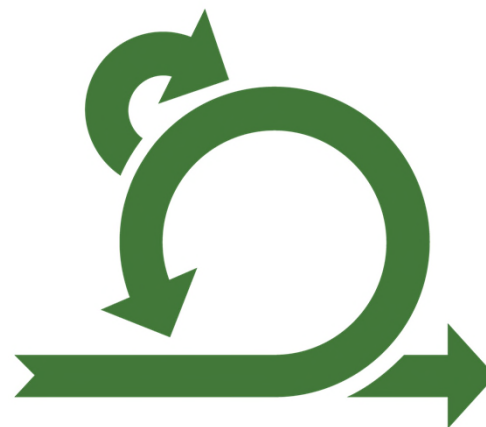
The more types of payment you accept, the more easily clients can pay you for services rendered.

The more global you are, the more valuable the cryptocurrency option is.



Bitcoin Downsides: it is Super Volatile!

- Can be super volatile: bitcoin's exchange rate against the U.S. dollar has frequently jumped or crashed over 20% (sometimes nearly 50%) in a single day
- By contrast, U.S. dollar-to-Euro exchange rate generally has not changed more than 2.5% in one day
- Such instability = not desirable in a currency, because holder's purchasing power can increase or decrease drastically and suddenly



And the regulators are watching!



SEC and CFTC: assuming joint regulatory oversight of virtual currencies

*Virtual currencies = commodities  CFTC oversight

CFTC regulates things like futures sales of virtual currencies, but also "spot" commodities transactions involving fraud/manipulation

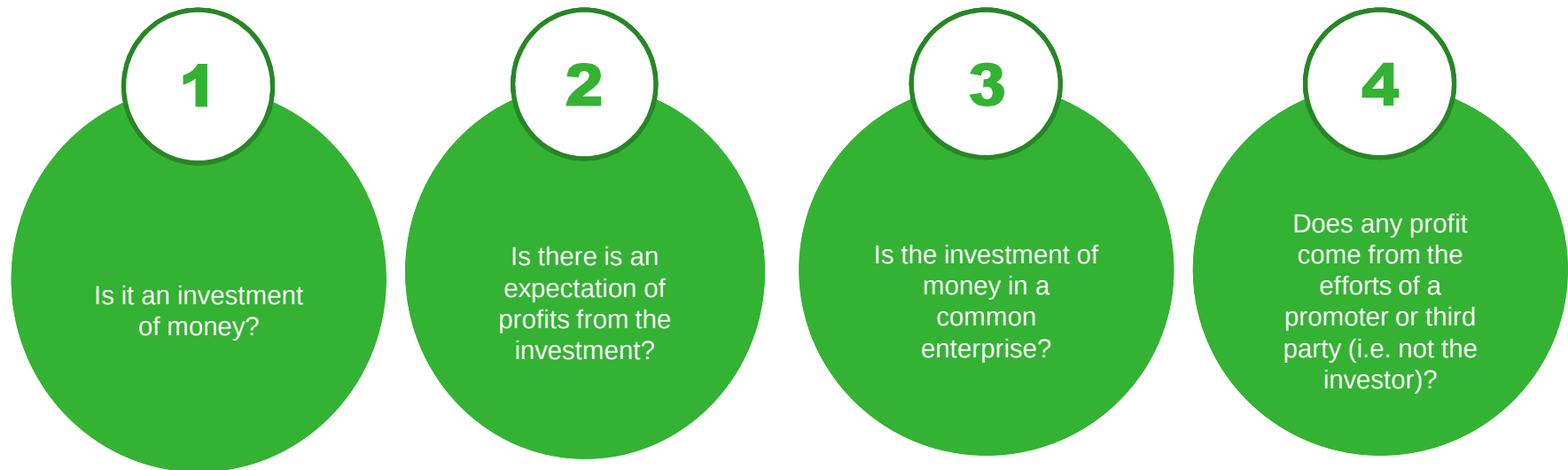
*SEC does not have direct oversight of transactions in currencies or commodities. BUT SEC does have oversight of cryptocurrencies that have the characteristics of securities, i.e. things like token offerings (i.e. initial coin offerings, or ICOs), where companies sell tokens or coins, like shares, during capital raises

- These ICOs are cryptocurrencies, like bitcoin, but more akin to company stock because are developed by an organization and issue primarily for capital formation and secondary trading

SEC & CFTC have established virtual currency task forces



SEC: The *Howey* test remains the appropriate standard for determining whether a particular token involves an investment contract:



"A rose by any other name would smell as sweet":
can't maneuver around SEC by offering "tokens" or "coins" rather than "shares"

Possible exception being lobbied for: if coins offer goods/services, similar to gift cards; i.e. if coins have a purely consumer use



In joint WSJ Op-Ed piece, Jay Clayton and J. Christopher Giancarlo likened interest in virtual currencies to interest in dot-com investing in 1990s - some people got really rich, lots of people lost a lot of money

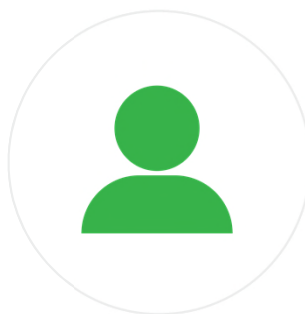
Issue of who else regulates?



"A key issue before market regulators is whether our historical approach to the regulation of currency transactions is appropriate for the cryptocurrency markets. Check-cashing and money-transmission services that operate in the U.S. are primarily regulated by states. Many of the internet-based cryptocurrency-trading platforms have registered as payment services and are not subject to direct oversight by the SEC or the CFTC. We would support policy efforts to revisit these frameworks and ensure they are effective and efficient for the digital era."

Generally need a state license to operate a money transmitting business, and can be federal felony to fail to get such a license

[Obopay/Payza](#) article



"MH Pillars, Ltd., doing business as Payza, has been indicted by a federal grand jury in the District of Columbia on charges alleging they operated an Internet-based unlicensed money service business that processed more than \$250 million in transactions."

FinCEN

- "In some areas, federal authority to police cryptocurrencies is clear. The Bank Secrecy Act and its implementing regulations establish federal anti-money-laundering obligations that apply to most people engaged in the business of accepting and transmitting, selling or storing cryptocurrencies."
- Under Bank Secrecy Act, banks & other financial institutions are subject to various registration and recordkeeping requirements.
- E.g., all "**money service businesses**" are required to register with the Dept. of the Treasury and **develop anti-money-laundering and customer identification programs ("KYC")**
 - These rules cover certain participants who transact in "convertible virtual currencies"
 - "Exchangers" and "administrators" are likely subject to regulation
 - "Exchangers" = persons/business that exchange virtual currency for real currency or other virtual currency
 - "Administrators" = persons/business engaged in putting into circulation a virtual currency who also have the authority to redeem virtual currency from circulation



FinCEN

- Any blockchain transaction is likely a virtual-currency transaction, but [end-users, such as merchants or consumers, are likely exempted](#); miners also likely exempted
- But businesses involved in creating and exchanging virtual currencies better be careful
- 2015 FinCEN enforcement action against Ripple for not having proper AML program in place



Other Regulators

- **IRS:** Virtual currencies are treated as property and income for federal tax purposes
 - <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>
 - Will be taxed for successfully "mining" and then receiving virtual currency
- **States:** Some states are aggressively regulating cryptocurrency businesses (California, New York, Texas). But some are trying to lure cryptocurrency businesses by offering little to no state regulation of certain cryptocurrencies
 - Wyoming: passed the Utility Token bill, which was designed to exempt specific cryptocurrencies from state money transmission laws and is the first of its kind to legally define the way in which specific types of crypto tokens are treated by regulatory bodies.



WHO'S IN CHARGE?

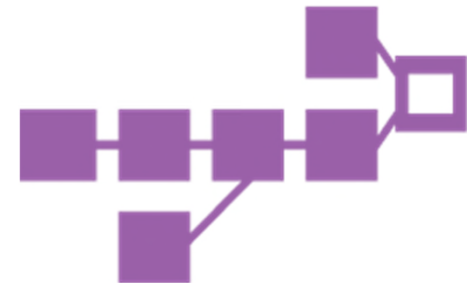


Who is in Charge??

- Public blockchains like to tout themselves as decentralized, autonomous organizations
- But they were also created by somebody! Who?

*The core developers (who write, evaluate, and modify software code) and the powerful miners (holders of significant chunks of computing power within the network)

- Interesting legal issues arise: are those people fiduciaries? If so, what are their duties?
 - Duty of Care (to act with competence)?
 - Duty of Loyalty (to act in the interests of those they serve rather than their own interest)?
 - Duty of Good Faith?
 - No duties at all?



Default position in tort law is that it is very difficult to hold software developers liable for the harms their software wreaks

- Software licenses - the terms on which people use software - generally **disclaim all liability for problems the software causes**
- One argument: if hold coders liable, won't feel free to create cutting-edge projects, **liability will inhibit innovation**
- Counter-argument: If think you are accountable, will slow down and act more carefully, get malpractice insurance, will evaluate whether you have the right expertise for the job or need to get some help
- Blockchain technology jumped into the big leagues when attempted to replace existing monetary, financial, property, contracting, and identity systems - **should they be held accountable for hacks, cybersecurity breaches, and other problems?**



WSJ: **More than 10%** of ICO (initial coin offering) proceeds have been lost to hackers and cyberattacks

Hack of the DAO (Decentralized Autonomous Organization) in June 2016

DAO - Decentralized investment fund; idea was that anyone who invested would have a say in where investments were placed; the more invested the more say

Built on the blockchain Ethereum, functioned through smart contracts

Fund was hacked in 2016, \$50 million in ether stolen

- Some think hacker can never spend stolen funds, as each unit is traceable
- Like stealing the Mona Lisa



- Hack was reversed through a "hard fork," because waiting period before funds could be removed; funds were returned to those who wanted them returned
- Very controversial move: DAO purists were against return of investments because meant someone was in charge

***Shows someone is running these blockchains - the developers, coders, and miners**

Thank you

大成 DENTONS



Rachel M. Cannon
Dentons US LLP
233 South Wacker Drive
Suite 5900
Chicago, IL 60606-6404
United States

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com.