BRAVE NEW LAW FIRM – BITCOIN, CRYPTOCURRENCIES AND BLOCKCHAIN

April 17, 2019

"FRIENDLY" (BUT REAL) DISCLAIMER

NOTHING IN THIS PRESENTATION CONSTITUTES LEGAL ADVICE. THIS IS A GENERAL CONCEPTUAL AND THEORETICAL HIGH-LEVEL OVERVIEW OF CRYPTOCURRENCY, BITCOIN, ETHEREUM, BLOCKCHAIN, INITIAL COIN OFFERINGS (ICO'S), TOKENS, THE U.S. SECURITIES LAWS, SOME OF THE REGISTRATION EXEMPTIONS WHICH MIGHT BE AVAILABLE, AND RELATED TOPICS. NOTHING HEREIN IS INTENDED OR RELATED TO ANY PARTICULAR FACTUAL SITUATION. NOTHING HEREIN FORMS AN ATTORNEY-CLIENT RELATIONSHIP. YOU ARE ADVISED TO CONSULT WITH YOUR OWN LAWYER, ACCOUNTANT AND OTHER PROFESSIONALS BEFORE MAKING ANY DECISIONS.
ABOUT ME AND THIS TALK

• I AM GORDON EINSTEIN, FOUNDER AND PARTNER OF CRYPTO LAW PARTNERS.

• I AM A US/CA (CALIFORNIA) ATTORNEY WHO SPECIALIZES IN BLOCKCHAIN AND CRYPTO LAW.

• I SPEAK IN FAST, TECHNICAL, LEGAL, “NERDY” ENGLISH. RAISE YOUR HAND IF YOU WANT ME TO DIVE INTO OR REPEAL SOMETHING.

• HAPPY TO SHARE THIS PRESENTATION. EMAIL ME AT G.EINSTEIN@CRYPTOLAWPARTNERS.COM, OR HIT ME UP ON LINKEDIN OR FACEBOOK.

• CAN DISCUSS IN MORE DETAIL AT EVENT. IF YOU SEE ME, COME UP AND SAY HELLO.

---

Forbes

How To Run A Successful Security Token Offering In Compliance With New SEC Guidance

With the help of Gordon Einstein, a US securities lawyer, chief legal officer of Distributed Labs, and advisor to over 20 Blockchain companies, I’ve compiled the most popular examples of what constitutes a compliant security token offering. Note that you should consult a lawyer for more precise legal information, and should consider this follow as general guidance.

---

Me - before
Keto diet 😄

Me - after
Keto diet 😄
ON APRIL 17, 2019, IS “CRYPTO” (STILL) A THING? IS IT A BUBBLE? DO WE CARE?

Questions for the room:

• Who thinks crypto represents a valid and significant development?
• Who thinks crypto is a scam or a bubble?
• Who has owned or owns any crypto?
• Whose law firm has advised or had meetings or interviews with any crypto or blockchain clients or prospective clients?
• Whose law firm has opened a crypto or blockchain practice group?

YES WE CARE! CRYPTO IS THE FUTURE OF LAW.

• Every crypto/blockchain startup is a startup. They all need startup legal work.
• This area is extremely international, so law firms with a global perspective have an advantage.
• “Smart Contract Attorney” is the specialization of the future.
• Tax planning plays a huge role in crypto.
• Securities regulation is at the start of a global revolution.
• Every large financial institution if getting involved in crypto, blockchain and FinTech.
• Every crypto/blockchain project involves complex intellectual property issues.
• “Legacy enterprises”, especially those with heavy regulatory compliance obligations and/or complex logistics are embracing blockchain.
• Cryptocurrency ventures need help with AML/KYC and general financial services compliance.
The “Crypto-Winter” was brutal. Killed many crypto projects.

Is it over, or is winter (still) coming?

From Coinbase.com - April 17, 2019

“Crypto-Spring”?

On April 1st (!!!) market sentiment suddenly shifted.

And, crypto projects are springing back to life.

Can we trust this? YES.
CURRENT CRYPTO MARKET CAP VS COUNTRY 2019
NOMINAL GDP (4-17-19)

Top 100 Cryptocurrencies by Market Capitalization

<table>
<thead>
<tr>
<th>Name</th>
<th>Price</th>
<th>Volume (24h)</th>
<th>Circulating Supply</th>
<th>Change (24h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>$10,715,984,799.99</td>
<td>$72,637,842,237.99</td>
<td>18,416,917 BTC</td>
<td>0.02%</td>
</tr>
</tbody>
</table>

NOSTALGIA TIME - CRYPTO MARKET CAP VS COUNTRY 2017 NOMINAL GDP AT BTC'S $17,132.11 HIGH (12-12-17)

Country: Poland
Market Cap: $482,005,992,262
Price: 482.920
Volume: 0619
Rank: 24

Country: Singapore
Market Cap: $290,484,830,665
Price: 291.860
Volume: 0.374
Rank: 41
THE EVOLUTION OF MONEY - BARTER

“Barter” is the direct exchange of goods (or services) without the use of money or a common “medium of exchange”. Aka, a “commodity exchange economy”.

Issues with barter:

• Lack of “double coincidence of wants”.
• Lack of common measure of value.
• Lack of standard of deferred payment.
• Difficulty in storing wealth.
• Indivisibility of goods. (how do you make change from a cow?)
**THE EVOLUTION OF MONEY – COMMODITY MONEY**

“Commodity Money” is a type of useful good which also functions as money – meaning a common “medium of exchange”. Beyond their “intrinsic value”, these goods had/have a generally accepted exchange value.

Commodity money goods also tend to be durable, portable and storable. Examples are beaver pelts, seashells, alcohol and cigarettes.

Better than barter, but still issues:

- Very much depend on historical context and culture.
- Not always fungible (are all cigarettes the same?).
- Indivisibility of goods. (how do you make change from a beaver pelt?)

**THE EVOLUTION OF MONEY – METAL MONEY**

“Metal Money” is a variant of commodity money where a precious metal (usually gold) is the common medium of exchange. One can argue that gold has less “intrinsic value” than other commodity money types - therefore it is more natural to view gold in light of its generally accepted exchange value. In a way, gold is a world-wide agreed-upon representation of wealth, not actual wealth.

Gold is actually a pretty good form of money, and very anti-inflationary, but it is not perfect.

Better than commodity money, but still issues:

- Hard to move. Hard to secure. Hard to trace.
- Supply of gold may not keep up with size of economy.
- “Gold as money” favors countries that mine gold.
THE EVOLUTION OF MONEY – THE GOLD STANDARD

The “Gold Standard” is where a government issues paper certificates (“bills”) which represent an amount of (usually) gold held by the government in its reserves. This gold is redeemable by the holder of the paper bills upon demand.

Consider - the paper bills are tokens whose only function is to represent or reference the truly valuable asset - gold. They have no intrinsic value. Paper bills are light, easy to divide (make change), traceable, etc.

Better than metal money, but still issues:

- Counterfeiting. And, who has the legal right to issue paper money?
- Relies on belief that government will honor its redemption commitment.
- Economy still limited by supply of gold. No Keynesian stimulus.

THE EVOLUTION OF MONEY – FIAT MONEY

“Fiat Money” is currency that a government has declared to be “legal tender”, but which is not backed by a physical commodity. When the US went off the gold standard in 1971, the US dollar became a fiat currency. “Fiat” means “it shall be”.

The US dollar was “pseudo gold” for a long time because of its international reserve status, the pricing of oil in dollars, and because the US economy produced the goods and services the world wanted.

With fiat, a government may engage in Keynesian stimulus as needed.

Every country in the world now issues fiat currency.

- But Russia and China are still buying gold… why?
- And the world still prices oil in US Dollars… why?
- And the US still has low inflation… why?
"PROBLEMS" WITH FIAT MONEY

- **INFLATION INEXORABLY DECLARES THE VALUE OF FIAT.** This is NOT the case in other money systems.
- There is **NOT** a single international currency, which often creates the necessity of exchanging fiat.
- **Converting** between different fiat currencies is **expensive.** And, currencies experience volatility vis-à-vis each other.
- Transmitting and spending fiat is **expensive** (wire fees, credit card fees, ATM fees, etc.)
- The banking system is **NOT** a reliable holder of fiat deposits. See..., Greece, Venezuela, Cyprus, etc.
- Fiat, especially in the banking system, is **NOT** private and leaves trails which can be followed by governments and others.
- Governments can impose **capital controls** on the movement of fiat.

DECLINE IN US DOLLAR PURCHASING POWER - THANKS (FOR NOTHING) FEDERAL RESERVE!

- **1913:** Federal Reserve is created
- **1923:** Fed's executive order makes it illegal to hold gold coins, bullion or certificates
- **1943:** Bretton Woods established USD as the world's reserve currency
- **1953:** Nixon closes "gold window", end of Bretton Woods, beginning of the modern day fiat currency system

Source: U.S. Bureau of Labor Statistics
(RE-)DESIGNING MONEY


### IDEAL (CRYPTO)CURRENCY DESIGN – PART 1

If you could DESIGN a new currency from scratch, what CHARACTERISTICS would you want it to have or not have?

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Legacy Currency/Money</th>
<th>Ideal (Crypto) Currency/Money</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliable store of value</td>
<td>Value constantly eroded due to inflation and politics.</td>
<td>Value either remains static or changes in predictable manner. Possible deflation.</td>
</tr>
<tr>
<td>Manner of creation</td>
<td>By government or central bank decree (fiat).</td>
<td>By action of reliable and known algorithm.</td>
</tr>
<tr>
<td>Form</td>
<td>Depending on circumstances, can be tangible like cash, coins or checks, or intangible electronic records.</td>
<td>Always represented by intangible electronic records. No physical cash.</td>
</tr>
<tr>
<td>Counterfeiting</td>
<td>Vulnerable to counterfeiting, including fake checks and credit cards.</td>
<td>Counterfeiting possible, but so cost-prohibitive that not issue.</td>
</tr>
</tbody>
</table>
If you could design a new currency from scratch, what characteristics would you want it to have or not have?

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Legacy Currency/Money</th>
<th>Ideal (Crypto) Currency/Money</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope of acceptance</td>
<td>Depend on location and agreement. Exchanges needed.</td>
<td>Currency accepted globally. No exchanges needed.</td>
</tr>
<tr>
<td>Parties to transfer</td>
<td>Either in person if cash, or through intermediary such as bank or credit card company/PayPal if electronic. Often delayed. Often reversible. Often expensive.</td>
<td>Nearly immediate transfers of value directly between parties over the Internet. Can be made irreversible. Little or no transaction fees.</td>
</tr>
<tr>
<td>Privacy (anonymity) and security</td>
<td>Cash is somewhat private, but not secure. Banked funds are subject to AML/KYC, tracing, and to government or court seizure.</td>
<td>Privacy and security determined and enforced by protocol, not by law or government action. NOTE, this does create new issues and vulnerabilities.</td>
</tr>
</tbody>
</table>

**BITCOIN** (BTC) was the first "cryptocurrency" which (mostly) successfully implemented these characteristics. It was created in direct response to the events leading up to 2008’s great recession.

Thus, on October 31, 2008, a paper written by a person or group named "Satoshi Nakamoto" released a white paper called "Bitcoin: A Peer-to-Peer Electronic Cash System."
**BITCOIN DESIGN OVERVIEW – PART 1**

**BITCOIN** (BTC) was the **FIRST** "crypto" or other non-flat currency to (mostly) resolve these design issues.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Bitcoin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliable store of value</td>
<td>Only 21 million BTC will ever be created. They are released on set schedule, in ever decreasing amounts. Bitcoin network is globally decentralized and distributed, with no one party in charge, so very difficult to shut down or corrupt. Inflation thus very unlikely.</td>
</tr>
<tr>
<td>Manner of creation</td>
<td>BTC is “mined” by competing parties at an algorithmically determined rate which continuously self-adjusts.</td>
</tr>
<tr>
<td>Form</td>
<td>BTC exists ONLY in digital and intangible form. Bitcoin is actually not a “coin” but rather a series of entries in a distributed ledger (explained soon). There are no BTC bills, coins, checks, etc.</td>
</tr>
<tr>
<td>Counterfeiting</td>
<td>Reliable cryptography makes BTC highly counterfeite-resistant. Attempts to “double spend” BTC fail because attempt is more expensive than any realistic gain.</td>
</tr>
</tbody>
</table>

---

**BITCOIN DESIGN OVERVIEW – PART 2**

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Bitcoin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope of acceptance</td>
<td>The Bitcoin network is global. Anyone with a software wallet and an Internet connection can accept BTC and transfer it to others. The assignment of value to BTC is based on collective consensus. Acceptance among mainstream merchants is small but increasing quickly. Government attitudes vary, but all are concerned about tax evasion, money laundering and terrorist financing.</td>
</tr>
<tr>
<td>Parties to transfer</td>
<td>The Bitcoin network is completely peer to peer, without any financial intermediaries such as banks or payment processors. Initial transfers take 10 minutes, subject to additional confirmation times. Network transfer fees are low, but are not yet trivial. Transfers are irreversible.</td>
</tr>
<tr>
<td>Privacy (anonymity) and security</td>
<td>BTC does a DECENT job of maintaining user privacy and anonymity. However, transfers are permanently recorded in a distributed ledger, unlike regular cash payments. Individuals face security vulnerabilities related to wallets, personal keys and custodians of their crypto.</td>
</tr>
</tbody>
</table>
THE BLOCKCHAIN – PART 1

- All BTC transactions since the start of the Bitcoin network are stored in the Bitcoin "blockchain".

- Each block in the blockchain is like the page in a ledger. The very first block in the Bitcoin blockchain is referred to as the "Genesis Block".

- As Bitcoin transactions occur, their details are entered into a "candidate" block, one after the other.

- Once a candidate block becomes full, "miners" compete to "validate" all of the transactions in that block by solving a difficult math problem uniquely-related to the content of that block.
The “Blockchain” – Part 2

- The first successful miner broadcasts its result to the other network nodes. As each node finds the solution to be true, it will add the candidate block to the blockchain as a “committed” block. “Bad” solutions are discarded.

- In addition to containing recent Bitcoin transactions, the newly committed block will contain a Bitcoin reward for the successful “miner”. In this way, miners are “paid” for validating transactions with newly issued Bitcoin, which Bitcoin can then be spent or sold by the miner.

- Each node on the Bitcoin network can keep a complete copy of the blockchain, so there is no single point of failure and every single transaction from the Genesis block forward can be independently validated. In fact, the blockchain is a true “distributed ledger”.

- No node need trust any other node. All nodes which receive a candidate block solution from a miner will verify that solution before adding the candidate block to its copy of the blockchain.

- If nodes have conflicting versions of the blockchain because different (valid) candidate blocks reached them first, the network has rules in place for resolving this and achieving “consensus”.

- No (vulnerable or malicious) central authority or service issues new Bitcoin. Rather, the issuance of new BTC results from thousands of independent miners operating globally. This distributed and decentralized network topography is thus very hard to attack or compromise.

- The rate of issuance of new BTC is self-adjusting. The network is programmed to automatically increase or decrease the difficulty of the candidate block math problem based upon how quickly the last several blocks were added to the blockchain. No inflation!
ALICE & BOB – PLAYING NICE ON THE BLOCKCHAIN

How the Bitcoin Blockchain Works

Alice wants to send digital currency to Bob. The transaction is represented online as a “block.” The block is broadcast to every mining node in the network. The money moves from Alice to Bob.

Miners in the network approve the transaction if it is valid. Mathematical proof is required. The block can then be added to the chain, which provides an indelible and transparent record of transactions.

BEYOND BITCOIN - SMART CONTRACTS AND DISTRIBUTED AUTONOMOUS ORGANIZATIONS

Traditional Top Down Organizations

- CEO
- Board
- Management

Distributive Autonomous Organizations

- Stakeholders
- No centralized legal entity
- No employment contracts
- Machine consensus blockchain governance and token contracts

Employment contracts are decentralized and managed through smart contracts. Top-down management is replaced by distributed ownership and control, eliminating the need for traditional hierarchy.

Digitize the LandDeed:

Sell

Buy

Digitalize the LandDeed

Clearing and settlement is automated. Ownership is undisputed.
**Beyond Bitcoin – The Question**

- BTC is great for irreversible one-way transfers of value across the globe. **BUT**, is it **NOT** great for multi-step or contingent transactions over time.

- For example, Bitcoin cannot handle an escrow, and two-way transfer of value (like a sale), the payment of interest, etc. And, you certainly **can't** run an automated business on Bitcoin.

- We need a system that has all the good features of Bitcoin, but which is also "contract aware".

---

**Beyond Bitcoin – The Answer (Ethereum, etc.)**

- The first real answer was "Ethereum", the brainchild of Vitalik Buterin. Ethereum can be referred to as the first "world computer". It is made up of a network of nodes all running Ethereum code in something called the “Ethereum virtual machine” (or, “Ethereum VM”).

- There is no central “Ethereum command” running these Ethereum VMs – the network is entirely **decentralized** and **distributed**. Each node has its own copy of the Ethereum blockchain and resolves network conflicts and achieves **consensus** with other nodes in a like manner to Bitcoin.

- So what can you **DO** with Ethereum? It is "Turing Complete" – so – Anything? Everything?
What if you could write a "contract" in code, publish it to the Ethereum blockchain, and have confidence that the Ethereum network and Ethereum VMs would execute this contract exactly as written (coded), without needing a judge to enforce it, without any global jurisdiction issues, and without the possibility of censorship or revision?

Such contracts are "smart contracts". You can publish a smart contract to an address on the Ethereum blockchain. Once written to that address, it will never change (so be careful).

If you send the desired inputs (arguments) to a smart contract’s address, and you or someone else pay the “Ether” (ETH) required to “power” this smart contract, it will run exactly as written.

A smart contract can also be programmed to check in with an external online data source—referred to as an "oracle"—when executing. For example, it can query an one oracle for the Federal Reserve benchmark interest rate, and query another oracle for the current temperature in Odessa, Ukraine.

HUGE OPPORTUNITY FOR A NEW BREED OF "SMART CONTRACT ATTORNEYS".

Ethereum allows more than simply smart contract execution. Because smart contracts are extremely flexible, and can be combined for effect, you can run entirely new business models, projects, and autonomous organizations off of Ethereum. And, many startups are doing this.

Recall that you power smart contracts with ETH, which is a form of cryptographic token for use on the Ethereum network. If you set up a new business or project on Ethereum, you may want to issue your own variant of token as “currency”, specifically designed to be used in your project.

In fact, you might want to SELL these “currency” tokens in advance of your project coming online in order to fund the building of the project. Then, once the project is built with the raised funds, the holders of the tokens will be able to use them to access the project, thus completing the circle.

From a process perspective, you set up a smart contract at a certain address. That smart contract provides that, for each unit of BTC, ETH or cryptocurrency sent to it, it will automatically return a certain number of your new tokens to the sender’s address.
A NEW SECURITIES WORLD - RAISING CAPITAL GLOBALLY WITH ICOs AND STOs

The London Stock Exchange Conducts World’s First Security Token Offering (STO) on the Blockchain

GOODBYE VENTURE CAPITAL. HELLO ICO/STO?

- INITIAL COIN OFFERINGS (ICOs) ARE BEING MERGED INTO COIN OFFERINGS RAISED TO FUND TECHNOLOGY STARTUPS
- ICO RAISING HAS TURNED INTO A BIG BUSINESS: IT MAY REPLACE THE TRADITIONAL INVESTMENT ROUTINE WHERE VCs fund startups with SEED CAPITAL

HOW ETHEREUM BECAME THE PLATFORM OF CHOICE FOR ICO’d DIGITAL ASSETS

At $200 million, Tezos ICO is already the biggest ever, and it's still going strong

$150 Million: Tim Draper-Backed Bancor Completes Largest Ever ICO

Chat app Kik to raise $125M through an ICO in September

$200 Million In 60 Minutes: Filecoin ICO Rockets to Record Amid Tech Issues

Altoin EOS joins Top Crypto League, Surges 321 Percent After ICO Launch

Blockchain Platform WAVES Finishes ICO, Raises Over $16,000,000 USD in Bitcoin
There are serious legal issues relating to ICOs including consideration of whether (i) the tokens being issued are securities, (ii) if they are securities at least until the project is useable, or (iii) if they are, and will always be, “utility” tokens.

The famous SEC vs. Howey (1946) case has enjoyed a renaissance. Every blockchain startup the world over is wrestling with the Howey Test when attempting to determine if its token sale needs to be registered with the SEC, or a registration exemption identified and complied with.

If tokens are NOT securities under Howey, then what are they? Answer – probably goods, products or services, meaning that FTC might have jurisdiction even if the SEC does not. Furthermore, the sale of such tokens probably constitutes a taxable event for the issuer.

ICOs are amazingly complicated from a legal perspective. Unlike regular small business sales of securities or products, they immediately reach a global audience. And, their operations usually extend across borders and jurisdictions. Finally, often no one knows if the promised project or business will actually be built, much less be successful.

BUT, among these ICOs is the next Apple, Amazon, Google, Microsoft, Baidu, Weibo, etc.

**INITIAL COIN OFFERINGS – BRAVE NEW LAW**

- Startup has great idea, needs funding.
- Startup decides to “issue” tokens to raise funds.
- Are tokens sold into U.S.?
- Are tokens “securities”?
- “Issuing” means original sale by startup to first purchasers, NOT trading on secondary (exchange) market, and NOT mining.
- Under the “Howey Test”, *** Need SEC “registration” or “exemption”. ***
- Really it is “sold” and/or “offered for sale” into U.S. market.
- Don’t panic! ☺

Top Level Approach

- No need for SEC “registration” or “exemption”.
- No “problems” – but smaller token sale. 😊
- BUT... watch out for tax (etc.) issues, because now selling non-security product or service.

*** Need SEC “registration” or “exemption”. ***
Blockchain Startup Tezos Faces Class Action Over $232M ICO

SAN FRANCISCO: Blockchain startup Tezos has been hit with a potentially groundbreaking class action lawsuit alleging it broke federal law by conducting a $232 million initial coin offering (ICO) over the summer in violation of U.S. securities laws and rules.

SAN FRANCISCO: Blockchain startup Tezos has faced a class-action lawsuit alleging it broke federal law by conducting a $232 million initial coin offering (ICO) over the summer in violation of U.S. securities laws and rules.

Two ICO Issuers Settle SEC Registration Charges. Agree to Register Tokens as Securities


Spotlight on Initial Coin Offerings (ICOs)