8-27-2018

Taxing & Zapping Marijuana: Blockchain Compliance in the Trump Administration Part 3

Richard Thompson Ainsworth

Brendan Magauran

BU School of Law

TAXING & ZAPPING MARIJUANA: BLOCKCHAIN COMPLIANCE IN THE TRUMP ADMINISTRATION
Part 3

Boston University School of Law
Law & Economics Paper No. 18-03

Revised August 27, 2018

Richard T. Ainsworth
Boston University School of Law

Brendan Magauran

Electronic copy available at: https://ssrn.com/abstract=3239977

TAXING & ZAPPING MARIJUANA:
BLOCKCHAIN COMPLIANCE IN THE TRUMP ADMINISTRATION
Part 3

Richard T. Ainsworth
Brendan Magauran

This is the third of a five-part series dealing with the rescission by U.S. Attorney General Jeff Sessions of the Obama-era policy that discouraged federal prosecutors from bringing charges in all but the most serious marijuana cases. The federal laws at issue are the Controlled Substances Act (CSA) and the Bank Secrecy Act (BSA). Twenty-eight states and the District of Columbia have laws that conflict with the CSA and BSA because of their legalization of marijuana.

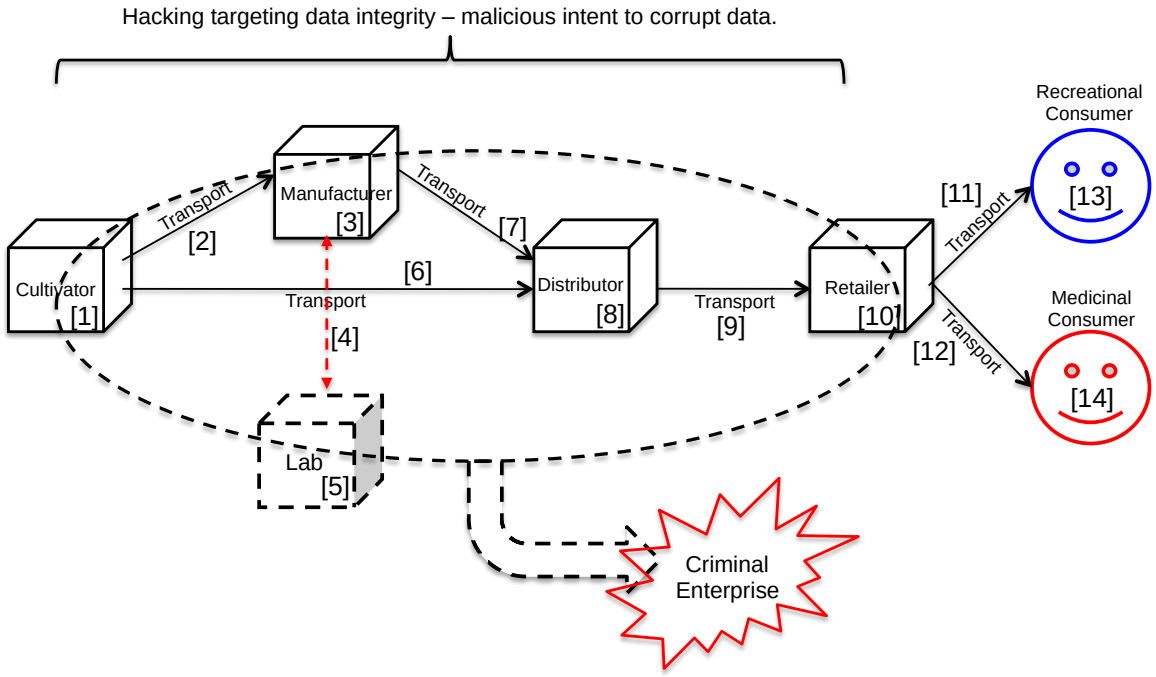
There are four basic fraud vectors through which criminal organizations may exploit the standard marijuana supply chain. Figure 1 (also discussed in parts 1 and 2 of this series) shows the 14 leakage points and four major fraud vectors in the standard METRC-protected marijuana supply chain. This article focuses on cyber-attacks on the main commercial chain – producing leaks at points 2 through 12.

Cyber-attack on the main commercial chain – leakage points [2] - [12]

This fraud is a direct, criminal attack; an attack designed to destroy/corrupt records of marijuana inventory and plant tags throughout the supply chain. The attack allows legalized marijuana to escape the system and be sold on the black market. A large scale cyber-attack impacts every commercial enterprise, transporter, and testing laboratory. See Figure 1 (below). If successful, a malicious cyber-attack would open up each "leakage point," [2] through [12] in the main commercial chain. Control collapses.

Electronic copy available at: https://ssrn.com/abstract=3239977

Figure 1:
Cyber Attack Frauds in METRC-protected Marijuana Supply Chains



All *track and trace* systems are designed around a centralized ledger.[1] They endeavor to be permanent (immutable).[2] Most are hosted, cloud-based, near-real-time systems that record marijuana inventory movements. The collected data is held on multiple vulnerable (or hackable) servers, and similarly vulnerable (hackable) State servers.

Hacking a major *track and trace* system is not merely a theoretical possibility. It happened to the largest (and oldest) system. Hackers took down MJ Freeway's Leaf Data System nationwide.[3] The seriousness of this hack was all too apparent to the government of Nevada which notified MJ Freeway on September 12, 2017 that, because of vulnerabilities in its

[1] Centralized ledgers are highly vulnerable to fraud, data corruption, and malicious attacks. Blockchain technology replaces centralized ledgers. Blockchain is a robust, secure, transparent *distributive* ledger that survives malicious attacks. Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, (March 12, 2015) *available at*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

[2] Data entered into METRC cannot be changed, although errors can be corrected. Patrick McCleary, *MTRC is Coming! Learning the Basics of METRC Compliance, Part II*, FLOWHUB (November 7, 2017) *available at*: https://flowhub.co/2017/11/07/metrc-coming-learning-basics-metrc-compliance-part-ii/

[3] Alex Halperin, *Cannabis Company Cyberattack Reveals Industry's Vulnerability to Hacking*, LA WEEKLY (February 6, 2017) (indicating that, "MJ Freeway is the largest provider of software to cannabis businesses – including grows, factories and shops — suffered a major crash, crippling all of its customers.") *available at*: http://www.laweekly.com/news/cannabis-company-cyberattack-reveals-industrys-vulnerability-to-hacking-7895250

Electronic copy available at: https://ssrn.com/abstract=3239977

system, the State was terminating its five-year contract (after less than two-years) effective November 1, 2017. Nevada switched to METRC.[4]

MJ Freeway sustained a series of hacks. They were aimed at widely corrupting (not stealing) *track and trace* files. The data targeted was sales, inventory, customer identity, and cultivation data (plant height, strains and yields). No data was extracted in the attacks. Encryption protections prevented HIPPA violations. However, large amounts of historical inventory data were lost. Nevada's traceability system was

> … knocked offline … [as was] the State's entire ability to function with its cannabis program … The hack was aimed at corrupting files and data and it was unprecedented in terms of its sophistication, and it impacted both our live or production servers, as well as our backup servers. We have multiple backup servers and multiple redundancy, and we have them in multiple locations and with multiple companies. The attack hit all of them.[5]

The specific incidents that have been reported are concentrated at the end of 2016 and the first few weeks of 2017. All together the damage extended for a full six months. The system was seriously compromised for a considerable period of time. The reported incidents were:

- December 27, 2016 – [State hack] Justin Shafer uncovers a leak of personal information in Nevada – the full applications of 11,771 individuals who applied to the State of Nevada Medical Marijuana Program under NRS 453A.117[6]
- January 7, 2017 – [first direct MJ Freeway hack] a malicious intrusion into MJ Freeway's digital information platform brought down Leaf Data Systems – hundreds of clients were thrown offline.
- January 8, 2017 – [second MJ Freeway hack] the MJ Freeway site became unusable, and went offline for all of its clients.
- January 16, 2017 – MJ Freeway is back on line, and data recovery is attempted.
- June 15, 2017 – [third MJ Freeway hack] MJ Freeway's source code is stolen and posted on Reddit and Gitlab.com.[7]

MJ Freeway provides software both (a) to the taxpayers in the commercial chain (cultivator, manufacturer, testing labs, distributors and retailers) and (b) to the government regulator that owns and operates the State portal. It provides data transmission and storage services for users and regulators. Because the MJ Freeway attack targeted the whole system the damage was substantial. Figure 2 diagrams an MJ Freeway installation.

---

[4] On November 29, 2017 California adopted METRC, making METRC arguably the largest track and trace system deployed in the US.

[5] Tom Hynes, *Anatomy of the MJ Freeway Hack*, MG NEWS FOR CANNABIS PROFESSIONALS (January 20, 2017) *available at*: https://mgretailer.com/anatomy-mj-freeway-hack/

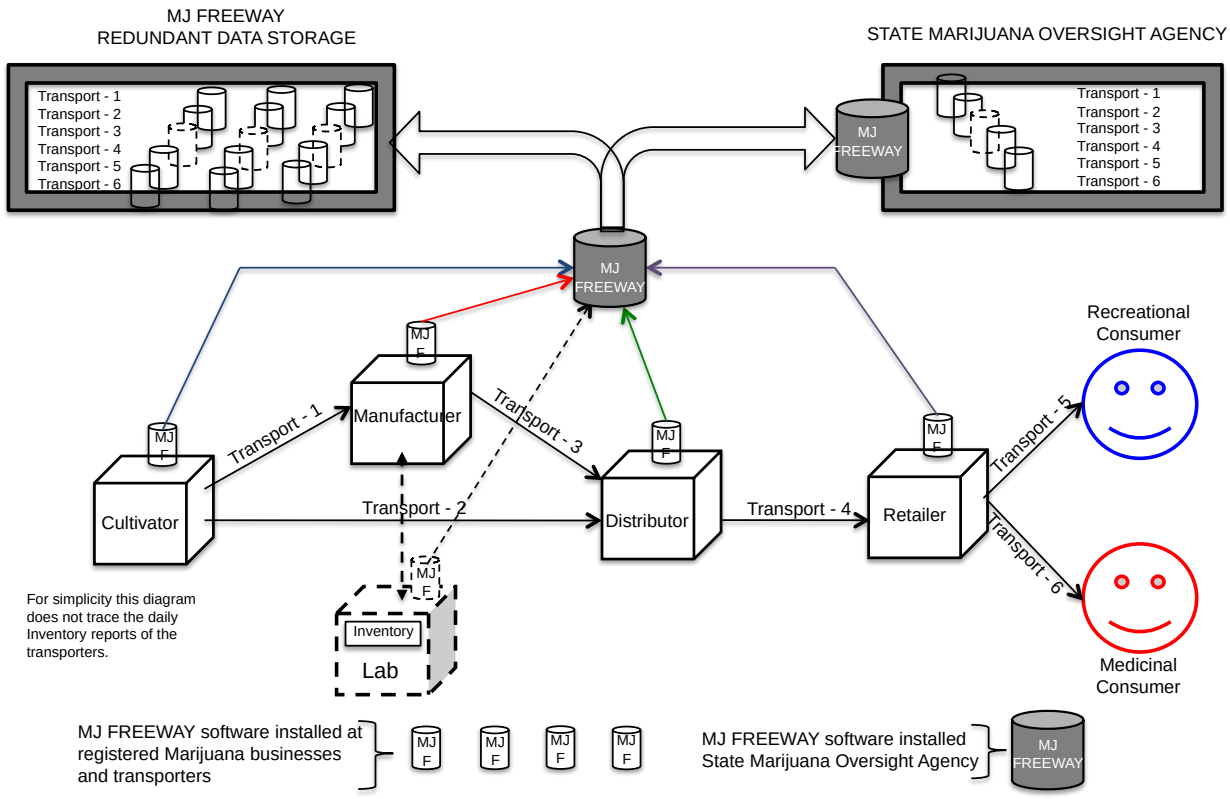
[6] *More than 10,000 Medical Marijuana Establishment Agent Applicants in Nevada had their Personal Info Exposed Online* (December 27, 2016) available at: https://www.databreaches.net/more-than-10000-medical-marijuana-establishment-agent-applicants-in-nevada-had-their-personal-info-exposed-online/

[7] Aaron G. Biros, *MJ Freeway's Source Code Stolen & Published Online*, CANNABIS INDUSTRY JOURNAL (June 20, 2017) *available at*: https://www.cannabisindustryjournal.com/news_article/mj-freeways-source-code-stolen-published-online/

Electronic copy available at: https://ssrn.com/abstract=3239977

The diagram below shows transmissions from MJ Freeway software at each registered marijuana business. These are daily inventory measures. They also track changes in the tracking numbers on each marijuana plant or product. The MJ Freeway client software is represented by a "can," (symbolizing a computer hard drive). This data transmission goes through the main MJ Freeway computers (represented by another "can"). From there it is stored by MJ Freeway in multiple (redundant) servers which back-up client data (for the client), and are also reported to the state through the on-line portal. Artificial intelligence is applied to this data base by the state performing risk analysis.

Figure 2:
MJ Freeway Installation



MJ Freeway is understandably cautious about discussing the hack of its system in the press or even with law enforcement. The early phase of the hack preceded the Trump administration, but the impact of the hack continued into the first six months of Trump's tenure. Immediately after the first wave of attacks Jeanette Ward, Vice President, Global Marketing and Communications made it clear that the company was not reporting the hack to the FBI:

> If we were not a cannabis company, federal law enforcement would handle this cybercrime, but we are not referring this to the FBI. One, we're not sure how interested they would be, but also out of respect for our clients, who would not be

Electronic copy available at: https://ssrn.com/abstract=3239977

> too keen to hear this case has been referred to the FBI and they are potentially digging through this information.[8]

Now that the cyber-attack is over, every post, public statement, and article on this incident walks around the elephant in the room – why did it happen? MJ Freeway's explanation is echoed widely. The attack was likely from an unhappy employee or by someone with a political interest in taking down the system. But, this was a highly sophisticated, criminal attack, one that is normally accompanied by a demand for ransom. However, "[t]here are no signs of ransomware nor was a ransom demanded by the attackers …"[9] If there was no ransom demand, no stolen data, and as of today, no one held accountable,[10] then why did it occur? One cyber commentator thought out loud as follows:

> Okay, this is interesting. Did the hacker(s) intend to corrupt the data or was that a byproduct of a failed attempt to access/exfiltrate encrypted data? What was the motivation behind this attack? To get data for extortion? To interfere with access to marijuana? To try to cross-match with another database for political purposes? Something else?[11]

The "something else" is very likely – the opening of every "leakage point," [2] through [12], in the main commercial chain so that legal marijuana could enter the black market undetected. The commercial marijuana businesses were clearly distracted. Nationwide, every business in MJ Freeway system went into overdrive *at the front door* recording transactions on paper, and then manually inputting data into local data bases. The state portals run by MJ Freeway were down. So, while all this was going on it is very likely (but unverified) that marijuana was leaving the system undetected *through the back door*. Acknowledging this during Trump's administration would not be optimal – hence the elephant in the room.

Preventing cyber-attacks on the main commercial chain

Cyber-attacks aimed at destroying reliable data in a commercial chain have a lot in common with VAT frauds that rely on obscuring transaction data behind rows of false "buffer" entities. Both are defeated by systems that lay bare and preserve highly trustworthy, real-time data about the intra-entity transactions within the commercial chain. AI has become very good at risk-analyzing these data flows.

Before blockchain, securing this data was difficult. Ledgers holding it were centralized, digital silos vulnerable to attack. The new VATs being deployed in the six states of the Gulf

---

[8] Jeanette Ward of MJ Freeway interviewed by Tom Hymes, in *Anatomy of the MJ Freeway Hack*, MGRETAILER.COM (January 20, 2017) *available at*: https://mgretailer.com/anatomy-mj-freeway-hack/

[9] Milena Dimitrova, *MJ Freeway Software Platform Targeted by Hackers*, SENSORS TECH FORUM (January 12, 2017) *available at*: https://sensorstechforum.com/mj-freeware-software-cannabis-platform-attacked/

[10] Tyler Koslow, *Leading Marijuana Sales Software Struggles to Recuperate from Systems Hack*, MERRY JANE (February 4, 2018) *available at*: https://merryjane.com/news/mj-freeway-cannabis-sales-software-hacked

[11] Dan Adams, *Marijuana dispensaries hit by hack of tracking software system* DATABREACHES.NET (January 10, 2017) available at: https://www.databreaches.net/marijuana-dispensaries-hit-by-hack-of-tracking-software-system/

Electronic copy available at: https://ssrn.com/abstract=3239977

Cooperation Council (GCC) are designed for *distributive ledgers*, or bockchain compliance.[12] The same is true of the five states of the East African Community (EAC).[13]

Blockchain creates a robust, secure, (fully or selectively) transparent[14] *distributive* ledger.[15] The technique is revolutionary. Blockchain is a software protocol based on cryptography, devised in 2008, and announced simultaneously with its most famous application – Bitcoin.[16]

Bitcoin (an application) is often confused with blockchain (a form of distributed ledger technology).[17] Recording Bitcoin transactions is only one application of blockchain technology; tracking commercial marijuana transactions is another. Ledger entries in the Bitcoin application are the Bitcoins generated by the Bitcoin protocol. In a marijuana protocol, the entries would be specifically identified plants, or grams of marijuana linked back to an identified plant. This difference is significant.

Marijuana is not inherently digital. As a result, external marijuana data in the supply chain must be securely transferred to the blockchain. There is, however, a problem trusting the transfer of external data into a blockchain. The problem exists because no matter how secure the blockchain is, if the data uploaded to it comes from unsecure API's, the unsecure API's become easy targets of data manipulation before the data enters the secure blockchain. The solution adopted here is to use a tamper proof blockchain middleware (Chainlink) to bridge the gap so

---

[12] The GCC is a regional intergovernmental political and economic alliance of six Middle Eastern countries – Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and he United Arab Emirates. It was formed in 1981. Richard T. Ainsworth & Musaad Alwohaibi, *The First Rael-Time Blockchain VAT: GCC Solves MTIC Fraud* 86 TAX NOTES INTERNATIONAL 695 (May 22, 2017).

[13] The East African Community (EAC) is a regional intergovernmental organization of 6 Partner States: the Republics of Burundi, Kenya, Rwanda, South Sudan, the United Republic of Tanzania, and the Republic of Uganda, with its headquarters in Arusha, Tanzania. Richard T. Ainsworth & Goran Todorov, *Stopping VAT Fraud with DICE – Digital Invoice Customs Exchange*, 72 TAX NOTES INTERNATIONAL 637 (November 18, 2013). Richard T. Ainsworth & Goran Todorov, *Plugging the Leaks in the East African Community's VATs,* 72 TAX NOTES INTERNATIONAL 561 (November 11, 2013).

[14] Blockchain is not inherently transparent – when used in a private / permissioned setting, information is only as transparent as the permissions in the network let it be. The key is the permissions that are set for each party. This is the case with the blockchain applied here. The public blockchain applied in the CALCoin solution further below, is far more transparent.

[15] A ledger, as used in this sentence and in this field generally, means a value recording and transfer system. Simply stated, a ledger is an accounting tool that keeps track of who owns what. Ledgers have long been digitized (in the 20th century), but it was only with blockchain that they have been *decentralized*. Prior to 2008 ledgers were only understood as *centralized*. Blockchain therefore, is really just one version of a distributed ledger, with its main feature being that it has provenance among its transactions which are cryptographically secured in a decentralized manner.

[16] Satoshi Nakamoto, Bitcoin, *A peer-to-peer electronic cash system* (2008) available at: https://bitcoin.org/bitcoin.pdf (note: Satoshi Nakamoto is a pseudonym).

[17] For a general and introductory discussion of blockchain, see: Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma & Vignesh Kalyanaraman, *Blockchain Paper: Beyond Bitcoin*, PANTAS AND TING SUTARDJA CENTER FOR ENTREPRENEURSHIP & TECHNOLOGY (October 16, 2015) *available at*:http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

Electronic copy available at: https://ssrn.com/abstract=3239977

that external data sources connect securely to the blockchain and allow smart contracts[18] within the blockchain to communicate with external resources on their own.[19]

It is axiomatic that wherever distributive ledgers are adopted, they will replace centralized ledgers. The MJ Freeway system is precisely this kind of multiple-redundant centralized ledger system that will be/should be disrupted (replaced) by a blockchain.[20]

Blockchain technology is nearly *trustless,*[21] in the sense that it does not require centralized third-party verification.[22] That is, it does not need a single *trusted* third party (a bank, or bank-like entity) to negotiate value transfer. In marijuana *track and trace* systems MJ Freeway, METRC, and other TAT and STS providers emulate banks. In marijuana control regimes, they are the *trusted third parties* that keep silos of centralized data. That data can be hacked and their systems fatally compromised.

Blockchain uses powerful *consensus mechanisms* to verify the authentic history of transactions in the database and secures new transactions when they are added into the main

[18] A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Hyperledger Fabric, the blockchain selected by this paper to run the marijuana blockchain, utilizes the term "chaincode" instead of smart contracts. A chaincode is software, running on a ledger, to encode assets and the transaction instructions (business logic) for modifying the assets.

[19] Securely entering inputs and outputs of non-digital content to a digital chain is a challenge. Any smart contracts within the system will be relying on unsecure human actors to provide triggering information to the smart contracts. For example, if cultivators *selectively* scan RFID codes, the validators will capture all reported data while *missing out* on the true volume of production. As Internet of Things (IOT) sensors advance, it may be possible to create adapters that allow their signals to interact directly with a blockchain middleware (such as the Chainlink project, a decentralized Oracle Network). They would be able to securely transfer triggering information into a smart contract, uploading marijuana cultivation data directly to the blockchain. The same process could be repeated for transportation information or any other objective data points. Steve Ellis, Ari Juels & Sergey Nazarov, *ChainLink – A Decentralized Oracle Network* (September 4, 2017) available at: https://link.smartcontract.com/whitepaper.

Although it is beyond the scope of this paper, if such a marijuana blockchain was adopted, the commercial contracts between parties in the marijuana supply chain could also be executed through this blockchain using Chainlink. The current paper contracts could be digitized such that data stored in the marijuana blockchain would provide triggering contract information for payments. For example, a cultivator could receive payment automatically from a distributer upon the blockchain confirming the transfer of marijuana from the cultivator to the distributor.

[20] Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, (March 12, 2015) at 4-8, *available at*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

[21] The trust element is very important to the adoption of blockchain in tax compliance areas. It needs to be stressed that trusting the blockchain technology is different than trusting Bitcoin. Europol contends that it is not blockchain, but the "… Bitcoin [application that] is establishing itself as the single common currency for cybercriminals within the EU." Europol, 2015 INTERNET ORGANIZE CRIME THREAT ASSESSMENT, *Key Findings* available at: https://www.europol.europa.eu/iocta/2015/key-findings.html

[22] There remains an element of trust needed – trust in the developers to build good software; trust in the consensus mechanism to be non-collusive; trust that no entity (government or corporation) could reach a 51% threshold and take over the blockchain.

Electronic copy available at: https://ssrn.com/abstract=3239977

chain.[23] The consensus mechanism can be adjusted or molded to fit specific applications.[24] But it is the consensus mechanism that makes a blockchain database highly trustworthy; *trustworthy even in the presence of hostile third parties trying to manipulate the registry*.

In a marijuana blockchain application, each daily inventory measure, each movement of marijuana (cultivator-to-transport-to-distributor) is recorded and protected in the same manner as an invoiced-sale is preserved in VAT compliance systems. Digital signatures are used. Records are sent by one party to the "public key" of the counter-party. The transmission is digitally signed using the sender's "private key." In order to complete the movement, the sender proves ownership of the "private key." The entity receiving the marijuana will verify the digital signature using the "public key" of the sender.

If the daily inventory measurement observes that a marijuana plant, or packet, or marijuana infused product has not moved since the previous day's inventory a self-assessment (cultivator-to-himself, or distributor-to-himself) transaction is recorded. In this way, we know with precision the location of all the marijuana in the supply chain.

A *private*, rather than a *public* blockchain is proposed to store the data that is transferred in the commercial production of legalized marijuana.[25] HyperLedger Fabric is the preferred

---

[23] Tim Swanson, *Great Wall of Numbers Cryptoeconomics for beginners and experts alike*, citing Vlad Zamfir of the Ethereum project at the Cryptocurrency Research Group conference (brainstorming session) on Cryptoeconomics as posted January 30, 2015 at: http://www.ofnumbers.com/2015/01/30/cryptoeconomics-for-beginners-and-experts-alike/. Cryptoeconomics is:

> A formal discipline that studies protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols.

[24] Cryptoeconomic incentives are most strongly associated with cryptocurrency systems. Bitcoin *mining* is such an incentive system. This is because Bitcoin uses pseudonymous and anonymous nodes to validate transactions, whereas a basic distributive ledger that engage entities with legal identities (banks, financial institutions, government agencies) will use "permissioned" nodes to validate transactions. This proposal of a marijuana blockchain uses permissioned nodes. For this reason, a basic distributive ledger is able to host off-chain assets (smart contracts) due to their authenticated, permissioned approach to validation. Tim Swanson, *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger System* (April 6, 2016) *available at*: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.

[25] A full examination of the selection of a *private ledger* is left for another time. Bitcoin uses a *public* (as opposed to a *private*) decentralized ledger. The term *public* means that a ledger is accessible by every internet user. Anyone can participate in the verification process and determine which blocks can be added to the chain (the *mining* process). Bitcoin's consensus mechanism is a very expensive *proof-of-work* mechanism. When the European Central Bank (ECB) considered blockchain for post trading activities in securities, it rejected *public* ledgers, and preferred *private* ledgers for the securities field. They did this to bring into sharp relief the use of white lists (or black list) of users, who are identified through KYB (know your bank) or KYC (know your customer) procedures. This process is common in traditional finance. Among all the following writers it is clear that *private*, *restricted*, or *permissioned* distributed ledgers work best in a governmental context. Vitalik Buterin, *On Public and Private Blockchain* ETHERIUM BLOG (August 7, 2015) available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/; Tim Swanson, *Consensus-as-a-Service: a brief report on the emergence of permissioned, distributed ledger systems* (working paper, April 6, 2015) at 4, *available at*: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf; European Central Bank, *Distributed Ledger Technologies in Securities Post-trading: Revolution or Evolution?* OCCASIONAL PAPER SERIES, No. 172 (April 2016) available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf; Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* (December 2015) at 16-24, *available at*:

Electronic copy available at: https://ssrn.com/abstract=3239977

blockchain platform.[26] Fabric is designed for consortiums where the participants are known, and has proven successful in a long-running proof-of-concept by the interbank messaging platform SWIFT.[27] Their identities are registered and verified with a central registry service inside the system.

The most popular consensus mechanism used in HyperLedger Fabric is the Practical Byzantine Fault Tolerance (PBTF), which employs three types of nodes (clients, peers and order servicing nodes in HyperLedger Fabric terminology[28]):

- **Clients** – are nodes that submit the actual transaction proposal to the endorsers, who in turn approve the transaction-proposal according to pre-defined endorsement policies determined by the configuration block[29] of the channel.[30] This is accomplished by endorser nodes providing a digital signature of validation. The endorser then returns the approved transaction proposal to the client so they can update their copy of the ledger. The client also "invokes"[31] the ordering service nodes, who will broadcast the transaction-proposal to the peers who in turn verify the endorser nodes validation of the client's transaction-proposal and assure that there has been no "double spending."[32]
    - In the marijuana blockchain configuration the clients are the cultivators, manufacturers, labs, distributors, retailers and each of the transporters that are sending daily inventory data to the state regulator.

---

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713 (discussing the difference between *private* and *public* distributive ledgers and opting strongly for *private* ledgers in the government sphere).

[26] HyperLedger is an open source collaborative effort to advance cross-industries blockchain technologies, hosted by Linux. Fabric is the private (permissioned) blockchain infrastructure, originally contributed by IBM and Digital Asset. HyperLedger Fabic is currently the most popular *private* distributive ledger. IBM states that Hyperledger Fabric deployed in a single cloud data center achieves an end-to end throughput of more than 3,500 transactions per second with latency of less than one second. See: Marko Vukolic, *Behind the Architecture of HyperLedger Fabric*, BLOCKCHAIN, CRYPTOGRAPHY, IBM RESEARCH-ZURICH, (February 2, 2018) *available at*: https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/. Additionally, as laid out in this paper, they believe the ordering service could theoretically reach a maximum rate of 8,400 signatures a second. If the block size is 10 transaction-proposals per block, we would have a theoretical upper bound of 84,000 transactions/second. Joao Sousa, Alysson Bessani & Marko Vukolic, *A Byzantine Fault-Tolerant Ordering Service for the HyperLedger Fabric Blockchain Platform*, arXiv:1709.06921v1 [cs.CR] (September 20, 2017) at § 6, *available at*: https://arxiv.org/pdf/1709.06921.pdf.

[27] Nkihilesh De, SWIFT Claims "Huge" Progress on DLT Bank Pilot, COINDESK (March 8, 2018) *available at*: https://www.coindesk.com/swift-announces-successful-proof-of-concept-trial-for-dlt-platform/

[28] Because HyperLedger Fabric has special terminology we have remained true to its usage, but provided definitions in notes to help the reader. All definitions taken from http://fabrictestdocs.readthedocs.io/en/latest/glossary.html.

[29] Configuration block: Contains the configuration data defining members and policies for a system chain (order service) or channel. Any configuration modifications to a channel or overall network (e.g. a member leaving or joining) will result in a new configuration block being appended to the appropriate chain. This block will contain the contents of the genesis block, plus the delta.

[30] Channel: A private blockchain overlay which allows for data isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be properly authenticated to a channel in order to interact with it. Channels are defined by a configuration-block.

[31] Invoke: Used to call chaincode functions. Invocations are captured as transaction proposals, which then pass through a modular flow of endorsement, ordering, validation, committal. The structure of invoke is a function and an array of arguments.

[32] Double spend: Refers to the transaction-proposal not already being "committed" to a block.

Electronic copy available at: https://ssrn.com/abstract=3239977

- **Peers** – are nodes[33] that execute, and maintain a ledger of transactions.[34] There are two roles for a peer – endorser[35] and committer. The architecture has been designed such that a peer is always a committer, but not necessarily always an endorser. When a peer "commits" a transaction, they are appending the validated transaction to the channel-specific ledger.[36] Peer nodes can also have a special role of being an endorser peer. There are two discrete peer-related functions that need to be performed by the States that have legalized marijuana in the marijuana blockchain proposed here. Governmental performance is bifurcated in two functional areas:
    - **First function**: the *State marijuana regulating agency* receives daily inventory/ RDID-based reports (transaction-proposals) from the supply chain entities (clients) under current State law. Under the proposed marijuana blockchain it will encrypt and endorse them if they meet the endorsement policy[37] criteria of the blockchain. The *State marijuana regulating agency* will then send back the signed transaction-proposal responses to the client nodes.
        - The client nodes then submit the transactions and signatures to the ordering service nodes, that is, they "invoke" the services of the order servicing nodes which create a batch, or block, of transactions and deliver them to committing peers.
        - When a committing peer receives a batch of transactions, it validates that the endorsement policy was met and checks in the read/ write sets to detect conflicting transactions.[38] If both checks are passed, the block is committed to the ledger, and the state updates for each transaction as reflected in the database.[39]
        - For purposes of the marijuana blockchain proposed here, the *State marijuana regulating agency* will also identify and verify marijuana loss estimates from each client entity. For example, in cultivation approximately 50% of tagged plants do not grow correctly and are discarded. Similarly, in the manufacturing process approximately 35% of

[33] Node: An individual entity in the blockchain network. Any entity (node) is required to maintain a member identity on the network.
[34] Transaction: Invoke or instantiate results that are submitted for ordering, validation, and commit. Invokes are requests to read/write data from the ledger. Instantiate is a request to start and initialize a chaincode on a channel. Application clients gather invoke or instantiate responses from endorsing peers and package the results and endorsements into a transaction that is submitted for ordering, validation, and commit.
[35] Endorsers: Refers to the process where specific peer nodes execute a chaincode (smart contract) transaction and return a proposal response to the client application.
[36] Peers can have specific roles. An endorser peer is responsible for simulating transactions, and in turn preventing unstable or non-deterministic transactions from passing through the network. Data is sent to an endorser in the form of a proposal. Endorsing peers are normally committing peers (i.e. they write to the ledger), except for highly regulated areas (like that involved with the marijuana blockchain considered here). A committing peer appends the validated transactions to the channel-specific ledger. Although a peer can act as both an endorser and committer, in highly regulated circumstances, it serves only as a committer. HYPERLEDGER, rev. 35dfac4e, *HyperLedger Fabric Glossary*, at Endorser and at Committer, available at: http://hyperledgerdocs.readthedocs.io/en/latest/glossary.html
[37] Endorsement policy: Defines the peer nodes on a channel that must execute transactions attached to a specific chaincode application, and the required combination of responses (endorsements). A policy could require that a transaction be endorsed by a minimum number of endorsing peers, a minimum percentage of endorsing peers, or by all endorsing peers that are assigned to a specific chaincode application.
[38] *Read* is a query to verify the status of something in the ledger. *Write* is to make a transaction in the ledger.
[39] *State* here is used to refer to the *current state data* that is stored in the blockchain.

Electronic copy available at: https://ssrn.com/abstract=3239977

products have defects and do not end up as finished product. State agencies acting as first function peers in this proposed blockchain would be: for example:

- California Department of Food and Agriculture (CDFA), or
- Vermont Department of Public Safety (VDPS);

- **Ordering-service nodes** (OSNs) or orderer nodes[40] – are a collection of network entities that perform the ordering service – ordering transactions into bocks according to the network's ordering implementation. Data is "broadcast" (by the orders) to the committing peers, and is "delivered" as blocks to the marijuana blockchain.[41]
    - **Second function**: the *State technology agency* will participate as OSNs and committing peers in the marijuana blockchain. They will assemble the blocks. This activity is independent of the oversight function performed by the *State marijuana regulatory agency* (above). State agencies acting as OSNs would be, for example:
        - California Department of Technology, or
        - Vermont Office of Technology Management.
- **Additional peers**. There is a critical need for additional peers (in addition to the State marijuana regulating agency and the State technology agency) to provide for a smoothly functioning marijuana blockchain. As a private blockchain those peers must be identified and highly trusted, and would probably include the State police, the State auditor's office (tax division) and the Department of Revenue.

Figure 3(below) illustrates a HyperLedger Fabric blockchain deploying a Practical Byzantine Fault Tolerance consensus mechanism in a legalized marijuana fact pattern. The illustration assumes that all 28 states that have legalized marijuana participate. Space allows only five of these States to appear in the diagram (California, Hawaii, Alaska, Vermont and Massachusetts). 448 nodes are easily foreseeable but cannot be easily diagramed.[42]

The illustration reads from the bottom-up. At the end of each day client nodes (cultivator, manufacturer, laboratory, distributor, retailer, and each third-party transportation firm) transmit the digital inventory report to the state marijuana oversight agency (endorsing peer #1). The example utilizes one supply chain in Massachusetts under the METRC TAT to submit inventory records (transaction-proposals) to the Massachusetts Cannabis Commission (MCC).

As an endorsing node the MCC will approve (or reject) the transaction-proposal according to pre-defined endorsement policies and communicate this assessment to the client (see the double arrows between each client and the first endorsing peer, marked by a "1" in a

[40] The ordering service can support multiple channels similar to the topics of a publish/subscribe messaging system. Clients can be given access to certain channels depending on the information that is shared or who it is relevant for. For example, there could be a California only channel or a channel only for cultivators. Channels can be thought of as partitions – clients connecting to one channel are unaware of the existence of other channels, but clients may connect to multiple channels.

[41] HYPERLEDGER, rev. 35dfac4e, *HyperLedger Fabric Glossary*, at Orderer, available at: http://hyperledgerdocs.readthedocs.io/en/latest/glossary.html

[42] 28 *State marijuana regulatory agencies* [28] + 28 *State technology agencies* [28] + 28 State police, State auditor (tax office), and State DOR [84] + 5 registered marijuana businesses in each state's supply chain [140] + 6 third-party registered transport firms in each state [168] = 448.

Electronic copy available at: https://ssrn.com/abstract=3239977

circle). Under the hypothetical marijuana blockchain represented in Figure 3 the OSNs cannot be "invoked" until three endorsing peers have validated a transaction-proposal. As a result, the cultivator (blue box) waits for additional endorsing peers. In this example endorsing peers from California [CA] and Washington [WA] validate.[43] See the double arrows marked by a "2" in a circle and a "3" in a circle.

When a client node receives validations from three endorsing nodes, it invokes the broadcast services of the OSNs (by submitting a copy of the transaction-proposal that includes the digital signatures of the three endorsers to the OSNs). This "invocation" is represented by the sweeping red arrow.

At this point the OSNs broadcast the transaction-proposal to other nodes and arranges the new transactions into bocks according to the network's ordering implementation.[44] The OSNs will respect any channeling protocols of the marijuana blockchain. Channeling protocols will limit access to the data based on permission-levels. (For example, State enforcement agencies may have wide access permission, but a specific manufacturer/ client may have permission to access data only from a channel that includes its immediate upstream cultivators and immediate downstream distributors).

When committing nodes receive the broadcast and new blocks they will "commit" the blocks to their copy of the distributed ledger. This action is deterministic – all nodes will reach the same valid/ invalid conclusion for the data. They will additionally verify that endorsement policies were followed when the endorsing peers validated the transaction-proposal. In Figure 3 committing nodes from the technology departments of the States of California, Hawaii, Alaska and Vermont represent all similar nodes.

In this illustration California (the Department of Technology), Hawaii (the Office of Technology Services), Alaska (the Office of Information Technology) and Vermont (Office if Technology Management) were selected as committing peers largely because time zone differences and estimated work-loads made it easy to see how these states could verify end-of-day inventory submissions from Massachusetts.[45]

---

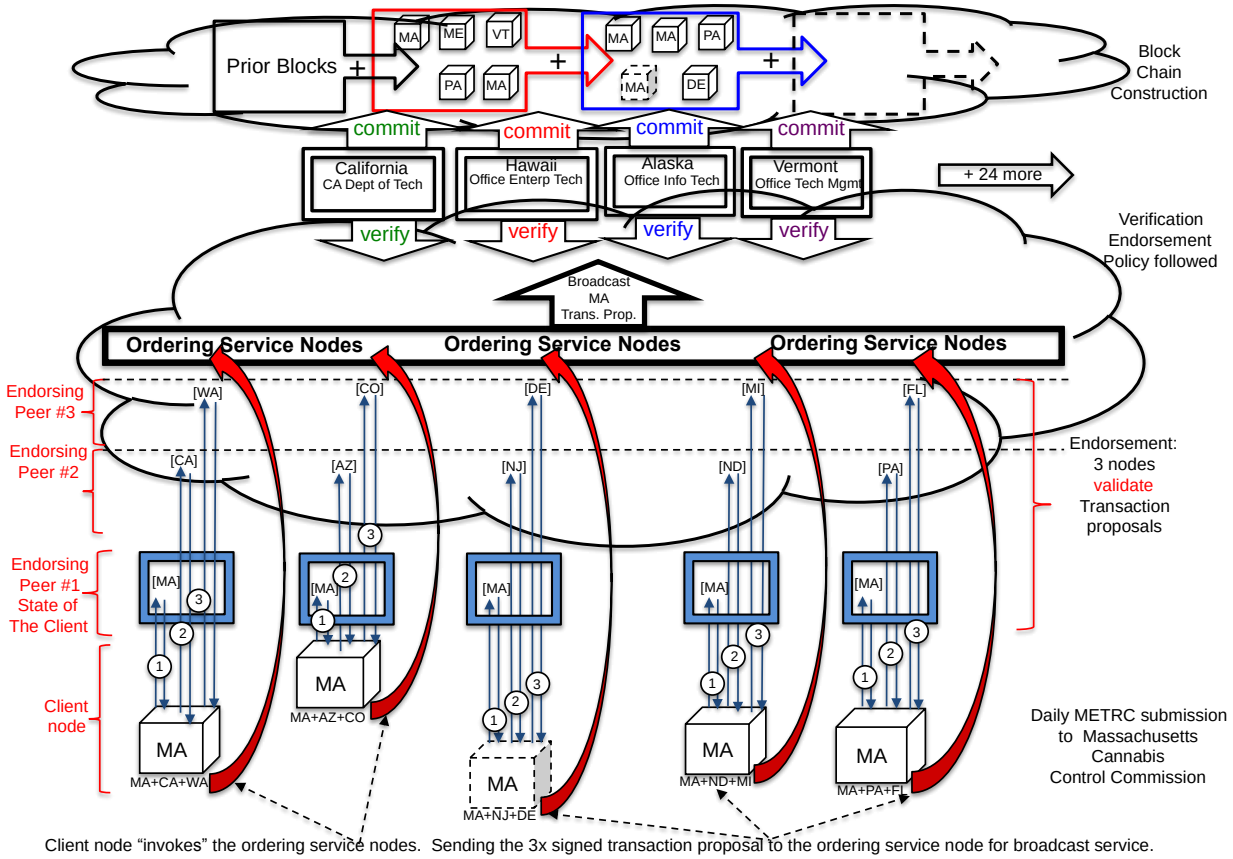
[43] There is an assumption that at close of business in Massachusetts it would be more likely to find an endorsing node on the West Coast than on the East Coast.

[44] During the ordering service process transaction-proposals are sorted on a first-come-first-serve basis. The organization is chronological by channel as information is placed into blocks. Transactions within the blocks are broadcast to the peer nodes who must verify them as valid or invalid. Figure 3 represented this first-come-first-serve sorting process by placing transaction-proposals from the *cultivators* in Massachusetts, Maine, Vermont, and Pennsylvania along with a Massachusetts manufacturer in the same block under the premise that East Coast cultivators would be first in line at business closing. It assumes that the timing of their submissions would closely approximate one another. The second new block collects the transaction-proposals from the remaining entities in the Massachusetts supply chain and bundles them with a Pennsylvania retailer and a Delaware distributor. For a discussion of some of the practical problems around organizing transactions within blocks see: Kostas Christidis, *A Kafka-based Ordering Service for Fabric*, available at: https://docs.google.com/document/d/1vNMaM7XhOlu9tB_10dKnlrhy5d7b1u8lSY8a-kVjCO4/edit

[45] Technically, there is no need for a "end-of-day" submission. State statutes and the METRC systems function on this schedule. The proposed system is designed to (theoretically) handle 84,000 transactions a second, which is a speed sufficient to enable real time data transmission and validation. Similarly, there is no need for an "end" to each day as the system will run 24/7.

Electronic copy available at: https://ssrn.com/abstract=3239977

Figure 3
HyperLedger Fabric with Practical Byzantine Fault Tolerance (PBFT)



In this illustration the marijuana blockchain is developed by the states. The blockchain could be started by one states, California for example, and other states could join in time. Then again, with a more cooperative federal administration the blockchain could be sponsored by the federal government. The Financial Times indicates that there have been discussions between *420blockchain*,[46] a group working to bring together the cannabis industry, and the Congressional Cannabis Caucus about using blockchain to regulate marijuana.[47] This is how such a blockchain would be designed.

CONCLUSION

The marijuana supply chain is (potentially) a highly porous highway distributing marijuana throughout a State. It is secured with technology (STS or TAT), but the data is

[46] 420Blockchain, *Uniting the Cannabis Industry: True Transparency, Smart Contracts & Mobile Engagement*, available at: http://420blockchain.cloud; Erin Mundahl, *Could Blockchain Technology Be the Answer for Regulating Cannabis Growth and Sales?* FINANCIAL TIMES (February 9, 2018) *available at*: https://www.ft.com/stream/837baaa6-b895-3123-9bd7-0553f688f8b9

[47] John Authers, *Authers Note: Tough Times for The Onion* (Premium) (February 8, 2018) available with premium subscription at: https://www.ft.com/stream/837baaa6-b895-3123-9bd7-0553f688f8b9

Electronic copy available at: https://ssrn.com/abstract=3239977

(currently) stored in vertical silos. There may be multiple layers of redundancy behind the silos, but they are vulnerable (hackable) silos non-the-less. No State has established security along a main marijuana supply chain comparable to that of a robust, well designed blockchain.

The blockchain envisioned in this paper would have in excess of 448 State controlled replicating nodes preserving transaction data in 28 or more States. Loosing encrypted transaction records from all or most of the nodes would be unlikely.

Data silos are vulnerable to malicious attack. Entire State systems have been taken down. MJ Freeway was taken off line nation-wide. TAT and STS data has been destroyed, lost and corrupted. When data security is compromised, marijuana can easily slip into the black market through any one of ten separate "leakage points."

As Part 4 of this series will explain, the marijuana that "leaks out" of the supply chain does not necessarily physically leave the chain itself; it may just leave the "digital record" of the chain. Untracked resales of marijuana may be processed (tax free) through a legitimate dispensary that is equipped with Zapper of Phantomware suppression device. There would be no record of the final sale, or the cash it was exchanged for. Once marijuana makes it outside the *track and trace* or *seed to sale* systems tax losses arise, and federal concerns under the Controlled Substances Act and the Bank Secrecy Act are heightened.

Electronic copy available at: https://ssrn.com/abstract=3239977