Taxing & Zapping Marijuana: Blockchain Compliance in the Trump Administration

Richard Thompson Ainsworth
Boston University School of Law

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship
Part of the Medical Jurisprudence Commons, and the Tax Law Commons

Recommended Citation
Available at: https://scholarship.law.bu.edu/faculty_scholarship/283

This Article is brought to you for free and open access by Scholarly Commons at Boston University School of Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarly Commons at Boston University School of Law. For more information, please contact lawlessa@bu.edu.
TAXING & ZAPPING MARIJUANA:
BLOCKCHAIN COMPLIANCE IN THE
TRUMP ADMINISTRATION

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

Revised March 15, 2018

Richard T. Ainsworth
Boston University School of Law

Brendan Magauran
TAXING & ZAPPING MARIJUANA:
BLOCKCHAIN COMPLIANCE IN THE TRUMP ADMINISTRATION

Richard T. Ainsworth
Brendan Magauran

On January 4, 2018, the Trump Administration through Attorney General Sessions rescinded an Obama-era policy\(^1\) that discouraged federal prosecutors from bringing charges in all but the most serious marijuana cases under the federal Controlled Substances Act,\(^2\) as well as under the Bank Secrecy Act.\(^3\) Federal law is at odds with state law in the majority of states on the legalization and subsequent state taxation of marijuana.\(^4\) Twenty-eight states and the District of Columbia have at least partially legalized marijuana. Eight of these states have legalized both medicinal and recreational use.\(^5\) With limited exceptions, legalized sales of marijuana are taxed.


\(^2\) 21 USC § 801 et. seq. With this act, in 1970, federal regulation of marijuana began. Congress divided drugs into five categories. Marijuana was placed in the same category as heroin (Schedule 1). It was deemed to have “no acceptable medical use,” even though its medicinal value had been observed as early as 1839. (See the research paper by Irish physician, Dr. Walter O’Shaughnessy, On the Preparations of the Indian Hemp, or Ganja referenced further in Cannabis Tinctures and Fluid-Extracts, THE ANTIQUE CANNABIS BOOK, Ch. 4, available at: http://antiquecannabisbook.com/chap4/Tincture.htm. O’Shaughnessy brought tinctures back from India to the UK.

\(^3\) 18 USC §§ 1956-57, 1960; 31 USC § 5318. The BSA requires US financial institutions to assist US government agencies to detect and prevent money laundering. All marijuana transactions, as schedule 1 transactions under 21 USC § 801 et. seq., are therefore money laundering transactions. Thus, the ABA observes:

All banks are subject to the requirements of the Bank Secrecy Act. Under the BSA, banks must report to the federal government any suspected illegal activity which would include any transaction associated with a marijuana business. These reports must be filed even though the business is operating legitimately under state law. Financial institutions face significant risk for violating EY Tax News Update for Thursday, January 18, 2018 (7:00 AM ET) federal law if they offer banking services to marijuana-related businesses.


\(^4\) This paper does not argue for or against the legalization of marijuana. It is only concerned with the taxation of marijuana by the states, and efforts to prevent fraud and improve related trust issues among the US states. It also does not consider the federal income taxation of marijuana businesses. In this area there is considerable concern with IRC § 280 which prevents the deduction of expenses from income generated by the sale of cannabis. The only reductions from Gross Income allowed are related to the Cost of Goods Sold (COGS). For many taxpayers determining what expenses count as COGS, and what do not is hard to say. As a consequence, many individuals and businesses end up afraid to file their taxes and filings.

Federal marijuana drug enforcement policy under the Obama Administration, created the space within which the states could legalize marijuana. Federal authority under Gonzales v. Raich and the interstate commerce clause broadly authorizes federal action. It permits granular federal enforcement of federal marijuana laws within any state, but the Obama administration limited these concerns and activities.

The now-rescinded AG memos declared that the federal interest in marijuana enforcement was not comprehensive. In particular, the memo by Deputy Attorney General Cole (August 29, 2013) limited the federal concern to:

1. Preventing the distribution of marijuana to minors;
2. Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs and cartels;
3. Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
4. Preventing the state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
5. Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
6. Preventing drugged driving and the exacerbation of other public health consequences associated with marijuana use;
7. Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on public lands; and
8. Preventing marijuana possession or use on federal property.

Staying clear of these eight problem areas seemed to assure the states that they could deal with marijuana as they saw fit. By reverse inference Cole’s instruction to “all United States Attorneys,” effectively was a request by the Attorney General that the states exercise tight and comprehensive physical [items 1, 3, 4, 7, & 8] and financial control [item 2] over all state-sanctioned marijuana transactions and their consequences [items 5, & 6]. With State success in these areas, the Federal government was willing to turn a blind eye to minor infractions of the federal law. Digital track and trace systems were created to meet this challenge.

Aside from “compassionate use” of medicinal marijuana, the States have seen real business development and job creation opportunities by legalizing the marijuana trade –

---

5 545 US 1 (2005) (involving agents of the Drug Enforcement Agency who seized and destroyed six marijuana plants being grown by two California residents for doctor recommended use to treat serious medical conditions under California’s Compassionate Use Act).

estimates of 250,000 new jobs by 2020 are common. In addition, there is revenue to be generated by imposing income, sales and excise taxes on the marijuana trade. The revenue yield should be sizeable – estimates are of an annual $28 billion in federal, state and local revenue from a mature industry; $7 billion in federal revenue; $5.5 billion in business taxes and $1.5 billion in income and payroll taxes. For example, if marijuana were to be taxed with a federal excise tax in the same manner and at the same rate as tobacco, then federal revenue would increase by $500 million annually. State revenue would increase many times more.

State marijuana revenue measures are not harmonized today. Both the tax rates and the commercial stages at which marijuana transactions are taxed diverge widely. Rates range from

<table>
<thead>
<tr>
<th>Year</th>
<th>Colorado Raised in the First Three Years of Legalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014 from 1-1-2014</td>
<td>$76,152,458</td>
</tr>
<tr>
<td>2015</td>
<td>$135,100,463</td>
</tr>
<tr>
<td>2016</td>
<td>$198,522,164</td>
</tr>
<tr>
<td>2017 through 5-31, 2017</td>
<td>$96,368,540</td>
</tr>
<tr>
<td>TOTAL</td>
<td>$506,143,625</td>
</tr>
</tbody>
</table>


10 Id. $500 million is what Colorado raised in the first three years of legalization.
zero for medicinal use (in Delaware, DC, Maine, Massachusetts, New Hampshire, New Mexico, North Dakota, and Oregon) to roughly 47% (for recreational marijuana, slightly less for medicinal) in Washington. The types of taxes imposed range from standard income, excise, and retail sales taxes (in most states), to wholesale taxes (Alaska, California, Colorado, Illinois, Nevada, Pennsylvania, and West Virginia). In California, distributors will collect state taxes from both the grower and the retailer. In some instances, the grower will pay taxes directly to the State on marijuana for the right to place it into commercial distribution (Rhode Island).

For the most part, state marijuana taxes cascade with excise taxes appearing in the retail sales tax base. In California, for example, an excise tax is imposed on marijuana flowers at $9.25 per oz. (it is paid to wholesalers by growers). This tax is included in the base when the wholesaler sells on to retailers. These retailers, in turn, collect an additional 15% excise tax on consumer sales before the State’s 6.25% state retail sales tax is imposed (along with city and county sales taxes). Because the 15% and $9.25 per oz. excise taxes are included in the retail sales tax base aggregate California taxes are much higher than they appear. See figure 1 (below).

other than the standard 6% rate, has not determined; (14) Massachusetts (imposing no tax on medical marijuana, however for recreational use the standard 6.25% sales tax applies in addition to a 10.75% excise tax and a local municipal tax of 3% - https://www.mass.gov/medical-use-of-marijuana-program); (15) Michigan (imposing a 3% excise tax on gross receipts of dispensaries in addition to the 6% state sales tax on medical marijuana - http://www.michigan.gov/documents/treasury/Tax_Policy_Newsletter_November_2016_544007_7.pdf); (16) Minnesota (imposing a $3.50 per gram tax in medical marijuana - http://www.revenue.state.mn.us/businesses/controlled_substance/Pages/Tax-Information.aspx); (17) Montana (currently imposing a 4% sales tax until June 30, 2018 when it drops to 2% - http://leg.mt.gov/bills/2017/Billpdf/SB0333.pdf); (18) Nevada (imposing a 2% medical excise tax, a 10% retail excise tax, and a 15% excise tax on wholesalers on the first wholesale sale by a cultivator - https://tax.nv.gov/Forms/MMT/); (19) New Hampshire (imposing no tax on medical marijuana, recreational use not allowed - https://www.dhhs.nh.gov/oos/tcp/); (20) New Jersey (imposing a 7% sales tax on medical marijuana, recreational use not allowed - http://www.state.nj.us/treasury/taxation/pdf/pubs/tb/tb68.pdf); (21) New Mexico (imposing no tax on medical marijuana, recreational use not allowed - https://nmhealth.org/about/mcp/svcs/); (22) New York (imposing a 7% tax on medical Marijuana, recreational use not allowed - https://www.tax.ny.gov/Forms/MMT/); (23) North Dakota (imposing no tax on medical marijuana in proposed rules due in February 2018 (24) Ohio tax rate TBD after September 2018 when the Medical Marijuana Control Program is fully operational - https://www.medicalmarijuana.ohio.gov; (25) Oregon no tax on medical marijuana, but recreational is taxed at retail at 17% with 3% local municipal tax - http://www.oregon.gov/DOH/programs/businesses/Pages/marijuana.aspx; (26) Pennsylvania wholesale tax at 5% excise tax; (27) Rhode Island (imposing a $25 per plant tag for patient/ caregivers on medical marijuana, a 4% surcharge paid by the seller, and the 7% regular sales tax - http://webserver.rilin.state.ri.us/Statutes/TITLE21/21-28.6/21-28.6-15.HTM; Emergency Regulation CCS 11-01 Compassion Center Surcharge at: http://www.tax.ri.gov/regulations/other/CCS-01.pdf); (28) Vermont (medical is exempt from sales tax, but pipes, vaporizers, and other items classified as drug paraphernalia sold in a dispensary are subject to the 6% sales tax, with local taxes at 1% in addition - (http://tax.vermont.gov/sites/tax/files/documents/MedicalMarijuanaFS.pdf); (29) Washington; (imposing a 37% excise tax on medical marijuana sales, but providing an exemption from the standard state sales tax only for medicinal marijuana – however for recreational use the 37% excise tax applies in addition to state and local sales taxes) - https://dor.wa.gov/find-taxes-rates/taxes-duo-marijuana); (30) West Virginia (imposing a 10% wholesalers excise tax - http://www.wvlegislature.gov/Bill_Status/bills_text.cfm?biddoc=sh386%20intr.htm&yr=2017&sesstype=RS&i=386)
This paper proposes to analyze state marijuana enforcement and taxation through the lens of European value added taxes (VAT). There is a closer harmony between the EU and the US in this area than might be expected.

**Cascading.** The EU VAT was developed in response to the common use of cascading sales taxes on goods in the EU as they passed through supply chains. This is precisely what is happening in the US marijuana market.

**Open borders.** In both the US and the EU, there is an economic union comprised of semi-independent jurisdictions. Each jurisdiction has separate taxing authority to collect revenue from domestic consumption, based on the market value of the goods sold. In both cases, the internal borders of the community allow taxable goods to flow freely, without customs controls. In both the US and the EU this porous border invites criminal fraud.

**Missing traders.** The most notable fraud in both systems is “missing trader” fraud. This is a fraud whereby traders ship goods (in the EU) or marijuana (in the US) from low-tax/no-tax jurisdictions to high-tax jurisdictions. The supplies are sold with tax, followed by the “disappearance” of the seller. The State of Washington’s aggregate 47% transaction tax on marijuana is likely to attract criminal organizations nation-wide, just as Hungary’s 27% VAT does in the EU.

**Inter-governmental trust.** Open borders and heightened enforcement efforts inevitably create inter-governmental trust problems. In the US, high-tax jurisdictions (Washington) will ask low-tax jurisdictions (North Dakota) to help them stem illegal cross-border marijuana flows, just as (high tax) Hungary often makes a similar request of (low tax) Luxembourg. States where marijuana sales remain illegal will be making criminal enforcement requests broadly.

Trust problems will arise in the US, just as they have in the EU. Revenue, business development, and employment concerns will all weigh against expeditious cooperation. This has
been a continuing area of concern in the EU where trust among the Member States has been eroded by the burden of shared-enforcement obligations tethered to disproportionate benefit outcomes. The most recent proposals for change in the EU VAT strongly stress the use of technology to increase trust.\textsuperscript{13}

There are also important differences between the EU and the US.

\textit{The EU - an idea-rich, but weak central government.} The EU has a weak central government in tax matters. Brussels works hard to harmonize tax rules, reduce tax frauds, promote Member State trust, and shared tax enforcement, but it is hamstrung. The EU Council\textsuperscript{14} does not have taxing authority, and it is limited in its ability to otherwise affect tax changes among the Member States by Article 93 of the Treaty of Rome, which requires \textit{unanimous} Member State consent before community tax laws are changed.\textsuperscript{15}

\textit{The US - an idea-resistant, but strong central government.} The US in contrast, has a strong central authority in tax matters. The Federal government can raise its own taxes. It plays a significant role in coordinating tax policy among the states both directly through the commerce clause, and indirectly through federal tax rules which are commonly adopted by the states.

With respect to marijuana, however, the federal government has been more hostile than helpful. As a result, we have the unusual situation where the best ideas on how to build trust and increase the enforcement and taxation of marijuana may be found in Brussels, not Washington.

\textsuperscript{13} Technology and trust are the themes of the most recent proposals for change in the EU VAT. \textit{COMMISSION STAFF WORKING DOCUMENT – IMPACT ASSESSMENT, accompanying the document Proposal for a Council Directive amending Directive 2006/112/EC as regards harmonizing and simplifying certain rules in the value added tax system and introducing the definitive system for the taxation of trade between Member States, SWD(2017) 325 final (October 4, 2017) at 11, 14 at n. 37, & 16 (emphasis added)

The efficiency of the VAT system needs to be further improved, in particular by exploiting the opportunities of \textit{digital technology and by enhancing greater trust} between business and tax administrations and between EU Member States’ tax administrations … the preferred Option 2 notably relies on the assumption that the VAT due on a cross-border transaction in a given Member State is collected by another Member State that will also have the main responsibility for auditing the VAT due. …. This [new] system would, in practice, create a collective responsibility whereas under the then existing system each Member State was individually responsible for the administration, control and collection of its own VAT. A \textit{high degree of trust} between Member States was therefore a pre-condition for the new system.

\textsuperscript{14} The EU Council is comprised of the Heads of State of the member States. The EU Commission, operating as a cabinet, would (in the normal course) recommend tax changes to the Council.

\textsuperscript{15} The Treaty of Rome established the European Economic Community (EEC) (later changed to the European Community). Signed on March 25, 1957. The Treaty has been revised many times, including the Treaty on European Union, signed in Maastricht on February 7, 1992, the Treaty of Amsterdam, signed on October 2, 1997, and the Treaty of Nice entering in force on February 1, 2003. Through all these changes the wording of the original Article 93 remained unchanged: the Council, “… acting unanimously on a proposal from the Commission and after consulting with the European Parliament and the Economic and Social Committee …” shall adopt provisions for the harmonization of the VAT within the Community.
This paper considers EU VAT proposals for tax harmonization and enforcement, and applies them to the US. The proposals are technology-intensive. They integrate well with the digital track and trace systems employed by US States to control legalized marijuana.

The first proposal is to place the central portion of the marijuana supply chain on a private blockchain that is shared among the states. Transactions in marijuana will be preserved in real-time (locally and centrally). Data will be shared among State authorities to aid enforcement, and tax collection.

The second proposal is for a limited-purpose crypto currency. This would be a crypto-token like VATCoin that is digitally minted by the government. For example, CALCoin. CALCoin would be the only currency allowed for marijuana-related purchases within California. CALCoin transactions would be placed on a separate public blockchain. CALCoin(s), would be available only from the State, and would be converted into fiat currency or an alternate crypto currency only by the State.

The EU is considering versions of both of these proposal, although progress toward adoption is slow under the constraints of Article 93. Two other economic communities have moved faster that the EU and have begun implementations. Initial implementation of both proposals is observable in the Gulf Cooperation Council (GCC). The first proposal is directly incorporated in The Unified VAT Agreement for the Cooperation Council for the Arab States of the Gulf. The second proposal of a limited purpose crypto currency is under consideration in the EU as VATCoin. Rwanda, in the East African Community (EAC), currently requires encrypted digital invoices collected centrally in real-time, and is waiting for another EAC State to join it in a blockchain exchange.

MARIJUANA SUPPLY CHAIN

Figure 2 (below) presents the typical marijuana supply chain. The cultivator sells its yield either to a manufacturer (for example a bakery making brownies or cookies with marijuana ingredients), or directly to a distributor. The distributor purchases both the cultivator’s and the manufacturer’s output, then sells on to retailers who re-sell either medicinal or recreational

---

17 The GCC is a regional intergovernmental political and economic alliance of six Middle Eastern countries – Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates. It was formed in 1981.
19 Richard T. Ainsworth & Goran Todorov, Stopping VAT Fraud with DICE – Digital Invoice Customs Exchange 72 TAX NOTES INTERNATIONAL 637 (November 18, 2013) (discussing the initial stages of the solution, the adoption of digital invoices which are encrypted, digitally signed, preserved locally and sent centrally in real-time, but without the blockchain element.
20 The EAC is a regional intergovernmental political and economic alliance of six East African countries – Burundi, Kenya, Rwanda, South Sudan, Tanzania/Zanzibar and Uganda.
marijuana to consumers. Any of the businesses along this supply chain may send the marijuana on hand to a third-party lab to verify quality, and may contract with a third-party carrier to deliver marijuana. Most of the other Figures in this text will reference the format of this diagram.

Figure 2:
Standard Marijuana Supply Chain

States that have legalized marijuana have two concerns with the standard supply chain. Both concerns harken back to the Cole memo, as the states are responding to the risk of federal enforcement. The legalization of marijuana burdens states with the responsibility of (a) monitoring the physical flows of marijuana through the supply chain (making sure the marijuana does not enter inter-state commerce; making sure it stays out of the hands of minors, etc.), and also (b) monitoring the fiscal flows (making sure the proceeds of marijuana production do not end up in criminal hands).

The first burden arises because of the Controlled Substances Act, and is based on federal authority to regulate inter-state commerce. The second burden is brought about by the Bank Secrecy Act, and federal authority to control money laundering. We will consider both of these monitoring responsibilities.

Monitoring Physical Flows

The states that have legalized marijuana need to closely monitor the physical flows in authorized supply chains. The states need to know that legalized marijuana is staying within the chains (within the state) – not leaking out. The type of physical controls favored by the states are track and trace (TAT) systems, or sometimes seed-to-sale (STS) systems.21

TAT and STS systems are complex, technology-based control systems. There are questions about whether they are adequate to the enforcement needs of the state. TAT is a derivative application of commercial inventory control systems. Radio Frequency ID (RFID) is

---

21 Seed-to-sale (STS) software is sometimes required by State law to track marijuana in the commercial chain, but it also provides valuable data to cultivators about plant yields, cultivation method successes and failures, forecasting productivity, or assessing the effectiveness of extraction methods. Track and trace (TAT) software provides regulator tools to assess aggregate compliance data from all licensed businesses in the cannabis chain of custody. MJ Freeway, Track and Trace vs, Seed to Sale, (June 19, 2016) available at: https://mjfreeway.com/blog/track-and-trace-vs-seed-to-sale
applied. STS is a derivative application of Artificial Intelligence (AI) and Internet of Things (IoT). It comes from the application of technology to “digital food production.” Neither TAT nor STS fully satisfy the enforcement needs of the State. Simply stated, these systems leak at both ends, and in the middle.

Under TAT and STS each marijuana plant under cultivation is specifically identified (digitally tagged), and then followed. Tracing includes movements within a cultivator’s establishment, carriage by third-party transporter along the supply chain, and movement in and out of every lab where the marijuana is sent for external testing. California, Colorado, Oregon, Alaska, Maryland, Michigan, Massachusetts, Montana, Ohio and Nevada use the METRC system. METRC was developed by Franwell Inc., and is based on RFID technology. Tagging with barcodes (as opposed to RFID chips) is an alternative, less efficient and less effective method of tracking. METRC is the dominant provider in the legalized marijuana market.

Track and trace systems are based on daily inventory measures reported to the state. METRC takes inventory with RFID tags. The METRC tagging process is sketched by Franwell, in ten steps. Steps 1-5 occur during cultivation; step 5(a) is the direct sale to a Distributor; step 5(b)-7 is the direct sale to a Manufacturer, or an “infusing” enterprise followed by a re-sale to a Distributor; step 8-9 is the sale to a Retailer; step 10 is the sale to the final consumer. As a marijuana plant moves through the supply chain it will be identified within one or more of these step-points.

There are four “RFID tagging events” in the standard METRC schedule. METRC explains the ten inventory steps, and the four “tagging events” as follows:

1. Immature plants are grouped and identified by the grower;
2. Vegetative plants (8 inches, or in a 2-inch pot) are tagged (first) with a discrete RFID tag;
3. Flowering plants (light cycle of 12 hours on/ 12 hours off);
4. Harvested plants are cut down, and a “wet weight” is secured;


23 Two applications of AI and IoT (a Malthouse that regulated higher starch and proteins content, thus higher alcohol content downstream, and a more complex [138 variable] application to Medical Marijuana cultivation) are presented by Rob Dolci, IoT Solutions for Precision Farming and Food Manufacturing, 2017 IEEE 41st Annual Computer Software and Applications Conference 384.

24 METRC is the name of the Franwell system, but it is also a descriptive string of words, functioning as an acronym meaning Marijuana Enforcement Tracking Reporting Compliance.

25 Franwell Inc. explains the METRC process at: https://www.metrc.com/the-system.

26 There are a number of commercial advantages to using RFID over bar codes. They include (1) read distances—a whole room can be read with RFID at 10 to 15 foot distances without touching the plants; (2) read speed—RFIDs are read 90% faster than barcodes; (3) RFIDs easily identify a single misplaced plant in a room; (4) errors with barcoding can require the inventory to be started from the beginning, whereas RFIDs simply require a second pass to be made of a room.

27 The Franwell steps are an expanded version of the traditional commercial supply chain. Franwell expanded it to isolate the various places in cannabis growth and distribution cycle where RFID chips are attached. Several times different RFID chips can be attached to a product while it is in the hands of a single member of the supply chain.
5. Marijuana is grouped by strain (buds or shake) gets a new (second) unique RFID. The product is now either:
   a. Packaged and sold; or
   b. Processed into hash, or infused in another product
6. Packaged product may be transferred to an infusing business
7. An infusing business will repackage the infused products for transfer, and will attach a (third) unique RFID chip;
8. Packaged inventory is transferred to a retail selling business;
9. Selling business will repackage inventory which is destined for another selling or infusing business. A (fourth) unique RFID is attached;
10. Retail selling business will sell to consumers from inventory.

In figure 3 (below) the four “RFID tagging events” are represented by letters “a,” “b,” “c,” and “d.” These figures are placed inside small boxes (to represent the “tagging” process.) A unique RFID is needed every time a product is transferred from one entity to another in the supply chain. Daily inventory counts are taken using the RFID chips within each entity, as well as by every transporting entity.

Each of the major software providers in the legalized marijuana market works in a similar fashion. They strive to become the (only) State-authorized software for the collection of compliance data at the taxpayer level. In addition, they provide back-end software that operates the State’s web-portal.

---

State enforcement should not be held captive by the available TAT or STS solutions. It is problematical to consider the State’s job “done” simply by assessing how well a chosen TAT or

---

MJ Freeway’s Leaf Data System and BioTrackTHC are the other major providers.
STS performs. States need to consider enforcement in an honest, independent manner. From this perspective, it is reasonably clear that there are fourteen points along the standard marijuana supply chain where there may be “leakage” into the hands of criminals, or unintended consumers (minors or cross-border residents). The ultimate goal of any State system is not to simply to follow METRC or another TAT or STS system, but to use every measure to securely monitor and plug up each of these leakage points.

Figure 4 (below) numbers the likely leakage points in a marijuana supply chain. The great majority of these points, [2] through [12], are covered by METRC. There are serious problems with basic coverage at both ends of the supply chain – at [1], [13], and [14]. But there are also vulnerabilities within the main part of the chain, [2] through [12].

**FRAUD DYNAMICS**

There are four basic fraud opportunities for criminal organizations seeking to exploit the standard marijuana supply chain. Criminal attacks can be:

- Front-end frauds – exploiting openings at point [1];
- Cyber-attacks on the main commercial chain – producing leaks at points [2] through [12];
- Sales suppression fraud – exploiting insecure transactions at point [10]; and

We will develop these frauds and explore their prevention in sequence. By and large, the prevention mechanisms (with the exception of the first) have been developed and perfected in VAT regimes. The reason is simple. Government monitoring of VAT compliance and government monitoring of the marijuana supply chain both involve securing accurate records of transactions as goods pass among multiple unrelated entities in close to real-time. Fraud prevention comes from rapid risk assessment and near immediate detection of unrecorded or illegal transfers. The following diagram (Figure 5) summarizes the fraud vectors in the basic marijuana supply chain.
The following discussion presumes the METRC system is used to monitor marijuana flows, but the same analysis would apply just as easily if another track and trace regime, like MJ Freeway, was used.

Front-end frauds – criminal exploitation at point [1]

Supplies escape METRC’s track and trace at the front end when cultivation is for personal use. In theory, personal use means there is no supply chain for METRC to control. It is pointless to require a personal use cultivator to attach an RFID chip to each plant, record daily inventory, and identify any movement of the plant or plant products to another entity. In other words, METRC is not designed to control all physical flows of legalized marijuana. It is designed for control of large-scale commercial flows. When “home growth” is authorized, States exercise control over the person, not the plant.

Consider the following three examples of weak enforcement at the beginning of the supply chain. (1) Maine allows “home grown” medical and recreational marijuana at a residence (six plants, no more than three of which are mature). It also permits “home growth” on another person’s land as part of a cooperative (farm), where the State only requires that each plant at this location be tagged with a ticket that records the owner’s Maine driver’s license number. There is no track or trace of the plant itself. (2) Vermont has legalized medical marijuana and permits home growth. There is a requirement that growers of medical marijuana register and obtain a Registry Identity Card. Securing the ID involves a process whereby a doctor certifies need. A patient (household) can cultivate up to two mature plants (or four immature plants). There is no provision for local control by city ordinances. Everything is

---

29 Because Maine has decriminalized possession of (recreational) marijuana, these rules on home grown medical marijuana carry over to recreational use. The same occurs in Vermont.

30 22 M.R.S.A. § 2423-A(1)(B)
determined between the doctor and the State. California, uses METRC (unlike Maine and Vermont), but like Vermont and Maine, it sets a State limit for home grown marijuana. Unlike Vermont it allows “home growth” for medical as well as recreational use. In addition, the California home-grow limit is three times the limit in Vermont (six mature plants/ twelve immature plants), but even more troubling, California defers actual control (enforcement) to the locality.

By definition, “home grown” marijuana is outside of physical control systems. It is not integrated into METRC’s RFID controls in California, nor is it otherwise controlled in states that have no technology-based system. In each case, there simply is no track and trace system in place. For example, when the California Department of Food and Agriculture (CDFA), CalCannabis Cultivation Licensing was contacted about the application of METRC or a similar system by small growers for personal use, the response was:

The track-and-trace system, METRC, is only for annually licensed commercial cannabis cultivation. CalCannabis Cultivation Licensing does not have regulations for personal use. You will need to contact your local jurisdiction regarding personal use.

The answer is effectively the same in Vermont. Lindsey Wells, the Marijuana Program Administrator for the Vermont Department of Public Safety indicates that there is no track and trace system in place for “home grown” marijuana. There is a statutory limit for the number of cultivated plants, and a requirement that the location of cultivation be disclosed. Ms. Wells indicated:

If you want to cultivate marijuana you would need to register as a patient or caregiver for a specific patient. We do not track the number of plants patients and/or caregivers cultivate. We only require applicants to inform us of where they would be cultivating.

States that have legalized both medical and recreational marijuana normally allow home growth. The norm is six plants per person (Massachusetts, Colorado, Maine, and Washington). The limit can be higher, for example twenty-five (Alaska) or lower, four (Oregon). Prior to

32 CA HSC § 11362.5.
33 Personal e-mail by the author, responded to by CalCannabis Cultivation Licensing staff (January 30, 2018) on file with author. Details and supporting regulations in the e-mail reference more information on complying with track-and-trace at Title 3, Division 8, Chapter 1 as follows: https://static.cdfa.ca.gov/MCCP/document/Proposed%20Emergency%20Regulations%20Final_12.12.17.pdf
34 Personal e-mail communication from Lindsey Wells to the author (February 1, 2018) on file with author.
35 Robert Bergman, I Love Growing Marijuana, (“The Alaska Constitution’s right to privacy act allows growers to cultivate 25 plants in a private residence for personal use. However, cultivating more than 25 cannabis plants in Alaska is a Class C felony. A fine up to $50,000 and 5 years in prison can be imposed.”) available at: http://www.ilovegrowingmarijuana.com/marijuana-laws-alaska/
36 Alaska allows 25 plants AK Const. Art. 1, §22, but AS § 17.38.020 limits this to six plants with no more than three flowering, and twelve within a single dwelling with no more than six flowering; California allows six plants, H.S.C. § 11362.2(b); Colorado allows six plants per person and twelve plants per residence C.R.S.A. Const. Art 18
June 8, 2017 Colorado allowed individuals to home-grow 99 plants. In California there is no limit on the amount of medical marijuana that can be home grown.

Six plants may not seem significant, but the annual revenue stream for a good cultivator (farmer) who does not consume his output may be a financially significant revenue source if his production makes it to the black market. In Maine legislation allows a grower to cultivate 36 plants at any one time – six for him/her and the same for another five “patients.” At average yield, these plants will bring in 40 to 50 pounds each 10-week cycle, or 200 to 250 pounds annually. Medical marijuana currently retails for $1,600 per pound, giving it a black-market cash return of between $320,000 and $400,000 for 36 plants.

It is no wonder that Colorado saw criminal activity in the marijuana market when it allowed individuals to “home grow” up to 99 plants (16.5 times higher than the individual norm of 6 in most states). Thus, the annual revenue stream of someone cultivating at the Colorado personal limit is roughly $880,000 to $1,100,000.

Preventing front-end leakage of marijuana to criminals

The only effective way to stop front-end leakage [1] is to do what ten (10) states and the District of Columbia have done – prohibit “home grown” marijuana for medical or recreational use.

The downside to this measure is that individuals with serious illnesses do not have access to inexpensive marijuana. This is a pricing issue. Italian and Canadian health authorities solved it by authorizing the production of medical marijuana on behalf of those patients at secure

§14, (4)(a)(II); C.R.S.A. § 25-1.5-106; Maine allows an individual to possess, grow, cultivate, process or transport up to 6 flowering marijuana plants, 12 immature plants and unlimited seedlings, and possess all the marijuana produced by the plants at the adult’s residence 7 M.R.S.A. § 2452 (1)(C); Massachusetts allows six plants per person and twelve per household M.G.L.A. 94G § 7(2); Nevada allows twelve plants N.R.S. § 453A.200; Oregon allows four plants O.R.S. § 475B.245 (1)(a); Washington allows six plants R.C.WA 69.51A.210(1).

37 HB 1220 reduced the 99-plant limit to 12.

38 Robert Bergman, Growing Marijuana in California, (“California weed growing laws are unique because there are actually no official limits on how much weed can be grown. If you have a medical need to grow marijuana, the state assumes that you will grow as much as you need.”) available at: http://www.ilovegrowingmarijuana.com/growing-marijuana-california/

39 Colorado’s 99 plant limit created an environment for criminal activity. For example, Megan Schrader reported in the DENVER POST on March 7, 2017 that:

Most recently, a 230-plant grow in Pueblo was busted in a residential neighborhood. In September, a raid of a dozen southern Colorado homes broke up a network holding 22,400 pounds of plant and product that was marked to be shipped out of state.

available at: https://www.denverpost.com/2017/03/07/shut-down-colorados-gray-marijuana-market/

When Maine considered the legal limit for “home grown” marijuana Andrew Freedman, the former director of Colorado’s regulatory agency, told Maine’s Marijuana Legalization Committee that, “Unlicensed residential grows were one of Colorado’s biggest, and most dangerous enforcement problems. Some landowners were growing huge marijuana crops disguised as personal grows and selling the overage at high profits in nearby states where marijuana remained illegal.” Penelope Overton, Lawmakers Propose Limits on Size of Marijuana Home Grow, PRESS HERALD (August 3, 2017) available at: https://www.pressherald.com/2017/08/03/lawmakers-propose-limits-on-size-of-marijuana-home-grow/.

In both instances, the government kept cost down by using advance growing technologies. Italy and Canada secure the front-end of the supply chain. See Figure 6 (below).

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 7 (below). If successful, a malicious cyber-attack would open up each “leakage point,” [2] through [12] in the main commercial chain. Control collapses.

---

41 In Italy home grown medical marijuana is illegal. Expensive supplies are imported from the Netherlands. As a result, the government announced that the Italian Army would begin growing marijuana at a pharmaceutical plant in a secure facility in Florence.

"The aim of this operation is to make available to a growing number of patients a medical product which isn't always readily available on the market, at a much better price for the user," [said] Col Antonio Medica.


All track and trace systems are designed around a centralized ledger.\textsuperscript{42} They endeavor to be permanent (immutable).\textsuperscript{43} 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.\textsuperscript{44} 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 system, the State was terminating its five-year contract (after less than two-years) effective November 1, 2017. Nevada switched to METRC.\textsuperscript{45}

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


\textsuperscript{43} 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/metr-coming-learning-basics-metrc-compliance-part-ii/

\textsuperscript{44} 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-industys-vulnerability-to-hacking-7895250

\textsuperscript{45} On November 29, 2017 California adopted METRC, making METRC arguably the largest track and trace system deployed in the US.
… 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.\(^{46}\)

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\(^{47}\)
- **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.\(^{48}\)

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 8 diagrams an MJ Freeway installation.

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.


\(^{47}\) 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/

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 too keen to hear this case has been referred to the FBI and they are potentially digging through this information. ⁴⁹

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 …”⁵⁰ If there was no ransom demand, no stolen data, and as of today, no one held accountable,⁵¹ 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?52

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 Cooperation Council (GCC) are designed for distributive ledgers, or blockchain compliance.53 The same is true of the five states of the East African Community (EAC).54

Blockchain creates a robust, secure, (fully or selectively) transparent55 distributive ledger.56 The technique is revolutionary. Blockchain is a software protocol based on

---

52 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/
53 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).
55 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.
56 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
cryptography, devised in 2008, and announced simultaneously with its most famous application – Bitcoin.\textsuperscript{57}

Bitcoin (an application) is often confused with blockchain (a form of distributed ledger technology).\textsuperscript{58} 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 that external data sources connect securely to the blockchain and allow smart contracts\textsuperscript{59} within the blockchain to communicate with external resources on their own.\textsuperscript{60}


\textsuperscript{59} 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.

\textsuperscript{60} 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, \textit{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 distributor upon the blockchain confirming the transfer of marijuana from the cultivator to the distributor.
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.61

Blockchain technology is nearly trustless.62 In the sense that it does not require centralized third-party verification.63 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 chain.64 The consensus mechanism can be adjusted or molded to fit specific applications.65 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-sal 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.

62 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
63 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.
64 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.
65 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.
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. HyperLedger Fabric is the preferred blockchain platform. 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. Their identities are registered and verified with a central registry service inside the system.

---

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

67 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 Fabric 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. There is a private blockchain project (Nuvus) that aims to be the global exchange for the cannabis and hemp industry. They also plan on using several versions of Hyperledger, including Hyperledger Fabric, to create a marijuana supply chain transaction verification system. John Verghese, Terry Gardner, Dali Kranthor, Sam Talari, Nubus – Cognitive IoT Artificial Intelligence Cannabis & Blockchain Merging the Fastest Growing Global Industries (Singular Universal Truth), available at: https://www.nuvus-iot-whitpaper-English.pdf.

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):

- **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 of the channel. This is accomplished by endorsing 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” 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.”
  - 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.

- **Peers** – are nodes that execute, and maintain a ledger of transactions. There are two roles for a peer – endorser 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. 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:

---

69 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://fabricstdocs.readthedocs.io/en/latest/glossary.html](http://fabricstdocs.readthedocs.io/en/latest/glossary.html).

70 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.

71 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.

72 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.

73 Double send: Refers to the transaction-proposal not already being “committed” to a block.

74 Node: An individual entity in the blockchain network. Any entity (node) is required to maintain a member identity on the network.

75 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 endorses into a transaction that is submitted for ordering, validation, and commit.

76 Endorsers: Refers to the process where specific peer nodes execute a chaincode (smart contract) transaction and return a proposal response to the client application.

77 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 Fabric Glossary](http://hyperledgerdocs.readthedocs.io/en/latest/glossary.html), at Endorser and at Committer, available at: [http://hyperledgerdocs.readthedocs.io/en/latest/glossary.html](http://hyperledgerdocs.readthedocs.io/en/latest/glossary.html)
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 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. If both checks are passed, the block is committed to the ledger, and the state updates for each transaction as reflected in the database.
- 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 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 are a collection of network entities that perform the ordering service – ordering transactions into blocks 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.

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:

---

78 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.

79 Read is a query to verify the status of something in the ledger. Write is to make a transaction in the ledger.

80 State here is used to refer to the current state data that is stored in the blockchain.

81 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.

• 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 9 (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. 83

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 circle). Under the hypothetical marijuana blockchain represented in Figure 9 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. 84 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 blocks according to the network’s ordering implementation. 85 The OSNs

---


84 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.

85 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 9 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 match closing times.
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 9 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.  

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

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.
In this illustration the marijuana blockchain is developed by the states. The blockchain could be started by one state, 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, a group working to bring together the cannabis industry, and the Congressional Cannabis Caucus about using blockchain to regulate marijuana.

Sales suppression fraud – exploiting insecure transactions at point [10]

At the retail level the MJ Freeway or METRC software essentially functions as a marijuana-industry-specific point of sale (POS) system. It is common in retail for different industry sectors (restaurants, hotels, convenience stores, or gasoline stations) to have market-specific POS systems that are molded to fit the unique characteristics of their trade. The systems created for the marijuana industry differ only in that they have “… [an elevated] level of sophistication … [with] more technology than almost any industry out there.”

---

88 John Authers, Authors Note: Tough Times for The Onion (Premium) (February 8, 2018) available with premium subscription at: https://www.ft.com/stream/837baba6-b895-3123-9bd7-0553f6888b9
90 Id.
Mark Goldfogel created the first marijuana-specific STS inventory management/POS system as the co-founder of MJ Freeway. According to Goldfogel, it is next to impossible to find comparable systems in any other industry, because only in the marijuana trade can the sale to a final consumer precisely identify the commercial trail that a product took to get to market. He indicates:

Every batch of cannabis sold in Colorado has a batch number that tracks back to a specific plant and the nutrients that were added to it. The vehicle that carried the plant material and the candy bars that were made from its trim have all been accounted for.

In this industry, when a dispensary enters an item into their inventory, it appears on Weed Maps, Leafly, and many other social media sites. Very few other industries offer real-time social media inventory sharing, and none were doing it four years ago. This is technology at its greatest — especially when it works!

And yet, with all this technology at its disposal, the marijuana trade remains a cash-only industry. This is entirely the result of the federal Drug Enforcement Administration classification of marijuana as a controlled substance, which in turn places banks and other financial institutions, at risk of violating federal anti-money laundering statutes, the unlicensed money­remitter statute, and the Bank Secrecy Act.

Soon after the DOJ issued the now rescinded eight-point guidance under the Controlled Substances Act (CSA), the Financial Crimes Enforcement Network (FinCEN) issued companion eight-point guidance under the Bank Secrecy Act (BSA). FinCEN identified the due diligence that financial institutions must undertake when dealing with marijuana-related businesses. The FinCEN guidance has not been rescinded. Banks must:

1. verify with appropriate state authorities that the business is licensed and registered
2. review submitted license application and related documents
3. request information about the business and related parties from state licensing and enforcement authorities
4. demonstrate comprehension of normal and expected activity of the business – products, types of customers, etc.
5. engage in ongoing monitoring of public sources for adverse information re: business and related parties
6. perform ongoing monitoring for suspicious activity and “red flags”
7. periodically update this information (with frequency to be “commensurate with the risk”)
8. provide consideration of whether the marijuana-related business either implicates a Cole Memo priority or violates state law.

---

91 18 USC §§ 1956-57.
92 18 USC §§ 1960.
93 31 USC § 5318.
In addition, after following the eight-point guidance, there are three categories of Suspicious Activity Reports (SARs) that must be submitted when dealing with a marijuana-related business. They are a *Marijuana Limited SAR*, the *Marijuana Priority SAR*, and the *Marijuana Termination SAR*.95

The assessment of the Association of Certified Anti-Money Laundering Specialist, is that this creates a situation where:

[W] hen deciding whether or not to offer financial services to marijuana businesses … members of the financial industry feel the odds are against them, because [even after they files reports] they could still be held accountable, criminally and civilly, if their marijuana business clients were found to have violated the law. … [F]inancial institutions feel they are held to a higher degree of scrutiny by federal regulators if they accept legitimate marijuana businesses as clients; thereby running the risk of their institution’s rating being downgraded. For these reasons, many financial institutions have refused financial services to marijuana businesses.96

As a result, “[m]ost cannabis businesses do all of their transactions in cash …”97 An estimated 70% of cannabis businesses have no bank accounts,98 most marijuana businesses do not accept any credit cards,99 and the common advice from accountants is to “keep the cash

95 *Id.*, The financial institution should file a “*Marijuana Limited*” SAR if, based on its customer due diligence, it has determined that the business neither implicates a Cole Memo priority nor violates state law. The report should contain identifying information (names and addresses) of the subject and related parties, as well as a narrative section specifying that the sole reason for filing is the marijuana-related nature of the business and that no additional suspicious activity has been observed. The institution’s responsibilities do not stop there; it must also file continuing activity reports with the same information, as well as details about all deposits, withdrawals, and transfers connected to the account since the previous filing.

The financial institution should file a “*Marijuana Priority*” SAR if, based on its customer due diligence, it holds the reasonable belief that the business implicates a Cole Memo priority or violates state law. The report should contain “comprehensive detail” about the subject and account: identifying information (names and addresses), details regarding the implicated enforcement priorities, and detailed financial records of the transactions involved in the suspicious activity.

The financial institution should file a “*Marijuana Termination*” SAR if it deems it necessary to terminate the relationship with the marijuana-related business in order to be in compliance with its anti-money laundering program. The institution must provide a narrative noting the basis for the termination, and if possible is urged to use Section 314(b) voluntary information sharing to alert the business’ new financial service provider of potential illegal activity.


99 Sophie Quinton, *Why Legal Marijuana Businesses Are Still Cash-Only*, GOVERNING STATELINE (March 22, 2016) available at: [http://www.governing.com/topics/finance/sl-marijuana-businesses.html](http://www.governing.com/topics/finance/sl-marijuana-businesses.html) (noting a small trend at the very end of the Obama administration in Denver, Colorado where a few local banks were beginning to accept deposits from marijuana-related businesses).
under your mattress.” As Stuart Leavenworth notes however, all-cash businesses and technology-based tax frauds go hand-in-hand.

Example: The State of Washington

The State of Washington presents a classic example of where technology-based sales tax fraud is a known problem in cash-based businesses (notably restaurants). Washington also has, far and away, the highest tax on marijuana in the country. Given that Washington collects 47.3% of its revenue (not including local government taxes) from the retail sales tax, and that technology has been the backbone of the State’s economy for years, one would expect that ECR/POS system security measures would be mandatory and abundant. But, Washington has nothing.

Washington knows it has a problem. The Washington Department of Revenue (DOR), Legislative Liaison, David Duvall, indicated in House Hearings on February 2, 2018 that Washington lost in excess of $1,000,000,000 over the previous four-year period from Electronic Sales Suppression (ESS) frauds. The DOR projected future losses of $1,565,764,000 through FY 2023.

The most common types of sales suppression technology are Zappers and Phantomware programming. In some instances, sales suppression is a personal (hands-on) service offered by installers or ECR/POS sales representatives, that is, Sales Suppression as a Service or SSaaS. Recently suppression technology has entered the Dark Cloud, a fully automated

---

100 Leavenworth, supra note 97.
101 Leavenworth, supra note 97 indicates:
   Yet for government agencies, it is harder to track sales from all-cash businesses than it is for those who rely on credit cards, and it becomes tougher still when those businesses can’t use banks. To pay their taxes in Sacramento, some 30 city-approved marijuana shops have to stuff cash into backpacks and duffel bags and haul it to a set location each month, kept secret for security reasons. This paragraph expressly links to an earlier tax fraud article that makes this connection to electronic sales suppression and the use of Zappers in Quebec. Stuart Leavenworth, That Sales Tax You Pay on your Meal? Some Restaurants Keep It, Using Illegal ‘Zappers,’ MCCLATCHY DC BUREAU (December 6, 2017) available at: http://www.mcclatchydc.com/news/nation-world/national/article188195589.html
104 Washington States House Finance Committee Working Session: Sales Suppression (February 2, 2018) at time mark 4:40, available at: https://www.tvw.org/watch/?eventID=2018021039;
107 Richard T. Ainsworth, Sales Suppression as a Service (SSaaS) and the Apple Store Solution, 73 STATE TAX NOTES 343 (August 4, 2014)
manipulation of sales data that (physically) takes place off shore and uses internet-based data transfers.\textsuperscript{108} If ESS is present in Washington’s marijuana supply chain, it is most likely Dark Cloud ESS.

There are no reported cases of Zappers, Phantomware, SSaaS, or Dark Cloud functionality deployed within the legalized marijuana supply chain in Washington, or in any State, but all of the warning signs are up and flashing. Marijuana is a high value/low volume good, being sold almost exclusively for untraceable cash, within a high-tax, technologically sophisticated commercial environment that has traditionally been closely associated with organized crime. If we assume that ESS devices are installed or operational in Washington State’s marijuana dispensaries as they are in an estimated 30% or more of its restaurants,\textsuperscript{109} then what would this fraud look like?

\textit{Fraud Patterns}

A marijuana dispensary is like a normal retail establishment. It can sell both taxable marijuana and regularly taxable items (like business-name promotional T-shirts). Non-taxable items could be sold as well. ESS allows sales to be initially recorded in a POS system, a receipt issued, taxes imposed, and collected, but then have certain transactions modified or eliminated after sales are completed. Fraud patterns could include:

- Selling recreational or medicinal marijuana to a consumer, collecting the tax, but having an ESS device delete the sale from the system;
- Selling recreational marijuana to a consumer (taxed at a 47% rate), but having the ESS device change the sale from recreational to medicinal (taxable at 37% – that is, exempt from the retail sales tax);
- Selling recreational marijuana to a consumer (at a 47% tax rate), but having an ESS device change the sale from recreational marijuana to a taxable T-shirt sale (taxed at a 6.5% rate);
- Selling recreational or medicinal marijuana to a consumer (taxed at a 47% or 37% rate), collecting the tax, and recording the sale, but where the actual product comes from smugglers. In this pattern the smuggled inventory is un-recorded (that is, not included in earlier reports to the State). The ESS device will simply eliminate the entire transaction from the business records. The source of the smuggled supply can be one of the following:

---

\textsuperscript{108} The Dark Cloud is a term coined for this discussion. As with the Phantomware term, there comes a time in this analytical effort where an activity is becoming common enough that a new term is needed. A Dark Cloud is an anonymous internet business which accepts data transmission from ECRs or POS systems, manipulates sales data with pre-determined algorithms on a specified schedule, and then returns the data to the systems from which it came. Dark Clouds operate both on a regular schedule (daily, weekly, monthly) or on a real-time basis. They have appeared in the New York and North Carolina markets. There is no evidence of Dark Clouds operating in the State of Washington (yet). The term is unrelated to and unintentionally borrowed from the old Japanese action role-playing video game \textit{Dāku Kuraudo} developed by Level-5 and published by Sony Entertainment around 2000.

\textsuperscript{109} Depending on the jurisdiction, and the research study consulted, ESS is estimated to be present in 34\% (of Canadian), 50\% (of German – two studies), and 70\% (of Swedish and Slovenian) businesses. Richard T. Ainsworth & Robert Chicoine, \textit{Washington’s Problematic Sales Suppression Enforcement Regime}, \textit{STATE TAX NOTES} (forthcoming, March 19, 2018) at n. 3, 4, 5, & 6.
Excess “home grown” marijuana cultivated within-the-state, but outside of the METRC system;

Excess marijuana un-reported to the State, because it is part of the estimated 50% of cultivated plants that do not grow well and are deemed to be “discarded” at the farm level;

Excess marijuana un-reported to the State, because it is part of the estimated 35% of quality defects (“waste products”) cast off during the manufacturing process, and that are deemed to be “discarded” at the manufacturer level;

Smuggled excess “home grown” marijuana from another State, most likely from a State with a liberal limit on “home grown” marijuana (probably for medical use);

Smuggled marijuana from outside the US.

Solutions

ESS has the ability to turn the Retailer in the basic marijuana supply chain into a platform for illegal distribution. ESS allows legal and illegal marijuana to be sold side-by-side for quick cash.

There are well established solutions to ESS. The solutions are technology-intensive and can be adopted country-wide (see Rwanda\textsuperscript{110} and more recently Fiji\textsuperscript{111}) or limited to a specific industry (see Quebec’s security mandate in the restaurant sector\textsuperscript{112}). The solutions guarantee that all sales information reaches an independent ratification service, which provides the issuer with a response that digitally confirms the sales information, and which allows asynchronous verification of that sale. This process of sharing sales information data will occur regardless of outside circumstances. The verification service must be available at any time and at any place.

Stated another way, a well-designed anti-ESS system will contain at least the following eleven elements:

1. A POS system must produce a document (receipt or invoice) with sufficient transactional data to confirm the proper tax calculations;
2. The document must be safeguarded with an electronic signature produced by a secure element that uses encryption to confirm authenticity and is free from manipulation;
3. The secure element used for signing the document must be independent of the creator of the POS system’s tax calculation engine;
4. The secure element and invoice system must be available in any place and at any time;
5. The secure element and invoice system must work together smoothly, avoiding any delay in document production;
6. The document must clearly identify the issuer;


\textsuperscript{112} Richard T. Ainsworth & Urs Hengartner, \textit{Quebec’s Sales Recording Module (SRM): Fighting the Zapper, Phantomware, and Tax Fraud with Technology} \textbf{57 CANADIAN TAX JOURNAL} 715 (2009)
7. A simple document inspection must immediately provide payment information;
8. Simple inspections do not require authorized personnel or technical knowledge to verify encrypted data;
9. Authorized personnel will use a prescribed method to inspect the secure element from which data about all transactions can be extracted (in encrypted form);
10. Electronic journals (in human readable format) must be provided through the invoicing system (or the secure element);
11. Verification services will authenticate documents for authorized personnel and for the general public (at any time – most likely on line)

One of the most critical of these eleven elements is the third. The security provider should never be the same firm that provides the POS system. That means MJ Freeway should not be asked to secure the POS and invoice production aspects of its Leaf Data Systems. Franwell Inc. should not be asked to secure the POS and invoice production aspects of its METRC system.

There are a large number of examples where POS manufacturers that are developing apparently secure systems, are discovered to have embedded Phantomware in their systems or developed a Zapper that defeats their own visible security regime. Canada has a large number of these cases.

The Canadian example that impacts Washington immediately is the InfoSpec/Profitek POS and Zapper, which crossed the border from Vancouver around 2008. More disturbing than InfoSpec/Profitek is a case out of Brazil in 2006.

A Brazilian software company [AGM Consultancy and Systems Corporation, Ltd.,] was hired to design a certified POS system (Robot) for the government. The system was mandated for use by the business community. This trusted company, under government contract nevertheless developed and sold a Dark Cloud Zapper (Quanto) that manipulated its own POS systems from the Internet.

It is reasonably clear that without a first-rate, independent, transactional security system transmitting verifiable data back to the State in real-time, that the Retailer in the basic marijuana supply chain can easily become a platform for fraud. All the Retailer needs is:
a) an ESS device (Zapper, Phantomware, SSaaS, or the Dark Cloud) that works with its POS, and
b) a supply of marijuana (Black Inventory) that had escaped the State’s TAT or STS system.

---

113 Richard T. Ainsworth, *Sales Suppression: The International Dimension*, 65 AMERICAN UNIVERSITY LAW REVIEW 1241 (2016) (discussing the rise of InfoSpec/Profitek in Canada, audit and subsequent litigation by the Canadian Revenue Authority, followed by the same cycle of audit and litigation that is still going on Washington State).

114 *Empresa de JF burlava o fisco via computador HOJE EM DIA (A JF-based Corporation defrauded the tax authorities via computer TODAY BRAZIL)* (May 12, 2006) available at: http://www.fazenda.mg.gov.br/empresas/ecf/noticias/hojeemdia12052006.pdf (in Portuguese) (translation on file with author) (discussing *Operation Internet* which was an effort to shut down a Dark Cloud ESS regime by the State Tax Administration of Minas Gerais, a Brazilian State in the Southeast region - close from Rio and São Paulo).
The most likely scenario? Dark Cloud Zapper working with Black Inventory. See Figure 10 (below):

Is there a Zapper that works with one of the major TAT or STS POS systems? If there is, then the most likely candidate for a vulnerable system is MJ Freeway’s. Not only was the system hacked, beginning in December 2016 – leading to the cancellation of the Nevada STS contract – but the company’s source code has been posted on the open net for anyone to see.¹¹⁵

Washington has first-hand experience with glitches in MJ Freeway’s software. After MJ Freeway was selected in June 2017 to replace Florida-based BioTrackTHC, MJ Freeway’s software had too many bugs to become operational on the November 1, 2017 contract date. The transition to MJ Freeway in Washington needed two-month more months. BioTrackTHC, the firm that was being replaced, refused to assist Washington, claiming that they experienced data breaches after MJ Freeway gained access to the BioTrackTHC legacy system.¹¹⁶

In short, there is clearly enough confidential MJ Freeway code available to hackers, and there are continuing problems with security in the MJ Freeway’s product to make it reliable. It is not hard to imagine that someone could assemble the kind of Dark Cloud Zapper that AGM Consultancy and Systems did in Brazil in 2006. The risk is serious.

¹¹⁵ See text supra associated with notes 42 through 52.
¹¹⁶ Lester Black, State’s Pot Tracking Software Causes Headaches for the Legal Weed Industry, THE STRANGER (October 24, 2017) available at: https://www.thestranger.com/slog/2017/10/24/25490384/states-pot-tracking-software-causes-headaches-for-the-legal-weed-industry Patrick Vo, CEO of BioTrackTHC indicated, … two months ago [August, 2017], an e-mail was sent to multiple licensees offering to sell the raw data behind Washington, Pennsylvania, and Nevada’s recreational and legal weed markets. … proprietary data was shared in this e-mail that made it appear to show that Washington’s data had been hacked.
Washington needs to mandate an advanced real-time digital security regime comparable to that recently deployed in Rwanda and Fiji throughout the basic marijuana supply chain. Based on the system installed to resolve Washington’s first Zapper case involving a Settle restaurant, *State of Washington v. Wong*, Wash. Super. Ct., No. 16-1-00179-0, the cost would be roughly $10,000 to $15,000 per marijuana dispensary.

*Back end leakage [13] & [14]*

The state’s obligation to control both the *physical flows of legalized marijuana*, as well as the related *fiscal flows (the proceeds of legalized marijuana sales)* intersect dramatically at points [13] and [14].

Points [13] and [14] present the most obvious *physical leakage* opportunities in the basic marijuana supply chain. In a jurisdiction that has legalized both medicinal and recreational marijuana consumers can re-sell any excess medical marijuana they have purchased from a retailer [14] to a recreational user [13]. This leakage is incentivized when there is a tax difference between the two classes of marijuana. In jurisdictions that have only legalized medicinal marijuana [14], consumers with medical authorization can purchase and re-sell directly into the black market.117

The Tax Foundation noted this concern with respect to Massachusetts, which is planning to sell and tax recreational marijuana alongside un-taxed medicinal marijuana as of July 1, 2018. It observed:

Despite the changes to the tax treatment, medical marijuana in Massachusetts will remain untaxed. This has the potential to create problems for the state as it might keep some recreational marijuana in the gray market. For instance, people with medical cards might resell their untaxed marijuana to those without medical cards.118

These transactions will be *un-traced* and *un-tracked* by the Massachusetts METRC system. There is no RFID tag placed on medicinal marijuana when it is sold to a consumer, nor is there a daily marijuana inventory report filed by consumers. The same scenario plays out with recreational marijuana that is re-sold to underage users in states that have legalized recreational use.

Far more important however, is the fact that points [13] and [14] are the places where all the cash that sustains the entire marijuana supply chain enters the system. All *fiscal flows* start at [13] and [14].

---


118 Morgan Scarboro, *Massachusetts Increases Marijuana Tax Rate* TAX FOUNDATION (August 1, 2017) available at: [https://taxfoundation.org/massachusetts-marijuana-tax-increase/](https://taxfoundation.org/massachusetts-marijuana-tax-increase/)
FinCEN’s eight-point guidance under the Bank Secrecy Act (BSA) is the reason the States are dealing with so much un-traceable cash in the basic marijuana supply chain. The FinCEN guidance identifies the due diligence obligations that financial institutions have when dealing with marijuana-related businesses. This Obama era FinCEN guidance has not been rescinded by the Trump Administration. All the BSA Expectations Regarding Marijuana-Related Businesses rules are still applicable.

Proposed State Solutions

Physical flows. There are very few new proposals on how to solve the physical flow problems with consumer re-sales into the black market at points [13] or [14]. Traditional enforcement is universally applied. It is highly indirect. There is however, one high tech proposal is being advanced by 420 Blockchain.

The traditional approach is to conduct audits enforcing rules that limit the amount of marijuana an individual can possess. The audit however, is of the retailer that sells, not the consumer who buys the marijuana. It has proven difficult to audit consumers directly. The audit methodology is based around stings using undercover police at dispensaries.

The violation (by the dispensary) is colloquially called looping. Looping means that when multiple separate sales of marijuana are made to the same individual on the same day, the amounts sold can be aggregated. If that total exceeds the allowable limit an individual can legally possess, then the retailer is presumed to have known that it was selling the consumer more than the statutory limit for possession in a single transaction. An enforcement letter sent by the Colorado Marijuana Enforcement Division explains:

Sales that are structured as multiple, stand-alone transactions may be viewed by the [Marijuana Enforcement] Division as an attempt to evade quantity limitations on the sale of Retail Marijuana, resulting in the recommendation for administrative action.

---

119 See supra text and notes at notes 94 through 101.
120 BSA Expectations Regarding Marijuana-Related Businesses (February 14, 2014) (directly following up on the now-rescinded August 29, 2013 Cole Memo was itself followed by a second, and also rescinded Cole memo, Guidance Regarding Marijuana Related Financial Crimes on the same date, February 14, 2014) available at: https://www.fincen.gov/resources/statutes-regs/guidance/bsa-expectations-regarding-marijuana-related-businesses. The FinCEN guidance remains in place, and was not among the documents rescinded by Attorney General Sessions on January 4, 2018. See also: Lane Powell PC, FinCEN Retaining Bank Secrecy Act Marijuana Guidance – At Least for Now (January 11, 2018), indicating:

This morning, we received the following note from the FinCEN’s Resource Center:

“The SAR reporting expectations outlined in the February 14, 2014 guidance, FIN-2014-G001 remains in place. FinCEN will continue to work closely with law enforcement and the financial sector to combat illicit finance, and we will notify the financial sector of any changes to FinCEN’s SAR reporting expectations.”

121 Randy Robinson, Bitter Sweet: Denver Shuts Down 11 Dispensaries for Double-Dealing Weed, MERRY JANE (December 20, 2017) available at: https://merryjane.com/news/bitter-sweet-denver-shuts-down-11-sweet-leaf-dispensaries-for-double-dealing-weed (noting also that the investigation involved police officers purchasing 1 oz. of marijuana at a retail establishment, and then returning as many as 16 times in the same day to purchase additional 1 oz. of marijuana from the same budtender).
Acting on an investigation that lasted from December 2016 through September 2017, the Denver Police moved on December 14, 2017 to shut down 26 cannabis operations licensed under Sweet Leaf, one of Colorado’s largest dispensary chains, for looping. Colorado law limits the adults 21 and over to possessing only 1 oz. of marijuana at any one time.

It is not clear if criminal charges (with jail time) will be brought against the 13 arrested budtenders. Nor is it clear if this enforcement measure will actually prevent consumers from re-selling marijuana into the black market. This enforcement is only effective when all the marijuana is purchased from the same dispensary. It would not identify a consumer who bought an amount that was just under the legal limit for possession from multiple retail establishments. There are 20 dispensaries in Seattle. Avoiding enforcement through “stings” is not difficult.

420 Blockchain122 is proposing something different – a blockchain. Based in Boca Raton, Florida, 420 Blockchain is (allegedly) beta-testing (in Rhode Island and California) a blockchain solution to the frauds at [13] and [14] based on Augusta High Tech’s Framework HyperLedger,123 running on the Google platform. Although a system launch was expected in January 2018, there has been no public announcement about it or about the system’s workability.124

The thrust of the 420 Blockchain effort is to track the consumer who makes purchases so that a more comprehensive picture of possession can be measured. Michael Kramer, the CEO of 420 Blockchain, explains:

“Besides, if someone really wanted to circumvent the rules, they could simply buy an ounce at Dispensary A, then drive over to Dispensary B across town and buy another ounce. There’s no system in place to trace who buys what, when, or where.” Michael Kramer believes blockchains could prevent looping while taking the burden of memorizing everyone’s IDs off budtenders.125

But there is a natural extension to the 420 Blockchain proposal. The State could turn each dispensary into an AmazonGo store,126 collect this data on a state-wide basis, load it on a blockchain, and conduct risk analysis of consumers through artificial intelligence (AI). The analytics of the AmazonGo extension will be developed more thoroughly in a forthcoming paper

124 Randy Robinson, supra note 121.
125 Id.
126 The first AmazonGo store opening in Seattle Washington on January 21, 2018. The Amazon web site explains the concepts as follows:

Amazon Go is a new kind of store with no checkout required. We created the world’s most advanced shopping technology so you never have to wait in line. With our Just Walk Out Shopping experience, simply use the Amazon Go app to enter the store, take the products you want, and go! No lines, no checkout. (No, seriously.)

Our checkout-free shopping experience is made possible by the same types of technologies used in self-driving cars: computer vision, sensor fusion, and deep learning. Our Just Walk Out Technology automatically detects when products are taken from or returned to the shelves and keeps track of them in a virtual cart. When you’re done shopping, you can just leave the store. Shortly after, we’ll send you a receipt and charge your Amazon account.

Available at: https://www.amazon.com/b?node=16008589011
by Peter Dutz Manda, *Taxing Non-Cash Sales: Is Dynamic Taxation A Remedy for Tax Uncertainty?*\(^{127}\)

**Fiscal flows.** Even the AmazonGo solution, while it would provide an excellent record of the physical flows of registered marijuana through the retail dispensaries, will not overcome the hesitancy of the banking system to more broadly facilitate the marijuana supply chain. Any kind of banking account (checking or savings, business or personal), check clearing, credit or debit card services is restricted. Thus, even if AmazonGo dispensaries “worked,” the upstream supply chain would still be awash in cash.\(^{128}\)

There are proposals to set up a state marijuana bank (in California)\(^{129}\) or a credit union (in Colorado).\(^{130}\) In each instance the proposed institutions are having problems. To function as a bank under either permutation would require recognition by the Fed to gain access to deposit insurance, and wire transfer services. These banking connections are not easily negotiated when the customers are marijuana-related businesses. They are privileges not freely or fully granted. Evidenced by the *Fourth Corner Credit Union v. Federal Reserve Bank of Kansas City* litigation and settlement where banking access was granted provided the Fourth Corner Credit Union limited its engagement to businesses on the periphery of the marijuana trade.\(^{131}\)

**CALCoin**

Faced with a similar problem of large numbers of improperly tracked transactions along complex supply chains, where traces of the funds and tax payments passing from one party to the next were misstated, the EU VAT has begun to look at a VATCoin solution that utilizes a

---


\(^{128}\) Bob Blumenfield, LA City Counselor-Third District, in an Opinion article suggests that cash can be removed from the retail stores by adopting a program like the LA Transit Access Pass, a pre-paid card that can be re-loaded at a kiosk. *Opinion: On Marijuana, Removing the Cash, Adding Legal Clarity Will Make Our Communities Safer, LA DAILY NEWS* (December 2, 2017), available at: [https://www.dailynews.com/2017/12/02/on-marijuana-removing-the-cash-adding-legal-clarity-will-make-our-communities-safer/](https://www.dailynews.com/2017/12/02/on-marijuana-removing-the-cash-adding-legal-clarity-will-make-our-communities-safer/)


\(^{130}\) In May 2014 Colorado established a new class of financial institutions called a cannabis credit cooperative that would not have to maintain deposit insurance, but the Federal Reserve seems unlikely to approve them. Later the Colorado legislature authorized a credit union for the cannabis industry, but the Fed denied access to a “master account,” which is essential to transfer money. The National Credit Union Administration also refused to insure deposits. Even transporting funds known to have been derived from the distribution of Marijuana is illegal according to the Federal Reserve Bank of Kansas City. Sophie Quinton, *Why Marijuana Businesses Are Still Cash-Only, GOVERNING,* (March 22, 2016) available at: [http://www.governing.com/topics/finance/sl-marijuana-businesses.html](http://www.governing.com/topics/finance/sl-marijuana-businesses.html) However, after the Fourth Corner Credit Union sued the Federal Reserve a settlement was reached granting conditional approval if (a) they can secure insurance, and (b) the Fourth Credit Union agrees to focus of individuals and companies that support legalized marijuana, such as vendors like accountants and landlords. The *Fourth Corner Credit Union v. Federal Reserve Bank of Kansas City*, 154 F. Supp. 3d 1185 (D.Colo. 2016); vacated by *Fourth Corner Credit Union v. Federal Reserve Bank of Kansas City*, 10thCir. (Colo.) June 27, 2017

blockchain to allow detailed, real-time, tracing of funds throughout a supply chain. VATCoin is a limited purpose crypto-tax-currency. It is issued on demand by the government, used for limited-purpose payments, and convertible back into fiat currency only by the state that minted it.

The States that have legalized marijuana could do the same with a similar limited purpose crypto-tax-currency. It would be mandated as the only legal token/currency allowed to be exchanged for marijuana. For example, in California this digital currency might be called CALCoin (this denomination is used in the remainder of this discussion). In brief, the following example shows:

- Consumers securing newly minted CALCoins\textsuperscript{132} from the State Treasury;\textsuperscript{133}
- Consumers purchasing recreational and medicinal marijuana from a Retailer with some of the CALCoins (saving others in their digital wallet);
- Retailer using the CALCoins received to re-stock inventory with purchases from a Distributor;
- Distributor redeeming some CALCoins for cash and using other CALCoins to restock a specialty blend of marijuana from a Cultivator, and some infused brownies from a Manufacturer;
- Manufacturer using some of the CALCoins received to secure third-party Lab services, other CALCoins to pay for more marijuana ingredients for infused products, and using the remaining CALCoins to directly pay State Income Taxes due;
- Lab redeeming the CALCoins it received to directly pay Local Property Taxes due;
- Cultivator redeeming some of the CALCoins it received to pay Federal Income Taxes (it is unlikely that the federal government would accept CALCoins directly for a tax payment, making conversion to CASH necessary before paying federal taxes) and other CALCoins are held in the Cultivator’s corporate wallet for later use;
- CALCoins that are redeemed at the State Treasury are transferred back to the State and destroyed. CALCoins are not a recognized investment vehicle, nor are they a substitute for fiat currency. They cannot be transferred other than in a marijuana-related activity, to a registered marijuana establishment.

In each case the diagram indicates that a CALCoin is \textit{not in use} by coloring in the coin (either blue to represent origination with the recreational consumer, or red to represent origination with the medicinal consumer). The diagram indicates the historical passage of a CALCoin \textit{through} an entity as a white coin edged in dashes.

There will be no cash hoard in any marijuana establishment. There may be digital wallets which may contain a large amount of CALCoins, but hacking the digital wallet would be pointless. The CALCoins contained there (a) have a digital history and would be immediately identify them as stolen CALCoins by the Artificial Intelligence (risk analysis) engine that is scanning all CALCoin transactions, and (b) CALCoins can only be used in another marijuana-

\textsuperscript{132} The dollar conversion rate in the diagram is $10.00 = 1$ CALCoin. Other conversion rates are possible. Fractional CALCoins are also possible.

\textsuperscript{133} Unlike the proposal of LA City Counselor Bob Blumenfield, CALCoins are not stored on anonymous “gift cards” or the LA Transit Access Pass (TAP). It is important to associate each CALCoin with the individual who first purchased the newly minted coin.
related purchase with a certified (registered) marijuana establishment, so it is impossible to escape the AI’s risk analysis. Used CALCoins will not be re-issued after redemption. They will be destroyed. They only have value within the marijuana commercial chain. When they leave the supply chain they become useless. Figure 11 (below) diagrams the above text.

**CALCoin Blockchain**

CALCoin lends itself naturally to blockchain. Each digital transfer of CALCoin is recorded, registered with the California Treasury. After the first transaction where a consumer acquires CALCoins, the California State Treasurer will broadcast the transaction to the nodes. [The California Treasurer will effectively be saying “I give the right to spend certain CALCoins to the person who owns the corresponding private key.”] The data for this (and all subsequent) transactions involving this CALCoin is stored in a chain of ownership in the cloud. Anyone can have access.

CALCoin’s blockchain follows the BitCoin model. The resulting distributive ledger will be a public, not a private blockchain (unlike the blockchain that was proposed for the main commercial chain). The consensus mechanism for the CALCoin blockchain however, should not be the cumbersome and expensive proof of work used by BitCoin. A new consensus mechanism for public ledgers developed by MIT Professor Silvio Micali seems ideal for the CALCoin

---

134 The CALCoin protocol will be based on asymmetric cryptography. Public key cryptography allows you to hand someone a public key and use the corresponding private key to prove the ownership. Using the associated private key, you can sign a message and other people can verify that you own the private key by using your public key.
application. It is called ALGORAND, and the details of its application are set out in
ALGORAND: The Efficient Public Ledger.\textsuperscript{135} Micali also describes Algorand on YouTube.\textsuperscript{136}

Micali calls his approach \textit{cryptographic certification}. The design is to cryptographically select a set of \textit{verifiers} who would collectively be in charge of creating the “next” block. This small group of people are selected randomly and suddenly in a way that is provably immune from manipulation. It is unpredictable until the last moment.

No person selects the group, it is done entirely by hash. Micali’s approach “… requires a negligible amount of computation, and generates a transaction history that does not fork with overwhelmingly high probability. In fact – over a million years statistically.”\textsuperscript{137} Kastelein explains:

The group [committee] decides the next block by a redesigned Byzantine Agreement where a leader is picked randomly from the group. If he’s a bad choice an agreement will not be able to be made. Everyone is forced to agree on nothing. Zero progress. With a bad leader, you just don’t get a block and if you have an empty block you get no money.

That’s the game theory.\textsuperscript{138}

The reward for performing the verification function in ALGORAND is a percent of the block transaction which is awarded to the group of verifiers. In the case of CALCoin the reward will be in CALCoin, which will make the entire system heavily California-based, because receiving an allocation of CALCoin in a digital wallet will only have value in California where CALCoin can be exchanged for marijuana. This is the preferred outcome. It is a blockchain enforced by California citizens, that assures that financial flows in the California marijuana market are secure (not leaking out to organized criminals.)

Algorand is being commercialized by a joint venture Toda-Algorand Corp.\textsuperscript{139}

\begin{thebibliography}{9}
\bibitem{135}Available at: https://arxiv.org/pdf/1607.01341.pdf
\bibitem{136}Silvio Micali, \textit{ALGORAND: A Better Distributed Ledger, ASSOCIATION FOR COMPUTING MACHINERY (ACM)} (November 7, 2017) available at: https://www.youtube.com/watch?v=_nQE_HAGlmM
\bibitem{138}\textit{Id.}
\bibitem{139}Charles Brett, Toda-Algorand Platform Scalable to >3M tps and >4B users? ENTERPRISE TIMES (July 31, 2017) available at: https://www.enterprisetimes.co.uk/2017/07/31/toda-algorand-platform-scalable-to-3m-tps-and-4b-users/
\end{thebibliography}

Toda-Algorand Corp. aims to deliver a decentralized transaction platform which combines the ledgerless ease and scalability of cash payment systems with a flexible ledger-based technology. The platform will enhance and incorporate features of existing financial payment systems.

The design of the Toda-Algorand platform aspires to a throughput of over three million confirmed transactions per second serving more than four billion users, all securely. It will combine:

\begin{itemize}
\item the decentralized ledger blockchain authored by Turing Award winner Silvio Micali
\item the secure decentralized on-chain ledgerless TODA protocol co-authored by Toufi Saliba.
\end{itemize}
CONCLUSION

The issue throughout this analysis has been trust. Once marijuana is legalized by a State, how can systems be put in place so that the federal government trusts that the State is able to monitor and control the physical flows of marijuana as well as the related fiscal flows within the basic marijuana supply chain? Given the variances in the state-by-state legalization regimes and the related tax and enforcement rules, there are also deep inter-state trust concerns echoing these federal concerns.

The near universal answer to these concerns has been the adoption of third-party track and trace technologies, and to require daily inventory and product movement reporting. The problem is that these systems leak and are vulnerable to hackers. Hackers may be the most serious threat. There is more than enough source code out on the net for fraudsters to be able to design Zappers that will work in the Dark Cloud to suppress (B2C) sales, and to corrupt upstream (B2B) records.

Solutions to this kind of fraud are well developed in the EU (and other) VAT jurisdictions. VATs are supply-chain-based taxes. We know what is needed to block VAT frauds. It works. There is a global track record of successes. What the US needs are third-party security systems where the secure element used for signing documentation is (and must be) independent of the creator of the inventory management/POS systems that monitor the physical and fiscal flows of the supply chain. America may have a blind spot here, because our tax system has negligible experience with VATs. We can learn from the EU.

Trust however, requires more than a technological black security box. Trust has a visual as well as a technological component. For this reason, two blockchains, one private (dealing with physical flows of marijuana), the other public (dealing with the financial flows related to marijuana sales) have been proposed. Blockchains are “trust machines,” and the legalized marijuana trade needs to build trust. 140 This is how to do it.

A sketch has been provided of the four major criminal attack vectors in this field indexed to fourteen major leakage areas. The major frauds and their proposed solutions are:

3. Sales suppression fraud – exploiting insecure transactions at point [10] – solved with anti-ESS security (an independent digital ratification service that confirms sales information and allows asynchronous verification); and

It is the strong belief of these authors that these frauds need to be addressed systemically (as a whole supply chain problem) not locally (targeting only specific points of leakage). The discussion of sales suppression at point [10] classically illustrate how a single point of leakage can become a platform for wide ranging frauds pulling resources from many weak spots in the supply chain.

This analysis also offers extraordinary enforcement opportunities. For example, the CALCoin blockchain not only provides California authorities with a tool to identify where frauds are occurring, it would allow them to terminate an individual’s or a business’ ability to buy or sell marijuana by immediately extinguishing all CALCoins in their possession, as well as their ability hold or acquire more. This would effectively remove problematical parties from the supply chain.

Adopting CALCoin is not going to automatically bring success. This is because FinCEN has determined that any administrator or exchanger of virtual currency is a Money Services Business (MSB). Also, according to FinCEN, any MSB is a “financial institution,” and this makes it subject to the Bank Secrecy Act. Thus, if the State of California adopted the CALCoin solution, the State would need to comply with all federal AML-requirements (unless a limitation or exemption applies).

---

141 Peter D. Hardy, David L. Axelrod, Marjorie J. Peerce, Terence M. Grugan & Andrew N. D’Aversa, FunCEN Letter to US Senate Committee on Finance Purports to Thread Needle of Potentially Competing Jurisdictions by Regulators over Cryptocurrencies, MONEY LAUNDERING WATCH (March 8, 2018) available at: https://www.moneylaunderingwatchblog.com/?utm_source=Ballard+Spahr+LLP+-+Money+Laundering+Watch&utm_campaign=943c4c5d8c-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_790b46fdeb-943c4c5d8c-73334677