4-30-2020

Blockchain Technology And The IRS: How The Use Of Blockchain Technology Could Interfere With A Taxpayer's Privacy Rights

Michelle Yang

Michelle Yang
Blockchain and the Law
April 30, 2020

Blockchain Technology And The IRS: How The Use Of Blockchain Technology Could Interfere With A Taxpayer's Privacy Rights

I. Introduction

Blockchain technology has introduced myriad ways to offer transparency, security, and efficiency in our everyday activities. As is the case with most technological innovations, an invention that brings convenience to its consumers also tacks on a host of unintended consequences. It has shown potential benefits for humanitarian movements, such as preventing global pandemics, as well as the mundane tasks, such as filing tax returns.

Using blockchain technology to file a tax return would be successful if the taxpayer inputs his/her income, assets, expenses, etc. onto an IRS blockchain. This immutable ledger would then be reviewed by the IRS. It would then be imperative for the IRS to access the different blockchain databases that identify that taxpayer's assets and liabilities. For example, if a taxpayer owns a home, the IRS would access and view the land registry database to verify that the information the taxpayer provided was accurate. This ability to access the different databases, some that would contain considerably sensitive information, could pose a privacy problem. This paper will explore how the IRS' use of blockchain technology could interfere with a taxpayer's privacy rights and whether the threat stops there.

We will examine the benefits and dangers of implementing blockchain technology within the IRS framework. In the context of filing and reviewing tax returns, implementing blockchain technology within the tax industry could soften the relationship between the government, particularly with the IRS, and the taxpayer with speedier refunds, more efficient communications, and a uniform effort to deal with controversy more effectively. Part II will provide a brief background on the pros and cons of using blockchain technology to file tax returns. Parts III and IV will focus on two of the current laws governing cyberspace technology and how each law would apply to blockchain technology within the IRS. In doing so, we will be confronted with problems that the convenience of technology would bring. Part V will then contemplate possible solutions. In conclusion, blockchain technology is a tool that should not be dismissed nor interpreted as an easy fix.

II. Background

Proponents can highlight efficient transactions between the taxpayer and agency, which means exemptions could be applied automatically and taxpayers could then receive their refunds more quickly. Smart contracts could also trigger payments or refunds promptly and more accurately. Audits would use up fewer resources, and the transparency of a block would create productive communications between the taxpayer and the agency during the audit. The opportunity for tax fraud or evasion due to the immutability of the blockchain would be limited since the taxpayer would be held more accountable from the transparency between the taxpayer and the agency of the self-reported information.

Opponents of this technology, however, would be quick to point to the vulnerability of each taxpayer's PII (personally identifiable information[1]) on a shared block. Skeptics may also emphasize the impracticality of adopting this technology across the various industries. Kem Musgrove, Chief Information Officer of California's Franchise Tax Board, shares that despite promises of any new technology, it is generally difficult to staff the agency around such new

[1] PII (personally identifiable information): information that can be used to distinguish or trace an individual's identity, either alone or combined with other information that is linked or linkable to a specific individual. IRM 10.5.1.2.3 (09-24-2019).

technology simply because not enough people are yet experts in the field[2]. Additionally, there is a protective use requirement that is in place to mitigate risk of new technology. This requirement establishes a 2-year minimum that prevents the agency from becoming beta testers, while determining whether the new technology would help or hinder the agency. Musgrove, however, finds optimism in the possibility and practicality of blockchain technology despite its potential for slow traction. If more taxpayers and staff were proficient with blockchain technology, implementing the technology within the context of filing and reviewing tax returns would be more seamless and in turn, beneficial.

III. The CFAA and Its Problems

In addition to the practicality of implementing the technology, there are very few federal privacy laws currently in place that question the trustworthiness of blockchain technology. For example, the Computer Fraud and Abuse Act (CFAA) was enacted in 1986 in response to the growing number of computer-related crimes that went unpunished. CFAA makes "whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer . . . and by means of such conduct furthers the intended fraud and obtains anything of value" criminally liable[3]. Although this law articulates the intent to punish malicious hackers, it has unintentionally indicted those without the intent to defraud.

In *United States v. Swartz*[4], Aaron Swartz was charged with breaking-and-entering for downloading academic journals in excess from JSTOR[5] by using a guest account issued to

[2] Telephone Interview with Kem Musgrove, Chief Information Officer, California Franchise Tax Board (March 13, 2020).
[3] *AtPac, Inc. v. Aptitude Solutions, Inc*., 730 F.Supp.2d 1174 (2010).
[4] *United States v. Swartz*, 945 F.Supp.2d 216 (2013).
[5] JSTOR: a digital library with access to books, journals, and other primary sources. Most publications are accessed by subscription, though some resources are public and available at no cost.

Swartz by Massachusetts Institute of Technology (MIT)[6]. The charge carried a penalty of $1 million in fines, 35 years in prison, asset forfeiture, restitution, and supervised release, and under CFAA, Swartz was prosecuted[7]. After pleading not guilty and refusing a plea bargain, Swartz was later found dead in his apartment, where he hanged himself[8].

Though *Swartz* may be an extreme example, it nevertheless demonstrates the extent to which CFAA could be dangerous to the reviewer of the tax return, who unintentionally violates the law when inadvertently accessing sensitive data on the IRS blockchain, as well as that of other blocks. As part of the IRS staff, the reviewer is carrying out his job responsibilities, but the CFAA warps a single, innocent mistake into criminal liability. Such regulation, or lack of a narrower regulation, may also hinder the different industries from trusting blockchain technology.

IV. <u>The SCA and Its Problems</u>

From the taxpayer's point of view, privacy rights are threatened. The information that a taxpayer inputs to file a tax return would subsequently be entered into an immutable ledger. Not only is the block immutable, it would be viewable to someone other than the taxpayer, leaving the PII vulnerable to breach. However, the Stored Communications Act (SCA)[9] states that "whoever:

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;

[6] ***United States v. Swartz***, 945 F.Supp.2d 216 (2013).
[7] ***Id.***
[8] ***Id.***
[9] Codified in 18 USCS § 2701(a).

> and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished . . .[10]"

In *Cousineau v. Microsoft Corp*., Defendant was an "electronic communication service" provider because Plaintiff's phone used Defendant's operating system that facilitated the "ability to send and receive electronic communications."[11] Similarly, the IRS would be providing the block onto which the taxpayer would be able to send and receive electronic communications. These communications would include certifying the tax return, confirming with asset sources from various blocks, and verifying the amount the taxpayer owes or is refunded.

To better understand how *Cousineau* would be applied to blockchain technology within the context of tax returns, it is helpful to break down the different socioeconomic statuses and profiles of taxpayers and the communications that arise therein. The varying profiles of each category of taxpayer will demonstrate which blocks from other registries will need to be accessed, assuming that each taxpayer has at least one bank account:

1. <u>Sophisticated real estate investor</u>

   A sophisticated real estate investor holds a significant amount of real estate in her name. In order to maintain privacy among public land records, she creates an LLC to continue acquiring real property. Her Social Security number used to create the entity, however, would ultimately tie her to the real estate. As her real estate empire grows, she decides to undertake house-flipping as well, which would mean more income and more communications with the IRS.

[10] See also *Cousineau v. Microsoft Corp*., 992 F.Supp.2d 1116, 1124 (2012).
[11] *Cousineau v. Microsoft Corp*., 992 F.Supp.2d 1116, 1125 (2012).

In reviewing this real estate investor's tax return, the IRS would need to access the blockchain that pertains to land registries. Although land records are currently public, the taxpayer may not necessarily want to disclose certain aspects of the transaction that are currently not a part of public records. Some property owners are aggrieved by some of the information that already is public, such as purchase price. The taxpayer's blockchain may also disclose that a shell entity had been created under her Social Security number.

2. <u>Police officer with pension and minimal investments</u>

A police officer in a small town has a solid retirement pension. He is not interested in investing any of his income into other securities. He owns his sole residence.

This return would be a simple return, and the IRS would need to access the blockchain that pertains to his retirement account and his residence. His decision to limit his investments and income means that his personal information may not be shared as often across different blocks, which may minimize chances of breach.

3. <u>Entrepreneur</u>

An entrepreneur in Silicon Valley starts a small company and hires employees, providing them with stock options and retirement benefits. The company profits and is later acquired by a publicly traded company. After the acquisition, she continues to invest in different ventures, including international funds, and even some out-of-state real estate. Meanwhile, her securities accounts continue to diversify and grow, and she has also invested in some cryptocurrency.

> This would be a very involved return, and the IRS would need to access blocks that pertain to land registries, securities, international ventures, and cryptocurrency portfolios. Due to the wide spectrum of investments and activity, she may even qualify for an audit. Because her investment outlook is ever-changing, her sensitive information is likely to be shared across different blocks frequently, leaving her information extremely susceptible to breach.

The trend from the above-scenarios is that the more diverse your tax return profile is, the more communication outlets you open with the IRS. This means that regardless of what category a taxpayer may be classified under, immutable information will be available to the reviewer, and each scenario leaves the taxpayer vulnerable to some breach because the taxpayer's PII would be shared at least once across different blocks. The more complex and diverse a taxpayer's profile is, the more times the taxpayer's information is likely to be shared. This vulnerability calls for narrower cybersecurity measures that would keep blockchain activity accountable. The accountability would create a deeper sense of trust from both the taxpayer's and the reviewer's perspectives, and in order for blockchain technology to be successful, in any terrain, that trust between the user and the block is imperative.

V. Recommendations

New privacy laws that cater to blockchain technology are urgently needed. Although the current climate of cybersecurity laws like the CFAA carry a tendency to over-criminalize, new regulations do not necessarily call for stricter language, as long as they are specific. In order for blockchain technology to be an optimal tool for tax payments, the IRS should support new legislation that specifically tailors to blockchain technology that impedes hacking, while protecting the reviewer when accessing the pertinent blocks. In order to take full advantage of blockchain technology in filing a tax return, it is imperative that both the reviewer and taxpayer trust the technology behind the process.

This means that more specific laws behind blockchain technology calls for more education to the public. More accessible education about blockchain technology would create more opportunities for the technology itself to gain trust from its users. Because trust is such an essential component to a successful use of blockchain technology, educating the public would expedite familiarity, general troubleshooting, and thereby more experience, as well as productive laws. In the context of filing tax returns, more education surrounding the technology would also bring about a more practical and efficient rollout.

Additionally, if a blockchain database is attached to an entity that anticipates sharing its data with the IRS, the blockchain database should operate under a permissioned block. For example, brokerage firms would need to implement permissioned blockchains for its clients. This way, the permissioned blockchain could grant the IRS exclusive access to the taxpayer's portfolio. The permissioned blockchain would be an added layer of security for a potential hacker. The IRS' block, in turn, would also be permissioned to ensure the public of the security of sensitive information. It would be ideal to bypass a financial incentive and preempt the data-selling that plagues today's markets. Perhaps the IRS could offer an incentive that would encourage the various entities to initiate blockchain collaboration with the IRS.

VI. Conclusion

Innovative technology can improve the lives of all involved parties, but these innovations are not without risk. Incorporating blockchain technology that heavily involves one's most sensitive information is rightfully viewed with skepticism and doubt. Specifically within the IRS space, the taxpayer's privacy rights are at stake. Moreover, as collateral, an effort to protect the taxpayer could inadvertently criminalize the reviewer who handles the sensitive data and even someone who is in mere possession of that data.

To mitigate the risk of exposing sensitive information and protecting staff members from criminal liability, narrowly tailored legislation around blockchain technology is crucial. It is also important for the public to become more well-versed in the technology in order to build a more well-oiled machine. On the technical side, building a permissioned block would also help impede hackers and in reducing breach of sensitive information. However, these proposed solutions are merely stepping stones that will ultimately launch blockchain technology as a powerful sword to enhance the way we carry out our everyday duties and activities. A more collaborative and dedicated effort will not only help ease the tedium of filing and reviewing tax returns but also illuminate the possibilities of new habits and lifestyles.