ZERO-KNOWLEDGE PROOFS AND THE IRS: A PROPOSAL FOR THE TAXATION OF ILLEGAL INCOME

J. REED TRUSLOW*

Under the U.S. tax framework, a person is subjected to the same federal income tax rules, regardless of whether the income was obtained legally or illegally. But unsurprisingly, taxes are not often paid on ill-gotten income. Without a practical, anonymous means of facilitating the taxation of such income, taxpayers have no incentive to report their illegality. In this article, I first analyze the taxation of illegal income and its current treatment, as well as potential conflicts with taxpayers' Fifth Amendment privilege against self-incrimination. I then discuss "zero-knowledge proof" cryptography, a method by which one party can communicate knowledge to another party and prove the veracity of that knowledge without disclosing sensitive information. Finally, I turn to the central thesis of this article, the proposal of an online application to be created and implemented by the IRS for the taxation of illegal income. I refer to this application as "SAPTIG," which is an acronym for "Secure Application for Paying Taxes on Illegal Gains." This would be a permissioned blockchain-based application that uses zero-knowledge proof cryptography, self-sovereign identities, and electronic ticketing to provide anonymity to taxpayers, which would both incentivize such taxpayers to maintain tax compliance as to their illegal income while also providing the IRS with a means to assess taxes on illegal income without implicating the taxpayers' Fifth Amendment privilege against self-incrimination. Moreover, the SAPTIG application proposed herein directly aligns with the goals set forth in the Service's recently published spending plan.

* J.D., Florida State University College of Law, 2022. LL.M. in Taxation, University of Florida Levin College of Law, 2023. Email: jreedtruslow@gmail.com. I would like to thank several of my former professors—David Hasen (University of Florida Levin College of Law) and Shawn Bayern (Florida State University College of Law) for providing valuable critiques and guidance on my paper, Douglas Kahn (University of Michigan Law School, Florida State College of Law) for inspiring my tax law studies, and Manuel Utset (Florida State University College of Law) for first introducing me to the concept of zero-knowledge proofs.

TABLE OF CONTENTS

INTRODUCTION

The federal income tax is constitutionally provided by the Sixteenth Amendment and is codified and regulated by the Internal Revenue Code, which in turn is supported by Treasury Regulations, court decisions, and IRS guidance in the form of revenue rulings and procedures.[1] Despite this extensive legal regime, there are gaps. One such gap is the taxation of illegal income. Treasury Regulation Section 1.61-14(a) provides: "Illegal gains constitute gross income."[2] Thus, taxpayers are expected to report illegal income and pay corresponding tax liabilities. But an apparent incongruity exists—the Fifth Amendment states: "No person shall . . . be compelled in any criminal case to be a witness against himself."[3] This excerpt is often referred to as the privilege against self-incrimination and conflicts with the Treasury Regulation subjecting illegal income to federal taxation. That is, how could one report the source of their illegal income without potentially incriminating themselves? Consequently, any attempt to enforce the taxation of illegal income would, at least in theory, be in violation of the Fifth Amendment privilege against self-incrimination (albeit, judicial decisions on this matter provide insight and guidance, as explored later in this article).[4] The proposal set forth in this article provides a solution: a permissioned blockchain-based application for the taxation of illegal income, which incorporates zero-knowledge proofs ("ZKPs") and self-sovereign identities, administered by the IRS to provide anonymity to taxpayers with illegal

[1] *Infra* Part I.
[2] Treas. Reg. § 1.61–14(a) (as amended in 1993).
[3] U.S. CONST. amend. V.
[4] *Infra* Section I.B.

income. Such an application would provide the Service with a method to constitutionally assess taxes on illegal income and incentivize individuals with such income to report without worrying about potential self-incrimination.

Stated broadly, a zero-knowledge proof is a cryptographic[5] technique by which one party can communicate and validate a statement to another party without disclosing ancillary knowledge. More specifically, it is a method by which "a prover is able to convince a verifier that a statement is true, without providing any more information than that single bit (i.e., that the statement is true rather than false)."[6] Accordingly, the use of ZKPs can, among other things, enable the prover to retain anonymity when communicating with the verifier and conceal sensitive information. The following scenario illustrates the basic function of a ZKP and the potential usefulness of ZKPs in the taxation of illegal income:

> During the course of the past year, Tom made $50,000 by means of illegal activity (for example, by selling illicit substances) in addition to his legal salary as a stockbroker. It has now come time for Tom to report his income to the IRS and pay the appropriate tax. Tom is a learned criminal and is aware that Treasury Regulation Section 1.61-14(a) provides that "illegal gains constitute gross income" under § 61 of the Code,[7] and thus Tom's $50,000 of illegal income is subject to taxation. Tom is thus faced with a predicament—report the $50,000 of illegal gains and risk inquiry and prosecution by the federal government, or omit the illegal income—a crime in and of itself—and risk audit by the IRS, potentially resulting in federal prosecution, among other penalties.[8] Tom's predicament is a no-win scenario, not only for himself but for the IRS as well; faced with such a decision, it is foreseeable that Tom may avoid reporting his taxes, and his $50,000 of illegal gains would escape taxation (unless and until the IRS or a police agency discovers his illegal conduct). And if this scenario was not problematic enough already, it's further complicated by the aforementioned conflict with a taxpayer's

[5] "Cryptography" refers generally to the study of creating codes and ciphers. *See ciphers and codes*, BRITANNICA KIDS, https://kids.britannica.com/students/article/ciphers-and-codes/273673 (last visited May 9, 2023).

[6] *Zero-Knowledge Proof*, NAT'L INST. OF SCI. & TECH., https://csrc.nist.gov/glossary/term/zero_knowledge_proof (last visited May 9, 2023).

[7] Treas. Reg. § 1.61–14(a) (as amended in 1993).

[8] I.R.C. § 7203.

> Fifth Amendment privilege against self-incrimination. This is where the concept of a zero-knowledge proof provides a potential solution.
>
> Assume that, as proposed by this article, the IRS creates and implements an online application utilizing zero-knowledge proofs for communication between taxpayers and the IRS. This would allow Tom to accurately report his $50,000 of illegal income anonymously, while also allowing the IRS to verify the truth/accuracy of Tom's reporting and maintain Tom's protection against self-incrimination. The benefit to Tom is that if he were caught and prosecuted for his illegal activity, he would not be guilty of failure to file and pay taxes associated with his illegal income (assuming he used the application and filed correctly). Tax crimes are often unearthed in discovery and prosecution of the underlying crimes,[9] so Tom is incentivized to report his illegal gains, and moreover, tax crimes often carry heavy penalties/sentences,[10] further incentivizing Tom's reporting responsibility. The benefit to the government is two-fold: (1) far more tax revenue may be captured, compounded by taxpayers' incentives to minimize their criminal liability; and (2) concern regarding potential violation of the Fifth Amendment is eliminated.

Part I of this article provides an outline of the United States' current system for the federal taxation of illegal income. Part II explains technical concepts including "zero-knowledge proofs" and blockchain. Finally, Part III incorporates these concepts into a comprehensive proposal for an online application that uses zero-knowledge proofs for the taxation of illegal income. Specifically, I propose a permissioned blockchain-based application utilizing zero-knowledge proofs, self-sovereign identities (SSIs), and electronic ticketing to provide a platform for taxpayers to self-manage their digital identity and pay taxes on their illegal income. Upon payment of tax liability, a unique ticket would be generated and assigned to the taxpayer's SSI, allowing the taxpayer to conceal incriminating information and retain anonymity upon audit. I refer to this application as "SAPTIG.": Secure Application for Paying Taxes on Illegal Gains.

---

[9] *Infra* note 54.
[10] I.R.C. § 7201.

I. THE TAXATION OF ILLEGAL INCOME

A. Overview

The policy of taxing illegal gains was introduced early in the evolution of the income tax by Justice Holmes, who notably remarked that "Congress may tax what it also forbids."[11] This sentiment by Holmes was later reinforced in the landmark case *United States v. Sullivan*.[12] Treasury Regulation Section 1.61-14(a) provides that "illegal gains" constitute "gross income" under Section 61 of the Code.[13] Accordingly, illegal income must be declared on Form 1040 if the gains are earned by an individual, or on Schedule C if earned by a business (including individual-led businesses, e.g., sole proprietorships, independent contractors).

Despite this taxability, the Code denies certain deductions for expenses paid in furtherance of illegal operations. Code Section 162 generally provides for the deductibility of "ordinary and necessary" expenses paid in "carrying on any trade or business."[14] However, it explicitly denies deductions for illegal payments or kickbacks paid to government officials, employees, or an agency/instrumentality of any government.[15] Other illegal payments are nondeductible under Code Section 162 if such payment would result in criminal penalty to the payor or would result in the payor losing the ability to engage in a certain trade or business.[16] By denying these deductions, Congress effectively taxes the gross amount of illegal income.

Borek highlighted the notion that the Sixteenth Amendment is traditionally viewed as empowering Congress to tax *net* income, rather than *gross* income.[17] This inconsistency results in a scheme that subjects illegal income to a higher tax burden than legal income.[18] Locker critiqued the nondeducibility of expenses attributable to certain illegal activities as illogical: since legal and illegal income are comparably included in "gross

---

[11] United States v. Stafoff, 260 U.S. 477, 480 (1923).

[12] *Infra* Section I.B.1.

[13] Treas. Reg. § 1.61–14(a) (as amended in 1993).

[14] I.R.C. § 162(a).

[15] I.R.C. § 162(c)(1).

[16] I.R.C. § 162(c)(2). It is important to recognize that this restriction on deductibility is drafted so as to deny deductions for certain, not all, expenses paid in conducting illegal conduct.

[17] Charles A. Borek, *Comments: The Public Policy Doctrine and Tax Logic: The Need for Consistency in Denying Deductions Arising from Illegal Activities*, 22 U. BALT. L. REV. 45, 48 (1992). *Commissioner v. Tellier* confirmed this position by reaffirming that "the federal income tax is a tax on net income, not a sanction against wrongdoing." Comm'r v. Tellier, 383 U.S. 687, 691 (1966).

[18] Borek, *supra* note 17, at 47–48.

income" and subject to taxation, both should reasonably be allowed deductions.[19] Thus, the denial of deductions for expenses attributable to illegal operations suggests an attempt to balance policy considerations—that is, a desire by the government to collect a portion of illegal income in the form of taxes, while disincentivizing illegality, particularly within the government. In addition, certain loss deductions that would otherwise be allowed under Code Section 165 are prohibited where public policy would be frustrated.[20]

Section 7203 of the Code states that any person who fails to comply with the Code and/or the corresponding regulations may be subject to penalties and/or prosecution.[21] Requiring taxpayers to report illegal income under threat of sanctions invokes consideration of whether such a requirement violates an individual's Fifth Amendment protections, namely the privilege against self-incrimination.

B. Conflict with the Fifth Amendment: The Privilege Against Self-Incrimination

1. Case Law Development and Doctrines

The Fifth Amendment, in part, provides: "No person . . . shall be compelled in any criminal case to be a witness against himself."[22] This is commonly referred to as the "privilege against self-incrimination." Within the scope of this privilege is the "act of production doctrine," under which the production of documents in response to a subpoena "may have a compelled testimonial aspect."[23] *Fisher v. United States* narrowed the applicability of this doctrine. In *Fisher*, a taxpayer attempted to invoke their Fifth Amendment privilege against self-incrimination in response to an IRS summons requesting the production of certain documents.[24] The taxpayer argued that the documents were privileged because they contained

[19] Melville E. Locker, *Public Policy in the Taxation of Illegal Incomes*, 29 GEO. L.J. 356, 359 (1940).

[20] *Richey v. Commissioner* denied a deduction, claimed by the taxpayer under Code Section 165, for a loss suffered as a result of the taxpayer's attempted participation in an illegal counterfeiting scheme. *See generally* Richey v. Comm'r, 33 T.C. 272 (1959). Moreover, Rev. Rul. 77-126 denied a loss deduction where the taxpayer's gambling devices, used in an illegal enterprise, were confiscated by the federal government, and the taxpayer had thereafter attempted to claim a loss deduction. Rev. Rul. 77-126, 1977-1 C.B. 47. For a more comprehensive discussion of this topic, see Part IV of Borek (1992). Borek, *supra* note 17, at 56–64.

[21] I.R.C. § 7203.

[22] U.S. CONST. amend. V.

[23] United States v. Hubbell, 530 U.S. 27, 36 (2000).

[24] Fisher v. United States, 425 U.S. 391, 393–94 (1976).

incriminating information.[25] The Court held that the taxpayer could not invoke the privilege as to these documents, reasoning that it protects only *compelled* testimony.[26] But this limitation from *Fisher* does not apply in the context of reporting income from illegal gain since such filing is compelled.[27] *Fisher* operates only to restrict already existing documents that were prepared voluntarily.[28]

Thus, the Fifth Amendment's privilege against self-incrimination, as well as the act of production doctrine, *should* apply to protect incriminating disclosures compelled by tax forms. Indeed, the Court in *United States v. Sullivan* stated:

> The questions asked in the required income tax return do not compel the disclosure of any fact which tends to incriminate. Only information of the most general character relating to the nature of the taxpayer's business is demanded, none of which in itself constitutes proof of unlawful dealings. . . . He must comply with the Government's demand on him for information at least to the point where the information would tend to incriminate.[29]

In other words, the Court in *Sullivan* held that a taxpayer may assert the privilege against self-incrimination and omit incriminating disclosures, but only to the extent the information is incriminating—the taxpayer is still required to disclose all non-incriminating information relevant in determining their tax liability.[30]

In *Garner v. United States*, the Court intimated that a taxpayer may assert the privilege on the tax return form instead of making disclosures.[31] However, if a court holds that the Fifth Amendment claim is not valid, the government may prosecute the individual for failure to properly comply with Section 7203 of the Code.[32] This mechanism is paradoxical. It ostensibly allows a taxpayer to assert the privilege against self-incrimination, but doing so may inadvertently result in that taxpayer being prosecuted or fined, thus making the privilege illusory.

---

[25] *Id.* at 395.
[26] *Id.* at 409–10.
[27] *See id.* at 398–99.
[28] *Id.*
[29] United States v. Sullivan, 274 U.S. 259, 260 (1927).
[30] Jacob Hoback, *Heads I Win, Tails You Lose: The Taxing Risk When Invoking the Fifth Amendment on a Tax Return*, 89 U. CIN. L. REV. 1003, 1004 n.9 (2021).
[31] Garner v. United States, 424 U.S. 648, 665 (1976).
[32] *Id.* at 651; IRC § 7203; Hoback, *supra* note 30, at 1004.

2. Policy and Academia Considered

Melville Locker identified the policy that everyone must share in the "burdens of taxation" since everyone, in theory, benefits from the tax regime.[33] Thus, taxing illegal gains is necessary to maintain an equitable taxing scheme; that is, to preclude individuals from using crime as a means to shield income from taxation.[34] But expecting criminals to voluntarily report their income without any incentive or anonymity underscores a conspicuous flaw.

After *Sullivan*, and prior to *Garner*, it was understood that taxpayers were required to report illegal gains and were entitled to the privilege against self-incrimination, but how or when the privilege could be invoked remained unclear.[35] *Garner* further complicated the issue.[36] As it stands, Donald DePass has argued that the current policy for taxing illegal gains is unfair, unjustifiable, and essentially functions as a punitive tax.[37] In furtherance of this argument, DePass cogently articulates the vexing dilemma faced by taxpayers with income derived by illegal means:

> If the tax-conscious criminal declares the income, the discrepancy between his legal income and the amount of income he is declaring may tip off law enforcement about possible illegal gains. Conversely, opting not to declare the illegal gain risks a tax penalty. Thus, a criminal declining to declare his illegal income may face a tax penalty in addition to any imprisonment, fines, and civil liability imposed for his crime.[38]

It is for this reason that I critique the blanket taxation of illegal gains as being inefficient, if not wholly paradoxical and potentially unconstitutional. Beyond the lack of any reasonably effective method of assessing taxes on illegal income, the taxation of illegal income also lacks any deterrent value.[39] And despite the efforts of the IRS Criminal

---

[33] Locker, *supra* note 19, at 358.

[34] *See id.*

[35] *Id.* at 461.

[36] *See supra* Part I(B)(1).

[37] *See* Donald DePass, *Reconsidering the Classification of Illegal Income*, 66 TAX LAW. 771, 771–72 (2013) (explaining that "the current policy of classifying unlawfully obtained funds as gross income challenges fundamental notions of fairness and justice" and represents a "punitive use of the taxing power").

[38] *Id.* at 771.

[39] *See id.* at 780 (explaining that "the deterrent value of taxing illegal gains appears dubious").

Investigation division, dedicated to tracking and pursuing noncompliant taxpayers, a substantial deficit exists. This deficit is referred to as the "tax gap," which represents the difference between the total amount of tax owed to the IRS and the amounts actually collected. [40] The IRS estimated a gross tax gap of $688 billion for the 2021 tax year alone.[41] Albeit, tax gap estimates generally do not include unreported illegal income due to lack of data and estimation difficulty.[42] The true, latent tax gap is likely far greater than estimates indicate. Indeed, a study by the Bureau of Economic Analysis estimated $40 billion of unpaid taxes on illegal income for the 2019 tax year.[43]

Beyond being practically inefficient, taxing illegal income may interfere with the restitution of a criminal's victim(s). By taxing amounts gained by illegal means, the federal government is essentially afforded priority over any potential victims whose money was wrongfully taken by the criminal.[44] The Code provides that a taxpayer's failure to pay tax liabilities may result in a lien in favor of the United States.[45] Although, case law has held that—at least in cases of embezzlement—a tax lien in favor of the government does not attach to the embezzled funds, as those funds are the rightful property of the victim.[46] However, even where a lien for nonpayment in favor of the government does not attach to the illegal income, merely seeking to tax illegal gains conflicts with a victim's right to those funds. For instance, embezzled funds rightfully belong to the victim; even if full restitution is granted by the court, taxing embezzled funds inherently reduces the stolen amount, allocating a portion to the government, despite no legal transfer or transaction occurring.[47] As a result, even if full restitution is granted, a portion of the original embezzled amount may have been claimed by the government in the form of tax paid by the embezzler. This concept may be illustrated by the following scenario:

---

[40] Natasha Sarin, *The Case for a Robust Attack on the Tax Gap*, U.S. DEP'T OF THE TREASURY (Sept. 7, 2021), https://home.treasury.gov/news/featured-stories/the-case-for-a-robust-attack-on-the-tax-gap.

[41] *Id.*

[42] Daniel J. Hemel et al., *The Tax Gap's Many Shades of Gray*, CHI. UNBOUND, at 3–4 (2021) (citing U.S. DEP'T OF THE TREASURY, *Reducing the Federal Tax Gap: A Report on Improving Voluntary Compliance*, at 6 (Aug. 2007)).

[43] This amount was calculated based on an estimate of $253 billion of unreported, taxable income attributable to illegal sources for the 2019 tax year. *Id.* at 24.

[44] Christine Manolakas, *The Taxation of Thieves and Their Victims: Everyone Loses but Uncle Sam*, 13 Hastings Bus. L.J. 31, 53 (2016).

[45] I.R.C. § 6321.

[46] Dennis v. United States, 372 F. Supp. 563, 567 (E.D. Va. 1974). In *Dennis*, the embezzler (Forbes) was deemed to be merely a conduit of funds, with only a right to possess, and thus no intent to transfer the funds existed between the victim and Forbes. *Id.* at 567–68.

[47] *Id.* at 567.

> John embezzles $100,000 of Bob's money. Under the tax regime described in this paper thus far, the $100,000 of embezzled funds are taxable income to John.[48] If John were to pay, e.g., $5,000 of tax on the embezzled amount, the total base amount remaining is $95,000. If John was later prosecuted and convicted, the court may grant full restitution of the $100,000. Even if Bob were able to recover the full amount, the government claimed a portion of the original amount—which rightfully belonged to Bob—in the form of tax, despite no legal transfer ever occurring.

This policy flaw is due to the blanket taxation of illegal income under Treasury Regulation Section 1.61-14(a). Without a more comprehensive and detailed statutory regime for the taxation of illegal income, a blanket tax on illegal income can result in additional harm to victims of crime.

On a semantic note, classifying money received illegally as "income"[49] seems improper, as income is generally considered to constitute amounts paid *voluntarily*, whereas "illegal income," by definition, includes stolen property. Nevertheless, the Code defines "gross income" as including illegal income, which is thus taxable.[50] So long as this tax treatment exists, Fifth Amendment concerns linger, necessitating the development of an efficient, constitutional method for collecting taxes thereof.

C. Taxing Illegal Income: Current Proposals

Zero-knowledge proofs, along with other complementary technology, provide a method by which to tax illegal income, while allaying any concerns of compulsory self-incrimination. Other proposals are demonstrably fallible. In a 2021 article, Jacob Hoback proposed the implementation of a pre-compliance review; that is, "an opportunity to have a neutral decisionmaker review the validity of an individual's Fifth Amendment claim before the individual would face penalties for tax evasion."[51] Taxpayers are not currently entitled to a preliminary compliance review,[52] and implementation

---

[48] *See* James v. United States, 366 U.S. 213, 218, 220 (1961) (declining to relieve embezzlers of a duty to pay taxes on unlawful gains, which should be included within taxable gross income).

[49] Treas. Reg. § 1.61–14(a) (as amended in 1993).

[50] *Id.*

[51] Hoback, *supra* note 30, at 1004; *see* City of Los Angeles v. Patel, 576 U.S. 409, 421 (2015).

[52] *See* Garner v. United States, 424 U.S. 648, 665 (1976) ("As long as a valid and timely claim of privilege is available as a defense to a taxpayer prosecuted for failure to make a

of such a mechanism would likely prove to be particularly onerous. By providing anonymity, individuals with illegal gains would be incentivized to report their gains to preclude any potential tax prosecutions. This is particularly valuable because tax investigations can be used to punish criminals where law enforcement lacks evidence of the individual's underlying crimes.[53] For instance, despite his public persona, law enforcement struggled to procure sufficient evidence against the notorious criminal Al Capone.[54] He eventually faced significant retribution, not for any one of his substantive crimes per se, but for failing to pay taxes on his illegal income.[55]

Moreover, individuals have no incentive to voluntarily report illegal gains—particularly since there is no anonymity, and voluntary reporting would thus greatly increase the chance of being caught and prosecuted.[56] Hence, characterizing income from illegal sources as taxable income seems aspirational at best—at least to the extent that no proper method of facilitating such taxation exists.

Sarin et al. proposed several important advancements towards deterring tax evasion and narrowing the tax gap.[57] While crucial to facilitate the development of the Service's efforts, these proposals offer only broad, generalized considerations rather than practical methods to close the tax gap. Specifically, the authors proposed increasing the IRS budget, improving tax enforcement efforts, and investing in advancements in the Service's technology.[58] At the time this paper was published, the Service's budget had declined by 15% over the course of the preceding decade, attributable to the

---

return, the taxpayer has not been denied a free choice to remain silent merely because of the absence of a preliminary judicial ruling on his claim.").

[53] DePass, *supra* note 37, at 781 ("It is well documented that the government occasionally uses tax prosecutions to punish known criminals when it lacks sufficient proof to obtain a criminal conviction."). Perhaps the most infamous example is the prosecution of Al Capone, the notorious kingpin of a criminal organization suspected of murder, drug trafficking, bribery, gambling operations, and a myriad of other crimes. *Al Capone*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/history/famous-cases/al-capone (last visited Jan. 1, 2024).

[54] FED. BUREAU OF INVESTIGATION, *supra* note 53.

[55] *Id.*

[56] *Cf.* DePass, *supra* note 37, at 780 ("[T]he [IRS] does not have unlimited resources to investigate and to prosecute suspected tax evaders. Hence, it seems likely that a substantial number of those who acquire illegal income and are not caught by normal processes of law enforcement will escape detection.").

[57] *See generally* Natasha Sarin et al., *Tax Reform for Progressivity: A Pragmatic Approach*, *in* TACKLING THE TAX CODE: EFFICIENT AND EQUITABLE WAYS TO RAISE REVENUE 317 (Jay Shambaugh & Ryan Nunn eds., 2020).

[58] *Id.* at 317–18, 331.

efforts of special interest groups.[59] And as recently as February 2023, it has been reported that the Service's Information Technology ("IT") systems are outdated, relying on archaic programming languages, exposing the Service to potential hacking and data breaches.[60] The current plan to renovate the Service's IT systems has an estimated completion date of 2030.[61]

In light of the Service's recent budget influx—a total of nearly $80 billion to be distributed over a 10-year period[62]—the Criminal Investigation division, and the IRS as a whole, are ripe for an overhaul. Indeed, the Service's spending plan includes $12.4 billion, or 15.6% of the total budget increase, allocated towards delivering "cutting-edge technology, data, and analytics."[63] The Service indicated plans to modernize the IT infrastructure by developing software and implementing new technology architecture in an effort to automate manual processes;[64] the Service also plans to discontinue outdated systems in favor of modern, efficient systems.[65]

In furtherance of these goals, the Service outlined eight core initiatives including the transformation of core account data and processing, acceleration of technology delivery, improvement of technology operation, maximization of data utility, and a focus on data security.[66] Specifically, the Service will update their programming language, introduce "zero-trust authentication security" to the IRS network, improve "digital identity management," and create "privacy-preserving analytic methods."[67]

The digital tax system I propose here directly aligns with the goals set forth in the Service's spending plan and would allow a taxpayer to anonymously report their tax and verify their tax compliance without disclosing any sensitive or incriminating information. This presents the government with an efficient method by which to collect taxes on illegal

---

[59] *Id.* at 324.

[60] *Outdated and Old IT Systems Slow Government and Put Taxpayers at Risk*, U.S. GOV'T ACCOUNTABILITY OFF. (Feb. 15, 2023), https://www.gao.gov/blog/outdated-and-old-it-systems-slow-government-and-put-taxpayers-risk.

[61] *Id.*

[62] Martha Waggoner, *IRS unveils $80 billion spending plan*, J. OF ACCT. (Apr. 7, 2023), https://www.journalofaccountancy.com/news/2023/apr/irs-unveils-80-billion-spending-plan.html. Note that this amount was slightly reduced by the Fiscal Responsibility Act of 2023. *Would Increased Funding For The IRS Narrow The Tax Gap?*, PETER G. PETERSON FOUND. (Dec. 7, 2023), https://www.pgpf.org/blog/2023/12/would-increased-funding-for-the-irs-narrow-the-tax-gap.

[63] INTERNAL REVENUE SERVICE INFLATION REDUCTION ACT STRATEGIC OPERATING PLAN, Publ'n 3744 (Rev. 4-2023) at 2, https://www.irs.gov/pub/irs-pdf/p3744.pdf.

[64] *Id.* at 80.

[65] *Id.* at 83.

[66] *Id*. at 84.

[67] *Id.* at 86, 90, 92, 100.

gains—one that incentivizes criminals to pay their taxes without violating their constitutional privilege against self-incrimination.

II. ZERO-KNOWLEDGE PROOFS

A. Overview: What is a ZKP?

The notion of a "zero-knowledge proof"—also known as a "ZKP"—is widely attributed to the collective scholarly contributions of Goldwasser et al. (1985) and Babai and Moran (1988).[68] A ZKP is an algorithm/protocol that allows parties to make truthful statements without revealing how or why those statements are accurate. For example, assume two parties—rather than texting, emailing, or using some other third-party messenger such as WhatsApp or Facebook—decide to use a hypothetical new application known as "Koala Messenger."[69] They chose this application because it uses zero-knowledge proof algorithms in its coding, allowing the parties to make statements, and prove the truth and accuracy of their statements, without disclosing how or why the statements are true.[70] In other words, they only have to communicate the statement itself and nothing more; the zero-knowledge proof will verify whether the statement is accurate and inform the party receiving the message.[71]

In technical terms, the party sending a message is known as the "prover" (so called because they will be proving the truth and accuracy of a statement, a statement which they are communicating to the other party) and the party receiving a message is the "verifier" (so called because they will be verifying that the prover's statement is indeed true and accurate).[72] These terms, "prover" and "verifier," are vital in discussing how ZKPs work; I will use these terms often to refer to the respective parties using a ZKP. In the context of an online IRS application that utilizes ZKPs for the taxation of illegal income, the taxpayer would be the "prover" and the IRS would be the "verifier."

---

[68] *Zero-knowledge proof*, GOLDEN, https://golden.com/wiki/Zero-knowledge_proof (last visited May 10, 2023); *see generally* Shafi Goldwasser et al., *The Knowledge Complexity of Interactive Proof-Systems*, 18 SIAM J. COMPUTING 186 (1989); *see generally* László Babai & Shlomo Moran, *Arthur-Merlin Games: A Randomized Proof System and a Hierarchy of Complexity Classes*, 36 J. COMPUT. & SYS. SCIS. 2, 254 (1988).

[69] Note that this is not a real application; it is a hypothetical application I use to illustrate how a ZKP works.

[70] M. Musharraf & Mrig P, *What is a Zero-Knowledge Proof? ZKPs Explained*, THIRDWEB (Apr. 10, 2023), https://blog.thirdweb.com/zero-knowledge-proof-zkp/.

[71] *Id.*

[72] *Id.*

It may also be helpful to briefly provide an understanding of encryption, a concept discussed throughout this article and inherent to zero-knowledge proofs. "Encryption" works by first inputting a normal line of readable text, "plaintext," which is then turned into unreadable text, "ciphertext," using specific mathematical algorithms.[73] If an individual wanted to read the ciphertext, they would need to turn it back into normal, plaintext—a process known as "decoding."[74] To do so, the individual would need to provide the "decryption key," which is essentially a password generated by the algorithm when it initially converted the text from plaintext to ciphertext.[75] The practice and study of encryption is often referred to as "cryptography."[76] There are two distinct forms of encryption—"private key" encryption and "public key" encryption.[77] Private key encryption refers to using the same key for the encryption and decryption processes.[78] Public key encryption refers to using two separate keys: a public key for the encryption process, and a private key for the decryption process.[79]

B. The Basic Requirements of a "Zero-Knowledge Proof"

A "zero-knowledge proof" protocol is predicated upon three conditions, or elements, each of which must be met to properly create a ZKP protocol: (1) Completeness; (2) Soundness; and (3) Zero-Knowledge.[80] Below, I explain each of these conditions. These conditions are met by creating a sufficient coding algorithm within the application that the two parties will be using to communicate. In other words, if a protocol is "complete," "sound," and features "zero-knowledge" capability, it is considered to be a "zero-knowledge proof."[81]

1. Completeness

[73] *Encryption*, GOOGLE CLOUD, https://cloud.google.com/learn/what-is-encryption (last visited May 10, 2023).

[74] *Id.*

[75] *Id.*

[76] *What is Cryptography*, IBM https://www.ibm.com/topics/cryptography (last visited May 10, 2023).

[77] Robert Dougherty, *Public vs. Private Key Encryption: A Detailed Explanation*, KITEWORKS, https://www.kiteworks.com/secure-file-sharing/public-vs-private-key-encryption/ (Aug. 12, 2023).

[78] *Id.*

[79] *Id.*

[80] Musharraf, *supra* note 70.

[81] *Id.* Real, feasible ZKPs are discussed later in this article to demonstrate their use and functionality. *See infra* Part II.E.

In the context of a ZKP, "completeness" means that the ZKP protocol must be able to verify that the prover's statement is true.[82]

2. Soundness

"Soundness" refers to the fact that a ZKP protocol will only provide the verifier with a "true" value—that is, the ZKP will inform the verifier that the prover's statement is true/accurate—if the claim is indeed true.[83] If the ZKP protocol is able to achieve this requirement, it is said to be "sound."[84] Completeness and soundness are related but distinct. "Completeness" entails that the verifier can be convinced that the prover's statement is true; conversely, "soundness" entails that an invalid statement will not convince the verifier.[85]

3. Zero-Knowledge

For an application to properly utilize a "ZKP" protocol/algorithm, the verifier must not receive any information beyond whether the prover's statement is true or false, hence the term "zero-knowledge." That is, the verifier has "zero knowledge" as to why or how the prover's statement is true, yet, by means of the ZKP protocol, the verifier is indeed able to verify the truth of the prover's statement.[86] The ZKP protocol/algorithm itself verifies the accuracy of the prover's statement and informs the verifier,[87] thus protecting the prover's sensitive information. In the context of an IRS application for the taxation of illegal income, this element allows the taxpayer (the prover) to report their illegal income without providing any incriminating or identifiable information to the IRS/government.

---

[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *See Zero-knowledge proofs explained in 3 examples*, CIRCULARISE (Dec. 21, 2022), https://www.circularise.com/blogs/zero-knowledge-proofs-explained-in-3-examples (explaining that satisfying the property of completeness requires that "if the statement is true, an honest verifier will be convinced by an honest prover," and satisfying the property of soundness requires that "if the statement is false, no dishonest prover can convince the honest verifier").
[86] *Id.*
[87] *See id.*

C. Interactive and Non-Interactive ZKPs

The early ZKP systems were "interactive."[88] In this context, "interactive" means that the prover and verifier have to participate, or interact, *simultaneously*—a cumbersome process that has since been improved by the advent of non-interactive ZKPs. During this interaction, the prover is required to complete multiple rounds of many tasks to verify the truth of the information that they are providing to the verifier.[89] The requirement that the parties interact in such a way caused the ZKP process to be "ambiguous" and "unscalable."[90]

In 1988, three researchers—Manuel Blum, Paul Feldman, and Silvio Micali—published a paper demonstrating the ability to replace the interaction in any zero-knowledge proof with a non-interactive structure.[91] Prior to this publication, it was generally understood that the operation of a zero-knowledge proof required interaction between the two communicating parties, but Blum et al. successfully rebutted this presumption.[92] The authors distinguished the "non-interactive" process as "mono-directional"; that is, operating in a single direction—from prover to verifier—as opposed to the simultaneous interaction required by an interactive ZKP.[93] Nearly a decade later, Feige et al. introduced "witness indistinguishability," which contributed an additional element of anonymity to the utility of ZKPs.[94]

There are several types of cryptographic methods and structures that can be used in creating non-interactive zero-knowledge proofs, including "elliptic curve cryptography" and "collision-resistant hashing." As this article

---

[88] ciberexplosion, *Non-Interactive Zero Knowledge Proof*, GEEKSFORGEEKS (May 11, 2022), https://www.geeksforgeeks.org/non-interactive-zero-knowledge-proof/.

[89] *Id.*; Danielle Enwood, *Zero-knowledge proofs – a powerful addition to blockchain*, BLOCKHEAD TECHNOLOGIES (June 1, 2021), https://blockheadtechnologies.com/zero-knowledge-proofs-a-powerful-addition-to-blockchain/; *Introduction to Interactive Zero-Knowledge Proofs*, CHAINLINK (Jan. 2, 2023), https://blog.chain.link/interactive-zero-knowledge-proofs/.

[90] ciberexplosion, *supra* note 88.

[91] Manuel Blum et al., *Non-Interactive Zero-Knowledge and Its Applications*, STOC '88: PROCEEDINGS OF THE TWENTIETH ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING 103, 103 (1988).

[92] *Id.* at 103–04.

[93] *Id.* at 104.

[94] Uriel Feige et al., *Multiple Noninteractive Zero Knowledge Proofs Under General Assumptions*, 29 SIAM J. COMPUTING 1, 17 (1999). Witness indistinguishability is a technical concept; a protocol is considered to be "witness indistinguishable" if the verifier is unable to know which witness a prover is using. Uriel Feige & Adi Shamir, *Witness Indistinguishable and Witness Hiding Protocols*, STOC '90: PROCEEDINGS OF THE TWENTY-SECOND ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING 416, 418 (1990).

is principally tax-oriented, I refrain from going into the technical, mathematical aspects of cryptographic coding structures.

D. zk-SNARKs and zk-STARKs

1. zk-SNARKs

There are two prominent zero-knowledge proofs commonly used in blockchain infrastructure for the secure and private transmission of personal data and information. The first is Zero-Knowledge Succinct Non-Interactive Argument of Knowledge ("zk-SNARK"). zk-SNARKs were first introduced in 2012,[95] and are revolutionary as operable ZKP protocol because they employ the previously-theoretical non-interactive feature.[96] One notable application of zk-SNARKs is ZCash, a cryptocurrency transaction application which uses zk-SNARKs to allow "senders and receivers of shielded transactions to prove that encrypted transactions are valid."[97]

Constructing zk-SNARKs presents a potentially significant vulnerability. The creation of a zk-SNARK requires a trusted setup using a private key that, if acquired by a hostile party, would allow them to forge transactions.[98] Thus, the key must either be kept secure or discarded. However, this risk can be reduced by using "multi-party computation," which involves using multiple parties, rather than a single party, to create the private key; each of these parties holds a piece of the key—an attacker would require every piece to alter transactions. [99] Thus, if even one of the parties involved in the computation deleted their respective piece, attacks on the zk-SNARK protocol would be made impossible.[100]

---

[95] zk-SNARKs were introduced in a paper published in 2012, authored by Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. *Understanding the Difference Between zk-SNARKs and zk-STARKs*, CHAINLINK, https://blog.chain.link/zk-snarks-vs-zk-starks (Nov. 30, 2023). *See generally* Nir Bitansky et al., *From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again*, ITCS '12: PROCS. 3D INNOVATIONS THEORETICAL COMPUT. SCI. CONF. 326 (2012).

[96] Lyle Daly, *zk-SNARK: Defined & Explained*, THE MOTLEY FOOL, https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/zk-snark/ (Mar. 7, 2024, 9:07 AM).

[97] David Dooley, *ZK-Snarks & Zero-Knowledge Proofs for Dummies*, LINKEDIN (Mar. 13, 2018) https://www.linkedin.com/pulse/zk-snarks-zero-knowledge-proofs-dummies-david-dooley. I further analyze ZCash as a use case later in this article. *See infra* Section II.E.1.

[98] Thomas Chen et al., *A Review of Zero Knowledge Proofs* 28-29 (Dec. 2021) (unpublished manuscript), https://timroughgarden.github.io/fob21/reports/r4.pdf.

[99] *Id.* at 29. It is worth noting that the process involved in multi-party computation can be burdensome. *Id.*

[100] *Id.*

2. zk-STARKS

zk-STARKs were introduced in 2018 as an alternative to zk-SNARKs.[101] zk-STARKs are more scalable[102] than zk-SNARKs "in terms of speed and computational size."[103] While zk-SNARKs require an initial trusted setup, which subjects it to potential misuse by attackers, zk-STARKs circumvent this requirement by having the parameters for generating randomness be public.[104] However, the superior scalability featured in a zk-STARK protocol requires much larger proofs prolonging the verification process, resulting in costlier transactions.[105]

E. Real-World Applications of ZKPs

Below I provide several examples of real-world uses and applications of ZKPs. My intention in doing so is to further contextualize what a ZKP is and how they can be used. In Part III of this article, I will propose an application for the taxation of illegal income, and several of the features I propose are demonstrated in the examples I discuss below.

1. "ZCash": Private Transaction Network

ZCash is a payment application that operates on a blockchain network; it was created by the Electric Coin Company and incorporates ZKPs (zk-SNARKS, to be specific).[106] Despite blockchains being public ledgers,[107] ZCash's use of ZKPs allows the transactions to be entirely encrypted and,

[101] zk-STARKs were introduced in a paper published in 2018, authored by Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. CHAINLINK, *supra* note 95; *see generally* Eli Ben-Sasson et al., SCALABLE, TRANSPARENT, AND POST-QUANTUM SECURE COMPUTATIONAL INTEGRITY (Int'l Ass'n for Cryptologic Rsch., 2018), https://eprint.iacr.org/2018/046.pdf. "zk-STARK" is an acronym for Zero-Knowledge Scalable Transparent Argument of Knowledge. *Id.* at 22.

[102] In this context, "scalability" refers to a system's ability to perform and adapt to increases or decreases in processing demands. *Scalability*, GARTNER, https://www.gartner.com/en/information-technology/glossary/scalability (last visited Feb. 3, 2024).

[103] Jose Segura, *What are zk-STARKs?*, BIT2ME (July 22, 2020), https://academy.bit2me.com/en/que-son-las-zk-stark/.

[104] *Zk-SNARKs vs zk-STARKs: Comparing Zero-knowledge Proofs,* PANTHER PROTOCOL (Sept. 2, 2022), https://blog.pantherprotocol.io/zk-snarks-vs-zk-starks-differences-in-zero-knowledge-technologies/#transparency.

[105] Chen et al., *supra* note 98, at 29.

[106] Benjamin Powers & Ollie Leech, *What Is ZCash? The Privacy Coin Explained?*, NASDAQ (Jan. 26, 2022, 10:00 AM), https://www.nasdaq.com/articles/what-is-zcash-the-privacy-coin-explained.

[107] *Infra* Section II.G.1.

thus, private.[108] To validate and privatize transactions, the ZCash application sends shielded values on the blockchain, using hash functions and zero-knowledge proofs.[109] One notable weakness of the ZCash application is its burdensome computing requirements which consequently may preclude users from using the application's "secure mode."[110] Computational difficulty could be lessened by use of "ZK rollups," which enhance computing efficiency by allowing portions of the transactional computations to be performed off-chain, while still using zero-knowledge proofs to verify the computations on-chain.[111] A final note on the security of the ZCash application—despite security existing on the ZCash ledger itself, nodes on the blockchain are still vulnerable to attack to the extent that a user's IP address is insecure.[112]

2. "MIRACL": Secure Identity Authentication

MIRACL[113] is a user authentication and information security company.[114] One of its applications is "MIRACL Trust," which incorporates zero-knowledge proof technology to provide a single-step, two-factor authentication.[115] MIRACL Trust does not rely on traditional security procedures such as passwords, text/push notifications, or physical measures such as key cards or biometrics, but rather requires users to provide only their PIN.[116] MIRACL Trust is a cloud-based service which bypasses the need to transmit authentication information over the internet, thus eliminating the risk of data breaches caused by compromised passwords.[117] A further benefit of MIRACL's use of ZKP protocols is that it does not store security-related

---

[108] *Id.*

[109] Chen et al., *supra* note 98, at 11.

[110] Dimaz Ankaa Wijaya et al., *A New Blockchain-Based Value-Added Tax System*, *in* PROVABLE SECURITY: 11TH INTERNATIONAL CONFERENCE, PROVSEC 2017 XI'AN, CHINA, OCTOBER 23–25, 2017 PROCEEDINGS 471 (Tatsuaki Okamoto et al. eds., 2017).

[111] Chen et al., *supra* note 98, at 16.

[112] *Id.* at 14.

[113] "MIRACL" is an acronym for "Multiprecision Integer and Rational Arithmetic C/C++ Library." *About MIRACL*, MIRACL, https://miracl.com/about-miracl/ (last visited May 10, 2023).

[114] *See id.*

[115] *Miracl Trust ID*, CITRIX, https://citrixready.citrix.com/miracl/miracl-trust-id.html (last visited May 10, 2023).

[116] "PIN" is an acronym for "personal identification number."

[117] *MIRACL Trust Multi-Factor Authentication*, MIRACL, https://miracl.com/miracl-trust-multi-factor-authentication/ (last visited May 11, 2023); *Introducing MIRACL Trust*, MIRACL, https://miracl.com/ (last visited May 11, 2023).

information on either its servers nor the user's server, thus protecting the prover's sensitive information.[118]

3. "The Sovrin Network": The Ability to Self-Manage Digital Identities

The concept of "digital identity" presents a serious problem with the ability to verify a person's identity on the Internet.[119] Since online interactions are virtual (rather than in-person), it is difficult to verify that a person is indeed who they claim to be; many applications use username-and-password schemes in lieu of the ability to verify a user's identity.[120] However, where an individual's identity verification is required, one common solution is to use a third-party identity verification website; the third-party verifies the user's identity by collecting personal data such as a Social Security number, driver's license, phone number, etc.[121] But this creates a massive security/privacy concern: third-party online usage and storage of such personal data is subject to data breaches, and may result in the user's personal data being obtained by hackers or other bad actors.[122] In the context of this article, this is a relevant discussion—if the IRS were to implement an online application for the taxation of illegal income, they would need a guaranteed method of verifying a taxpayer's identity while simultaneously allowing the taxpayer to retain their anonymity. The innovative technology utilized by the Sovrin Network provides a solution by allowing individuals to self-manage their personal data and securely verify their identity.

The "Sovrin Network" is "a public service utility enabling self-sovereign identity on the Internet. The Sovrin Network is decentralized, meaning individuals can collect, hold, and choose which identity credentials—such as a driver's license or employment credential—to use without relying on individual siloed databases that manage the access to those credentials."[123] This application allows users to create and manage a "self-sovereign identity," which is a "digital identity"[124] managed directly by the

[118] *Zero Knowledge Proof*, MIRACL, miracl.com/zero-knowledge/ (last visited Oct. 19, 2023).

[119] Phil Windley, *Fixing the Five Problems of Internet Identity*, WINDLEY.COM (Oct. 31, 2017), https://www.windley.com/archives/2017/10/fixing_the_five_problems_of_internet_identity.shtml.

[120] *Id.*

[121] *Id.*

[122] Alastair Parr, *Third-Party Data Breaches: What You Need to Know*, PREVALENT (Oct. 11, 2022), https://www.prevalent.net/blog/third-party-data-breaches/.

[123] *FAQs*, SOVRIN, https://sovrin.org/faqs/ (last visited Oct. 21, 2023) ("What is Sovrin?" > "Foundation Basics").

[124] Charlotte Bowyer, *What is digital identity? Your guide to digital identity*, ONFIDO, https://onfido.com/blog/digital-identity (Jan. 12, 2024) ("Digital identity [refers to] a collection of information about a person that exists online.").

user, thus eliminating intervention by third-parties that would otherwise store and manage the data.[125] That is, when data exchange happens between parties on the internet, it is often done via a third-party which stores the data/information; the individuals trust that the system is reliable and secure against breaches.[126] A self-sovereign identity ("SSI") eliminates this flaw by allowing users to self-manage their digital identity.

The Sovrin Network is a blockchain which allows users to manage their SSI on a decentralized platform.[127] The Sovrin Foundation "administers" the Sovrin Network, but the use of SSIs allows users to self-manage their digital identity; moreover, since the Sovrin Network exists on a decentralized blockchain, it is not governed by any central authority.[128] As discussed later in this article, a similar feature would be valuable in an online application for the taxation of illegal income.[129]

Zero-knowledge proofs are essential to this operation. Each piece of personal information (e.g., their Social Security number, driver's license, phone number) that a user provides is called an "attribute."[130] The user then creates a ZKP which is used to prove one of the following about the attribute:

> 1. Equality: if the attribute is equal to the value or an identity holder can just reveal the attribute itself in the proof
>
> . . . .
>
> 2. Inequality: if an attribute lies in a specific range without revealing the actual value. This is helpful when dealing with something that has a numerical attribute, like age or money.
>
> . . . .
>
> 3. Set Membership: ZKPs can prove if a value is contained in a set without revealing [the] value.[131]

---

[125] *Sovrin*, GOLDEN, https://golden.com/wiki/Sovrin-99B8EJ4 (last visited May 11, 2023); *Digital identity – enabling secure collaboration with blockchain technology*, BOSCH, https://www.bosch.com/stories/self-sovereign-identities/ (last visited Oct. 21, 2023).

[126] BOSCH, *supra* note 125.

[127] SOVRIN, *supra* note 123 ("Technical" > "How does Sovrin use Blockchain?").

[128] *Id.* ("What does 'decentralized' mean?").

[129] *Infra* Section III.A.2.

[130] *The Sovrin Network and Zero Knowledge Proofs*, SOVRIN (Oct. 3, 2018), https://sovrin.org/the-sovrin-network-and-zero-knowledge-proofs/ (under the question titled "How does Sovrin use ZKPs?").

[131] *Id.*

Using the Sovrin Network, individuals and organizations may self-manage their digital identity, allowing for personal information to remain confidential and avoiding threats posed by potential data breaches of third parties that would otherwise store the personal data.

F. The Intersection of Tax and ZKPs

The convergence of taxes and ZKPs has already received a degree of attention. In a 2022 article, Matthew Niemerg described the concept of "Zero-Knowledge Taxes" as "a situation in which taxes can be filed and verified with zero-knowledge proofs."[132] In 2018, EY released a protocol that operates on a public blockchain, but uses zero-knowledge proofs to privatize transactions, providing necessary information to auditors and regulators without revealing the content of any transactions.[133] Also in 2018, QED-it and Deloitte collaborated to implement a zero-knowledge proof blockchain that would allow users to accurately report their taxes without disclosing sensitive data.[134] The QED-it blockchain essentially functions by collecting the user's income documents and generating a ZKP as to the calculated tax liability.[135] At no time does the user's data leave their node, and no details of the data are revealed to the verifying party, yet the verifier can be certain that the tax amount is accurate.[136] While these examples differ from the system I propose here, they nevertheless serve to substantiate the value zero-knowledge proofs present in the realm of taxation.

---

[132] Matthew Niemerg, *What Will It Look Like When Taxation and Privacy Collide?*, YAHOO! (Nov. 16, 2022), https://www.yahoo.com/video/look-taxation-privacy-collide-200552419.html.

[133] *EY releases zero-knowledge proof blockchain transaction technology to the public domain to advance blockchain privacy standards*, EY (Apr. 16, 2019), https://www.ey.com/en_bg/news/2019/04/ey-releases-zero-knowledge-proof-blockchain-transaction-technology-to-the-public-domain-to-advance-blockchain-privacy-standards.

[134] Kobi Gurkan, *Zero-Knowledge taxation on Ethereum*, MEDIUM (June 24, 2018), https://medium.com/qed-it/zero-knowledge-qed-it-sdk-b20a6526e0a6.

[135] *Id.*

[136] *Id.*

G. The Role of Blockchain

1. Blockchains: Defined

ZKPs are often discussed within the context of blockchain technology.[137] A "blockchain" is a digital ledger used to record transactions among its users. They are composed of a series, or chain, of "blocks" (hence, "blockchain"); each block contains data documenting a closed transaction.[138] The data comprising a "blockchain" is shared among the network's nodes.[139] A "node" is any computer or device participating in the blockchain network.[140] Each node has a copy of the entire blockchain database/ledger.[141] As a result, blockchains are secure because any node can verify, cryptographically, the validity of each block in the chain.[142] It is worth noting that blockchains may be subject to compromise to the extent of any vulnerabilities in the underlying coding.[143] Many blockchains are "public": that is, transactions are publicly recorded and freely visible to anyone; some blockchains, on the other hand, are private, meaning that access requires approval.[144]

Most blockchain are considered "open-source," meaning that their underlying code can be viewed by anyone;[145] as a result, true anonymity generally does not exist. For example, the popular cryptocurrency Bitcoin operates on a public blockchain and is not truly anonymous, but rather pseudonymous—all transactions are recorded on a public ledger that can be accessed by anyone; as a result, transactions can be traced to a user's digital wallet.[146] The element of anonymity only exists to the extent users do not display their real identity on their digital wallet address, which are publicly visible as well.[147] To this point, ZKPs provide several valuable features to the realm of blockchain: a blockchain that uses ZKPs and self-sovereign

---

[137] *See* Adam Hayes, *Blockchain Facts: What Is It, How It Works, and How Can It Be Used*, INVESTOPEDIA (Apr. 23, 2023), https://www.investopedia.com/terms/b/blockchain.asp.

[138] *Id.*

[139] *Id.*

[140] Lyle Daly, *What is a Blockchain Node?*, THE MOTLEY FOOL (Feb. 1, 2024, 9:42 AM), https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/blockchain-node/.

[141] Hayes, *supra* note 137.

[142] *See id.*

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] Fergus O'Sullivan, *Is Crypto Anonymous in 2024 & Is It More Traceable Than Cash?*, CLOUDWARDS (Jan. 23, 2024), https://www.cloudwards.net/is-crypto-anonymous/.

[147] *See id.*

identities[148] can improve anonymity, avoid the need to store certain personal data, and minimize online transmission of the prover's verification information.

Blockchain infrastructure is not without its flaws—as noted by researchers, anonymity on a blockchain "provides an umbrella for some illegal and criminal acts."[149] But there are solutions to this concern. Discussing the intersection of blockchain technology and taxation schemes, one scholar has presented the concept of "permissioned" blockchains, in which "the platform controls who is allowed to participate in the validation processes and in the protocol itself."[150] It is notable that permissioned blockchains "have a stronger notion of identity."[151]

2. Blockchain Use Cases

a. Blockchain Taxation: Use Cases

With the growing popularity of blockchain technology, the possibilities seem endless as to how it can be implemented and to what extent it can facilitate advancements in both transaction and communication services. One scholar has asserted that blockchain—while not entirely a remedy to deficiencies in the tax system—can reform the world tax regime by reducing administrative burdens, lowering the costs of tax collection, and narrowing the tax gap.[152] Several proposals have been introduced for blockchain-based taxation schemes. In 2017, Wijaya et al. introduced a blockchain-based system for the Value-Added Tax ("VAT"); in the system therein proposed, users would obtain a blockchain account, and would be able to carry out transactions via this account (on the blockchain).[153]

In 2019, Habip Demirhan authored a study dedicated to the intersection of blockchain and taxation.[154] Demirhan identifies tax collection optimization as vital to government efficiency and emphasizes the ability of

---

[148] *See supra* Section II.F.

[149] Huimin Niu et al., *A Blockchain-based Certifiable Anonymous E-Taxing Protocal*, PLOS ONE, July 2022, at 1, 2.

[150] Michał R. Hoffman, *Can Blockchains and Linked Data Advance Taxation?*, WWW '18: COMPANION PROCEEDINGS OF THE WEB CONFERENCE 2018 at 1179, 1180 (2018).

[151] *Id.*

[152] Derya Yayman, *Blockchain in Taxation*, 21 J. ACCT. FIN. 4, 140, 153 (2021).

[153] *See generally* Dimaz Ankaa Wijaya et al., *A New Blockchain-Based Value-Added Tax System*, *in* PROVABLE SECURITY: 11TH INTERNATIONAL CONFERENCE, PROVSEC 2017 XI'AN, CHINA, OCTOBER 23–25, 2017 PROCEEDINGS (Tatsuaki Okamoto et al. eds., 2017).

[154] *See generally* Habip Demirhan, *Effective Taxation System by Blockchain Technology*, *in* BLOCKCHAIN ECONOMICS AND FINANCIAL MARKET INNOVATION 347 (Umit Hacioglu ed., 2019).

blockchain technology to provide digital services to taxpayers.[155] Use of blockchain infrastructure in a tax system may expedite transactions, reduce transaction costs (both for taxpayers as well for the governmental entity), and increase efficiency.[156] For example, proper tax compliance often requires complex computations; human errors in performing these computations may result in reporting discrepancies. Use of a digital tax system would decrease the likelihood of such discrepancies.[157]

b. Blockchain Anonymity: Use Case

The concept of blockchain anonymity, by use of ZKPs as well as other complementary methods, is one that has already garnered academic consideration. In 2018, Wang and Kogan proposed a framework design for a transaction processing system on a blockchain infrastructure, with reliance on ZKPs; their framework was intended to be used for accounting and auditing purposes while preserving confidentiality.[158] Central to their proposal is the use of homomorphic encryption.[159] Homomorphic encryption is a method of encryption which enables computations and generates an encrypted output, which can be decrypted to verify that the result conforms with the operations performed;[160] in the context of Wang and Kogan's framework, use of homomorphic encryption allows the application to perform complex mathematical operations on encrypted data.[161] This model allows users to participate on the blockchain even if they do not trust one another, by providing data anonymity and identity confidentiality.[162] While this proposal merits value for comparison and as a use model, the proposal I make herein differs. My proposal uses a permissioned blockchain and incorporates zero-knowledge proofs, as well as self-sovereign identities. Furthermore, the scheme I propose is intended solely to facilitate payment of tax liabilities on illegal gains; the permissioned aspect would limit transactions to those directed to the IRS for tax reporting and would not

[155] *Id.* at 353.

[156] *Id.* at 353–54. It is worth noting that Demirhan's paper is particularly focused on discussion of blockchain in terms of payroll taxation, value-added taxes, taxation of transfer pricing, and tax audit.

[157] *Id.* at 353.

[158] *See generally* Yunsen Wang & Alexander Kogan, *Designing Privacy-Preserving Blockchain Based Accounting Information Systems*, 30 INT'L J. ACCT. INFO. SYS., 1, 2 (2018).

[159] *Id.* at 6.

[160] Imdad Ullah et al., *Privacy in targeted advertising on mobile devices: a survey*, 22 INTL J. INFO. SEC. 3, 647, 664 (2023).

[161] Wang & Kogan, *supra* note 158, at 6.

[162] *See generally id.*

permit user-to-user transactions, so as to prevent any form of abuse or illegal activity.

III. "SAPTIG": AN ANONYMOUS, PERMISSIONED BLOCKCHAIN-BASED ONLINE TAX FILING APPLICATION FOR THE REPORTING AND TAXATION OF ILLEGAL INCOME WITH RELIANCE ON ZERO-KNOWLEDGE PROOFS

A. An Overview of "SAPTIG.": The Application

Having established a foundation for understanding the current tax treatment of illegal income as well as an analysis of the concept of zero-knowledge proofs and blockchain technology, I turn now to the central thesis of this article: a proposal for an online application for the taxation of illegal income that incorporates zero-knowledge proofs, one which I refer to as "SAPTIG": Secure Application for Paying Taxes on Illegal Gains. SAPTIG would be a permissioned blockchain-based application, administered by the IRS. SAPTIG's user interface would incorporate zero-knowledge proofs, specifically zk-SNARKs,[163] to allow users (taxpayers) to self-manage their personal information via a self-sovereign identity, similar to the technology used by the Sovrin Network.[164] This use of self-sovereign identities would allow users of the SAPTIG application to enter their personal information—including their name and identity verification (such as their Social Security Number)—as well as information regarding the source and amount of their illegal income, while maintaining anonymity.

It may be helpful to think of the user's self-sovereign identity as their "account" on the application. SAPTIG would then compute the user's tax liability and present that amount to the user. The user would pay the amount using SAPTIG's payment platform: the application would process the user's tax payment, confirm the accuracy of the payment amount, deliver payment to the IRS's account, and provide the user/taxpayer with a unique "ticket," which would be assigned to their self-sovereign identity. If the individual were to be audited, the ticket could be presented to SAPTIG for verification, at which point SAPTIG would confirm the accuracy of the payment and income amounts, while keeping the details of the income source private.

---

[163] The use of zk-SNARKs in the SAPTIG application is preferable to zk-STARKS because, while zk-STARKS are generally considered more scalable, they require much larger proofs and utilize public parameters, whereas zk-SNARKs use an initial trusted setup that more appropriately fits the centrally administered nature of the SAPTIG application and its user interface. *See* supra Section II.D.

[164] *See supra* Section II.F.3.

Moreover, SAPTIG would be a "permissioned" blockchain and as such would only allow transactions made by taxpayers to the IRS in the amount of their computed tax liability. This framework would allow individuals to avoid prosecution for failure to report their illegal income, while also presenting the IRS, and the federal government at-large, a way to administer taxes on illegal income without concern of any potential breach of the taxpayer's Fifth Amendment privilege against self-incrimination.

1. A Permissioned Blockchain Network

Below, I expound upon the different features of this proposed application.

a. Why Blockchain?

ZKPs do not necessarily need to exist on a blockchain platform; they can be used in non-blockchain applications and contexts as well. Thus, an important consideration at this point is why the SAPTIG application should be based on a blockchain network. One may wonder why the taxation of illegal income couldn't be accomplished by a simpler method. In other words, why couldn't a non-blockchain application be used to accomplish the goal of this article? A significant consideration in proposing a system for the taxation of illegal income is that individuals with illegal gains likely wouldn't trust an application administered by the government *if* it stored their personal identification information. Moreover, any application that accesses and stores personal data is subject to cybersecurity breaches. But if self-sovereign identities were used, the SAPTIG application wouldn't need to store the individual's identification information. Rather, the individual would be able to self-manage their digital identity. Assuming that self-sovereign identities (SSIs) were indeed incorporated into the SAPTIG application, SSIs require a blockchain network to operate,[165] thus why I herein propose the use of blockchain. And if that blockchain were a "permissioned" blockchain, it would essentially enable the SAPTIG application to operate as a tax computation and payment application, while still being able to host the self-sovereign identity feature, thus providing both anonymity and data security to taxpayers.

[165] *Self-Sovereign Identity: The Ultimate Guide 2023*, DOCK (May 14, 2024), https://www.dock.io/post/self-sovereign-identity.

b. Incorporating Blockchain into the SAPTIG Application

With advancements in computer technology and paper tax systems becoming antiquated, governments have begun experimenting with electronic tax filing systems. In 2024, the IRS launched a "direct file" pilot system allowing taxpayers to electronically file their taxes for free.[166] The IRS has since announced that this system will be permanent beginning in 2025, claiming the pilot to have been a success.[167] However, this program has faced backlash in that the IRS would essentially be directly operating as both tax collector and tax preparer, creating a potential conflict of interest between taxpayers and the government.[168] Further criticism has noted that such a system would be costly in terms of IRS resources that may be better allocated elsewhere.[169] However, an application operating on a blockchain network and utilizing ZKP algorithms would resolve these criticisms by presenting the IRS with a means to administer taxes while allowing taxpayers to retain anonymity, privatizing their tax payments, and addressing conflict of interest concerns by employing a trustless zero-knowledge system.

While I present the hypothetical "SAPTIG" application principally as a means to tax illegal income, the same technology could eventually be integrated to streamline the entire federal income tax regime. Consider the following case study. In 2022, three researchers proposed the framework for a "blockchain-based self-certified and traceable e-taxing scheme that verifies the authenticity of taxpayers without revealing their true identity, thus balancing the contradiction of taxpayer privacy and supervision."[170] In making this proposal, the researchers sought to balance taxpayer privacy and supervision.[171] The researchers pointed out a notable flaw in the concept of an electronic tax filing system: "If tax authorities and taxpayers do not trust each other in handling data, it will be more difficult to implement a centrally administered tax system."[172] An application that utilizes a blockchain

---

[166] Wyatte Grantham-Philips & Fatima Hussein, *IRS moves forward with free e-filing system in pilot program to launch in 2024*, THE ASSOCIATED PRESS (May 16, 2024, 4:39PM), https://apnews.com/article/tax-irs-taxpayers-direct-file-ef2e9f92ad45984487fd368b851773af.

[167] U.S. Department of the Treasury, IRS Announce Direct File as Permanent Free Tax Filing Option, All 50 States and D.C. Invited to Join in Filing Season 2025, U.S. DEP'T OF TREAS. (May 30, 2024), https://home.treasury.gov/news/press-releases/jy2385.

[168] *Id.*

[169] *Id.*

[170] *See generally* Huimin et al., *A Blockchain-based Certifiable Anonymous E-taxing Protocol*, 2022 PLOS ONE.

[171] *Id.* at 1.

[172] *Id.* at 2.

network that incorporates zero-knowledge proofs and self-sovereign identities would eliminate the distrust concern.

While the SAPTIG application I herein propose would indeed be a permissioned blockchain,[173] it would conceal the taxpayer's true identity by way of their self-sovereign identity, thus preserving user anonymity while preventing malicious use of the application. The SAPTIG application would only serve the following functions: (1) verification of the user's identity by use of a self-sovereign identity; (2) computation of the user's tax liability; (3) processing the user's tax payment from the user to the IRS, while concealing the identity of the user/taxpayer (so as to retain anonymity); and (4) issuing the user/taxpayer a "ticket" (in essence, a receipt) as verification of their payment and assigning that ticket to their self-sovereign identity.

2. Self-Sovereign Identities and Electronic Ticketing

A "self-sovereign identity"[174] is a feature, enabled by the use ZKPs, that allows a user to self-manage their identity verification information (e.g., their Social Security Number) rather than allowing a third party to manage and store such information; this minimizes risk of data breach, protecting the user's identity and personal data.[175] SAPTIG would incorporate the concept of self-sovereign identity technology, thus allowing it to verify the identity of a user/taxpayer while allowing the user to retain anonymity. The SAPTIG application would use zk-SNARKs, e.g., for tax computations and payment transactions, which would require the user to store the private key in a secure location. Upon creating their account, the SSI feature would serve to verify the user's identity while shielding it, via zero-knowledge proofs, from being viewable by the SAPTIG central administer, that is, the IRS. Since the SSI stores personal, identifiable information such as the user's social security

[173] *Supra* Part 3.

[174] *Supra* Section II.F.3.

[175] In addition to countering the security vulnerability posed by third-party data storage, use of self-sovereign identities would also overcome the element of distrust among the taxpaying public. Even among law-abiding taxpayers, distrust of third-party storage of personal data prevails. In January 2022, the IRS announced that it would implement a third-party facial recognition software, known as "ID.me," that by the summer of that same year would be a taxpayer's only means to log in and manage their tax accounts online. Corin Faife, *IRS Will End Use of Facial Recognition After Widespread Privacy Concerns*, THE VERGE (Feb. 7, 2022, 1:50 PM), https://www.theverge.com/2022/2/7/22922212/irs-id-me-facial-recognition-end-privacy-concerns. This announcement was met with overwhelming backlash; the taxpaying public expressed concern in being required to trust a third-party software company with their personal data, resulting in the Service cancelling its proposal. *Id.*

number, it would ensure that the user is indeed who they claim to be while precluding any self-incrimination concerns.

Xuelian Li et al. proposed a blockchain-based electronic "ticketing" system in which a user's identity information is bound to a unique ticket—a concept that is adaptable to the SAPTIG application.[176] Specifically, this ticketing concept could serve as a supplement for taxpayers to maintain a unique digital identity used specifically for reporting and paying taxes on their illegal income.[177] While the scheme proposed by Xuelian Li et al. differs in purpose and function from the SAPTIG application I propose here, the concept they introduced—that is, binding a user's identity to a unique ticket—is one that would be a valuable aspect of SAPTIG.[178]

Upon a user's payment of their computed tax liability, SAPTIG would generate a unique ticket and assign the ticket to that taxpayer's self-sovereign identity. For all intents and purposes, this ticket serves as the user's receipt. If said taxpayer was ever subject to audit, they could provide that unique ticket, thus proving their tax compliance while maintaining anonymity and avoiding any self-incrimination. In other words, SAPTIG would confirm (1) that the ticket is valid and (2) the amount of the tax payment, while concealing any incriminating information, such as the source of the income. This would allow the user-taxpayer to remain tax compliant and avoid prosecution for failure to report their illegal income (e.g., upon being audited or independently investigated for their illegal activity) while precluding any potential violation, by the IRS/federal government, of the taxpayer's Fifth Amendment privilege against self-incrimination.

B. Notable Critiques of This Proposal

There are several notable critiques of the application proposed in this article.

1. Computational Difficulty

First, it would require a massive computational capacity. Presently, much of the technology currently employed by the IRS relies on infrastructure built in the 1960s.[179] Thus, the efficiency of such an application

---

[176] Xuelian Li et al., *Secure Electronic Ticketing System Based on Consortium Blockchain*, 13 KSII TRANSACTIONS ON INTERNET & INFO. SYS. 5219, 5220 (2019).

[177] *Id.* at 5222, 5220.

[178] *Id.* at 5219.

[179] Alexander Ray, *Challenges of Zero-Knowledge Proof Technology For Compliance*, FORBES (Aug. 30, 2023, 9:15 AM), https://www.forbes.com/sites/forbesbusinesscouncil/2023/08/30/challenges-of-zero-knowledge-proof-technology-for-compliance/?sh=5fd0c60d4071; Grace Dille, *Outdated*

would require an overhaul of the IRS's technological infrastructure. Such outdated systems cause delayed processing of tax returns and pose an increased risk of cybersecurity breaches and, relatedly, result in unforeseen expenses.[180] Historically, the need for such a massive overhaul would be dismissed in light of the IRS's past underfunding.[181] However, a recent funding bonus of $80 billion, to be allocated over the course of the next decade, presents an opportunity to completely rebuild their technological infrastructure and potentially introduce a comprehensive, electronic tax filing system.[182] The IRS has already begun developing and implementing programs for direct filing online.[183]

2. Operating a Self-Sovereign Identity on a Permissioned Blockchain

Another conflict is the use of self-sovereign identities on a permissioned blockchain network. Permissioned blockchains, which I have proposed be incorporated to limit the use of the SAPTIG application,[184] are considered "partially," rather than fully, decentralized because the users are known;[185] in a permissioned blockchain, users must be admitted or given "permission" to join the blockchain network.[186] While this aspect would seemingly sacrifice the element of anonymity that is central to my proposal, the use of self-sovereign identities and unique "tickets" assigned to users' self-sovereign identities, and the incorporation of zero-knowledge proofs, would, theoretically, achieve anonymity. That being said, self-sovereign

Tech at the IRS is Slowing Down Your Tax Refund, MERITALK (Feb. 16, 2023, 2:21 PM), https://www.meritalk.com/articles/outdated-tech-at-the-irs-is-slowing-down-your-tax-refund/.

[180] Dille, *supra* note 179; *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements*, GAO (Jan. 12, 2023), https://www.gao.gov/products/gao-23-104719.

[181] *See Chart Book: The Need to Rebuild the Depleted IRS*, CTR. ON BUDGET & POL'Y PRIORITIES 1, https://www.cbpp.org/sites/default/files/7-2-21tax-chartbook.pdf (last updated Dec. 16, 2022) (explaining that the "the IRS budget has been cut dramatically over the past decade, severely undermining the agency's ability to perform its fundamental jobs of enforcing the nation's tax laws and helping taxpayers navigate a tax system that relies on voluntary compliance").

[182] Benjamin Guggenheim, *IRS releases plan to spend $80 billion windfall – with critical details missing*, POLITICO (Apr. 6, 2023, 3:57 PM), https://www.politico.com/news/2023/04/06/irs-releases-plan-with-critical-details-missing-00090811.

[183] *Id.*

[184] *Supra* Section III.A.2.

[185] *Permissioned blockchain vs. permissionless blockchain: Key differences*, COINTELEGRAPH, https://cointelegraph.com/learn/permissioned-blockchain-vs-permissionless-blockchain-key-differences (last visited Oct. 21, 2023).

[186] *Id.*

identities require decentralization to operate.[187] Thus, creating the SAPTIG application would have to be done meticulously to allow self-sovereign identities to operate on a permissioned blockchain.

3. User Accountability and Private Key Storage

The SAPTIG application's use of zk-SNARKs relies on the user retaining their private key and storing it in a secure location to avoid fraudulent activity, such as accessing personal data, being conducted by hostile parties. In other words, the security of zk-SNARKs generally relies on the prover (or, in the context of the SAPTIG application, the user) to keep their private key secure and unobtainable by a hostile party.[188] However, this risk could be mitigated by implementing a technique similar to the previously discussed "multi-party computation."[189] Specifically, the zk-SNARK protocol could generate multiple private keys and provide the individual user with each of the multiple private keys (rather than providing each key to a different party). Thus, a hostile party would need to obtain each of these keys to perform fraudulent proofs.

4. Taxpayer Trust in the Administration of the SAPTIG Application

Finally, perhaps the most obvious critique is the paradoxical element of trust—while proper implementation of zero-knowledge proofs into an application can provide anonymity to preclude the need for trust between the parties, use of such an application inherently requires users to trust that the software works correctly. Undoubtedly, many potential users of the SAPTIG application would be unfamiliar with zero-knowledge proofs and computer science at-large. Such users would have to trust that anonymity indeed exists and that the IRS will centrally administer the blockchain appropriately and honestly. Moreover, users might be dissuaded by the complexity involved. The application would therefore need a simple, unsophisticated user interface.[190] But these concerns would likely only persist initially and would assuage as use of electronic taxing and the anonymity provided by zero-knowledge proofs become mainstream and more widely understood. Moreover, the development and implementation of this application are not solely to provide taxpayers with a method to anonymously report illegal income; conversely, it provides the government with a constitutional means

[187] DOCK, *supra* note 164.
[188] *See supra* Section II.D.
[189] *See supra* Section II.D.1.
[190] *See* FORBES, *supra* note 179.

to assess taxation of illegal income, which would counter Fifth Amendment defenses in prosecutions against taxpayers for failure to report illegal income.

CONCLUSION

My proposal is for a permissioned blockchain-based protocol for the taxation of illegal income, which incorporates zero-knowledge proofs ("ZKPs") and would be administered by the IRS. Such an application would allow users to retain anonymity, despite being created and operated by the IRS. Specifically, the use of self-sovereign identities would prevent disclosure of potentially incriminating information, thus eliminating any potential violation by the federal government of taxpayers' Fifth Amendment privilege against self-incrimination. Upon payment of the computed tax liability, the proposed protocol would generate a unique electronic "ticket," which would be assigned to that user's self-sovereign identity. In the event of an audit, the taxpayer would be able to demonstrate their tax compliance by providing their unique ticket, which would allow their tax payment to be confirmed while concealing any incriminating information.