MARTIN YAT-CHEUNG KWAN*

Liabilities for Unknowingly Being Paid with Misappropriated Cryptocurrencies: Can U.S. and U.K. Laws Respond Properly?

* Kwan Yat Cheung Martin is an Honorary Fellow at the HKU Asian Institute of International Financial Law, with established expertise in international business and global markets. He is a strategic adviser to senior executives and family offices. He also consults for international institutions, most recently for the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) on digital business development and market regulation. With extensive experience in technology regulation and policy, Martin Kwan is an affiliated member of Monash Business School's Centre for Development Economics and Sustainability, and the UNC Center for Information, Technology, and Public Life. The author would like to thank the editorial team at *ORIL*. Contact: mkwan1@connect.hku.hk.

ABSTRACT

Inspired by recent incidents of crypto platforms allegedly misappropriating their clients' investments, this Article explores the potential liabilities faced by a third-party payee of the misappropriated cryptos. This is a timely topic as more and more businesses (such as luxury goods retailers) accept crypto payment.

In the absence of tailored laws for the blockchain commercial context, general legal principles apply in the United States to determine criminal and civil liabilities for the above context. However, current U.S. law treats "suspicion" as a key and substantial consideration—unfortunately a standard that is not just unbefitting for the blockchain context, but also unfairly shifts the regulatory burden to the payee by imposing impractical obligations to act prudently and to inquire further. This is because blockchain analysis (e.g., tracing wallet addresses) could readily reveal seemingly suspicious circumstances sufficient for triggering the legal obligations and liabilities, even if the payee could not realistically ascertain whether there was misappropriation or just a false alarm. Upon comparison, English law establishes the knowledge requirement based on probable existence—as opposed to mere suspicion—of interference with victims' rights. The higher threshold under English law suits the blockchain context better than the U.S. law.

Any future rulings should distinguish the blockchain context when applying generic legal principles that are heavily premised on suspicion, though it is unclear if the existing strict legal thresholds in the United States could provide the space for the court to do so. The English formulation of legal principles, by contrast, allows judicial deference to the market's choice of how to process crypto payments.

INTRODUCTION

This Article analyzes underexplored legal issues in relation to a legitimate payee's obligations and potential liabilities for having unknowingly received misappropriated cryptocurrencies. Inspired by an ongoing investigation of an alleged widespread crypto fraud in Asia[1] and the case of Binance in the United States,[2] a hypothetical scenario can be laid down as follows:

> Party A holds funds on behalf of their clients. They can, for example, be a crypto-currency investment platform where clients also deposit funds and cryptos for exchange.
>
> Party A pays for the product or service of Party B with cryptocurrencies.
>
> The products or services provided by Party B can be—for example—marketing, advertising, consultancy services, luxury goods, etc. Party B is a legitimate provider that is independent of Party A.
>
> Party A should have paid Party B with its own money that is separate from clients' money. But blockchain-based analysis (explained in Part I) suggests that the digital payment made to Party B *might* come from the funds held on trust by Party A for their clients.
>
> After receiving the payment, it turns out Party A—now insolvent or absconded—paid with misappropriated cryptos.

This Article will explore the legal risks faced by Party B—as a legitimate payee with clean hands—when the payment was merely suspicious. The problem is that just because there are suspicious circumstances, it does not necessarily mean there must have been

---

1 A crypto-currency exchange platform under investigation, JPEX, sponsored a sporting event. Reportedly, some speculated, based on the method mentioned in Part I, that the sponsorship payment came from clients' funds deposited with JPEX. *See* JKL Group, *September Overview: Your Monthly Brief into the World of Digital Assets*, MEDIUM (Sept. 29, 2023), https://jkl-capital.medium.com/september-overview-cc4b01dc8497#_ftn3 [https://perma.cc/SX34-9KY4] ("After the boxing match, it was discovered that the prize money sponsored by JPEX was transferred directly from the exchange's wallets that contained user deposits. This was reported in major Chinese crypto news outlets and led to renewed suspicion from existing users of JPEX in Hong Kong, as well as those in Taiwan who were new to this brand"). The investigation is still ongoing, so this Article will not delve into the details of that investigation. Instead, it will put forward a hypothetical situation for analysis raising some unexplored legal issues.

2 Rohan Goswami, *SEC Sues Binance and CEO Changpeng Zhao for U.S. Securities Violations*, CNBC (June 23, 2023), https://www.cnbc.com/2023/06/05/sec-sues-binance-and-ceo-changpeng-zhao-for-us-securities-violations.html [https://perma.cc/8Q3R-KKK2] (Binance allegedly runs an "unregulated international exchange, commingled investor funds with their own and violated securities laws.").

criminal misappropriation. It could be a false alarm caused by noncriminal poor management of crypto wallets, for example. Blockchain analysis cannot realistically ascertain whether there has been misappropriation. Yet mere suspicion can trigger criminal and civil liabilities.

It is foreseeable that a legal analysis will be relevant and necessary to many other analogous situations—for example, when the fund manager or trustee of a crypto investment fund purchases luxury properties and goods with misappropriated cryptocurrencies. Many retail venues now accept payment via cryptocurrencies.[3] A legal analysis will inform the future regulation of cryptocurrencies and platforms and will help to clarify obligations of involved parties.

Clarifying these obligations is important for three reasons. First, the victims may want to apply for an injunction against Party B in relation to the proceeds and pursue recovery. Second, Party B, as any business, should know the potential risks and liabilities of accepting cryptos as payment. Third, regulators need to act upon uncertainties to ensure market functioning and integrity for all stakeholders.

Practicality aside, the Article also concludes that the current state of US law—of which liabilities are centered on the threshold of suspicion—imposes unbefitting legal obligations that do not keep up with the technological circumstances and the blockchain development. Exposing Party B to the legal risks is disproportionate and will not help resolve or prevent the problems caused by Party A.

The crux of the problem is that the US does not have a tailored legal regime for the blockchain commercial context, meaning that general legal principles and causes of action have to be applied.[4] Notably,

---

3 Shilpa Dhamija, *Why Do Luxury Brands Accept Crypto Despite Its Volatility? Gucci, Balenciaga, Hublot, Soneva Resorts, Kessler Collection and Farfetch Still Deal in Digital Currencies. . . With Safety Nets in Place*, S. CHINA MORNING POST (Nov. 17, 2022), https://www.scmp.com/magazines/style/luxury/article/3199925/why-do-luxury-brands-accept-crypto-despite-its-volatility-gucci-balenciaga-hublot-soneva-resorts [https://perma.cc/PC6S-EBMT].

4 *See, e.g.*, Andrew W. Balthazor, *The Challenges of Cryptocurrency Asset Recovery*, 13 FIU L. REV. 1207 (2019) (discussing the range of generic legal measures); Joshua A.T. Fairfield, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, 97 IND. L.J. 1261, 1282 (2022) (citing traditional remedies including conversion, replevin, and trespass to chattels); Farshad Ghodoosi, *Crypto Litigation: An Empirical View*, 40 YALE J. ON REG. 87 (2022) ("The causes of action were divided into (a) contract, (b) tort, (c) securities, (d) consumer protection statutes, (e) trademark, and (f) derivative (fiduciary duty) actions. For coding purposes, contract claims include breach of contract, breach of duty of good faith and fair dealing, unjust enrichment (quasi-contract), and breach of fiduciary duties (other than derivative suits). Tort claims include misrepresentation,

practitioners have resorted to the "ancient" tort of conversion for recovery in the blockchain context.[5] That said, applying generic principles to novel issues—just like the present one involving the intersection between blockchain, commerce, and law—is not necessarily an issue if they can adequately resolve the matter. However, this is not the case under U.S. law which is centered on suspicion—a threshold that is unsuitable for the blockchain context. By contrast, English law does not share the same problem, even though similarly only generic principles are available.

This Article compares the legal positions under United States and United Kingdom law. They are particularly noteworthy because Anglo-American laws are popular common law jurisdictions in the commercial and crypto contexts.[6] The evolving nature of the precedential common law, in theory, should allow the law to develop more flexibly than statutory law in catering to the fast-developing market needs.[7] Nevertheless, when the existing generic common law

---

fraudulent concealment, fraud in the inducement, and conversion. Securities-based suits include violations of Sections 5, 12, 15, and 17 of the Securities Act and Sections 10(b) and 20 of the Exchange Act, along with violations of state securities laws. Consumer protection causes of action include suits brought under statutes such as the California Unfair Competition Law, California Consumer Legal Remedies Act, and Civil RICO among others."). *See also* Jacobo v. Doe, No. 1:22-cv-00672-DAD-BAK, 2022 U.S. Dist. LEXIS 101504, at 1 (E.D. Cal. June 7, 2022) ("[A]sserting claims of fraudulent inducement, negligent misrepresentation, replevin, conversion, unjust enrichment, imposition of a constructive trust and disgorgement of funds, and possession of stolen property in violation of California Penal Code § 496.").

5 Robert A. Schwinger, *Blockchain Law Ancient Torts and Modern Assets*, NORTON ROSE FULBRIGHT (Jan. 23, 2024), https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/nylj-ancient-torts-and-modern-assets.pdf [https://perma.cc/NFK8-RUFT].

6 *See, e.g.*, Andrew Taylor, *A Comparative Analysis of US and English Contract Law Interpretation and Implied Terms*, INT'L IN-HOUSE COUNS. J., 2015, 1 ("English law is the governing law of choice for many international cross-border contracts and many international companies have manufacturing, trading or operational hubs in the US and the UK. British-American relations of course remain strong ensuring trade and investment between the US and UK, giving rise to a variety of cross-border contractual arrangements governed by either English or US law."); Iris H-Y Chiu, *Central Bank Digital Currency for The Crypto-Economy: An Experimental Proposal Based on the European Single Market and Institution-Building*, 51 CAL. W. INT'L L.J. 253, 310 (2021) (remarking on the prevalence of crypto activities in the United States and the U.K.); Omri Marian, *Blockchain Havens and the Need for Their Internationally-Coordinated Regulation*, 23 FLA. TAX REV. 770 (2020) (noting the "top jurisdictions" for crypto activities include the United States and the U.K.).

7 *See, e.g.*, Matthias Lehmann, *National Blockchain Laws as a Threat to Capital Markets Integration*, 26 UNIF. L. REV. 148, 152 (2021) (Lehmann also compared the Anglo-

offenses and private law principles are already well-established long before the age of cryptos, their rigid application to this modern context could easily lead to undesirable outcomes.

In the criminal context, English law establishes liability based on a commercially sensible basis, such as requiring proof of dishonesty which will not pose any problem to a Party B who unknowingly received an embezzled sum. By contrast, U.S. law triggers criminal liability based on constructive and/or imputed knowledge, which is detrimental to Party B, who is suspicious. In the civil liability context, English law shares similar causes of action to U.S. law, such as restitution. English law, however, requires proof of a probable cause for Party B to believe the payment was stolen, which is a higher threshold than suspicion under U.S. law. Besides, Party B is not required to act prudently/cautiously under English law. The prudence requirement under U.S. law—a standard imposing a higher expectation than a reasonableness requirement—is incompatible with the pseudonymous and complex nature of cryptos that is prone to incite suspicion to a Party B. It is legally, and hence commercially, uncertain as to what a prudent/cautious business (Party B) should have done, and whether Party B's response has been prudent *enough*. This in effect is asking the U.S. court to review how a crypto payment should have been prudently processed when things now turn out to be wrong. But by adopting a higher threshold, English law provides more flexibility for the courts to accord deference to the market choice of processing crypto payment.

Part I will first explain more about the technical background as to how a blockchain-based transaction can reveal some signs for suspecting the legitimacy of the crypto payment. Parts II and III will explore the potential criminal and civil liabilities faced by Party B under U.S. law. Part IV argues that the risk of attracting liabilities cannot be easily resolved because it is not always practical to conduct due diligence. Part V compares the U.S. approach with the English approach and argues that the latter is more desirable. Part VI captures the gist of the distinction between the United States and English approach as to whether the formulation of legal principles is broad enough to provide the courts with the leeway needed to defer to market's handling of crypto payments, when it is an inherently riskier form of payment given its novelty and insufficient regulation.

American legal approaches, and noted for example, that the English court can swiftly make a disposition on the debatable property nature of crypto assets via the common law system).

I
WHEN THE PAYMENT SEEMS SUSPICIOUS

There are technical ways to investigate the source of the fund, commonly known as "blockchain monitoring" or "blockchain analysis" in the literature.[8] For example, one can look at the digital address (a unique string of numbers) of the cryptocurrency wallet.[9] If the wallet address used for payment is the same as the wallet used for collecting clients' money, it could suggest inappropriate mingling and/or misappropriation of funds. Normally, Party A's own funds should not be mixed with that of their clients.[10] Other suspicion-triggering indicators include, for example, when Party A's wallet for payment has voluminous traces of receiving sums, something that usually only happens with an account for depositing clients' investments.

But usually there is no conclusive evidence as to whether there has been mingling or misappropriation of funds, for example, when Party A avers that the money paid to Party B is separate from its clients' money. From a technical standpoint, the general inability to accurately ascertain the ownership (e.g., pinpointing the name of the owner), apart from tracing wallet addresses, has been widely acknowledged by

---

8 *See, e.g.*, DOMINIQUE BERNARD KANGA ET AL., *Methodology of the Blockchain Monitoring Framework*, *in* BLOCKCHAIN APPLICATIONS—TRANSFORMING INDUSTRIES, ENHANCING SECURITY, AND ADDRESSING ETHICAL CONSIDERATIONS 36 (Vsevolod Chernyshenko & Vardan Mkrttchian eds., 2023); Ly-Yu Dieu et al., *AML Due Diligence for Virtual Assets Using Blockchain Analysis*, LEXOLOGY (Oct. 11, 2023), https://www.lexology.com/library/detail.aspx?g=fb8ff84d-72ac-4429-86eb-5db09f16e8a0 [https://perma.cc/JR2T-5ZWS]; Sophie Hares, *5 Ways Accountants Can Track Cryptocurrency*, CPA INSIDER (June 2020), https://www.journalofaccountancy.com/newsletters/2020/jun/accountants-track-cryptocurrency.html [https://perma.cc/YPN8-3W3B] ("Using blockchain, the transparent ledger that records the transaction history of each coin, investigators can then start to piece together any scraps of information they glean to try to prove ownership of the virtual funds."); Robert A. Schwinger, *Anonymous No More: Blockchain Analytics in the Courts*, N.Y.L.J. (May 23, 2022), https://www.law.com/newyorklawjournal/2022/05/23/anonymous-no-more-blockchain-analytics-in-the-courts/ [https://perma.cc/AN7V-4SNY]; *In re Search Multiple Email Accounts Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956*, 585 F. Supp. 3d 1 (D.D.C. 2021) at 7–8 (D.D.C. Aug. 26, 2021).

9 Fatema Merchant et al., *Money Laundering and High-Value Art: Treasury's Study Discusses Financial Crimes and NFTs*, L. LEDGER (Mar. 2, 2022).

10 *See, e.g.*, Cooper v. Union Bank, 9 Cal. 3d 371, 382–83 (1973) ("funds, instead of being mingled, must be kept separate from the agent's own funds and identified as the property of the principal").

practitioners.[11] The pseudoanonymous nature of crypto precludes a third party, like Party B, to verify who owns the paid sum comprising of multiple tokens.[12] Only the flow is traceable.[13]

It is also impractical for Party B to ascertain, especially during a transaction, whether there was fraud or theft by Party A against the clients. On the one hand, the whole investment platform could be a Ponzi scheme. On the other hand, Party A's platform itself could be legitimate. However, personnel within Party A could have gone rogue and misappropriated the sum. The point here is that Party B would not know the exact details behind the red flags.

This is why this Article focuses on situations in which the payment is *suspicious*. The gist of the problem is that the existence of suspicion can form the preliminary basis for both criminal and civil liabilities under U.S. law—thereby exposing Party B to legal risks and uncertainties.

The discussion below proceeds on the basis that Party A actually paid Party B with clients' money. There were suspicious circumstances (e.g., Party A seemingly paid from a wallet address that could be used for holding clients' funds, or simply that Party A is a crypto investment platform claiming unusually high returns for clients), but Party B did not know the actual truth (e.g., source of payment and whether any crime was involved) at that time, and could not have realistically ascertained the legitimacy of the payment.

---

11 This is self-evident from the Singaporean judgment *CLM v. CLN* [2022] SGHC 46, where the petitioner and the Singaporean court traced the misappropriated proceeds to a specific wallet and imposed a freezing injunction against it, despite not knowing the identity of malefactor. Alessio D. Evangelista et al., *Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview*, SKADDEN (Sept. 7, 2022), https://www.skadden.com/insights/publications/2022/09/cryptoasset-seizures-and-forfeitures [https://perma.cc/4LXS-73LQ]; *See also supra* note 9 (noting similar observations by practitioners and other courts). *See also* discussion *infra* note 104.

12 *See, e.g.*, *In re Search*, 585 F. Supp. 3d at 7 ("Cryptocurrency transactions that occur on a blockchain are, by design, publicly available, and thus are pseudoanonymous").

13 *Id.* at 8 (quoting *In re Search* of one address in Washington, D.C., under rule 41, 512 F.Supp.3d 23, 29 (D.D.C. 2021) that "the public nature of the blockchain makes it exponentially easier to follow the flow of cryptocurrency over fiat funds"). *See also* Jacobo v. Doe, 1:22-cv-00672-DAD-BAK (BAM) (E.D. Cal. June 7, 2022) at 3 (traced a number of crypto wallets of which the ownership of some of the accounts were "unknown").

II
POTENTIAL CRIMINAL LIABILITY UNDER U.S. LAW

Under the U.S. Model Penal Code, it is an offense to knowingly possess stolen property.[14] Although Party B does not have actual knowledge as to the source of the payment, the offense is still applicable. Unlike theft, this offense generally does not require proof of dishonesty.[15]

A. A Criminal Conviction Does Not Strictly Require Proof of Actual Knowledge

The defendant, Party B, can be convicted even though it does not have *actual* knowledge as to whether the property was stolen. The knowledge requirement is defined by many states to include situations where Party B "should know," "should have known," or "has reasonable cause to know" the property was stolen.[16] This means an

---

14 Stuart P. Green, *Thieving and Receiving: Overcriminalizing the Possession of Stolen Property*, 14 NEW CRIM. L. REV. 35 (2011); Model Penal Code, § 223.6 (2017). For Wyoming, see WYO. STAT. ANN. § 6-3-402 (2022). For Florida, see FLA. STAT. § 812.019 (2023) (providing for the offense of dealing or trafficking in stolen property); FLA. STAT. § 812.012(2)(b) (2023) (defining "traffic" to include to "receive" and "possess"). Given the borderless nature of fund transfer, the federal offense of knowing receipt becomes relevant if there is an interstate element. 18 U.S.C § 2315.

15 Green, *supra* note 14. For example, the offense of "dealing in stolen property" in Florida neither requires dishonesty nor an intent to permanently deprive others of the property. *See* FLA. STAT. § 812.019 (2023); United States v. Sanchez-Rodriguez, 830 F.3d 168, 174 (5th Cir. 2016) (noting that this offense in Florida is broader than theft as the former does not require proof of the intent to deprive others of the property).

16 For Ohio, see OHIO REV. CODE ANN. § 2913.51 ("No person shall receive, retain, or dispose of property of another knowing or having reasonable cause to believe that the property has been obtained through commission of a theft offense"); State v. Peck, 4835 Ohio 1, 12 (Ohio Ct. App. 2013) (applying the standard of "should have known"). For Florida, see FLA. STAT. § 812.019 (2023). For Colorado, see COLO. REV. STAT. § 18-5-903 (2022) ("A person commits criminal possession of a financial device if the person has in his or her possession or under his or her control any financial device that the person knows, or reasonably should know, to be . . . stolen . . . ."). For Illinois, see, e.g., People v. Nelson, 336 Ill. App. 3d 517, 521 (2003) (applying the test of whether "a person of ordinary intelligence presented with the [property] under these circumstances would reasonably be induced to believe that the merchandise had been stolen"; confirming the constitutionality of such objective standard; and also noting that "Illinois courts have consistently used an objective test for the *mens rea* element of theft by receiving stolen property."). *See also* Rollin M. Perkins, "*Knowledge" as a Mens Rea Requirement*, 29 HASTINGS L.J. 953, 954 (1978).

Cf. Nebraska adopts a subjective standard of knowledge, requiring *actual* knowledge. *See* State v. Almasaudi, 282 Neb. 162, 170–73 (2011) (where the Nebraska Supreme Court noted

objective standard is applied in many states.[17] This forms a contrast to other states where their equivalent offense applies the subjective standard based on the "know or have reason to know" standard without adopting the term "should have known."[18] That said, the subjective standard is still a much looser one that takes into account circumstantial evidence and the inference of knowledge,[19] sometimes even taking reference of what a reasonable person would have been aware of.[20]

In addition, the mere possession of stolen property itself could lead to an inference of knowledge.[21] The courts have explained that, as

---

that other states adopt the objective "should know" standard). Another state which adopts the subjective standard is Pennsylvania. *See* 18 PA. CONS. STAT. § 3925 (2022) (did not use the terms indicating an objective standard like "should have known"); Commonwealth v. McFarland, 226 Pa. Super. 138, 138 (1973) ("the question is not what a reasonable man would have known but what the defendant knew; and the only pertinence in asking what a reasonable man would have known is in considering whether, because a reasonable man would have known it, the defendant did.").

17 *See, e.g.*, State v. Calloway, 1 So. 3d 417, 422 (La. 2009) ("we also recognized that jurors may infer guilty knowledge from the circumstance of the offense, i.e., that defendant knew 'or had good reason to believe' that the goods in her possession had been stolen. La. R.S. 14:69(A) . . . The statute permits a *purely objective inquiry* into the element of guilty knowledge") (emphasis added). The same quote was applied in State *ex rel.* T.C., 361 So. 3d 505, 505 (La. Ct. App. 2023).

18 D. Randall Johnson, *The Criminally Derived Property Statute: Constitutional and Interpretive Issues Raised by 18 U.S.C. § 1957*, 34 WM. & MARY L. REV. 1291, 1320, 1348 (1993). In D.C., the "knowing or have reason to know" standard under D.C. Code § 22-3232 is a subjective one. Owens v. United States, 90 A.3d 1118, 1121 (D.C. 2014). Oregon also adopts the same standard. State v. Smith, 252 Or. App. 707, 715 (Or. Ct. App. 2012). Pennsylvania adopted this standard as well. Khan v. Garland, 69 F.4th 265, 270 (5th Cir. 2023) ("Pennsylvania's receipt of stolen property offense does not have an objective element and is 'purely subjective.'"). *Cf.* The position is rather uncertain in Arizona, as the statutory "know or have reason to know" standard under AZ Rev. Stat. § 13-1802(A)(5) seemed to be considered objective in State v. Wright, 214 Ariz. 540, 545 (Ariz. Ct. App. 2007) but old precedents considered the former version of the offense to be subjective. State v. Ware, 27 Ariz. App. 645, 650 (1976) ("In fact, in 1924 the Arizona Supreme Court in *Reser v. State* [citation omitted] adopted the subjective test. Although the statute the court interpreted did not contain the 'having reason to believe' language now contained in [the former A.R.S. § 13-621(A) which was based on "knowing or having reason to believe that the property is stolen," a provision now repealed and replaced by § 13-1802(A)(5) which uses similar language of "knowing or having reason to know'] the reasoning of the court remains dispositive today.").

19 *See, e.g.*, Harman R. Clark, *Receiving Stolen Goods*, 58 DICK. L. REV. 270, 277 (1954); Owens v. United States, 90 A.3d at 1121.

20 Thomas v. United States, 557 A.2d 1296, 1300 (D.C. 1989) ("a showing that a reasonable person would have been aware of a risk is often the best available evidence that the defendant was aware of it"); applied in *Owens*, 90 A.3d at 1121.

21 In Georgia, there is an offense of theft by receiving stolen property, which is committed when one "retains stolen property which he knows or should know was stolen" and "receiving" includes mere possession. GA. CODE ANN. § 16-8-7 (2020); Ingram v. State,

direct proof of knowledge can be difficult, presenting circumstantial evidence can adequately sustain conviction.[22]

On the present facts, the source of the payment to Party B seemed suspicious (see Part I). It is now well established by case law that "guilt may be inferred from possession along with other evidence—including circumstantial evidence—of guilty knowledge which would excite suspicion in the mind of an ordinarily prudent person."[23]

A comparison with the former legal position will help understand and apply the present lower thresholds of proof.[24] The existence of objectively suspicious circumstances used to be inadequate to establish knowledge.[25] Besides, the "prudent person" standard was considered

---

268 Ga. App. 149, 150 (2004) ("Possession (of stolen property) alone is not sufficient to show guilty knowledge; however, possession together with other circumstances and evidence may be used to infer the knowledge required by the statute"). This judicial quote was affirmed in Wells v. State, 601 S.E.2d 433 (Ga. Ct. App. 2004). The same holds true for some other states. For Ohio, see State v. Cottey, 3044 Ohio 1, 4 (Ohio Ct. App. 2012) ("an individual's unexplained possession of stolen property may give rise to the permissive inference that the defendant is guilty of a theft offense or that the individual knew or should have known that the property in question has been stolen"). In Florida, see FLA. STAT. § 812.022 (2023) ("proof of possession of property recently stolen, unless satisfactorily explained, gives rise to an inference that the person in possession of the property knew or should have known that the property had been stolen").

22 *See, e.g.*, Allison v. State, 683 S.E.2d 104, 108 (2009) ("such possession, coupled with facts and circumstances from which knowledge may be inferred that the property so received was stolen is sufficient to support the verdict."); Prather v. State, 116 Ga. App. 696, 696 (1967).

23 Slaughter v. State, 240 Ga. App. 758, 760 (1999) (emphasis added); Xiong v. State, 295 Ga. App. 697, 701 (2009); United States v. Topaz Darden, 829 F. App'x 411, 414–15 (11th Cir. 2020); Commonwealth v. Gazal, 194 Pa. Superior Ct. 132, 135 (1960) ("Circumstances which would lead a reasonably prudent man to suspect that the goods have been stolen may be properly considered by a trial judge sitting without a jury in arriving at the determination of an accused's guilt."); Newsome v. State, 355 Ga. App. 13, 15 (2020) ("Guilty knowledge may be inferred from circumstances which would excite suspicion in the mind of an ordinary prudent man").

24 Old precedents emphasized the necessity for actual knowledge of the stolen status based on former statutes. *See, e.g.*, Commonwealth v. Boris, 317 Mass. 309, 315 (1944) ("if the defendant did not in fact know or believe that the property had been stolen, he cannot be found guilty. The knowledge or belief of the defendant must be personal to him and our statute furnishes no substitute or equivalent"). The statute at that time adopted the subjective standard of "know" or "have reason to know."

25 Peterson v. United States, 213 F. 920, 922–23 (9th Cir. 1914) ("[C]ircumstances which would create a strong suspicion in the mind of one man might have little significance for another, and one is not to be convicted of a crime because he is of a less suspicious nature than the ordinary man, and where, therefore, he may have acted in entire good faith in the face of conditions which might have put another upon his guard.").

inapplicable.[26] The obsoleteness of these two subjective knowledge-based standards is not only confirmed by the quote that explicitly emphasizes the relevance of "suspicion" and the "prudent person"[27] but can also be discerned from the statutory adoption of the *objective* "should have known" standard in many states.[28]

The departure from the subjective, actual knowledge basis is a logical move, when the court has rightly conceded that

> The receivers of stolen goods almost never 'know' that they have been stolen, in the sense that they could testify to it in a court room… Nor are we to suppose that the thieves will ordinarily admit their theft to the receivers: that would much impair their bargaining power.[29]

Given such impracticality,[30] it explains why the courts, even in states which statutorily apply a subjective knowledge test, are willing to accept circumstantial evidence of knowledge as sufficient proof.[31]

It is still uncertain how the courts will interpret "suspicious circumstances" based on the blockchain analysis, whilst bearing in mind that Party B is a sophisticated business. There is not yet a definite answer to this novel tech topic. However, this legal starting point certainly does not favor Party B, especially when the next legal consideration must also be taken into account.

B. Party B Is Expected to Be Not Just Reasonable But Also Prudent

The statutes and case law above demonstrate that the legal standard is objectively whether a "reasonable" person should have known the

---

26 *Boris*, 317 Mass. at 315 ("The infraction of this statute is not proved by negligence nor by failure to exercise as much intelligence as the ordinarily prudent man. The statute does not punish one too dull to realize that the goods which he bought honestly and in good faith had been stolen."); *see also* Clark, *supra* note 19, at 274–75 (noting the development of case law from originally rejecting the "prudent" person standard to now applying it); Thomas A. Wadden Jr., *Criminal Law—Receiving Stolen Goods—Elements in the Crime,* 26 N.C. L. REV. 192, 193 (1948) ("it is necessary that the receiver shall know that the property has been stolen at the moment he receives it . . . in many jurisdictions the reasonably prudent man rule is applied.").

27 *See* text accompanying *supra* note 23.

28 *See supra* note 16.

29 *See, e.g.*, State v. Sheffey, 234 N.W.2d 92, 97 (Iowa 1975); Fletcher v. State, 241 Ind. 409, 415 (1961); State v. Beale, 299 A.2d 921, 924 (Me. 1973).

30 *See Calloway*, 1 So. 3d at 422 ("Must the offender subjectively know, or is he taken to know what any reasonable person so situated would have known? This section adopts a completely objective test here, because of the difficulty of proof by the prosecution."). The quote was applied again in *State ex rel. T.C.*, 361 So. 3d at 505.

31 *See* Clark, *supra* note 19, at 279; *Calloway*, 1 So. 3d at 422 ("The requirement that a defendant have guilty knowledge of the stolen status of acquired goods, does not mean, however, that direct evidence of actual knowledge is necessary.").

property to be stolen.[32] But it is not just about "reasonableness," as the quote above emphasizes: it is also about "prudence."[33]

Arguably, the use of the term "prudence" hints at the different judicial expectations that come from "reasonableness" (despite their conceptual overlap). Professor Marcia Baron compellingly discussed their subtle differences:

> In its broader meaning 'prudent' is closely enough aligned to 'reasonable' to be a tolerable substitute for that term; but in the narrower-end, I think, more common-sense, prudence has more to do with being cautious. To treat 'prudent' in that sense as interchangeable with 'reasonable' thus invites a picture of reasonableness as mainly concerned with not taking unnecessary risks.[34]

Prudence could denote the need to adopt "responsible business practices."[35] One might take reference from existing market practices. For example, the car company Ferrari accepts payment by cryptocurrencies. But the payment must be performed via a payment processing intermediary who "will ensure that the virtual currencies come from legitimate sources and not derived from criminal activity or to be used to launder the proceeds of crime or evade tax."[36]

---

32 *See* text accompanying *supra* note 16.

33 *See* text accompanying *supra* note 23.

34 Marcia Baron, *The Standard of the Reasonable Person in the Criminal Law*, *in* THE STRUCTURES OF THE CRIMINAL LAW 11 (R.A. Duff et al. eds., 2011); *see also* Heidi Li Feldman, *Prudence, Benevolence, and Negligence: Virtue Ethics and Tort Law*, 74 CHI.-KENT L. REV. 1431, 1431 (1999) (highlighting that reasonableness and prudence are separate virtues). The same understanding of prudence is adopted in the context of a police's stop and search, where the Supreme Court of the state of New York held that "[r]easonable suspicion is defined as the 'quantum of knowledge sufficient to induce an ordinarily prudent and cautious [person] under the circumstances to believe criminal activity is at hand.'" *See, e.g.*, People v. Gibson, No. 2022-00042, slip op. at 1107 (2d Dep't May 29, 2024).

35 For example, statutes concerning retail of alcoholic beverages apply the "ordinarily prudent person" standard in terms of whether "responsible business practices" have been taken. NH Rev. Stat. Ann. § 507-F:6 (2022); MICH. COMP. LAWS § 436.1815 (2022). *See also* Leslie C. Griffin, *The Prudent Prosecutor*, 14 GEO. J. LEGAL ETHICS 259, 261 (2001) ("By 'prudent,' the Supreme Court presumably meant cautious or careful, perhaps pragmatic. Prudence also means the habit of good judgment.").

36 Giulio Piovaccari, *Ferrari to Accept Crypto as Payment for Its Cars in the U.S.*, REUTERS (Oct. 13, 2023), https://www.reuters.com/business/autos-transportation/ferrari-accept-crypto-payment-its-cars-us-2023-10-14/ [https://perma.cc/QF7L-FPWH].

The prudential standard is particularly relevant here because the crypto sector remains largely unregulated.[37] The sector's proneness to misconduct arguably calls for more care from a reasonable and prudent person. It is imaginable that some judges might frown upon those who have not adopted safeguarding measures (like Ferrari has done) when they choose to accept such an inherently risky form of pseudo-anonymous payment.[38]

It is uncertain as to whether a prudent business would need to conduct some basic blockchain analysis. However, the failure to do so will expose Party B to legal risk. The courts can impute knowledge that would have been revealed from due diligence.[39]

III
POTENTIAL CIVIL LIABILITY OWED TO THE VICTIMS OF MISAPPROPRIATION UNDER U.S. LAW

The victims of misappropriation—i.e., clients of Party A—may be interested in suing Party B to recover the sum. This may happen when, for instance, Party A has absconded.

In the United States, there are two major private causes of action against Party B, namely (1) unjust enrichment and (2) replevin.[40] These two alternatives have some conceptual overlap in scope, but they bear different legal requirements.

To be clear, there are actually many other possible causes of action. One example is the tort of conversion, which has been successfully tested in court in the crypto context.[41] Conversion is particularly detrimental to Party B because there is no defense based on good faith,

---

37 *See, e.g.*, Simon Constable, *Up to Four-Fifths of Crypto Trading Could Be Phony, New Research Shows*, FORBES (Dec. 31, 2022), https://www.forbes.com/sites/simonconstable/2022/12/31/much-crypto-trading-on-unregulated-platforms-could-be-phony-new--research-shows/?sh=3108bb6618da [https://perma.cc/EF8C-6U5F]; Steven Zeitchik, *Bad News for Thousands of Crypto Investors: They Don't Own Their Accounts*, WASH. POST (Jan. 5, 2023), https://www.washingtonpost.com/technology/2023/01/05/celsius-crypto-bankruptcy-ruling/.

38 People v. Devine, 95 Cal. 227, 230 (1892) ("There are cases in which all the knowledge which a person might have acquired by due diligence is to be imputed to him.").

39 *Id. See also* accompanying text of *infra* note 48. For the same reason, in the context of buying stolen art, buyers are advised to conduct due diligence even though there is not an express legal obligation to do so. Marilyn E. Phelan, *Scope of Due Diligence Investigation in Obtaining Title to Valuable Artwork*, 23 SEATTLE U. L. REV. 631, 633–34 (2000).

40 Colleen P. Murphy, *What Is Specific About "Specific Restitution,"* 60 HASTINGS L.J. 853, 865 (2009) (noting that replevin is a legal remedy, whilst unjust enrichment is equitable in nature).

41 *See supra* notes 4–5.

so a legitimate innocent business (like Party B) can be held liable.[42] Besides, there is no need to prove the defendant's knowledge of the misappropriation to establish an action in conversion.[43] Furthermore, a less-mentioned potential consideration for choosing conversion over replevin is that the damages in conversion are calculated based on the value of the property (as the price of crypto can fluctuate and its value could rise); whereas replevin is about the return of the same property (not value).[44]

This Article focuses on those two actions because (1) they helpfully illustrate the problem of how the law approaches mere suspicion in an unbefitting manner for the commercial blockchain context, (2) their application in the blockchain context is relatively less explored, unlike the conversion claim which has already been tested in court, and (3) a claim for conversion could fail if Party B obtained better title than the victims (which will be explained below where Party A misappropriated the cryptos by fraud).[45]

---

42 Berry v. Frazier, 90 Cal. App. 5th 1258, 1271 (2023) (in discussing the "essential elements of conversion," the court explained that the "defendant's conduct must be knowingly or intentionally done, but a 'wrongful intent' or motive is not a requirement . . . . Because the defendant's conduct must be knowingly done, 'neither negligence, active or passive, nor a breach of contract, even though it results in injury to, or loss of, specific property, constitutes a conversion' . . . . It follows therefore that *mistake, good faith, and due care are ordinarily immaterial, and cannot be set up as defenses in an action for conversion*.") (emphasis added). This legal understanding is not only applicable in California. For North Carolina, see *In re* Renshaw, No. 06-11028C-13G, at 12 (M.D.N.C. May 5, 2009). For Arizona, see 4801 E. Wash. St. Holdings, LLC v. Breakwater Equity Partners LLC, No. CV-13-01475-PHX-DGC, 2015 U.S. Dist. LEXIS 53436, at 13 (D. Ariz. Apr. 23, 2015) ("Good faith belief or intention is no defense to a conversion action in Arizona.") For Michigan, see Hunt v. Hadden, No. 14-10713, 2015 U.S. Dist. LEXIS 70763, at 10 (E.D. Mich. June 2, 2015) (quoting the case of Bensmiller v. Elias Bros. Rest., Inc., No. 194144, 1997 WL 33343875, at *3 (Mich. Ct. App. Oct. 31, 1997) which held that "[a]n act for conversion does not rest on the knowledge or intent of the defendant, does not require wrongful intent, and is not excused by care, good faith, or lack of knowledge."); Attorney General v. Hermes, 127 Mich. App. 777, 786–87 (1983). *See also* Kelley v. Laforce, 288 F.3d 1, 12 (1st Cir. 2002) ("It is no defense to conversion for defendant to claim that he acted in good faith, reasonably believing that he had a legal right to possession of the goods.").

43 Douglass v. Wones, 120 Ill. App. 3d 36, 41 (Ill. App. Ct. 1983) ("Relief in an action for conversion may be had without establishing malice, culpability or conscious wrongdoing . . . Thus, knowledge is not an element of the cause of action.").

44 Ludwig Teller, *Restitution as an Alternative Remedy for a Tort*, 2 N.Y.L. SCH. L. REV. 40, 59 (1956).

45 *See, e.g.*, Bergeron v. Aero Sales, Inc., 205 Or. App. 257, 134 P.3d 964 (2006) ("[I]f [Party B]'s interest is superior to [the plaintiff-victims], then [Party B] is not liable for conversion."); Noble v. Moistner, 180 Ind. App. 414, 417 (Ind. Ct. App. 1979).

A. Liability in Restitution Can Be Established Based on Constructive, Not Actual, Knowledge

A claim of unjust enrichment (sometimes called "disgorgement") would allege that Party B knowingly received the misappropriated sum from Party A.[46] Establishing such a claim does not require a preexisting direct relationship (e.g., privity of contract) between the victims and Party B.[47]

The knowledge requirement goes against Party B in two ways. First, it covers the situation where they "should have known" the payment belonged to the victims.[48] This resembles the criminal law situation

---

46 *See, e.g.*, Murr Plumbing, Inc. v. Scherer Brothers Financial Services Co., No. C1-98-107 (Minn. Ct. App. Aug. 25, 1998) (the "court has defined unjust enrichment as the knowing receipt and unjust retention of something of value to which one is not entitled"); Southtown Plumbing v. Har-Ned Lumber Co., 493 N.W.2d 137, 140 (Minn. Ct. App. 1992) ("To establish an unjust enrichment claim it must be shown that a party has knowingly received something of value, not being entitled to the benefit, and under circumstances that would make it unjust to permit its retention."); City of Almaty v. Sater, 503 F. Supp. 3d 51, 60 (S.D.N.Y. 2020) ("the well-settled rule that a claim for unjust enrichment lies against the knowing recipient of wrongfully obtained property"); Middle E. Banking Co. v. State St. Bank Int'l, 821 F.2d 897, 906 (2d Cir. 1987) ("New York law requires the following elements: '(1) defendant received money belonging to plaintiff; (2) defendant benefitted from the receipt of money; and (3) under principles of equity and good conscience, defendant should not be permitted to keep the money'"); Clarke v. Newell, 05cv1013 (E.D. Va. Oct. 12, 2006) at 5 ("there must have been: (1) a benefit conferred on defendant by plaintiff; (2) the defendant's knowledge of receipt of the benefit; and (3) inequitable retention by the defendant"). There are many different formulations of what a claim of unjust enrichment entails. *See* James Steven Rogers, *Indeterminacy and the Law of Restitution*, 68 WASH. & LEE L. REV. 1377, 1395–96 (2011); Emily Sherwin, *Restitution in the United States*, CORNELL L. SCH. LEGAL STUD. RSCH. PAPER SERIES NO. 23-02, Jan. 9, 2023, at 21, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4321016 [https://perma.cc/5YDH-SJJ5]. In the present context, the extent to which the defendant had knowledge or awareness of taking advantage of the victims of misappropriation arguably constitutes a crucial factor for determining the unjust or inequitable nature of the retention.

47 Freitas v. Freitas, 31 Cal. App. 19, 20 (Cal. Ct. App. 1916) ("An action for money had and received 'may be successfully maintained even though not founded upon allegations showing an express privity of contract between the parties. This is so upon the theory that one of the parties has received money due and owing under the circumstances which make it his duty to surrender the money to the rightful owner, the law will imply the promise to do so, and thereby create the requisite contractual privity."). This trite understanding is an oft-cited quote. *See, e.g.*, Coombs v. Minor, 60 Cal. App. 2d 645, 649 (Cal. Ct. App. 1943).

48 *See, e.g.*, Stiller v. Rogers, Civ. A. No. 5963, ¶ 2b (L.A. Super. Ct. App. May 29, 1945) ("the defendant either knew or should have known that at least part of the moneys so received by him were stolen funds, and that such knowledge disqualified the defendant from becoming a holder in due course"); Ying Hu, *Mainstreaming Unjust Enrichment and Restitution in Data Security Law*, 13 UC IRVINE L. REV. 855, 870 (2023) (noting that a restitution claim can be established when the defendant "knew or should have known that some portions" of the payment belonged to the plaintiffs). The "should have known" standard also extends to situations where the payment included the victim's money by

analyzed above. The victims can argue that, based on the objectively suspicious circumstances highlighted in Part I, Party B "should have known" about the breaches by Party A. The victims can make an arguable case based (solely) on suspicion, as legally speaking,

> [i]f the facts within the knowledge of [] [Party B] are of such a nature, as, in reason, to put him upon inquiry, and to excite the suspicion of an ordinarily prudent person and he fails to make some investigation, [then] he will be chargeable with that knowledge which a reasonable inquiry, as suggested by the facts, would have revealed.[49]

In other words, such a claim does not strictly require proof of *actual* knowledge. By contrast, although the law of lien shares similar legal prerequisites to an unjust enrichment action, establishing a lien generally requires *actual* knowledge.[50] So Party B can defend against a claim of lien by contending that they did not know the payment was a stolen sum—a defense that is not possible with unjust enrichment.

Second, the evidential threshold for knowledge is not stringent. In the restitution case of *Aetna Health Inc. v. Biodiagnostic Lab. Servs.*, the plaintiff sought to recover the proceeds of a crime paid to the defendants who knowingly received the money.[51] The Superior Court of New Jersey affirmed that there is no need to provide *direct* evidence of knowledge, and circumstantial evidence, for inference is sufficient.[52] The court will take into account, for instance, the defendant's intellect.[53] This factor goes against Party B as a running business, as opposed to being a commercially inexperienced layperson.

---

mistake. *See* Brad Reed, *Restitution-1963 Tennessee Survey*, 17 VAND. L. REV. 1139, 1148 (1964) (a claim of restitution can be made out when, for instance, Party B "knew or should have known that plaintiff had made an error").

49 Anderson v. Blood, 152 N.Y. 285, 293 (1897). This is still an oft-cited and widely approved quote. *See, e.g.*, Miner v. Edwards, 221 A.D.2d 934, 934 (N.Y. App. Div. 1995); U.S. Bank v. Jordan, 176 A.D.3d 1523, 1524 (N.Y. App. Div. 2019).

50 *See, e.g.*, Tutor Perini Bldg. Corp. v. N.Y.C. Reg'l Ctr., 525 F. Supp. 3d 482, 509–10 (S.D.N.Y. 2021) ("New York courts have interpreted this [N.Y. Lien Law] to require a plaintiff to show subjective, not objective, notice").

51 Aetna Health Inc. v. Biodiagnostic Lab. Servs., No. A-3335-17, at 3 (N.J. Super. App. Div. Oct. 7, 2021).

52 *Id.* at 13.

53 *Id.*

B. Recovery By Challenging Party B's Title of Ownership

Another possible cause of action for recovery in the United States is replevin.[54] It applies differently depending on whether Party A's misappropriation was perceived as fraud or as theft (i.e., a fact specific question).

1. Title Over the Stolen Sum

If Party A's misappropriation involved theft, it refers to a situation in which Party A (the fund holder) stole money from their clients, which was subsequently paid to Party B. This has two possible legal implications; either (1) the victims have superior title over Party B, or (2) the title has not successfully passed to Party B at all.

In relation to the first legal implication, the legal position has been succinctly summarized by the courts:

> [U]nder New York law, an owner of property that is stolen has superior title to a subsequent possessor, superior even to a bona fide purchaser, i.e., one who obtains an item for value and without notice of any adverse claims . . . 'New York case law has long protected the right of the owner whose property has been stolen to recover that property, even if it is in the possession of a good-faith purchaser for value.'[55]

Applying this to the present facts, the victims have superior title to the stolen sum over Party B. It does not matter whether Party B received the payment in good faith.

Another possible legal reasoning is that Party A did not obtain a valid title from the victims at all, so Party A had no title that could be passed to Party B.[56] This is because

> if [Party A] buys goods from [clients], he gets [clients'] title and can transfer it to any subsequent purchaser; if [Party A] steals goods from

---

54 *See, e.g.*, 71 N.Y.C.P.L.R. (CONSOL. 2022) (Recovery of Chattel); Colleen P. Murphy, *Money as a "Specific" Remedy*, 58 ALA. L. REV. 119, 146 (2006) (emphasizing the suitability of replevin for recovering non-fungible currency).

55 Shubert Org., Inc. v. Partridge, 2020 N.Y. Slip Op. 32748, at 5 (N.Y. Sup. Ct. 2020). *See also* Richard. H. Helmholz, *Wrongful Possession of Chattels: Hornbook Law and Case Law*, 80 NW. U.L. REV. 1221 (1985).

56 *See, e.g.*, Bakalar v. Vavra, 619 F.3d 136, 141 (2d Cir. 2010) ("a cause of action for replevin against the good-faith purchaser of stolen property accrues when the true owner makes demand for return of the chattel and the person in possession of the chattel refuses to return it. Until demand is made and refused, possession of the stolen property by the good-faith purchaser for value is not considered wrongful").

> [clients], he gets no title and can transfer none to any subsequent purchaser [Party B], no matter how clear the purchaser's good faith.[57]

2. Title Over a Sum Derived from Fraud

The facts can alternatively be about fraud. Where Party A *defrauded* the clients for the deposits (e.g., through a Ponzi investment scheme), Party A would obtain a voidable title to the tokens, which can be subsequently transferred to Party B.[58] A good faith purchaser's title ranks higher than the original owner.

But still, there remains the contentious issue as to whether Party B received the sum in good faith when there were suspicious circumstances. The starting point is already against Party B in the sense that "[e]vidence of suspicious circumstances is of probative value," which "conduces to a finding of active bad faith."[59]

Further, the good faith requirement is rather uncertain. The "modern" view of courts is that its proof is an objective test[60] while some courts

---

57 Grant Gilmore, *The Commercial Doctrine of Good Faith Purchase*, 63 YALE L.J. 1057, 1059 (1954). *See also* Kunstammlungen Zu Weimar v. Elicofon, 536 F. Supp. 829, 846 (E.D.N.Y. 1981) ("In applying the New York rule that a purchaser cannot acquire good title from a thief")—quote affirmed in *Bakalar*, 619 F.3d at 145.

58 Gilmore, *supra* note 57, at 1059; TENN. CODE ANN. § 47-2-403(1) (2024); First National Bank of Cicero v. Lewco Securities Corp., 860 F.2d 1407, 1414 (7th Cir. 1989) ("a good faith purchaser of goods may receive good title from one who possessed only voidable title").

59 Joseph v. Lesnevich, 56 N.J. Super. 340, 348 (N.J. Super. Ct. App. Div. 1959); Gutekunst v. Continental Insurance Company, 486 F.2d 194, 195–96 (2d Cir. 1973) ("the New York law is that . . . disregard of suspicious circumstances may constitute evidence of bad faith").

60 Mallory A. Sullivan, *When the Bezzle Bursts: Restitutionary Distribution of Assets After Ponzi Schemes Enter Bankruptcy*, 68 WASH. & LEE L. REV. 1589, 1618 (2011) ("the modern good faith standard is objective, not subjective, so actual good faith is irrelevant"); Melanie E. Migliaccio, *Victimized Again: The Use of an Availability Presumption and the Objective Standard of Good Faith to Deprive Ponzi Victims of Their Defenses*, 8 LIBERTY U. L. REV. 209, 213 (2013) ("Most courts, however, now apply an objective standard, rather than the traditional subjective standard to good faith."). By comparison, Canadian law also adopts an objective test in the title transfer context. *See* LLS America, LLC (Trustee of) v. Bjarnason, 2016 CanLII 909 (Can. B.C.S.C.) at [52] ("courts measure good faith by an objective standard, looking to what a transferee 'knew or should have known' in questions of good faith, rather than examining what the transferee actually knew from a subjective standpoint"). It similarly expects inquiry to be made if suspicions arise. *See, e.g.*, Bank Leu AG v. Gaming Lottery Corp., (2003) 231 D.L.R. 4th 251, para. 38 (Can. Ont. C.A.) ("Suspicions combined with blindness adds up to an absence of good faith."); Dominion Bank v. Fassel & Baglier Constr. Co. Ltd., [1955] 4 D.L.R. 161, 166 (Can. Ont. C.A.) ("Given facts exciting suspicion, i.e., actual suspicion arising from facts known or believed to exist, and either an absence of inquiry or an inquiry which does not remove the suspicion,

requires a subjective test.[61] The objective good faith test requires the transferee (Party B) to be "diligent" when "put on inquiry of . . . possibly fraudulent purpose of the transfer."[62] This puts Party B in the difficult situation where they are expected to make inquiries upon suspicion, despite any doubt that the inquiry is pragmatic and useful at all in the present context.[63]

Irrespective of being objective or subjective, the courts have long reiterated that when "the circumstances or *suspicions* are so cogent and obvious . . . to remain passive would amount to bad faith."[64] When suspicions arise, the courts expect Party B to make inquiries.[65] Coincidentally, but also understandably, this corresponds to Section II(B)'s analysis on "prudence."

IV
LEGAL UNCERTAINTY AND RISK: UNRESOLVABLE?

A. Should Party B Conduct Due Diligence?

The above has demonstrated Party B's legal risk and uncertainty when a blockchain-based payment is merely suspicious. Given the risks, one might argue that Party B should always conduct due diligence. For

---

the situation is incompatible with good faith."). The same problem does not exist under English law, which applies a subjective test for good faith. GRAHAM VIRGO, THE PRINCIPLES OF THE LAW OF RESTITUTION 658 (2015) ("At Common Law the notion of good faith is equated with honesty. This is a subjective test which will not be satisfied if the defendant knew or suspected that the transferor had a defective title to the property which was transferred."). Australian law also applies a subjective test. *Foods Bis Ltd & Ors v. Riley & National Australia Bank Ltd* [2007] QDC 201 6, 24 [66] (Austl.) ("The requirement of good faith is a subjective test.").

61 Sullivan, *supra* note 60, at 1616, 1623.

62 *In re* Bayou Group, LLC, 439 B.R. 284, 312 (S.D.N.Y. 2010).

63 *See* Part I.

64 *See, e.g.*, Sasner v. Ornsten, 93 Cal. App. 2d 467, 471 (Cal. Ct. App. 1949); Hollywood Nat. Bank v. IBM Corp., 38 Cal. App. 3d 607, 614 (Cal. Ct. App. 1974); Oliver v. CIT Group/Consumer Fin., Inc., No. A117400 (Cal. Ct. App. Jan. 15, 2008); *In re* Nusor, 123 B.R. 55, 60 (B.A.P. 9th Cir. 1991) (emphasis added). *See also* State of the Netherlands v. Fed. Rsrv. Bank, 99 F. Supp. 655, 667 (S.D.N.Y. 1951) ("Even if his (holder's) actual good faith is not questioned, if the facts known to him should have led him to inquire, and by inquiry he would have discovered the real situation, in a commercial sense he acted in bad faith, and the law will withhold from him the protection that it would otherwise extend . . . One who suspects, or ought to suspect, is bound to inquire, and the law presumes that he knows whatever proper inquiry would disclose.").

65 Hollywood Nat. Bank, 38 Cal. App. 3d at 615 ("unwillingness to make any inquiries—other than a last minute phone call to the credit bureau—indicate a studied refusal to make inquiries that were likely to 'disclose a vice or defect' in a rush transaction that reeked of chicanery"); First Nat'l Bank v. Goldberg, 17 A.2d 377, 379 (Pa. 1941).

example, they can use a verifying intermediary, like how Ferrari receives payment through BitPay.[66]

But due diligence is not an effective solution for three reasons. First, it might not be financially feasible for all, especially for small and medium-sized businesses and contracts involving a small amount.

Second, blockchain's key feature of immutability is meant to eliminate the need for intermediaries.[67] Requiring an intermediary would therefore defeat its fundamental purpose.

Third, it is legally uncertain as to when exactly due diligence should be conducted under U.S. law. There exist some judicial dispositions which confusingly and inconsistently suggest mere suspicion does not always trigger the obligation to inquire:

> It has also been held that a purchaser is not charged with the duty to make inquiry by the fact alone that he had knowledge of the want of honesty in business matters of the party from whom he received the instrument.[68]

Such an unhelpful legal discrepancy is not a one-off. Part I explained that suspicious circumstances can be discerned from analyzing open-source blockchain information or the doubtful business practices of Party A (e.g., boasting high return in crypto investments, sometimes like Ponzi schemes). But a court in New Jersey has held that a "purchaser of a negotiable instrument is not subject to constructive notice *afforded by public record* or newspaper."[69] This reasoning makes practical sense as not everyone can or will refer to public records, realistically speaking. Yet, this does not sit well with another commonly adopted judicial view that "[i]ntentional ignorance, such as a willful evasion of knowledge of the facts, constitutes bad faith."[70]

---

66 *See supra* text accompanying note 36.

67 *See, e.g.*, Jill Gunter, *Wait, Wasn't Bitcoin Supposed to Solve This?*, FIN. TIMES (Nov. 15, 2022).

68 Stiller v. Rogers, Civ. A. No. 5963. (L.A. Super. Ct. App. May 29, 1945) ¶ 6. *Cf. supra* note 64 and the accompanying text.

69 Joseph v. Lesnevich, 56 N.J. Super. 340, 348 (N.J. Super. Ct. App. Div. 1959) (emphasis added).

70 Torosian v. Paulos, 82 Ariz. 304, 314 (1957). *See also* Stiller, Civ. A. No. 5963 ¶ 4; *In re* Harbour, 845 F.2d 1254, 1258 (4th Cir. 1988) ("willful ignorance in the face of facts which cried out for investigation may not support a finding of good faith on her part").

B. The Point of Making Inquiries Upon Suspicious Circumstances

If Party B has suspicions, they should make inquiries.[71] Their actions will be evaluated against what a "prudent" person would do[72] in similar circumstances.[73] But the key question remains: what steps can Party B take after an inquiry has been made?

Smart contracts are integral to blockchain-based transactions. These contracts automatically execute payment obligations and cannot be breached or modified once initiated. This automated, immutable execution is what makes them "smart" and effectively "unbreakable."[74] So even if inquiries uncover issues, once the smart contract has been entered into, the payment will be automatically performed. Once initiated, Party B cannot stop the contract's execution or request an alternative payment method outside the token system.

Party B may become aware of the red flags only *after* entering into a contract. One could argue that Party B should make inquiries *before* the formation of a contract. But this is not always pragmatic, and the legal obligation to inquire is triggered upon suspicion.[75] In this sense, the law sits awkwardly with the technological circumstance of a smart contract and fails to properly guide Party B away from risk and uncertainty.

Besides, inquiries do not always produce useful answers. Courts have recognized that Party A is unlikely to confess to wrongdoing.[76] As explained in Part I, this Article specifically addresses situations where suspicions exist but verification is practically impossible. Party B faces challenges in alleging fraud, given the high burden of proof required.[77]

V
WILL ENGLISH LAW PRODUCE DIFFERENT OUTCOMES?

This Article compares U.S. law to English law for two reasons: England's influence on other common law jurisdictions like

---

71 *See* text accompanying *supra* note 64.

72 *See* text accompanying *supra* note 23.

73 *See* text accompanying *supra* note 23.

74 Tatiana Cutts, *Smart Contracts and Consumers*, 122 W. VA. L. REV. 389, 392 (2019).

75 *See* text accompanying *supra* note 64.

76 *See* text accompanying *supra* note 29.

77 *See, e.g.*, Weaver v. Travers, 631 S.W.2d 81, 83 (Mo. Ct. App. 1982) ("Fraud is not presumed and an inference of its presence can be drawn only if the evidence rises above mere suspicion and points logically and convincingly to fraud.").

Singapore,[78] and its position as a leading jurisdiction embracing blockchain technology.[79] Like U.S .law, English law does not provide a blockchain-specific legal regime or statute, so legal issues are decided on precedent-based common law.[80] Other jurisdictions, like France and Liechtenstein, practice within a civil law system (based on statutory law) and have enacted specific legislation for blockchain governance.[81] This Article will demonstrate that both criminal and civil liability can be more readily established in the United States than under English law.

A. Criminal Liability Under English Law

Under English law, it is illegal to handle stolen goods.[82] The law provides that "[a] person handles stolen goods if (otherwise than in the course of the stealing) knowing or believing them to be stolen goods he dishonestly receives the goods . . . ."[83] But this charge is inapplicable to blockchain transactions. One way in which this differs from U.S. law is that the English offense requires proof of dishonesty.[84]

---

78 *See* Kwai Hang NG & Brynna Jacobson, *How Global Is the Common Law? A Comparative Study of Asian Common Law Systems – Hong Kong, Malaysia, and Singapore*, 12 ASIAN J. COMP. L. 209 (2017); Martin Kwan, *Is the Hong Kong Courts' Ability to Refer to Foreign Authorities Unrestrained?*, 4 AMICUS CURIAE 71 (2022); Martin Kwan, *Applying Law Without Borders? Hong Kong's Curious Practice and Problems of Applying Foreign Authorities from Multiple Jurisdictions Simultaneously*, 31 TUL. J. INT'L & COMPAR. L. 1069 (2023).

79 Shivaune Field, *Ranked: World's Most Crypto-Friendly Countries*, FORBES (Sept. 6, 2023), https://www.forbes.com.au/news/investing/crypto-wealth-report-reveals-six-bitcoin-billionaires/ [https://perma.cc/D7V5-GTF4] (noting that the U.K. and Singapore are within the top 10 crypto-friendly countries).

80 *See, e.g.*, Gretel Scott, *Remedies for Victims of Crypto Fraud*, BUTTERWORTHS J. INT'L BANKING & FIN. L. (Aug./Sept. 2023), https://3vb.com/wp-content/uploads/2023/08/Remedies-for-victims-of-crypto-fraud-2023-8-JIBFL-539.pdf [https://perma.cc/BJW5-HR7L].

81 Lehmann, *supra* note 7, at 151–52. For example, in a transfer of crypto assets, the Liechtenstein statutory law establishes a presumption of good faith on the part of the transferee. Lehmann, *supra* note 7, at 160. *Cf.* Patricia Youngblood Reyhan, *A Chaotic Palette: Conflict of Laws in Litigation Between Original Owners and Good-Faith Purchasers of Stolen Art*, 50 DUKE L.J. 1041 (2001) (under U.S. law, the purchaser must meet the burden of establishing his good faith. Thus, he must not have known, nor have had reason to know, of the owner's superior claim. The purchaser is required to exercise diligence in this regard, a diligence that may demand reasonable inquiry regarding the chain of title to the work.).

82 Theft Act 1968, c. 60, § 22 (U.K.).

83 *Id.* § 22(1).

84 *See supra* note 15.

In this case, Party B acted in good faith, harboring only suspicions about the payment rather than engaging in any dishonest conduct.

Nevertheless, Party B can alternatively be charged with money laundering, which, under English law, does not require the proof of dishonesty.[85] By contrast, Party B cannot be charged with money laundering under U.S. law, because mere suspicion is not sufficient to establish knowledge.[86]

Under English law, money laundering is premised on mere suspicion that the property is criminally tainted:

> A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.[87]

The notion of "suspicion" under English law has a low threshold. It is established when Party B thinks "that there is a possibility" that the property is criminally tainted.[88]

The U.K. Proceeds of Crime Act has been amended recently to allow law enforcement authorities to seek freezing orders against crypto wallets.[89] Leading criminal law academics Ormerod and Laird describe this offense is "draconian" and "extraordinarily broad."[90]

However, it is still arguable that the English approach (based on the money laundering offense) is not as problematically expansive as the U.S. approach (based on a charge of possession of stolen goods). First, the U.K. Supreme Court specifically warned against the prosecutorial reliance on this offense because it is an easy charge with a low evidentiary threshold.[91] Prosecution should rely on this offense only "in serious cases," and a defendant should not be "over-charged."[92]

---

85 Proceeds of Crime Act 2002, §§ 328–29 (U.K.).

86 18 U.S.C. § 1956; Jimmy Gurule, *The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing Specified Unlawful Activity?*, 32 AM. CRIM. L. REV. 823, 837–38 (1995) ("Mere suspicion that the proceeds were derived from unlawful activity is not enough. The statute requires a 'knowing' state of mind.").

87 Proceeds of Crime Act 2002, § 328 (U.K.); DAVID ORMEROD & KARL LAIRD, SMITH, HOGAN, AND ORMEROD'S CRIMINAL LAW ch. 33 (2021).

88 R. v. Da Silva [2006] EWCA Crim. 1654 [16].

89 Proceeds of Crime Act 2002, § 303Z36 (U.K.).

90 ORMEROD & LAIRD, *supra* note 87, at para. 33.1.3.

91 R. v. GH [2015] UKSC 24 [49].

92 R. (on the application of Wilkinson) v. Director of Public Prosecutions [2006] EWHC 3012 [7].

Furthermore, the U.K. Proceeds of Crime Act notably includes an inbuilt safe-harboring mechanism where Party B can avoid future liability by making a disclosure to a public law enforcement authority.[93]

Furthermore, in the money laundering context, it is important to bear in mind that Party B is not a bank or regulated financial institution, but a business (e.g., a retailer).[94] Unless Party B is a "high value dealer" who accepts payment for "goods" valued at more than 10,000 euros, they have no obligation to conduct due diligence as to the actual ownership of the crypto.[95] So, if Party B is a professional service firm (e.g., it offers marketing services) and no goods are involved, it is not subject to the money laundering regulation.

Party B is required to conduct a "customer due diligence" as a "high value dealer," which requires collecting customer identification, but not necessarily the verification of the source of funds.[96] By contrast, under U.S. law, where the offense of possession of stolen property applies, Party B of any sector is required to be "prudent" and "cautious"—a vague obligation that could be interpreted to require due diligence in the form of basic blockchain tracing.[97]

In other words, both offenses (possession of stolen goods and money laundering) under English law do not generate unmanageable legal risks to Party B as a legitimate business.

---

93 Proceeds of Crime Act 2002, § 328(2) (U.K.).

94 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, § 8 (U.K.) (specifying that legal obligations, like the need to conduct risk assessments, are applicable only to regulated entities like financial institution, law firms, accounting firms, etc.).

95 *Id.* §§ 14, 27(3) (on what a "high value dealer" is).

96 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, § 28 (U.K.) (on what customer due diligence entails). Even for the gambling sector in the U.K., they "are under no legal obligation to ask customers to present identification, nor is there a threshold that would require staff to question the size of customer deposits, stakes, or withdrawals." Kane Pepi, *An Exploratory Study into the Money Laundering Threats, Vulnerabilities, and Controls Within the UK Bookmaker Sector, With a Specific Focus on Fixed-Odds Betting Terminals*, 22(1) UNLV GAMING RES. & REV. J. 1, 5 (2018), https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1368&context=grrj [https://perma.cc/E5JK-GBJY].

97 *See* Section II(B).

B. Civil Liability Under the Insightful English Law: Setting the Threshold Based on Probable Existence Versus Mere Suspicion

Under English law, the victims whose money has been misappropriated by Party A would want to rely on comparable courses of actions based on civil restitution and tracing. Party B will be liable to repay the victim if knowing receipt can be established. Constructive knowledge can be established based on a "should have known" standard:

> (1) Where the recipient appreciates that a proprietary right in the property *probably exists*, the recipient would have actual notice of the right;
>
> (2) Where a reasonable person with the attributes of the recipient *should have appreciated, based on facts already available* to him, that the right *probably* existed, the recipient has constructive notice of the existence of the right; and
>
> (3) If the facts known to the recipient would give a reasonable recipient in the position of the particular recipient *serious cause to question the propriety of the transaction*, the recipient should have made inquiries or sought advice, which would have revealed the probable existence of a proprietary right.[98]

On first sight, these "should have known" principles are comparable to the U.S. approach. But upon closer examination, they are materially different in two respects.

First, these English principles put the emphasis on the "probable" existence, as opposed to suspected existence. "Probable" existence is a commonly seen threshold in common law.[99] Under U.S. law, the standard of "probable cause" is generally understood as being a higher standard than "reasonable suspicion."[100] This holds true also under

---

98 Papadimitriou v. Crédit Agricole Corpn and Investment Bank [2015] 1 WLR 4265, 14–16 (emphasis added).

99 The standard of "probable cause" is applicable in Canada. *See* Terry Skolnik, *The Suspicious Distinction Between Reasonable Suspicion and Reasonable Grounds to Believe*, OTTAWA L. REV. 223 (2016). In the U.K., see O'Hara v. Chief Constable of the Royal Ulster Constabulary [1996] UKHL 6 (noting that the English common-law-based power of arrest must be justified by "reasonable and probable cause" but the statutory power of arrest under section 24 of the Police and Criminal Evidence Act 1984 is based on reasonable suspicion).

100 *See, e.g.*, Lauryn P. Gouldin, *Crimes of Suspicion*, 72 EMORY L.J. 1429, 1446 (2023); Cynthia Lee, *Probable Cause with Teeth*, 270 GEO. WASH. L. REV. 269, 271 (2020); Geoffrey C. Sonntag, *Probable Cause, Reasonable Suspicion, or Mere Speculation?: Holding Police to a Higher Standard in Destruction of Evidence Exigency Cases*, 42 WASHBURN L.J. 629 (2003); Joseph G. Cook, *Probable Cause to Arrest*, 24 VAND. L. REV. 317, 317 (1971) ("probable cause is clearly more than 'mere suspicion'"); State v. Marr, 499 S.W.3d 367, 374 (Md. 2016) ("Reasonable suspicion . . . is a less stringent standard than probable cause.").

English law.[101] While their exact difference has not been clearly stipulated by U.S. courts,[102] one interesting distinction is that "probable cause" concerns whether a reasonable person would "believe" and "reasonable suspicion" refers to whether a reasonable person would "suspect."[103]

This Article will not dwell on their differences which have been explored repeatedly in the literature.[104] The point here is, English law adopts a more stringent threshold than mere suspicion as in the United States. Arguably, the "probable existence" standard is more suitable for the present blockchain context. The higher threshold is more commercially sensible as it is not always practical for businesses to derive a firm answer as to whether the payment is tainted or not. Wallet tracing is not only complicated but can easily trigger a false alarm.[105] A more stringent standard is necessary to curb the disproportionate legal risks.

Notably, this English standard—which finds knowledge upon probable existence—has been adopted in other common law jurisdictions such as Singapore.[106]

---

101 *See, e.g.*, Clifford v. The Chief Constable of the Hertfordshire Constabulary [2008] EWHC 3154 [45]–[46].

102 Gouldin, *supra* note 100, at 1445; Kit Kinports, *The Quantum of Suspicion Needed for an Exigent Circumstances Search*, 52 U. MICH. J.L. REFORM 615 (2019); Kit Kinports, *Diminishing Probable Cause and Minimalist Searches*, 6 OHIO ST. J. CRIM. L. 649, 656 (2009).

103 *See, e.g.*, People v. Alemayehu, 494 P.3d 98, ¶ 35–36 (Colo. App. May 20, 2021); *Probable Cause Versus Reasonable Suspicion*, GOV'T MARICOPA CNTY., https://www.maricopa.gov/919/Probable-Cause-Versus-Reasonable-Suspici [https://perma.cc/G8X5-JZK2].

104 *See* cases cited *supra* note 99.

105 *See* Part I. From the technical standpoint, there is a myriad of literature exploring ways to reduce false positives or negatives, which implicitly indicate the inherent complexity and challenges. *See, e.g.*, Dan Amiram et al., *Coins for Bombs: The Predictive Ability of On-Chain Transfers for Terrorist Attacks*, 60(2) J. ACCT. RES. 427, 460 (2022) (noting that predictive blockchain-based models generate many false positives or negatives); Constantinos Patsakis et al., *Cashing Out Crypto: State of Practice in Ransom Payments*, INT'L J. INFO. SEC. (2023) (emphasizing the need to apply a "variety of techniques" to "filter out false positives and refine the analysis"); Haaroon Yousaf et al., *Tracing Transactions Across Cryptocurrency Ledgers*, PROCS. 28TH USENIX SEC. SYMP. (2019), https://www.usenix.org/system/files/sec19-yousaf_0.pdf [https://perma.cc/9PKG-FNWS]. At the same time, there are means to strengthen anonymization, which could hinder traceability. *See, e.g.*, Ardeshir Shojaeinasab et al., *Mixing Detection on Bitcoin Transactions Using Statistical Patterns*, 3(3) IET BLOCKCHAIN 136 (Aug. 14, 2023).

106 Perry v. Esculier [2022] SGHC(I) 10.

There is another difference between the English and U.S. positions. English courts will "impute knowledge, on the basis of what a *reasonable person* would have learnt, to a person who is guilty of *commercially unacceptable* conduct in the particular context involved."[107]

As mentioned in Section II(B), the United States has adopted the prudential standard that expects something more than reasonableness.[108] The prudential standard is also applicable in the civil context in the United States.[109] But the English position is different and less stringent. Firstly, the U.K. test maintains the focus on the reasonable person (as opposed to the prudent person). Secondly, it merely deters "commercially unacceptable practices" (a negative formulation), as opposed to requiring businesses to be prudentially cautious under U.S. law (a positive/obligatory formulation).

This second difference has also been adopted in other common law jurisdictions, such as Singapore.[110] The United States should therefore review how the difference in thresholds with other jurisdictions will affect the United States' competitiveness and market friendliness for the blockchain-based commercial context.

Applying the English test to our scenario, Party B will not be liable for civil restitution for two reasons. First, Party B does not "believe"—but at best merely suspects—the potential existence of some unknown victim's property right in the cryptos. This is far short of meeting the "probable existence" and "serious cause to believe" thresholds. Second, Party B is not required to act prudently under English law, and there is nothing on the facts that is "commercially unacceptable," including the acceptance of crypto as payment.

---

107 Cowan de Groot Properties Ltd. v. Eagle Trust Plc. [1992] 4 All ER 700, 761, applied in Vestergaard Frandsen A/S v. Bestnet Europe Ltd. [2013] UKSC 31 [26]; Executive Authority for Air Cargo and Special Flights v. Prime Education Ltd. [2023] EWHC 1634 (KB) [66] (emphasis added). *See also* Malcolm Cope, *A Comparative Evaluation of Developments in Equitable Relief for Breach of Fiduciary Duty and Breach of Trust*, 6(1) QUEENSLAND U. TECH. L. & JUST. J. 118 (2006) (noting the U.K. approach "to impute knowledge to a person guilty of commercially unacceptable conduct.").

108 *See* text in *supra* notes 34–35.

109 *See, e.g.*, Kirk v. Tomulty, 66 Wn. App. 231, 232 (Wash. Ct. App. 1992) ("If the purchaser of property has some actual or constructive knowledge of facts which would cause an ordinarily prudent person to make further inquiry, but fails to act on such knowledge with reasonable diligence, the purchaser will be charged with knowledge of defective title or of equitable rights of others and will be denied bona fide purchaser status.").

110 *See, e.g.*, George Raymond Zage III v. Rasif David [2008] SGHC 244 [23].

C. Probable Cause to Believe the Payment Was Tainted

Apart from being commercially sensible, there is another justification for adopting the probable existence/cause threshold: avoiding logical incoherence. English law is coherent—the United States' law is not.

In applying for a civil forfeiture order in the United States against property involved in money laundering, "the government must establish that probable cause exists to believe that the property was 'involved in' a money laundering offense."[111] This means that, in relation to dubious property that could be tainted, the government cannot forfeit it upon mere suspicion.[112] This is highly analogous to the present situation because the payment to Party B is suspected to be tainted. U.S. law is logically incoherent because, on the one hand, the dubious property can be forfeited only upon proof of *probable cause* of being involved in money laundering. On the other hand, a legitimate business could be compelled to return the property to the victims upon a civil action premised on *suspicion*.[113] This discrepancy (between the two applicable standards of probable cause versus mere suspicion) should be considered by the U.S. courts when reviewing the appropriateness of treating suspicion as the threshold in the commercial blockchain context.

There are other areas of U.S. law that sensibly apply the probable cause standard, which are apparently at odds with how Party B is made liable for not acting upon mere suspicion. For example, in a civil dispute, a party "assumes the *risk* for special damages liability for unusual losses arising from special circumstances only if . . . the defendant was clearly warned of the *probable existence* of [those] unusual circumstances."[114] Although this area of law is not directly relevant, it reflects how the law approaches the assumption of risk in the private law context. Applying the same reasoning, a party should be liable only for the risk taken if that risk has probable, as opposed to suspected, existence. As Party B has to the deal with the risk that the

---

111 *See* 18 U.S. Code § 981; Stefan D. Cassella, *Establishing Probable Cause for Forfeiture in Federal Money Laundering Cases*, 39 N.Y. L. SCH. L. REV. 163, 165 (1994).

112 *Id.* at 169.

113 *See* Section III(B)(2) (in the sense that the existence of suspicion hinders the proof of good faith in a title-based recovery action).

114 Diya TV, Inc. v. Kaxt, LLC, H042255, at 4 (Cal. Ct. App. Mar. 14, 2018) (emphasis added).

payment was tainted, and the legal question should have been whether there was probable cause to believe as such.

VI
THE GIST OF THE DISTINCTION BETWEEN THE U.S. AND ENGLISH APPROACHES

The starting point of this analysis is that cryptocurrency is susceptible to be perceived as inherently risky. In the absence of legislative intervention, there is no way to control or predict how a judge will perceive the use of cryptocurrencies and the way it should be processed in commercial settings. Risk-averse judges could see this as unduly risky and expect more measures in place to uphold the integrity of market transactions; whilst some others may conversely be more open to it and are willing to overlook the risks involved in newer forms of business practices.

The diverse spectrum of judicial attitudes can be readily observed. On the one hand, it is observable that some U.S. judges are less confident with crypto transactions. The District Court of the Eastern District of California remarked generally that "there is a high risk of asset dissipation with cryptocurrency."[115] The Delaware Bankruptcy Court also commented generally that

> Yield-earning platforms are generally risky due to their promises of high returns (often in excess of 8–12%), the volatility of cryptocurrency prices, and a lack of a clearly applicable regulatory scheme.[116]

The English High Court demonstrated a more understanding approach:

> It is also right to say that though cryptocurrencies and similar offerings have attracted their fair share of fraud, many honest start-ups are small operations with unsophisticated operators who struggle to attract investment—those who put money into these ventures do so as risk capital, with potentially high rewards should the start-up hit the jackpot. I fully accept that when allegations of fraud are made by disappointed investors in start-ups, considerations like these have to be taken into account.[117]

It cannot be fairly concluded that English courts are more open to cryptocurrencies than U.S. courts. Ultimately, it is more of a matter of

---

115 Jacobo v. Doe, 1:22-cv-00672-DAD-BAK (BAM), at 7 (E.D. Cal. June 7, 2022).

116 Cred Inc. v. Uphold HQ Inc. (In re Cred Inc.), 650 B.R. 803, 814 (Bankr. D. Del. 2023).

117 Blockchain Optimization SA & Anor v. LFE Market Ltd & Ors [2020] EWHC 2027 (Comm) [42].

judicial judgment. After all, it is important to bear in mind that crypto payment is relatively novel and underregulated.

The same diverse opinions also exist in the minds of legal practitioners. A reputable English law firm rightly observed that it is a question of *subjective* perception:

> [T]he use of crypto-assets therefore seems to be regarded, even by sophisticated players, as inherently suspicious even though . . . there is limited evidence that crypto-assets are being used (at present) for money laundering . . . as crypto-assets become an increasingly established method of payment, volumes increase, and it becomes easier for criminals to obscure the proceeds of crime.[118]

Another English law firm attributed the cause of the diverse opinions to the nature of crypto payment:

> At the heart of the matter lies the question of suspicion . . . [b]y contrast with traditional finance, which aims through the application of rigorous due diligence to create a hermetically sealed system that excludes criminal proceeds, crypto assets flow where they will—and are undoubtedly used by criminals as a means of storing and laundering their ill-gotten gains.[119]

In the present context, the riskier nature of crypto transactions does not mean it must involve negative, sharp/aggressive or criminal business practices. Instead, it is riskier because of its *neutral* characteristics like being pseudo-anonymous.

A. The Formulation of Legal Principles Matters: Any Room for Judicial Deference?

Even with an open-minded court that welcomes crypto transactions, the formulation of legal principles matters. The higher thresholds provide more freedom for the market to opt for a riskier form of payments. It makes room for an open-minded judge to *defer* to commercial practice.

---

118 Simmons & Simmons, *Crypto-Asset Compliance Myths and Misconceptions* (July 4, 2018), https://www.simmons-simmons.com/en/publications/ck0apkz0qdnoa0b59eob4gdsj/050718-crypto-asset-compliance-myths-and-misconceptions [https://perma.cc/GHY8-A5YK].

119 Jonathan Grimes & Daniel Browne, *Buying Property with Crypto Assets: Can It Ever Be Justified?*, KINGSLEY NAPLEY REAL EST. L. BLOG (June 24, 2021), https://www.kingsleynapley.co.uk/insights/blogs/real-estate-law-blog/buying-property-with-crypto-assets-can-it-ever-be-justified [https://perma.cc/39DK-V6BF].

Under U.S. law, it is imaginably difficult for a judge—despite being market-inclined—to compellingly aver that it is "prudent" for a business to not inquire about a suspicious payment. Instead, the stringent standards could leave a judge with little discretion, instead with the only option to legalistically or rigidly hold that the failure to act upon suspicion will, by law, result in imputed knowledge for establishing liabilities.

By contrast, the English approach is better suited for the present crypto context because it applies higher thresholds for establishing the knowledge requirement for both criminal and civil liabilities than the United States (e.g., probable cause to believe versus suspicion; what a reasonable business would know versus what a prudent business would know). A pro-market judge can easily utilize the ample discretion accorded by the higher thresholds and hold that there is no probable cause to believe the involvement of tainted proceeds.

CONCLUSION

Party B is unfairly and disproportionately exposed to the above legal risks and business uncertainty. When attributing culpability, it is important to bear in mind that the wrong committed by Party A is not caused by Party B. Also, the blockchain sector is underregulated.[120] In effect, the regulatory burden is shifted to Party B under U.S. law because the law requires Party B to act upon suspicious circumstances. Perhaps surprisingly, debates are still ongoing at this stage as to how they should be regulated despite their prevalence with both institutional and retail users and investors.[121] It is important not to forget that Party B is also a victim.

This Article shows that current U.S. generic principles are incompatible with the present state of technology involving blockchain. For example, the law triggers the obligation to make inquiries upon suspicion,[122] but this obligation is unbefitting as suspicious circumstances can come to mind after the contract has been entered into, when there is no way to halt automatically executed smart contracts.

---

120 *See* text in *supra* notes 2, 37.

121 Matthew Goldstein & David Yaffe-Bellany, *Is Cryptocurrency Like Stocks and Bonds? Courts Move Closer to an Answer*, N.Y. TIMES (Jan. 25, 2024), https://www.nytimes.com/2024/01/26/technology/cryptocurrency-stocks-bonds-courts-move-closer-to-an-answer.html [https://perma.cc/62RC-Q2XR].

122 *See* text in *supra* note 64.

Blockchain-based payment is different from cash. Cash is fungible/interchangeable, and this form of financial anonymity absolves the payee's concern of whether the money received is tainted.[123] Setting the thresholds for civil and criminal liabilities based on suspicion is therefore not an issue for cash. But for blockchain-based payment, its non-fungible and immutable character makes it semitransparent in the sense that blockchain analysis might be able to discern some red flags (e.g., having the same wallet address as mentioned in Part I), yet unable to provide third parties like Party B a firm answer on the suspicion, like the actual ownership.[124]

To be clear, suspicion itself is not a problematic threshold as it encourages proper inquiry. But it is simply not suitable for the commercial blockchain context when there are complicated considerations like whether blockchain analysis is necessary and pragmatic, and how suspicion can be too easily triggered when such analysis, at its present technological state, could be prone to false alarms.[125]

The awkward compatibility of the suspicion threshold under U.S. law becomes more revealing when a comparison is made with English law. The latter establishes knowledge based on probable cause to believe the payment was stolen, instead of mere suspicion. Liability

---

123 *See, e.g.*, Alastair Berg, *Anonymous Money Is Fungible Money*, THE FINREG BLOG (Duke Financial Economics Center) (Aug. 23, 2018), https://sites.duke.edu/thefinregblog/2018/08/23/anonymous-money-is-fungible-money/ [https://perma.cc/XEB7-3SJR]; Steven M. D'Antuono, *Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform*, FEDERAL BUREAU OF INVESTIGATION STATEMENT BEFORE THE SENATE BANKING, HOUSING, AND URBAN AFFAIRS COMMITTEE (Nov. 29, 2018), https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance [https://perma.cc/MV8Q-MUWW] ("Cash is anonymous, fungible, and portable; it bears no record of its source, owner, or legitimacy.").

124 Merchant et al., *supra* note 9 ("NFTs are pseudonymously held, which may make them particularly vulnerable to illicit use. However, NFTs are stored on a blockchain with a unique crypto wallet address. Some crypto wallets may reveal the identity of the owner, while others only reveal a string of characters known as a 'public key'") https://www.lawoftheledger.com/2022/03/articles/blockchain/money-laundering-high-value-art-treasurys-study-financial-crimes-nfts/#more-1791 [https://perma.cc/H9RJ-5XGY]; Diana Clement, *Congratulations, You've Been Served – Over the Blockchain*, N.Z. L. ASSOC. (Aug. 25, 2022) (noting that whilst the courts can trace the transfer of funds between wallets, they cannot ascertain the exact identity of the owner), https://thelawassociation.nz/congratulations-youve-been-served-over-the-blockchain/ [https://perma.cc/AT3G-EGPV]. *See also* text in *supra* notes 11–13.

125 *See* Parts I, IV.

justifiably arises only when Party B fails to act despite believing that irregularity against the victims' rights probably exists.

There are many other potentially incompatible aspects between the present generic law and blockchain. For example, U.S. courts have held that the circumstances that will lead to deduced knowledge include "conduct and behavior, the character of the person from whom received, and the kind of goods."[126] In terms of the "kind of goods," cryptocurrencies are known for inadequate regulation given its emerging character.[127] They are more prone to crimes like money laundering. Will this create a negative starting point for Party B in terms of establishing the knowledge requirement, for having chosen to accept risky forms of payment? This is another unresolved uncertainty for businesses.

One might counterargue that Party B should be deemed to have accepted all these legal risks under U.S. law, and that they can protect themselves by conducting due diligence like what Ferrari does. However, this Article has explained that conducting due diligence is simply commercially unrealistic; not to mention that the U.S. legal principles on due diligence cannot be unambiguously applied to the blockchain payment context. These unresolved legal conundrums should not be unfairly transformed into legal risks for Party B as a legitimate business.

Adopting higher legal thresholds for civil and criminal liabilities has the advantage of providing the judiciary with the flexibility to defer to the market's choice of processing crypto payment. Crypto transactions are a fast-developing area. If the market accepts crypto payment, and Party B's way of processing payment materially conforms with that practice, there is a compelling case that the courts—especially in the absence of legislative intervention—should not second-guess the market's choice and undermine this freedom in the absence of legislative intervention. Any future rulings should distinguish the unprecedented blockchain payment context, and Party B should not be readily held liable solely based on suspicion.

---

126 Prather v. State, 116 Ga. App. 696, 696 (1967).

127 *See* text in *supra* note 37.