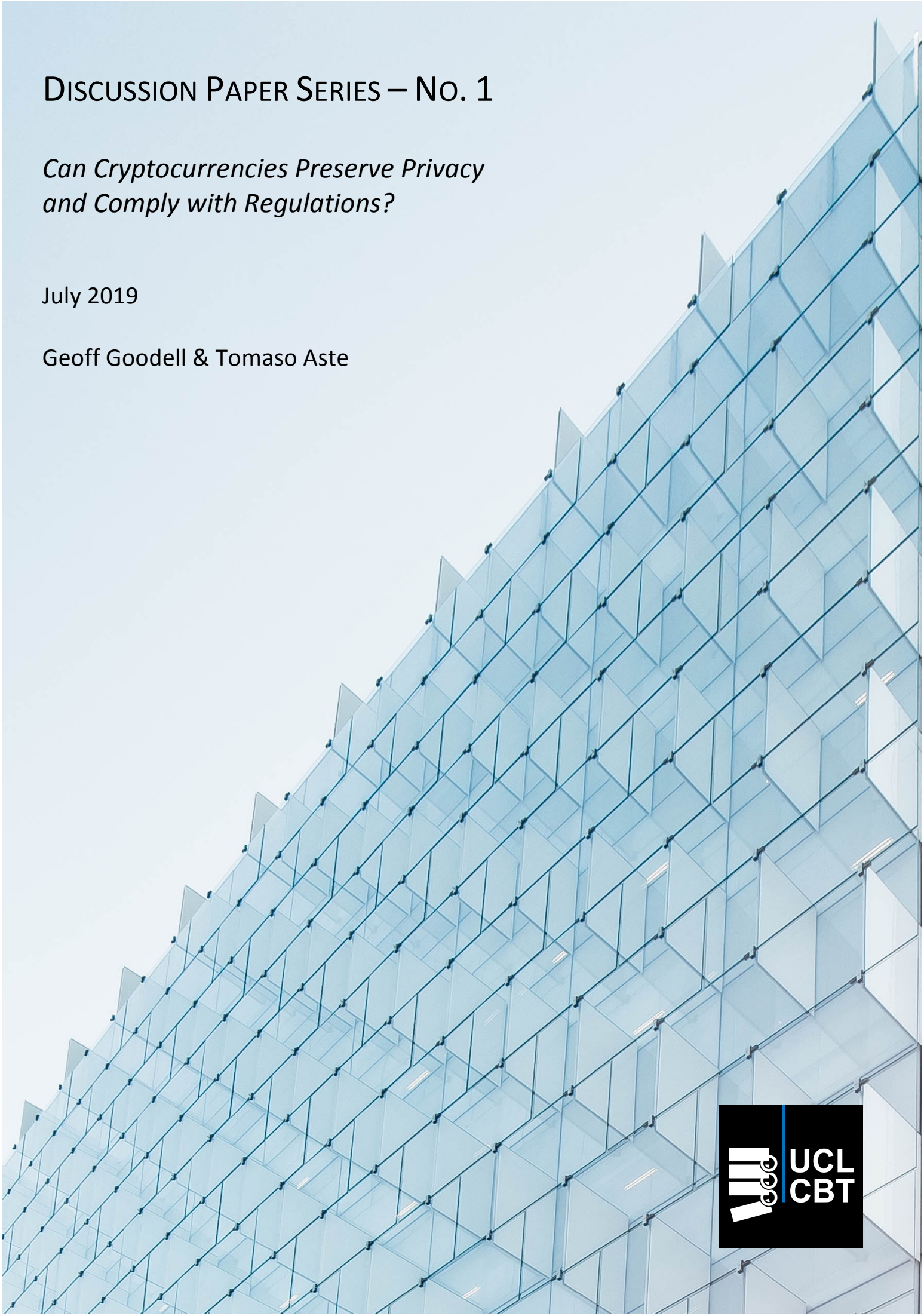

DISCUSSION PAPER SERIES – NO. 1

Can Cryptocurrencies Preserve Privacy and Comply with Regulations?

July 2019

Geoff Goodell & Tomaso Aste

UCL CBT

Can Cryptocurrencies Preserve Privacy and Comply with Regulations?

Geoff Goodell
Centre for Blockchain Technologies
University College London
g.goodell@ucl.ac.uk

Tomaso Aste
Centre for Blockchain Technologies
University College London
t.aste@ucl.ac.uk

Abstract

Cryptocurrencies offer an alternative to traditional methods of electronic value exchange, promising anonymous, cash-like electronic transfers, but in practice they fall short for several key reasons. We consider the false choice between total surveillance, as represented by banking as currently implemented by institutions, and impenetrable lawlessness, as represented by privacy-enhancing cryptocurrencies as currently deployed. We identify a range of alternatives between those two extremes, and we consider two potential compromise approaches that offer both the auditability required for regulators and the anonymity required for users.

1 Introduction

The surveillance economy has arrived [1]. The popularity of online service platforms has enabled service providers to collect, aggregate, and analyse data about the behaviour of individuals with a volume and scope never before possible. Data brokers have created a marketplace for exchanging information about individuals that can be used to link their various online actions, including but not limited to financial transactions. Such information, including the reuse of credentials over successive transactions, can be used to link the transactions to the transacting parties [2, 3]. Such a linkage can greatly simplify successive transactions, reducing costs for the provider and improving customer experience. However, the potential for monitoring profoundly influences the everyday behaviour of individuals as they conduct their various activities [4]. The value of such control is reflected in an emerging marketplace for record linkage via *entity resolution*, which seeks to determine the specific individual person associated with any given activity and, correspondingly, the history of activities associated with any given individual person [5, 6].

In the context of longstanding arguments that privacy is a public good [7, 8, 9, 10], it is worthwhile to consider whether such practices may serve to exacerbate social inequity by restricting the ability to transact privately to those with sufficient wealth and power [11, 12]. Financial transactions are no exception, since they reveal information about not only the volume and recipients of individuals' purchases and remittances but also their patterns, location histories, social networks, and so on. Modern retail banking creates a kind of panopticon for consumer behaviour, ultimately promising to implement a mechanism that binds all of the financial activities undertaken by an individual to a single, unitary identity. Consumers have legitimate reasons to resist such surveillance, particularly in cases wherein monitoring is carried out without their knowledge and judgments based upon such monitoring are used to disincentivise or punish legitimate activities. The risk to consumers increases with the ever-increasing share of financial transactions that are performed electronically. The increasing capability of third parties to aggregate and analyse data about retail financial transactions fundamentally changes the relationship between individuals and their financial institutions.

Cryptocurrencies seem like a natural alternative for exchanging value that can avoid the watchful eye of state actors, powerful corporations, hackers, and others who might be well-positioned to build a dossier of one's activities. However, a lack of appropriate regulation generally burdens cryptocurrency users with practical limitations and risks. The risks include the lack of financial products and services, the inability to earn interest, basic consumer protection, and the absence of legal infrastructure for adjudicating disputes. China has also restricted the use of cryptocurrency exchanges as a means of addressing capital outflows [13].

Additionally, most cryptocurrencies are not as privacy-enhancing as is commonly perceived, and as state actors attempt to erect a cordon around criminal activity that relies upon cryptocurrencies, some

Robust to cyberattacks
Usable without registration
Unlinkable transactions
Electronic transactions
Suitable for taxation
Can block some illicit uses
Can be denominated in units of fiat currency

Table 1: *Desiderata for an electronic payment method.*

governments have actively sought to undermine the adoption of cryptocurrencies that are most respectful of an individual's privacy. For example, the Financial Services Agency in Japan pressured cryptocurrency exchanges to drop privacy-enhancing tokens such as Monero [14], one of the largest cryptocurrency exchanges in South Korea subsequently delisted privacy-enhancing tokens [15], the US Department of Homeland Security specifically called for methods to circumvent privacy protections in privacy-enhancing cryptocurrencies [16], and the UK Financial Conduct Authority offered guidance indicating its intention to "prevent [rather than simply prosecute] the use of cryptoassets for illicit activity" [17]. Furthermore, whether or not these government initiatives succeed in preventing untraceable cryptocurrencies from achieving mainstream adoption, even the most private cryptocurrencies suffer from the arguably intractable governance challenges associated with building a decentralised network that respects the interests of its users.

Following the G20 summit held in Buenos Aires in 2018, leaders resolved to "regulate crypto-assets for anti-money laundering and countering the financing of terrorism in line with FATF standards" [18]. Earlier, the UK Parliament had published a report citing lack of consumer protection and regulated marketplaces for crypto-assets as major drawbacks associated with cryptocurrencies as a medium of exchange, also noting the possibility that anonymous transactions might promote money laundering is a significant perceived risk, despite that the UK National Crime Agency had assessed the risk as low [19]. So we have reached an impasse, with institutions demanding control and countenancing surveillance at one extreme, and cyberlibertarians demanding privacy at the expense of regulation on the other.

Let us commence this article by introducing a set of "desiderata": properties that a payment system should have. They are listed in Table 1. In addition to usefulness, security, and privacy, we also note the various arguments for money as a "valid payment for all debts" [20], as a means of funding government activity through taxation [21]. We discuss how we can reframe our requirements such that we might achieve a parsimonious set of regulatory objectives while also respecting privacy and fulfilling the desiderata. We follow and extend the ongoing discussion of how to regulate cryptocurrency payments [22, 23], with a view toward respecting human rights [24].

The paper is organised as follows. In the remainder of the first section, we discuss the regulatory context surrounding modern retail financial transactions, and we introduce cryptocurrencies as a prospective substitute for regulated payments. In the second section, we compare and contrast three methods of conducting financial transactions online: modern, regulated retail banking; classic cryptocurrencies such as Bitcoin; and privacy-enabling cryptocurrencies such as Monero. In the third section, we introduce two candidate approaches that each offer individuals a verifiable means of transacting privately and also provide suitable mechanisms by which institutions can enforce regulatory compliance. In the final section we conclude with a discussion of the opportunities and tradeoffs.

1.1 Institutional Posture

Banks and other financial intermediaries in many jurisdictions around the world are subject to anti-money laundering (AML) or "know your customer" (KYC) regulations that require them to collect data on individual accountholders and others who make use of their services [25, 26]. The penalties for non-

compliance are potentially severe. In recent years, banks have dedicated significant resources to building and maintaining compliance infrastructure, evidenced by the thousands of employees that they have hired to monitor "high-risk" transactions, as well as "tens of thousands of costly customer calls every month to refresh KYC documents" [27].

An international organisation named the Financial Action Task Force (FATF) was established by the G7 in 1989 as a trans-national effort to monitor financial activities, with the stated purpose of investigating and preventing money laundering and terrorist financing [28]. FATF provides one of the mechanisms by which AML/KYC regulations in different jurisdictions are promulgated and coordinated. FATF also publishes a blacklist of nations who fail to enforce rules that facilitate the identification and investigation of individual accountholders, with the purpose of coordinating sanctions that force blacklisted nations to conform [29].

The financial regulations imposed by economically powerful jurisdictions such as the United States and the European Union share common features. In the US, AML regulations provide for customer identification and monitoring, as well as the reporting of suspicious activities [30]. In the EU, Directive (EU) 2018/843 ("5AMLD") requires that every financial transaction must be associated with an account, and that every account must be associated with a strongly identified responsible individual [31]. The directive also significantly reduces the maximum allowed value for prepaid cards and stipulates that remote transactions above EUR 50 must be accompanied by customer identification [31]. Note that 5AMLD specifically includes cryptocurrencies as subject to its prescribed regulations on financial transfers.

Although the systematic collection of identifying information for individual accountholders might facilitate important investigations, it also provides a mechanism by which authorities can browse comprehensive or near-comprehensive financial information about individuals without their knowledge. Authorities with those capabilities, and the businesses positioned to aggregate and analyse data collected for compliance purposes, may also be able to conduct statistical evaluations of individuals based upon the information available to their financial institutions. Once aggregated and linked to unitary identities, the transaction data collected by financial institutions offer a detailed look into the habits, patterns, travels, associations, and financial health of individuals.

The risks associated with such surveillance of electronic transactions were recognised fifty years ago by Paul Armer of the RAND Corporation, who identified the risk in a 1968 US Senate deposition [32] and later argued that "if you wanted to build an unobtrusive system for surveillance, you couldn't do much better than an [electronic funds transfer system]" [33]. Indeed, payment networks routinely share information about financial transactions with credit bureaus such as Experian [34], who are in the business of judging individuals by their behaviours and whose judgments form the basis of decisions made by lenders, insurers, and other clients of analytics companies [35]. Additionally, documents released by Edward Snowden have revealed that the US National Security Agency has a division called "Follow the Money" (FTM) that systematically collects and analyses data from payment networks [36].

1.2 Cryptocurrencies

Cryptocurrencies have enjoyed popularity in recent years, and people have flocked to cryptocurrencies for a variety of reasons. The idea of accountless digital cash is hardly new, dating at least as far back as the 1982 paper by David Chaum on blind signatures [37], the technology that he later used to start DigiCash Inc, which folded in 1999 [38]. Other attempts to develop accountless electronic payment systems such as E-Gold [39] and Liberty Reserve [40] were designed with privacy in mind, and ultimately ran afoul of authorities when criminals used those systems for nefarious purposes.

By the time Bitcoin emerged in early 2009 [41], the financial crisis had prompted aggressive responses from central banks around the world, and surely it was no coincidence that the message of circumventing inflationary monetary policy enjoyed appeal among would-be hoarders. However, given the history of privacy as a primary motivation for the adoption of digital cash, we surmise that many of the cryptocurrency adopters (other than speculators) are primarily seeking privacy, whether to circumvent capital controls or just to avoid the "pastoral gaze" of state or corporate surveillance [42]. Some important developments in recent years corroborate this view, most notably the attempts to develop a "stablecoin": a cryptocurrency that avoids the volatility of cryptocurrency prices by establishing a market peg, for

example to a fiat currency [43]. The most notorious example of a stablecoin is Tether, a cryptocurrency that was established for the purpose of maintaining a one-to-one peg with the US Dollar [44, 45]. For this reason, stablecoins can be denominated in units of fiat currency. However, stablecoins have important limitations, including well-justified concerns about unilateral exchange rate pegs in general [46].

As a replacement for the "legitimate" currencies underwritten by the full faith and credit of sovereign governments, cryptocurrencies are far from perfect. There are structural reasons for this, including:

1. *Absence of financial services.* There is a notable absence of reliable organisations that offer routine financial services such as lending, and more importantly, there is a lack of regulatory support for crytpocurrencies. Further, in contrast to transactions conducted via global messaging systems such as SWIFT [47], there is generally no way to correct or unwind erroneous transactions performed with permissionless cryptocurrencies, a critical operational limitation. For cryptocurrencies to be a true substitute for government-issued currencies, they must support a range of marketplaces and financial products.

2. *Absence of regulated marketplaces.* History tells us that unregulated marketplaces for financial products can be harmful to ordinary citizens and businesses alike; consider for example the misbehaviour of brokers and market participants that led to the creation of the US Securities and Exchange Commission [48]. Cryptocurrency markets lack such controls and mechanisms to ensure accountability, and unchecked market manipulation is commonplace [49, 50].

3. *Absence of legal context.* There is no generally applicable mechanism for adjudicating disputes arising from transactions that are executed in cryptocurrency. When automatically executable contracts such as those that underpinned the "Decentralised Autonomous Organisation" that roiled the Ethereum community in 2016 [51] are exploited, there is little legal recourse for hapless victims. Although "certain operational clauses in legal contracts" may be automated to beneficial effect [52], it would seem that a maximalist conception of the principle of "code is law" may not be workable without a suitable legal framework.

Furthermore, cryptocurrencies often fail to deliver on their key promises. For example, they are often not as private as is commonly believed. Analysis of Bitcoin transactions can deanonymise them, and researchers have shown that it is eminently possible to identify meaningful patterns among the transactions [53, 54]. The problem persists not only as a result of prevalent web trackers and the reuse of pseudonyms linked to Bitcoin wallets [55] but also because inbound transactions to a Bitcoin address can fundamentally be linked to outbound transactions from that address [56]. Indeed, it has even been argued that the explicit traceability of transactions on the Bitcoin ledger, combined with a straightforward approach to tagging suspect transactions [57], make it even less private than traditional mechanisms of payment. Even cryptocurrencies such as Monero, which are designed for privacy, have been shown to have important weaknesses [58, 59]. Another, perhaps equally important deficiency of cryptocurrencies is that they are not as decentralised as is commonly believed. Although decentralisation is often touted as the raison d'être of cryptocurrencies [60], in practice the governance, "mining," and infrastructure services associated with cryptocurrencies have remained stubbornly centralised for a variety of reasons [61]. The problem of decentralisation is intimately related to the more elemental governance problem how to ensure that the system serves the interest of its users. Without institutional support, there is little to ensure that this remains the case.

The governance problem is of particular significance to stablecoins. Importantly, if a stablecoin is not maintained and controlled by a central bank, then its users would need to be concerned about who is ultimately providing assurance that it will retain its value.

2 Electronic Payments Today

As electronic funds transfer systems have proliferated in recent decades, so has the expectation that people will make use of those systems. If this trend were to continue, we would anticipate that the fixed costs associated with infrastructure to support cash transactions would become harder to justify, and

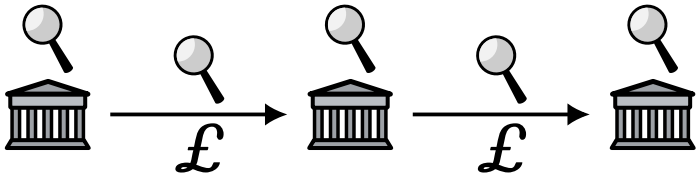

Figure 1: *Schematic Representation of Modern Retail Banking Transaction Flows.* The buildings with columns represent financial institutions with which the transacting parties hold accounts. Money is exchanged in state-issued currency, as represented by the Pound Sterling symbols. Authorities and other powerful actors can monitor both the institutions and the flows, as represented by the magnifying glasses.

variable costs such as widespread deployment of ATM machines would be reduced. Individuals and small businesses have various options to conduct transactions electronically. "Electronic" financial transactions include nearly all economic transactions that are not conducted using cash, notwithstanding the use of precious metals, money orders, and barter. For our purposes, all payments involving institutional accounts, including card payments (via payment networks), wire transfers, ACH, and even physical cheques, are conducted electronically, as are payments conducted using cryptocurrency. Next, we shall consider the characteristics of transactions in three examples of electronic payments: those involving institutional accounts, those involving "basic" cryptocurrencies, and those involving "privacy-enabling" cryptocurrencies.

2.1 Modern Retail Banking

Modern retail banking involves electronic transactions between *accounts*, each of which represents a bilateral relationship between a financial *institution* (e.g., a bank) and another entity, perhaps an individual. Institutions are generally regulated by governments. Individuals and businesses may agree to exchange value (for example, in return for goods and services), but in reality the transaction takes place between institutions, which mutually agree to modify the state of the accounts such that the account of the "receiver" is incremented and the account of the "sender" is decremented correspondingly. Record of the transactions and their results are generally visible to the institutions, accountholders, authorities, and auditors. Figure 1 offers an illustration of the data flows corresponding to two transactions. Institutions are direct participants in the transactions. Both the accounts and the transactions may be monitored, i.e. "external" *observers* such as authorities (and in some cases others, such as unprivileged employees of the institutions and hackers) are able to examine the records of the transactions, their results, and the transactions themselves. Since the set of regulated institutions is small, it is efficient for an observer to collect, aggregate, and analyse the data associated with substantially all of the transactions that take place within the system.

By contrast, data on transactions involving cash are relatively difficult to observe in this fashion, and are therefore more private. However, although cash remains a popular instrument for retail transactions, its use is decreasing as consumers become more comfortable with electronic means of payment [62]. Some economists such as Kenneth Rogoff hail this transformation as a welcome development, citing reductions in tax evasion and crime as primary benefits as anonymous payments are curtailed [63]. Others are more circumspect. Citing Sweden's drive to become cashless, Jonas Hedman recognised the loss of privacy as the primary disadvantage of a cashless society, although he also acknowledged that the transition to cashlessness is inevitable [64]. Assuming that the insistence on unitary identifiers for all electronic financial transactions as proposed by regulations such as 5AMLD [31] is satisfied, and combined with large-scale aggregation and analysis of the sort already in practice [36], cashlessness means the creation of a browseable "permanent record" for every individual containing his or her entire transaction history.

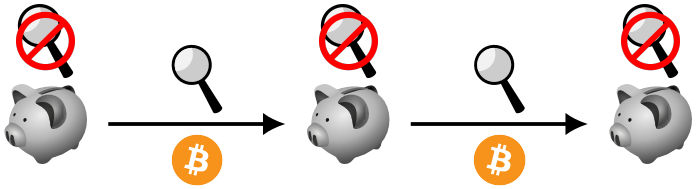

Figure 2: *Schematic Representation of Bitcoin Transaction Flows.* Transacting parties can store value on their own devices, represented as piggy banks. The flows can be monitored by anyone.

2.2 "Basic" Cryptocurrency, e.g. Bitcoin

Cryptocurrencies offer an alternative payment mechanism that avoids some aspects of the surveillance infrastructure that characterises institutionally-mediated retail bank transactions. Modern cryptocurrencies generally take the form of bearer instruments, in the sense that their units are each represented by a public key on a public ledger and controlled by the knowledge of the matching private key. Users are not required to establish accounts or furnish identification information of any sort to receive, possess, or spend cryptocurrency. This is not to say that accounts do not exist; most users of popular cryptocurrencies such as Bitcoin and Ethereum establish accounts with centralised wallet providers such as *blockchain.info* or *myetherwallet* [61]. Providers of accounts could be compromised or subverted by state actors or other powerful groups with an interest in surveillance. Some account platforms cooperate with national regulators [65], and some national regulators have declared that they will limit the scope of the rules that would apply to such platforms [66]. Many if not most cryptocurrency transactions are done by speculators, not those who intend to use cryptocurrency for its fundamental properties [67], so even if most traders in practice might be indifferent to strong identity requirements crafted by regulators to satisfy AML goals, such rules undermine a key design objective of cryptocurrencies themselves.

In principle, however, users of cryptocurrencies are not required to register with platforms, and they may possess cryptocurrency tokens on their own devices. Figure 2 shows how this works in practice. Assuming that cryptocurrency users take precautions not to reveal their identities whilst transacting, for example by using anonymity systems such as Tor [68], they might expect to avoid identity-based blacklisting when they receive tokens. However, depending upon the system design, adversaries may still be able to monitor the flows. Because successive Bitcoin transactions are linkable to each other, those able to monitor the network can determine successive transactions associated with specific tokens and ultimately deanonymise Bitcoin users [53, 54, 56].

The fact that individual tokens can be traced means that cryptocurrencies such as Bitcoin may not be entirely fungible, in the sense of being "easy to exchange or trade for something else of the same type and value" [69], as an individual might be less willing to accept certain specific cryptocurrency tokens because doing so might implicitly link that individual to previous owners of the tokens. Traceability has created demand for newly-minted or "clean" tokens that are harder to link to the previous owners or (ultimately) the previous transactions of the current owner [70], and the proposed blacklists of cryptocurrency addresses associated with suspicious operators could further exacerbate this distinction [71]. To avoid this problem, a cryptocurrency implementation would need to offer assurance that a transaction by an asset holder would generally not, directly or indirectly, result in that asset holder being linked to other transactions that had taken place previously. Additionally, cryptocurrencies that make use of immutable ledgers and do not protect against traceability may for that reason be non-compliant with data protection regulations such as GDPR that specify a "right to be forgotten" [72].

2.3 "Privacy-Enabling" Cryptocurrency, e.g. Monero

Some cryptocurrencies, most notably Zcash and Monero, are explicitly designed to address traceability concerns [73]. Monero in particular takes an approach that incorporates several security mechanisms, including:

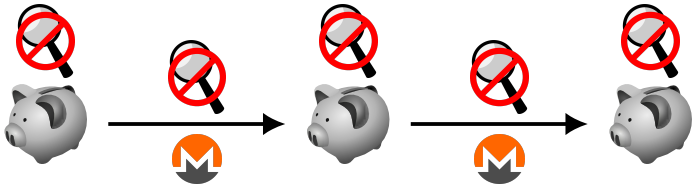

Figure 3: *Schematic Representation of Monero Transaction Flows.* In an "idealised" version of Monero or other privacy-enabling cryptocurrency, observers would not be able to infer information about transacting parties or the relationships between transactions by monitoring the ledger or the transactions themselves, as indicated by the magnifying glasses with the negation symbol. The piggy banks indicate that users are storing the tokens privately rather than relying upon accounts.

1. *Ring Signatures,* which allow signed messages to be attributable to "a set of possible signers without revealing which member actually produced the signature" [74].
2. *Stealth Addresses,* which refer to methods for key management in which public keys are derived separately from private keys for the purpose of obscuring the public keys [75], and
3. *Confidential Transactions,* which use Pedersen commitment schemes [76] to restrict disclosing the amounts transacted to anyone other than the transacting parties [77].

Figure 3 illustrates how, in a successfully implemented privacy-enabling cryptocurrency, metadata associated with transactions would be hidden such that the data flows or the ledger would not reveal relationships among transactions or any information about the transacting parties. That said, the Monero design and implementation still do not completely realise this goal; its process for mixing transactions suffers from inconsistent selection probability among all elements of the anonymity set [58]. Monero spokesperson Riccardo Spagni countered that "privacy isn't a thing you achieve, it's a constant cat-and-mouse battle" [78], echoing longstanding arguments by others that privacy is inevitably an endeavour of vigilance and responsiveness [79].

Some authorities such as the Japanese Financial Security Agency (FSA) [80, 81] and the United States Secret Service [82] have responded to so-called "privacy coins" by banning the use of privacy-enhancing cryptocurrencies whilst accepting other cryptocurrencies as legitimate by comparison. For a cryptocurrency exchange or other provider of cryptocurrency-based financial services to be compliant under such rules, it would need to restrict its activities to cryptocurrencies such as Bitcoin and Ethereum which do not have the privacy characteristics that have been sought by cryptocurrency advocates for decades.

There have also been some attempts, notably Mimblewimble [83], to retrofit basic cryptocurrencies with some of the characteristics of privacy-enabling cryptocurrencies, although it remains to be seen whether such approaches will turn out to be more effective than cryptocurrencies designed with better intrinsic privacy features in the first instance.

3 Proposed Hybrid Approaches

We consider the following challenge facing policymakers, regulators, and technologists alike: *how can we achieve realise the benefits of government regulation without creating a central database that irreversibly connects all persons with all of their transactions?* There are two parts to this question. The first part is primarily about *technology:* can we build a system that securely processes financial transactions conducted electronically without revealing data about the transacting parties? The answer is yes, as described in our discussion of privacy-enabling cryptocurrency, with an important qualification that privacy is really an iterative process that can only really be developed through active commitment and ongoing vigilance. The second part is primarily about *government policy:*

	cash	modern retail banking	"traditional" cryptocurrency (e.g. Bitcoin)	"traditional" stablecoins (e.g. Tether)	privacy-enabling cryptocurrency (e.g. Monero)
Robust to cyberattacks	●	○	○	○	○
Usable without registration	●	○	●	●	●
Unlinkable* transactions	◑	○	○	○	●
Electronic transactions	○	●	●	●	●
Suitable for taxation	◑	●	○	◑	○
Can block some illicit uses	○	●	○	○	○
Can be denominated in units of fiat currency	●	●	○	●	○

*Potentially

Table 2: *Comparison of various existing electronic payment methods.* [*Potentially]

- What exactly are the key government objectives for regulating transactions?
- Which objectives are essential, and which can be deprioritised?
- Do any of the objectives conflict with the human right to privacy?

Table 2 shows how the existing payment methods achieve the desiderata listed in Section 1. (None of the popular cryptocurrencies are known to offer totally unlinkable transactions, continual improvements notwithstanding.) Can we achieve a compromise that does better than the prevailing methods for electronic payments?

In this section we introduce two approaches to frame the discussion of how to resolve the tension. The first approach, *institutionally supported privacy-enabling cryptocurrency*, provides regulated institutions with tools and procedures for interacting with privacy-enabling cryptocurrencies, creating a structure for legal interpretations of their use. We assume that the distributed ledgers underlying such cryptocurrencies *are not* controlled by regulated financial institutions. The second approach, *institutionally mediated private value exchange*, establishes a method by which regulated institutions can conduct financial transactions on a distributed ledger that shares essential characteristics with privacy-enabling cryptocurrencies. In this case, we assume that the distributed ledgers used for this purpose *are* controlled by regulated financial institutions. The main difference between the two approaches is that the first approach allows businesses to transact with cryptocurrencies that are managed and governed outside the mainstream financial system, and the second approach provides a way for regulated financial institutions to offer a mechanism for their clients to exchange money that resembles cryptocurrency in that clients can withdraw money electronically and subsequently use it without reference to an account, as they would with cash.

There is a third possibility, which we might describe as "institutionally supported privacy-enabling stablecoins," in which the privacy-enabling cryptocurrencies in question are actually stablecoins. This possibility is theoretically worth pursuing if stablecoins achieve popularity commensurate with cryptocurrencies, although the experience of Tether suggests it might not be easy. It is worth considering that the proposal for institutionally mediated private value exchange is similar to a stablecoin in that the tokens represent units of fiat currency. However, because the regulated financial institutions are assumed to be part of the banking system they would not need to bear the risk associated with maintaining a market peg.

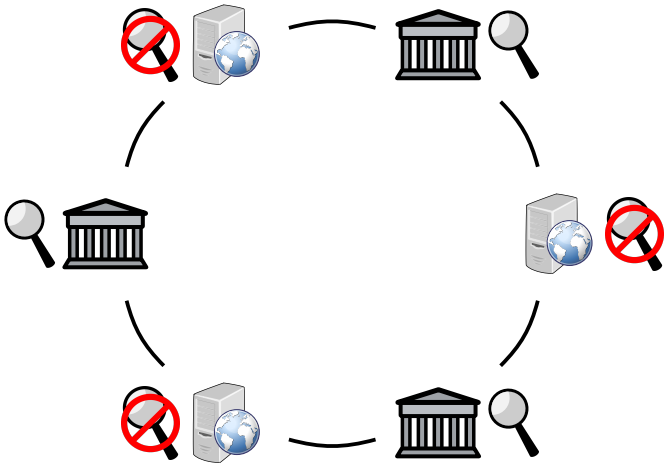

Figure 4: *Schematic Representation of Institutionally Supported Privacy-Enabling Cryptocurrency: Nodes.* Institutions would join global networks of servers operating as nodes in existing cryptocurrency networks; not all participants in these networks are regulated institutions.

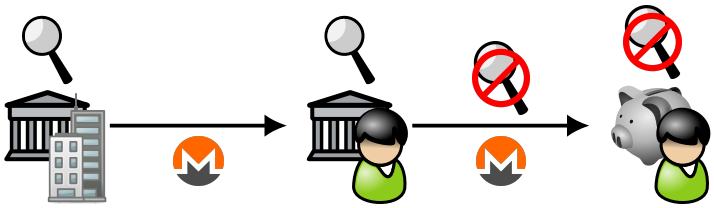

Figure 5: *Schematic Representation of Institutionally Supported Privacy-Enabling Cryptocurrency: Transaction Flows (1).* (We use the Monero symbol to represent any privacy-enabling cryptocurrency without loss of generality.) Corporations and registered businesses with accounts held by regulated financial institutions (leftmost icon) that would be subject to monitoring and may only remit cryptocurrency payments to other accounts held by regulated financial institutions. Individuals and non-business partnerships (centre icon) may transfer cryptocurrency from accounts to unmonitored, private storage (rightmost icon).

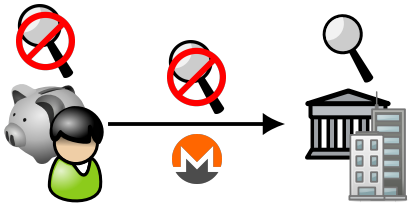

Figure 6: *Schematic Representation of Institutionally Supported Privacy-Enabling Cryptocurrency: Transaction Flows (2).* An individual (shown at left) with a private store of cryptocurrency could remit payments without revealing her identity to a business with accounts held by a regulated institution (shown at right).

3.1 Institutionally Supported Privacy-Enabling Cryptocurrency

Our first approach starts with existing, privacy-enabling cryptocurrencies such as Zcash or Monero and assumes that regulators have chosen to embrace the new methods for exchanging value and accept, if not support outright, at least some of the various communities that have formed around particular cryptocurrencies to provide governance and software development. Acceptance of cryptocurrencies by governments and other institutions is certainly plausible; for instance, the Bank of England concluded that cryptocurrencies "currently do not pose a material risk to UK financial stability" [84]. It assumes that government priorities include collecting taxes and monitoring transactions undertaken by businesses and regulated institutions.

Figure 4 illustrates how institutions would join existing cryptocurrency systems as full participants. The motivation for broker-dealers and other institutions to participate is well-established; financial services related to cryptocurrencies are in demand by hedge funds and other clients [85, 86]. Of course, this implies that broker-dealers would likely undertake activities related to unregulated markets and marketplaces (i.e., the cryptocurrencies themselves), and presumably the governance of the cryptocurrencies would not be under institutional control. That said, the distributed ledger underlying the cryptocurrencies would ensure that there would be an audit trail of all transactions, even if the details of those transactions might be inscrutable to authorities, auditors, or others without the active participation of the transacting parties.

To facilitate monitoring, auditing, and taxation, we assume that regulators would stipulate that all cryptocurrency transactions undertaken by certain legal entities other than individual persons, such as registered corporations, licensed businesses, charities, trusts, and some partnerships, must take place via regulated institutional intermediaries such as banks, custodians, or broker-dealers. In general, such legal entities are already subject to various forms of government oversight, for example tax reporting requirements, so to introduce additional requirements and enforceability for cryptocurrency transactions is not unfathomable. The institutions would carry out AML/KYC compliance procedures as they currently do, and regulators would require that all cryptocurrency disbursements from such registered corporations or organisations, including dividends, interest, proceeds from disposal of cryptocurrency-denominated assets, and payments, including without limitation payments to suppliers, service providers, employees, and contractors, would take the form of remittances to other institutional accounts that hold cryptocurrency.

Individuals and non-business partnerships would not be subject to the same requirements and would be permitted to transact and hold cryptocurrency privately, as they do in many countries today. Figure 5 shows how this would work in practice. Businesses would maintain accounts with institutions and could direct the institutions to remit payments to other institutionally held accounts, including those whose beneficial owners are individuals, and individuals could in turn direct their institutional accounts to remit payments to their private cryptocurrency storage, which might or might not be hosted by a wallet provider. Individuals could then remit payments from their own private storage to regulated businesses, such as merchants, private organisations, or service providers, without necessarily revealing their identities or a link to previous transactions such as those from which they received the cryptocurrency in the first place; Figure 6 offers an illustration. Given that the legal entities covered in the last paragraph

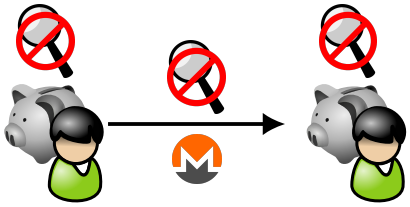

Figure 7: *Schematic Representation of Institutionally Supported Privacy-Enabling Cryptocurrency: Transaction Flows (3).* Individuals with private stores of privacy-enabling cryptocurrency may transact directly without revealing their identities.

are typically subject to financial reporting requirements, for example to quantify reimbursements or to reconcile changes in assets with income, we assert that it would be no easier for a business to deputise an individual to conduct cryptocurrency transactions on its behalf than it would for a business to deputise an individual to conduct any other financially meaningful aspect of its business.

Dividing the different ways of holding the cryptocurrency into two categories based upon whether or not it is held via accounts associated with regulated institutions may be considered analogous to dividing Zcash into "T" (Transparent) and "Z" (Shielded) addresses [87].

Because all cryptocurrency accounts held by corporations and registered businesses would be subject to monitoring by regulated institutions, the infrastructure would ensure that the taxable income of such corporations and businesses would be known. Because all payments from corporations and registered businesses must be remitted to other institutional accounts, the infrastructure would ensure that the income of their shareholders, suppliers, service providers, and employees would be known and attributable to the correct legal entities. Authorities would realise other benefits as well. The distributed ledger maintained by the cryptocurrency node operators would be observable by regulators and other authorities and cross-referenced against any cash flow statements of businesses engaged in cryptocurrency transactions. Private transactions suspected of criminal activity could be verified by investigators with the cooperation of one of the counterparties, even if the investigation might not necessarily reveal identifying details of the other counterparty.

One type of transaction under this system that might be of particular concern to authorities is illustrated by Figure 7, in which an individual with a private cryptocurrency store remits cryptocurrency to another individual with a private cryptocurrency store, not involving a regulated institution. The fact that such transactions could take place without the involvement of institutions means that authorities would be unable to completely enforce restrictions on who is able to transact, in accordance with the FATF recommendations [28]. We could argue that value will find its way to criminal organisations with or without the sanctions advised by FATF [88], or that those willing to break the law have many options to anonymously acquire "legitimate" accounts [89], or that prospective money launderers with sufficient assets will find other ways to transact outside the the system. Whether or not such arguments are sound, cryptocurrencies might become a dominant form of exchanging value precisely because people value privacy, in which case regulators will need to support cryptocurrency transactions simply because those are the transactions that are taking place. After all, people certainly exchanged value before central banks started issuing currency.

Another, equally important, characteristic of this approach is that without institutional mediation at their core, cryptocurrencies are subject to the vicissitudes of mining pools, hackers, and powerful global-scale actors who might compromise or hijack them, as well as speculators and market manipulators who might simply deplete their value. However, an alternative interpretation of that property is that different cryptocurrencies would compete with each other, not only on the basis of market penetration but also on the basis of privacy. It is difficult to imagine a currency in a monopoly position, state-sponsored or otherwise, having this characteristic.

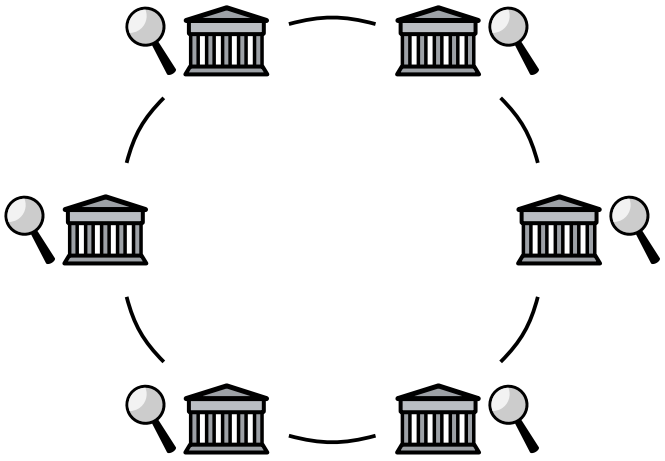

Figure 8: *Schematic Representation of Institutionally Mediated Private Value Exchange: Nodes.* The distributed ledger is operated by a federation of regulated institutions.

3.2 Institutionally Mediated Private Value Exchange

Our second approach starts with the assumption that the "public" cryptocurrencies are not suitable for all kinds of institutional support, perhaps for the reasons cited in Section 3.1. Instead, it proposes to establish a distributed ledger for conducting financial transactions, and that each node of the distributed ledger would be owned and operated by a regulated institution, as shown in Figure 8. This could be achieved with a "permissioned" distributed ledger system such as Hyperledger [90], using an energy-efficient Byzantine fault-tolerant consensus algorithm such as PBFT [91]. Users and governments would benefit from the fact that transacting parties would not need to use cryptocurrency of dubious value but in fact could transact using digital versions of state-issued currency, i.e. *central bank digital currency* (CBDC), which is currently under consideration by central banks around the world and may offer a variety of economic and operational benefits [92].

At this point it might be tempting to suggest that since the entire network consists of regulated or otherwise approved financial institutions, then governments should require the establishment of a "master key" or other exceptional access mechanism, so that they might be able to break the anonymity of users. We argue that this temptation should be resisted. Over the years, policymakers have called for broadly applied exceptional access mechanisms in a variety of contexts, and after considerable debate, such calls have been found to be premature and subsequently withdrawn [93, 94, 95]. Indeed, legislators in the United States [96] and France [97] have gathered opposition to exceptional access mechanisms, citing their intrinsic security weaknesses and potential for abuse.

Indeed, for the approach we present to be a private value exchange, the regulated institutions must *commit to facilitating private transactions.* At one level, the institutions must adopt the specific technologies such as ring signatures, stealth addresses, and confidential transactions used by privacy-enabling cryptocurrencies such as Monero. At another level, the institutions must commit to an ongoing effort to audit, challenge, and improve the technology and operational procedures, because privacy-enhancing technologies require vigilance [79]. It follows that the institutions and the authorities of the jurisdictions in which they operate must commit to ensuring that the technology and operational procedures are effective in safeguarding the privacy of transacting parties against politically, financially, and technologically powerful groups who might have contrary interests.

It is assumed that authorities would take the same measures described in Section 3.1 to ensure that corporations and registered businesses use known, monitorable accounts for all of their transactions. Enforcement of such a policy would be qualitatively easier in this case since the entire network is owned and operated by regulated institutions, and regulators could expect the same benefits associated with

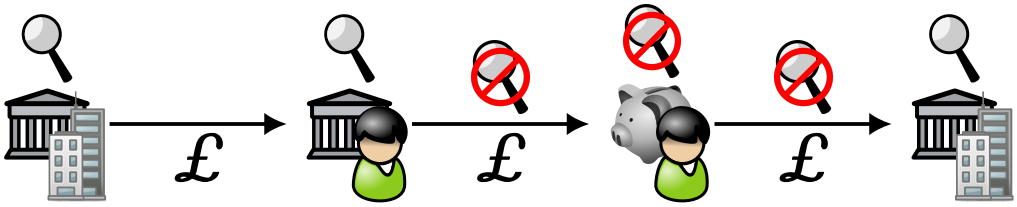

Figure 9: *Schematic Representation of Institutionally Mediated Private Value Exchange: Private Transactions.* As in Figure 5, an individual receives funds into her institutional account (second icon from left) and transfers them to her private store (second icon from right). Unlike in Figure 5, the funds may be state-issued currency, as indicated by the Pound Sterling symbols, rather than cryptocurrency. When she wants to make a payment, she must remit it from her private store to an account held by a regulated institution (rightmost icon).

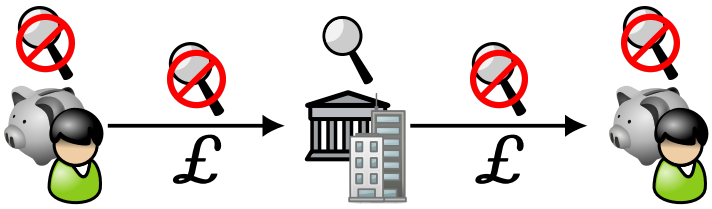

Figure 10: *Schematic Representation of Institutionally Mediated Private Value Exchange: Mediated Transactions Between Consumers.* Individuals (outer icons) wishing to transact with each other via their private stores rather than accounts with regulated institutions must transact via a regulated intermediary (centre icon).

monitoring taxable income and reconciling line items in cash flow statements against actual, auditable transfers on the distributed ledger.

State actors would realise another important benefit from this approach as well. Because all transactions must necessarily involve a regulated institution, transactions of the sort described in Figure 7, in which private actors exchange value directly via their own private stores, would not be possible. Figure 9 illustrates how a user would make payments privately. A user would initially receive funds into her account with a registered institution, which she would in turn remit to her private store. When she wants to make a payment to a merchant or service provider, she can remit the funds to the account that that organisation holds with a registered institution. The privacy features of the distributed ledger, such as ring signatures, stealth addresses, transaction confidentiality, and any other necessary features that may be developed from time to time, would ensure that when the individual makes the payment, she does not reveal either her identity or any information about her prior transactions, including the transactions from which she originally received the funds.

By ensuring that no single enterprise receives too large a share of any individual's transactions in the system, the use of a distributed ledger achieves an essential requirement of the design. Individuals would be expected to use their private stores to transact with many different counterparties, via their own regulated intermediaries, so no single intermediary would have a global, "panopticon-like" view of all of the individual's transactions.

Since individuals cannot transact directly via their private stores, to exchange value they must transact via a regulated intermediary as shown in Figure 10. Individuals conducting transactions might not need to have accounts to exchange value with each other; we surmise that the regulated intermediary would perform the service for a fee. We also suggest that the intermediary would not be required to carry out strong identification of the sort required by the FATF recommendations [28] but might require a less-stringent form of identification, such as an attribute-backed credential indicating that either the

	cash	modern retail banking	"traditional" cryptocurrency (e.g. Bitcoin)	"traditional" stablecoins (e.g. Tether)	privacy-enabling cryptocurrency (e.g. Monero)	inst. supported privacy-enabling cryptocurrency	institutionally mediated private value exchange
Robust to cyberattacks	●	○	○	○	○	○	○
Usable without registration	●	○	●	●	●	●	○
Unlinkable* transactions	◑	○	○	○	●	●	●
Electronic transactions	○	●	●	●	●	●	●
Suitable for taxation	◑	●	○	◑	○	●	●
Can block some illicit uses	○	●	○	○	○	○	●
Can be denominated in units of fiat currency	●	●	○	●	○	○	●

*Potentially

Table 3: *Comparison of various electronic payment methods, including the new proposed methods.*

sender or the receiver are eligible to transact [98]. Regulated intermediaries could also provide token mixing services for groups of individuals who satisfy AML criteria, without explicitly requiring knowledge of their unitary identities.

If successfully operationalised, the approach described in this section would offer governments the same benefits to taxation and auditing as the approach described in Section 3.1, and governments would additionally gain the ability to impose blacklists or economic sanctions on targeted recipients. Individuals would receive the same privacy benefits described in Section 3.1 for transactions involving merchants and service providers, and identification requirements of intermediaries for other transactions could be made parsimonious. However, there are two main drawbacks for individuals seeking privacy, the first being that individuals would need to interact with a registered intermediary before they are able to make or receive payments. The other, more serious concern is the question of the mechanism by which the privacy-enabling properties of the system is assured. Inasmuch as cryptocurrencies represent a check on state power [42], we have reason to believe that the privacy characteristics of cryptocurrencies will continue to improve, despite their demonstrable shortcomings [58, 59].

If the regulated institutions that design, deploy, and maintain the infrastructure for executing transactions are asked to carry the flag for the privacy of their clients, then there could be a misalignment of interests. Clients would need to know the actual privacy limitations of the infrastructure, so adversarial audits would need to be carried out from time to time in the interest of the public. Then, institutions would need incentives and resources to continuously improve the infrastructure and fix any deficiencies on an ongoing basis. A process for admitting new participants would be necessary to ensure that the network remains distributed, and it would need to satisfy an openness criterion to ensure that privacy-threatening procedures do not develop outside the view of the public eye. There would also need to be a diversity of implementations, such that sporadic vulnerabilities do not threaten the privacy of a significant share of the users of the system.

Arguably, such incentives exist among cryptocurrencies, since they must compete for business. It remains to be seen whether effective auditing and competition could assure the privacy-enabling properties of a value exchange operated entirely by institutions.

4 Conclusions

Framing the ongoing conversation about the future of payments as a set of tradeoffs, we introduced two possible candidate architectures for a privacy-enabling electronic value exchange: *institutionally*

supported privacy-enabling cryptocurrency and *institutionally mediated private value exchange*. Both architectures require both the design, implementation, deployment, and maintenance of new technology as well as the development of regulatory policy in which such technology will operate. Table 3 summarises the tradeoffs and contextualises our two prospective approaches. Cash has many desirable properties, such as universality (i.e., its use does not require a relationship with a registered institution) and privacy in practice (serial numbers on banknotes can be traced but generally are not). However, it cannot be sent across computer networks and is sometimes used for illicit transactions, including tax evasion. In contrast, modern retail banking requires accounts and facilitates large-scale surveillance. The most popular cryptocurrencies such as Bitcoin do not actually avoid surveillance and are in some ways potentially easier to trace than ordinary retail transactions. Privacy-enabling cryptocurrencies promise to address both deficiencies, although research has shown that the goals motivating their development have not yet been fully achieved.

The various approaches to electronic payments each have their own advantages and limitations, and by elaborating the tradeoffs, we hope to facilitate a more fulsome conversation among the stakeholders and offer a useful framework for discussing future solutions. We believe that both approaches have their place and prospective adherents, and the adoption of one would not exclude the adoption of the other. Businesses that offer services to cryptocurrency users and traders would find value in the first approach, and businesses seeking to facilitate private, cash-like electronic transactions within a regulated system would find value in the second approach. Correspondingly, some regulators might be troubled by supporting trade in assets whose value and uses are beyond their reach, as would be the case in the first approach, and some privacy-minded individuals might be troubled by the possibility that the regulated financial institutions that operate the system described in the second approach might secretly collude to compromise the anonymity of their clients.

We suggest that institutionally supported privacy-enabling cryptocurrency would be strictly better than privacy-enabling cryptocurrency without institutional support, mainly because regulators would benefit from the ability to monitor corporations and registered businesses that use cryptocurrencies. We also suggest that institutionally mediated private value exchange would be strictly better than modern retail banking as currently practiced, mainly because users would avoid payment networks and enjoy an improved expectation of privacy in their ordinary activities. However, neither approach achieves all of the objectives of both parties. For example, the ability to transact without interacting with a regulated institution may be incompatible with the ability for a government to block illicit use. Similarly, monetary policy might not be possible if cryptocurrency governance were exogenous to the state, although the possibility of this happening at scale seems remote. As the hard choices for the future of payments come to light, we believe that acknowledgment and discussion of these tradeoffs, as well as a commitment to both serious privacy and serious regulation, are prerequisites for advancing the interests of all stakeholders.

Acknowledgements

The authors would like to thank Edgar Whitley and David Pym for their insightful contributions. Geoff Goodell is also an associate of the Centre for Technology and Global Affairs of the University of Oxford. We acknowledge the Engineering and Physical Sciences Research Council (EPSRC) for the BARAC project (EP/P031730/1) and the European Commission for the FinTech project (H2020-ICT-2018-2 825215). Tomaso Aste acknowledges the Economic and Social Research Council (ESRC) for funding the Systemic Risk Centre (ES/K0 02309/1).

References

[1] S. Zuboff. "Big Other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* **30**, 2015. pp. 75–89. [online] `http://www.palgrave-journals.com/jit/journal/v30/n1/pdf/jit20155a.pdf` [retrieved 2018-09-17]

[2] A. Rieke et al. "Data Brokers in an Open Society: An Upturn Report." Prepared for the Open Society Foundations, November 2016. [online] `https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf` [retrieved 2017-06-21]

[3] L. Beckett. "Everything We Know About What Data Brokers Know About You." ProPublica, 2014-06-13. [online] https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you [Retrieved 2017-03-28.]

[4] T. Schep. "Social Cooling." [online] http://www.pineapplejazz.com/socialcooling/ [retrieved 2017-06-21]

[5] P. Waldman, L. Chapman, and J. Robertson. "Palantir Knows Everything About You." Bloomberg, 2018-04-19. [online] https://www.bloomberg.com/features/2018-palantir-peter-thiel/ [Retrieved 2018-04-19]

[6] Pitney Bowes. "Entity resolution solutions help combat AML and other financial crimes." [online] https://www.pitneybowes.com/hk/customer-information-management/case-studies/entity-resolution-aml.html [Retrieved 2018-11-14]

[7] S. Warren and L. Brandeis. "The Right to Privacy." *Harvard Law Review* **4**(5), 1890-12-15. [online] https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [retrieved 2018-10-11]

[8] Australian Law Reform Commission. *Serious Invasions of Privacy in the Digital Era (DP 80)*, 2014-03-31. [online] https://www.alrc.gov.au/publications/serious-invasions-privacy-dp-80 [retrieved 2018-10-11]

[9] J. Fairfield and C. Engel. "Privacy as a Public Good." *Duke Law Journal*, **65**(3), 2015, pp. 385–457. [online] https://scholarship.law.duke.edu/dlj/vol65/iss3/1/ [retrieved 2018-10-11]

[10] A. Gaur and N. Mukherjee. "Saving privacy for public good." *The Times of India*, 2017-09-14. [online] https://blogs.economictimes.indiatimes.com/et-commentary/saving-privacy-for-public-good/ [retrieved 2018-10-11]

[11] D. Cole. "Can Privacy Be Saved?" *The New York Review of Books*, 2014-03-06. [online] https://www.nybooks.com/articles/2014/03/06/can-privacy-be-saved/?insrc=toc [retrieved 2018-10-11]

[12] A. Hess. "How Privacy Became a Commodity for the Rich and Powerful." *The New York Times Magazine*, 2017-05-09. [online] https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html [retrieved 2018-10-11]

[13] T. Chen and Y. Zhao. "China's Capital Controls Keep a Bad Year From Getting Worse." Bloomberg, 2018-11-21. [online] https://www.bloomberg.com/news/articles/2018-11-21/china-s-capital-controls-keep-a-very-bad-year-from-getting-worse [retrieved 2018-03-11]

[14] J. Adelstein. "Japan's Financial Regulator Is Pushing Crypto Exchanges To Drop 'Altcoins' Favored By Criminals." *Forbes*, 2018-04-30. [online] https://www.forbes.com/sites/adelsteinjake/2018/04/30/japans-financial-regulator-is-pushing-crypto-exchanges-to-drop-altcoins-favored-by-criminals/#72ae85861b8a [retrieved 2019-03-11]

[15] K. Dixit. "Korbit says goodbye to DASH, Monero [XMR], Zcash [ZEC], REP, STEEM – Will they come back?" AMB Crypto, 2018-05-22. [online] https://ambcrypto.com/korbit-dash-monero-xmr-zcash-ec-rep-steem/ [retrieved 2019-03-11]

[16] United States Department of Homeland Security. DHS-FY19-SBIR-PreSolicitation. [online] https://www.fbo.gov/utils/view?id=f0e31ab37561cac3cc4a4ab88d9059b0 [retrieved 2019-03-11]

[17] HM Treasury. "Cryptoassets Taskforce: final report." 2018-10-29. [online] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf [retrieved 2019-03-11]

[18] G20 Summit (Argentina, 2018). "G20 Leaders' Declaration: Building consensus for fair and sustainable development." 2018-12-01. [online] https://www.consilium.europa.eu/media/37247/buenos_aires_leaders_declaration.pdf [retrieved 2019-03-11]

[19] House of Commons Treasury Committee. "Crypto-assets." *Twenty-Second Report of Session 2017-19.* 2018-09-12. https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf [retrieved 2018-09-26]

[20] British Royal Mint. "Legal Tender Guidelines." [online] https://web.archive.org/web/20081217182521/http://www.royalmint.com/corporate/policies/legal_tender_guidelines.aspx [retrieved 2019-03-11]

[21] M. Forstater. "Tax Driven Money: Additional Evidence from the History of Thought, Economic History, and Economic Policy." Working Paper No. 35, University of Missouri – Kansas City, August 2004. [online] http://www.cfeps.org/pubs/wp-pdf/WP35-Forstater.pdf [retrieved 2019-03-11]

[22] S. Hughes and S. Middlebrook. "Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries." *Yale Journal on Regulation* **32**, 2015. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1417&context=yjreg [retrieved 2018-11-22]

[23] P. Tasca and T. Aste. "Crypto assets and the regulator's role: Ignore, regulate or kill?" Open Access Government, 2018-07-18. https://www.openaccessgovernment.org/crypto-assets-and-the-regulators-role-ignore-regulate-or-kill/47858/ [retrieved 2018-11-22]

[24] G. Goodell and T. Aste. "Blockchain technology for the public good: Design constraints in a human rights context." Open Access Government, 2018-04-17. https://www.openaccessgovernment.org/blockchain-technology-for-the-public-good-design-constraints-in-a-human-rights-context/44595/ [retrieved 2018-11-22]

[25] GOV.UK "Money Laundering Regulations: who needs to register." 2014-10-23. [online] https://www.gov.uk/guidance/money-laundering-regulations-who-needs-to-register [retrieved 2017-05-28]

[26] Better Business Finance. "What are the AML and KYC obligations of a Bank in the UK?" [online] https://www.betterbusinessfinance.co.uk/aml-and-kyc/what-are-the-aml-and-kyc-obligations-of-a-bank-in-the-uk [retrieved 2017-05-28]

[27] S. Breslow, M. Hagstroem, D. Mikkelsen, and K. Robu. "The new frontier in anti–money laundering." McKinsey & Company, November 2017. [online] https://www.mckinsey.com/business-functions/risk/our-insights/the-new-frontier-in-anti-money-laundering [retrieved 2019-03-11]

[28] Financial Action Task Force (FATF). *The FATF Recommendations.* Updated February 2018. [online] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf [retrieved 2018-09-16]

[29] Financial Action Task Force (FATF). "Public Statement 22 February 2013." [online] http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatfpublicstatement22february2013.html [retrieved 2017-05-28]

[30] United States Securities and Exchange Commission. "Anti-Money Laundering (AML) Source Tool for Broker-Dealers." 2017-01-11. [online] https://www.sec.gov/about/offices/ocie/amlsourcetool.htm#10 [retrieved 2017-05-28]

[31] European Parliament. "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018." 2018-05-30. [online] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018L0843 [retrieved 2018-09-26]

[32] Armer, P. "Privacy Aspects of the Cashless and Checkless Society." Testimony before the Senate Subcommittee on Administrative Practice and Procedure. 1968-02-06, as published by the RAND Corporation, April 1968. [online] https://www.rand.org/content/dam/rand/pubs/papers/2013/P3822.pdf [retrieved 2017-05-28]

[33] P. Armer. "Computer Technology and Surveillance." *Computers and People* 24(9), pp. 8–11, September 1975. [online] https://archive.org/stream/bitsavers_computersA_3986915/197509#page/n7/mode/2up [retrieved 2017-05-28]

[34] J. Steele. "Everything You Need to Know About Credit Card Issuers." Experian, 2018-03-27. [blog] https://www.experian.com/blogs/ask-experian/everything-you-need-to-know-about-credit-card-issuers/&udata=247da8adbe7dc7f7a37817eafd060745 [retrieved 2017-09-27]

[35] W. Christl. *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions.* Cracked Labs, Vienna, June 2017. [online] http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf [retrived 2018-09-30]

[36] Der Spiegel. "NSA Spies on International Payments." 2013-09-15. [online] http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html [retrieved 2018-10-05]

[37] D. Chaum. "Blind Signatures for Untraceable Payments." *Advances in Cryptology: Proceedings of Crypto* **82**(3), pp. 199–203, 1983. [online] http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF [retrieved 2018-09-28]

[38] J. Pitta. "Requiem for a Bright Idea." *Forbes.* 1999-11-01. [online] https://www.forbes.com/forbes/1999/1101/6411390a.html

[39] J. Meek. "Feds out to bust up 24-karat Web worry." *New York Daily News*, 2007-06-03. [online] http://www.nydailynews.com/news/crime/feds-bust-24-karat-web-worry-article-1.219589 [retrieved 2018-10-05]

[40] BBC. "Liberty Reserve digital money service forced offline." 2013-05-27. [online] https://www.bbc.co.uk/news/technology-22680297 [retrieved 2018-10-05]

[41] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2009-01-03. [online] https://bitcoin.org/bitcoin.pdf [retrieved 2018-10-04]

[42] N. Sotirakopoulos. "Cryptomarkets as a libertarian counter-conduct of resistance." *European Journal of Social Theory.* **21**(4), July 2017.

[43] V. Buterin. "The Search for a Stable Cryptocurrency." Ethereum Blog, 2014-11-11. [online] https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/ [retrieved 2018-10-05]

[44] N. Popper. "Warning Signs About Another Giant Bitcoin Exchange." The New York Times, 2017-11-21. [online] https://www.nytimes.com/2017/11/21/technology/bitcoin-bitfinex-tether.html [retrieved 2018-10-05]

[45] O. Williams-Grut. "Everything you need to know about Tether, the cryptocurrency academics claim was used to manipulate bitcoin." Business Insider, 2018-06-13. [online] http://uk.businessinsider.com/tether-explained-bitcoin-cryptocurrency-why-people-worried-2018-1 [retrieved 2018-10-05]

[46] K. Rogoff and A. Meltzer. "The Risks of Unilateral Exchange Rate Pegs." *The Implications of Globalization of World Financial Markets.* Seoul: Bank of Korea, pp. 153–170, 1998. [online] http://scholar.harvard.edu/files/rogoff/files/bokpaper.pdf [retrieved 2019-05-02]

[47] Society for Worldwide Interbank Financial Telecommunication. "Introduction to SWIFT." [online] https://www.swift.com/about-us/discover-swift [retrieved 2018-10-05]

[48] K. Durr and A. Kinnane. *431 Days: Joseph P. Kennedy and the Creation of the SEC (1934-35).* Securities and Exchange Commission Historical Society. [online] http://www.sechistorical.org/museum/galleries/kennedy/index.php [retrieved 2018-10-08]

[49] T. Tam. "How bots are manipulating cryptocurrency prices." Venture Beat, 2017-12-14. [online] https://venturebeat.com/2017/12/14/how-bots-are-manipulating-cryptocurrency-prices/ [retrieved 2018-10-08]

[50] O. Williams-Grut. "Walkthrough: How traders 'pump and dump' cryptocurrencies." Business Insider, 2017-11-14. [online] https://www.businessinsider.com/how-traders-pump-and-dump-cryptocurrencies-2017-11?r=UK&IR=T [retrieved 2018-10-08]

[51] S. Falkon. "The Story of the DAO – Its History and Consequences." Medium, 2017-12-24. [online] https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee [retrieved 2018-10-08]

[52] International Swaps and Derivatives Association, Inc (ISDA) and Linklaters. "Smart Contracts and Distributed Ledger – A Legal Perspective." August 2017. [online] https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf [retrieved 2018-10-08]

[53] S. Meiklejohn et al. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names." *USENIX*, December 2013. [online] https://smeiklej.com/files/login13.pdf [retrieved 2018-11-14]

[54] P. Tasca, S. Liu, and A. Hayes. "The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships." SSRN 2808762, 2016-07-01. http://dx.doi.org/10.2139/ssrn.2808762

[55] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan. "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies." arXiv:1708.04748 [cs.CR], 2017-08-16. [online] https://arxiv.org/pdf/1708.04748 [retrieved 2018-10-09]

[56] H. Al Jawaheri, Y. Boshmaf, M. Al Sabah, and A. Erbad. "When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis." arXiv:1801.07501v2 [cs.CR], 2018-04-11. [online] https://arxiv.org/pdf/1801.07501.pdf [retrieved 2018-10-09]

[57] R. Anderson, I. Shumailov, and M. Ahmed. "Making Bitcoin Legal." April 2018. [online] http://www.cl.cam.ac.uk/~rja14/Papers/making-bitcoin-legal.pdf [retrieved 2018-10-09]

[58] M. Möser et al. "An Empirical Analysis of Traceability in the Monero Blockchain." *Proceedings on Privacy Enhancing Technologies* **2018**(3), pp. 143–163.

[59] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn. "An Empirical Analysis of Anonymity in Zcash." *Proceedings of the 27th USENIX Security Symposium (USENIX Security '18).* [online] https://smeiklej.com/files/usenix18.pdf [retrieved 2018-10-13]

[60] V. Buterin. "The Meaning of Decentralization." Medium, 2017-02-06. [online] https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274#.x5k6j4cxg [retrieved 2018-10-09]

[61] A. Chepurnoy. "Centralized cryptocurrencies." IOHK SCOREX Blog, 2017-03-05. [online] https://iohk.io/blog/scorex/centralized-cryptocurrencies/ [retrieved 2018-10-09]

[62] W. Matheny, S. O'Brien, and C. Wang. "The State of Cash: Preliminary Findings from the 2015 Diary of Consumer Payment Choice." Federal Reserve Bank of San Francisco, 2016-11-03. [online] https://www.frbsf.org/cash/publications/fed-notes/2016/november/state-of-cash-2015-diary-consumer-payment-choice/ [retrieved 2018-10-09]

[63] K. Rogoff. "Should We Move to a Mostly Cashless Society? Yes: It Would Mean Less Crime and Greater Fed Flexibility." *The Wall Street Journal*, 2017-09-25. [online] https://www.wsj.com/articles/should-we-move-to-a-mostly-cashless-society-1506305220 [retrieved 2018-10-09]

[64] Knowledge@Wharton. "Going Cashless: What Can We Learn from Sweden's Experience?" Interview with Jonas Hedman, University of Pennsylvania. 2018-08-31. [online] http://knowledge.wharton.upenn.edu/article/going-cashless-can-learn-swedens-experience/ [retrieved 2018-10-09]

[65] United States Securities and Exchange Commission. "Statement on Potentially Unlawful Online Platforms for Trading Digital Assets." Public Statement, 2018-03-07. [online] https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading [retrieved 2018-10-10]

[66] S. Higgins. "UK Treasury Won't Seek AML Rules for Bitcoin Wallet Providers." Coindesk, 2016-04-25. [online] https://www.coindesk.com/uk-treasury-we-wont-regulate-bitcoin-wallet-providers/ [retrieved 2018-10-10]

[67] C. Russo. "Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now." Bloomberg, 2018-08-07. [online] https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now [retrieved 2018-10-10]

[68] R. Dingledine, N. Mathewson, and P. Syverson. "Tor: The Second-Generation Onion Router." Proceedings of the 13th USENIX Security Symposium, 2004. [online] https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/Dingledine%20etal2004.pdf [retrieved 2018-10-10]

[69] Cambridge English Dictionary. *'fungible,'* meaning. [online] https://dictionary.cambridge.org/dictionary/english/fungible [retrieved 2019-05-02]

[70] C. Osborne, "Arrests made over Bitcoin laundering scheme, Dark Web drug deals." ZDNet, 2016-01-20. [online] https://www.zdnet.com/article/arrests-made-over-bitcoin-laundering-scheme-dark-web-drug-deals/ [retrieved 2018-10-10]

[71] A. Hinkes and J. Ciccolo. "OFAC's Bitcoin Blacklist Could Change Crypto." Coindesk, 2018-03-24. [online] https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto/ [retrieved 2018-10-10]

[72] W. Maxwell and J. Salmon. "A guide to blockchain and data protection." Hogan Lovells, September 2017. [online] https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf [retrieved 2018-10-10]

[73] K. Sedgwick. "Most Privacy Coins Aren't That Private." Bitcoin News, 2018-05-29. [online] https://news.bitcoin.com/most-privacy-coins-arent-that-private/ [retrieved 2018-10-10]

[74] R. Rivest, A. Shamir, and Y. Tauman. "How to Leak a Secret." *Lecture Notes in Computer Science* 2248, pp. 552—565, 2001-11-20. [online] https://link.springer.com/content/pdf/10.1007%2F3-540-45682-1_32.pdf [retrieved 2018-10-10]

[75] N. Courtois and R. Mercer. "Stealth Address and Key Management Techniques in Blockchain Systems." *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pp. 559–566. [online] http://www.scitepress.org/Papers/2017/62700/62700.pdf [retrieved 2018-10-10]

[76] T. Pedersen. "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing." Advances in Cryptology (CRYPTO '91), 1991, pp. 129–140. [online] https://link.springer.com/content/pdf/10.1007%2F3-540-46766-1_9.pdf [retrieved 2018-10-10]

[77] A. van Wirdum. "Confidential Transactions: How Hiding Transaction Amounts Increases Bitcoin Privacy." Bitcoin Magazine, 2016-06-02. [online] https://bitcoinmagazine.com/articles/confidential-transactions-how-hiding-transaction-amounts-increases-bitcoin-privacy- 1464892525/ [retrieved 2018-10-10]

[78] A. Greenberg. "The Dark Web's Favorite Currency is Less Untraceable Than It Seems." *Wired*, 2018-03-27. [online] https://www.wired.com/story/monero-privacy/amp [retrieved 2018-10-10]

[79] P. Zimmermann. "Why I Wrote PGP." *PGP User's Guide*, 1991. [online] https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html [retrieved 2018-10-11]

[80] J. Wilmoth. "Japan Wants Cryptocurrency Exchanges to De-List Anonymous Altcoins: Report." CCN, 2018-04-30. [online] https://www.ccn.com/japan-is-pressuring-cryptocurrency-exchanges-to-de-list-anonymous-altcoins-report/ [retrieved 2018-10-11]

[81] R. Viglione. "Japan's Ban Is a Wake-Up Call to Defend Privacy Coins." Coindesk, 2018-05-29. [online] https://www.coindesk.com/japan-wake-call-get-ready-defend-privacy-coins/ [retrieved 2018-10-11]

[82] R. Novy. Prepared Testimony Before the United States House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, 2018-06-20. [online] https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-rnovy-20180620.pdf [retrieved 2018-10-11]

[83] T. Jedusor. "Mimblewimble." 2016-07-19. [online] https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt [retrieved 2018-10-10]

[84] Bank of England. Financial Policy Committee statement from its meeting – 12 March 2018, 2018-03-16. [online] https://www.bankofengland.co.uk/statement/fpc/2018/financial-policy-committee-statement-march-2018 [retrieved 2018-10-12]

[85] J. Verhage, S. Morris, and S. Basak. "Barclays Is Sounding Out Clients About Trading Crypto." Bloomberg, 2018-04-16. [online] https://www.bloomberg.com/news/articles/2018-04-16/barclays-is-said-to-be-sounding-out-clients-about-trading-crypto [retrieved 2018-10-12]

[86] A. Hankin. "Goldman Sachs to launch cryptocurrency trading desk." Financial News, 2018-05-03. [online] https://www.fnlondon.com/articles/goldman-sachs-to-launch-cryptocurrency-trading-desk-20180503?mod=article_inline [retrieved 2018-10-12]

[87] P. Peterson. "Anatomy of A Zcash Transaction." Zcash Company Blog, 2016-11-23. [online] https://z.cash/blog/anatomy-of-zcash/ [retrieved 2018-10-12]

[88] Competitive Enterprise Institute. *The Future of Financial Privacy,* ISBN 1-889865-03-6, October 2000. [online] https://cei.org/studies-books/future-financial-privacy [retrieved 2018-10-12]

[89] A. Hern. "Stolen credit card details available for £1 each online." *The Guardian*, 2015-10-30. [online] https://www.theguardian.com/technology/2015/oct/30/stolen-credit-card-details-available-1-pound-each-online [retrieved 2018-10-12]

[90] Hyperledger. [online] https://www.hyperledger.org/ [retrieved 2018-10-12]

[91] M. Castro and B. Liskov. "Practical Byzantine Fault Tolerance." *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, USA, February 1999. [online] http://pmg.csail.mit.edu/papers/osdi99.pdf [retrieved 2018-10-12]

[92] Bank for International Settlements. "Central bank digital currencies." Markets Committee, Committee on Payments and Market Infrastructures, March 2018. [online] https://www.bis.org/cpmi/publ/d174.pdf [retrieved 2018-10-12]

[93] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, and B. Schneier. "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption." doi:10.7916/D8GM8F2W, 1997-05-27. [online] https://academiccommons.columbia.edu/doi/10.7916/D8R2176H/download [retrieved 2019-03-11]

[94] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. Neumann, R. Rivest, J. Schiller, B. Schneier, M. Specter, and D. Weitzner. "Keys under doormats: mandating insecurity by requiring government access to all data and communications." *Journal of Cybersecurity* **1**(1), pp. 69–79, doi:10.1093/cybsec/tyv009, 2015-11-17. [online] https://academiccommons.columbia.edu/doi/10.7916/D82N5D59/download

[95] J. Benaloh. "What if Responsible Encryption Back-Doors Were Possible?" Lawfare Blog, 2018-11-29. [online] https://www.lawfareblog.com/what-if-responsible-encryption-back-doors-were-possible [retrieved 2018-12-11]

[96] 115th Congress of the United States. H.R. 5823, "Secure Data Act of 2018.", introduced by Representative Zoe Lofgren [D-CA-19], 2018-05-15. [online] https://www.congress.gov/bill/115th-congress/house-bill/5823 [retrieved 2019-03-11]

[97] I. Thomson. "French say 'Non, merci' to encryption backdoors." The Register, 2016-01-15. [online] https://www.theregister.co.uk/2016/01/15/france_backdoor_law/ [retrieved 2019-03-11]

[98] J. Camenisch, M. Dubovitskaya, A. Lehmann, G. Neven, C. Paquin, and F.-S. Preiss. "Concepts and Languages for Privacy-Preserving Attribute-Based Authentication." *IFIP Advances in Information and Communication Technology* **396**, 2013, pp. 34-52. [online] https://link.springer.com/content/pdf/10.1007%2F978-3-642-37282-7_4.pdf [retrieved 2018-10-04]

Diagram Clip Art Image Credits: publicdomainvectors.org, bitcoin.org, twitter.com