In Pich C & Newman BI (eds.) *Political Branding: More Than Parties, Leaders and Policies*. London: Routledge: https://www.routledge.com/Political-Branding-More-Than-Parties-Leaders-and-Policies/Pich-Newman/p/book/9780367492274

Why Cryptocurrencies want Privacy: A Review of Political Motivations and Branding Expressed in 'Privacy Coin' Whitepapers

ABSTRACT

New currencies designed for user anonymity and privacy – widely referred to as 'privacy coins' - have forced governments to listen and legislate, but the political motivations of these currencies are not well understood. Following the growing interest of political brands in different contexts, we provide the first systematic review of political motivations expressed in cryptocurrency whitepapers whose explicit goal is 'privacy'. Many privacy coins deliberately position themselves as alternative political brands. Although cryptocurrencies are often closely associated with political philosophies that aim to diminish or subvert the power of governments and banks, advocates of privacy occupy much broader ideological ground. We present thematic trends within the privacy coin literature and identify epistemic and ethical tensions present within the communities of people calling for the adoption of entirely private currencies.

KEYWORDS *Cryptocurrency, Bitcoin, Blockchain, Privacy, Political brands, Money*

WORKERS OF THE WORLD, UNITE! YOU HAVE NOTHING TO LOSE BUT YOUR BLOCKCHAINS!

Cryptocurrencies have their political roots in anarchist, hacker, hippy, and cypherpunk cultures (Maurer, Nelms and Swartz, 2013). Many designers, activists, and advocates of cryptocurrency want to dismantle the nation state and its associated corporations (Karlstrøm, 2014). Subversion of government and the removal of commercial influence over money is a widespread theme in cryptocurrency canonical literature (e.g. Nakamoto, 2008), but this trope is no longer universal. Indeed, increasingly, those cryptocurrencies that succeed in creating value for their users are often explicitly branded and positioned to aid hegemonic political interests.

Recent work on political branding highlights the diverse nature of political brands (Smith and French, 2009) and draws attention to the need to understand political branding in different contexts (Needham and Smith, 2015). This paper contributes to the understanding of political branding by uncovering different types of motivation underpinning privacy coins. We show how notions of politics emerge in cryptocurrencies which are explicitly positioned as political brands.

Through the notion of *privacy as politics*, we submit that cryptocurrencies, though often branded and positioned as apolitical or anti-political (Herian, 2018), are always a form of 'alternative' political movement. The desire to be a-political represents a political position itself (Kostakis and Giotitsas, 2014) and it is important to understand the political underpinnings behind the blockchain technology as it is driving social change (Filippi and Loveluck, 2016). The identification of political dimensions and ideologies in cryptocurrency challenges the idea that digital currency is removed from the influence of politicians (Dierksmeier and Seele 2016) and unveils a new context to research political branding. This is important because political ideology drives consumer decisions (Crockett and Pendarvis, 2017) and in the context of cryptocurrency those decisions are likely to be significantly different if digital currencies are associated with particular political ideologies.

In the following sections of this paper, we briefly review extant literature around 1) cryptocurrency and the recent emergence of ‘privacy coins’; 2) The relation of privacy to politics, including nuanced definitions of anonymity and privacy; and 3) the integration of cryptocurrencies, privacy and alternative political brands that will inform the subsequent discussion. Afterwards, we outline the methods used to generate a corpus of whitepapers and conduct a systematic review. In following section, we present an exposition of the findings and discussion. Focus is directed toward emergent themes within the literature and ethical and epistemic conflicts present in the positioning of privacy cryptocurrencies. In the final section, we conclude the paper and put forward an agenda for future research to help broaden the academic study of privacy coins and their social impact.

CRYPTOCURRENCIES AND THE POST-BITCOIN EMERGENCE OF ‘PRIVACY COINS’

In the wake of the 2008 financial crash a pseudonymous author named Satoshi Nakamoto outlined a vision for an alternative monetary future using Bitcoin and the blockchain protocol (Nakamoto 2008). Nakamoto drew attention to the failings of modern banking institutions and sought to challenge their dominance by enabling decentralized peer-to-peer transactions. People, Nakamoto argued, should be free and able to control their personal wealth anonymously without relying on a centralized 3rd party (Dodd, 2017).

Anonymity is a central issue for many Bitcoin users. No fixed identity is explicitly linked to a Bitcoin wallet address and ‘privacy’ is a key concern in Nakamoto’s initial Bitcoin whitepaper (Nakamoto, 2008). However, the idea that underpins Bitcoin (a public distributed ledger) raises some tricky challenges for maintaining user privacy. While it is easy to protect the identity of the owner of a Bitcoin wallet, it is harder to protect users from inferred conclusions about their identity that can be reached by analyzing wallet transfers. If Account A sends a specific amount at a specific time to Account B it is sometimes possible to triangulate and determine the offline identities of the people associated with the transaction. Indeed, in reviewing the privacy of Bitcoin, Nakamoto noted that:

‘The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions [in the Bitcoin protocol] publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the ‘tape’, is made public, but without telling who the parties were. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.’ (Nakamoto, 2008, 6)

Various authors have shown that blockchain analysis can reveal connections between users and their transactions, and that further data can be inferred because of these connections which might jeopardize privacy (Ober, Katzensbeisser and Hamacher 2013, Reid and Harrigan 2013, Ron and Shamir 2013). Cookies have been shown to jeopardize the privacy of cryptocurrency payments (Goldfeder et al. 2018) and similarly IP addresses have been associated with Bitcoin account use, which can provide a basis for identity inference (Bohannon 2016). Despite the clear value Nakamoto placed on 'privacy' the metadata that Bitcoin usage generates makes it a less than optimal solution for maintaining true privacy of users. Consequently, a wide variety of cryptocurrency designers and advocates have criticized the architecture of Bitcoin and proposed alternative overlays to the existing design or entirely new solutions (Meiklejohn and Orlandi 2015). These alternative cryptocurrencies typically try to hide or obfuscate user metadata and are thus widely referred to as 'privacy coins' (Nakamoto 2008).

Privacy coins vary in technological sophistication, but they have gained widespread notoriety from their increasing use in nefarious transactions, particularly on the so-called 'Dark-web' (Recorded Future 2018). Reports illustrate that privacy coins are being used by rogue states (Hurlburt 2017), drug dealers (Van Hout and Bingham 2013), illicit traders; and that they help hide sexual exploitation (Zulkarnine et al. 2016), terrorism, weapons trafficking (Weimann 2016), and money laundering (Dostov and Shust 2014). These activities have caught the eye of governments around the world. But governments are not simply interested in illicit behavior, some have legislated against, and even banned cryptocurrencies because absolute privacy of transactions threaten the possibility of audited ownership and taxation (Dierksmeier and Seele 2016). 'Know your customer' regulations, which associate passport details with exchange users, are now widely adopted worldwide to surveil fiat-crypto conversions and provide the possibility of audit trails (Berentsen and Schar 2018).

Despite the negative press cryptocurrencies receive they also present an opportunity to positively transform the economic lives of people. Whether in banking the unbanked billions of people around the world (Larios-Hernández 2017), eliminating the fees imposed on remittances sent by the poorest workers in the world to their families (Scott 2016), or providing novel means for people to share, donate, or tip, many new cryptocurrencies have an obviously prosocial aim (Pittman 2016). Indeed, many crypto initiatives clearly fall within the category of *prosocial interaction design* (Harvey *et al*., 2014), echoing the old Marxist adage that good philosophy aims not merely to describe or interpret the world, instead the point is to change it. The imagination, development, and adoption of a new currency is always a potentially transformative political act.

Cryptocurrencies have been championed by advocates of a range of political philosophies. Nakamoto originally argued that Bitcoin was 'very attractive to the libertarian viewpoint if we can explain it properly,' but also added 'I'm better with code than with words though'. But as Maurer, Nelms and Swartz (2013, 262) note 'in the world of Bitcoin, there are goldbugs, hippies, anarchists, cyberpunks, cryptographers, payment systems experts, currency activists, commodity traders, and the curious' Although arguments made in favor of cryptocurrency are justifications for shrinking or eradicating the influence of government or banks over money, there are nonetheless at the time of writing numerous movements by national governments towards adopting cryptocurrency in place of or alongside fiat currency. For example, the Marshall Islands have been heavily criticized by the International Monetary Fund over their plans to introduce a digital currency in 2019, and Venezuela have reportedly raised over 5 billion USD in an initial coin offering in early 2018 (Petro 2018). This tension illustrates that cryptocurrency is no longer the preserve of those seeking to subvert the dominant monetary systems, it is also being co-opted by those national banks and governments it was created to counteract. We might ask the question then, what political purpose do privacy coins serve, and for whom?

PRIVACY AS POLITICS

Every society ‘sets a distinctive balance between the private sphere and public order based on the society’s political philosophy’ around two alternative societal models, namely Authoritarian (i.e. rejecting legally or socially protected privacy) and Democratic societies (i.e. having a strong commitment to individualism and freedom) (Westin 2003, 3). A long history of privacy research exists within the computing and politics academic literatures, respectively. Recent research draws attention to how metadata associated with ubiquitous forms of computing can inadvertently reveal identity or behavior of people without them giving informed consent (Luger and Rodden 2013). Although no single definition of privacy is accepted, the concept is obviously nuanced and has a meaning which cannot be universally understood outside of the particular contexts in which it is a concern (Smith, Dinev and Xu 2011). Privacy becomes a more ambiguous concept when human-computer interaction is enabled by data managed or processed centrally by commercial or governmental third parties. Privacy online is treated variously as either an inalienable right to which individuals and groups are entitled, or as a commodity best thought of as something which has an economic value that can be evaluated and traded as part of a cost-benefit analysis (Walsh, Parisi and Passerini 2017).

In this paper we subscribe to Westin’s (1967, 7) classic definition of privacy as ‘the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’. Westin’s (1967) account introduces subtlety into the understanding of privacy, by making a distinction between privacy ‘states’ and privacy ‘functions’. Four privacy states that individuals are said to experience can be paraphrased as: (1) Solitude: the most complete state of privacy, here the individual is separated from the group and the observations of other people; (2) Intimacy: here the individual is acting as part of a small group that can exercise corporate seclusion to achieve a close, relaxed or frank relationship between individuals; (3) Anonymity: here privacy relates to the individual that when in public spaces is able to find freedom from surveillance and identification; and (4) Reserve: this occurs when an individual’s need to limit communication about their self is protected by the willing discretion of those surrounding them.

Westin contrasted states of privacy with functions, suggesting that in democratic societies privacy can ‘perform’ different instrumental roles for individuals according to their own personal lives. Functions are said to include: (1) Personal autonomy: the need to maintain social processes that safeguard a person’s sense of individuality and avoid being manipulated or dominated wholly by others; (2) Emotional release: the recognition that people ‘perform’ many different roles in their lives e.g. father, son, husband, friend, lover, colleague, boss, student, teacher, and that privacy affords at least temporary respite from these roles to relax from the pressure of playing social roles; (3) Self-Evaluation: privacy serves not only a processing but a planning need by providing time to anticipate, to recast, and to originate. Every individual integrates their experiences into a meaningful pattern through self-evaluation and this activity requires privacy; and (4) Limited and Protected Communication: among mature adults all communication is partial and limited, based on the complementary relation between reserve and discretion.

We also note that where money and surveillance technology are concerned what is private today may not be private tomorrow. Consequently, privacy can be conceptualized either as a static, unchanging and universal value maintained by social rules or more pragmatically as something dynamic, which requires constant vigilance to revise and update protective measures according to changing socio-cultural and technological contexts. The relation between digital money and privacy has been an ongoing source of concern for computing academics for over three decades. In 1985, Chaum argued that new forms of transaction systems would work to ensure user privacy and make ‘Big Brother obsolete’. Okamoto and Ohta (1991) similarly suggested that any future Universal Electronic Cash would ideally ensure that ‘the privacy of the user should be protected. That is, the relationship between the user and his purchases must be untraceable by anyone’. But in practice this is has proven a difficult challenge to implement. It requires a system that can guarantee the untraceability of money and the unlinkability of people to said money, but it also requires a system which can publicly record transactions to ensure decentralized trust, while also preventing the ‘double spend’ problem i.e. the risk of fraud through a currency being spent twice.

The possibility of trust within Bitcoin and most other cryptocurrencies comes from a massively-distributed ledger that serves as an immutable historical record of transactions. Money, as Hart (2000) argues, always serves as a form of social memory. Whether as a special-purpose money used in a limited domain, or as a general-purpose money meant to operate across all spheres of human life, money functions as memory to establish ongoing social relations. Distributed memory is fundamental to the operation of Bitcoin. But the immutable transaction history which enables trust between strangers is also a potential source of identifying the behavior of individual accounts, even when identity is pseudonymized. This raises not just a technical problem, but also political one: given that monetary transactions and the externalities which are associated with trade affect people beyond those transacting, should money ever be entirely private to the two individuals that transact? One criticism of Bitcoin raised by Dodd (2018) is that many advocates frame the political economy of the cryptocurrency as if it exists as a ‘thing’ outside of human control, a natural, or in other words, non-social process.

‘*If Bitcoin succeeds in its own terms as an ideology, it will fail in practical terms as a form of money. The main reason for this is that the new currency is premised on the idea of money as a ‘thing’ that must be abstracted from social life in order for it to be protected from manipulation by bank intermediaries and political authorities. The image is of a fully mechanized currency that operates over and above social life. In practice, however, the currency has generated a thriving community around its political ideals, relies on a high degree of social organization in order to be produced, has a discernible social structure, and is characterized by asymmetries of wealth and power that are not dissimilar from the mainstream financial system.*’ (Dodd, 2018).

Economic transactions and the money that accompany them do not exist in a void free of social consequences, and as Seele (2018) notes, ‘let us not forget: crypto means secret’. Secrecy and currency are not common bedfellows, and the social implications of secret transactions echo far beyond the dyad of sender and recipient. If humanity widely adopts privacy coins for the practical purposes of paying wages and buying goods and services, the political ramifications will be gargantuan for existing social institutions. Considering the neglect of privacy issues in branding (Ohm, 2012) and the political underpinnings of privacy (Westin, 2003), now is an opportune moment to assess how privacy coin designers conceptualize, justify and implement privacy protective technologies to attain different political ends.

CRYPTOCURRENCIES, PRIVACY AND POLITICAL BRANDS

A minimal definition of political branding is ‘*political representations that are located in a pattern, which can be identified and differentiated from other political representations’* (Nielsen, 2013). According to Nielsen, ‘identification’ and ‘differentiation’ are the two simple attributes that need to be emphasized in the definition of political brands (Nielsen, 2016; 71; Nielsen, 2017; 126), meaning the concept can be applied widely to numerous research objects. Although most political branding research to date has focused on policies, parties and politicians (Speed, Butler and Collins, 2015), recent studies suggest the importance of exploring how political brands are positioned in different contexts and settings (Needham and Smith, 2015). Among new contexts of inquiry researchers have investigated ‘nations, parties, nongovernmental organizations (NGOs), interest organizations, leaders, candidates, policies, communication, or rhetoric’ (Nielsen, 2017; 120) and the symbolism in the construction of selected Islamist audio-visual propaganda made available on the internet (O’Shaughnessy and Baines 2009). These approaches illustrate the diverse nature of political brands as a concept (Smith and French, 2009) researched from multiple perspectives (Nielsen, 2016). The need to understand alternative political brands becomes more relevant in a climate where political parties show an image of crisis and the traditional dominant modes of political organization are being challenged (Husted et al., 2018).

Cryptocurrencies such as Bitcoin are designed to eradicate the influence of politicians and bankers over the productive control of money, such that top-down coercion is removed from the system. Political and commercial institutions are thus to be avoided by design, and their influence is therefore reduced (Dierksmeier and Seele, 2016). Although government influence on cryptocurrencies is limited, some authors suggest that many advocates of Bitcoin use it for political reasons (Ron and Shamir, 2015), while others suggest that the blockchain system (underpinned by a ‘neoliberal political economy’ that enables cryptocurrency transactions) is trying to hide the politics involved (Herian, 2018). The politics of cryptocurrencies are made visible where designers identify and differentiate varied approaches to privacy. In the following section, we outline a method for studying cryptocurrencies through the descriptions that designers give of privacy, to reveal the varied ways these systems are positioned as political brands.

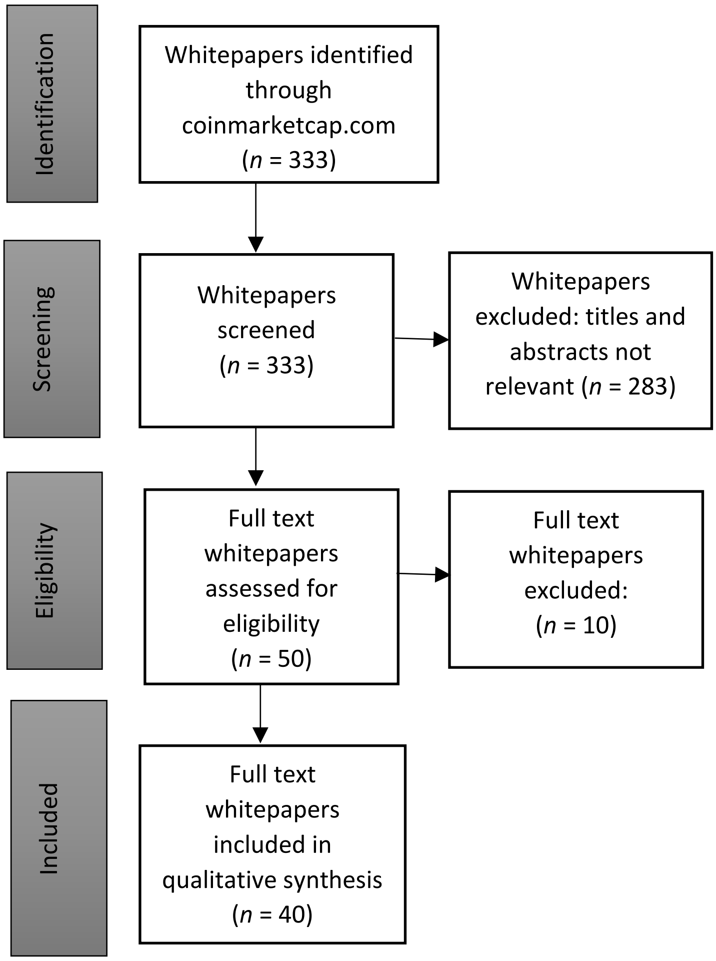
METHODOLOGY

Research method

We conducted a systematic review of cryptocurrency white papers using a method inspired by the PRISMA protocol (Preferred Reporting Items for Systematic Review and Meta-Analysis) (Shamseer et al. 2015), a ‘well-respected evidence-based approach from medical science’ recently used in management research (Kranzbühler et al. 2018, 434). Review protocols are used to help protect against arbitrary decision making during the review, and also to enable the reader to assess the presence of selective reporting, by documenting a clear and replicable process. Though systematic reviews have been used before in the area of political branding

(Nielsen, 2017) they are a relatively novel approach within the field. An overview of the method can be seen in Figure 1 which was used as follows.

Figure 1: Systematic review method for generating a corpus of privacy coin whitepapers


Identification
Whitepapers identified through coinmarketcap.com (n = 333)
Screening
Whitepapers screened (n = 333)
Whitepapers excluded: titles and abstracts not relevant (n = 283)
Eligibility
Full text whitepapers assessed for eligibility (n = 50)
Full text whitepapers excluded: (n = 10)
Included
Full text whitepapers included in qualitative synthesis (n = 40)

Identification. First, an initial corpus of cryptocurrency whitepapers was selected by using the market cap tracking website coinmarketcap.com. This service follows the live price fluctuations of cryptocurrency exchanges and publish the details on their websites. Aggregated statistics are used to rank the total volume and market value of each currency/token such that potential investors can broadly analyze the market. It is important to note that it is practically impossible to review all privacy coin whitepapers, due to the enormous growth in coins which have created hardforks of existing privacy coins. Many of these coins are referred to as ‘altcoins’ and others more disparagingly as ‘shitcoins’ due to their low market capitalization, lack of innovation and user engagement. On the day the corpus of whitepapers was generated 1981 coins/tokens were listed on coinmarketcap.com with a known total market capitalization of $193,560,063,184. We observed that 98% of the USD value of this market was shared between the top 333 coins and we decided to focus on those coins as the limit of our corpus because they are demonstrably successful compared with the innumerable copycats. Those included have persuaded the imagination, and perhaps more importantly the wallets, of users across the globe.

Screening. Using these ranked lists the top 333 cryptocurrencies (as of 11/09/2018) were identified and the associated whitepaper of each coin/token was specifically analyzed for the presence of 'privacy' claims where the designers sought to create a financial instrument that masks user behavior and metadata which could be inferred to reveal identity.

Whitepapers occupy an unusual genre of writing, straddling technical report and manifesto simultaneously. Most papers describe their innovation, but also aim to persuade the audience to use the currency as a solution to particular political economy problems. Though many are written by practicing cryptographers and economists, most are styled in a pseudo-academic fashion to ensure rigor and accessibility. They are thus as much a stylistic heir to the tradition of pamphleteering as to academic journals. To our knowledge most of the whitepapers selected in the corpus were not subjected to the traditional academic double-blind peer review process, other than a few notable exceptions (e.g. Zerocoin and Zerocash). But those currencies that receive popular attention do nonetheless receive whitepaper scrutiny and discussion by users and investors on public Web forums such as Bitcointalk, Reddit, and Telegram.

Eligibility. After the corpus was assembled the research team read the abstracts and/or introductions of each paper to look for claims of privacy. If an abstract used privacy or an obvious synonym for obfuscation (e.g. 'anonymous', 'pseudonymous', 'cloaking', 'hiding', 'obscuring', 'dark') the full paper was included in the corpus. The papers were then assessed for full eligibility by examining the design described in each paper for evidence of technological innovation explicitly regarding privacy. Those papers that described privacy as an aim but did not describe a particular privacy innovation were excluded at this stage.

Included. The inclusion criteria used to assess whitepaper suitability for the corpus were twofold. To be included in the corpus a coin/ or token must: 1) advertise its purpose as defending and/or improving privacy of its users; and 2) Develop technology to create untraceability or unlinkability in the specific domain in which the currency is used. As a result of this stage, we removed ten white papers that did not meet these criteria and we obtained a sample of 40 white papers (over 1000 pages of text) for scrutiny.

Data analysis

After completing the stages of identification, screening, eligibility and inclusion, we focused on data analysis. Drawing on Westin's (1967) definition of privacy around the states (i.e. solitude, intimacy, anonymity, reserve) and functions of privacy (i.e. personal autonomy, emotional release, self-evaluation and limited and protected communication), we developed a series of questions to ask of each paper to compare the practical, political and technical aspects of privacy described by each whitepaper. The questions included: 1) is privacy described as an end in itself or is privacy instrumental to some other moral aim? (e.g. happiness, safety); (2) is privacy described as a right or a commodity?; (3) what technologies are deployed to protect privacy?; (4) what states of privacy if any are said to be protected by the technology?; (5) What function of privacy is served by the technology?; (6) Is there an obvious allegiance to a political philosophy?; (7) Does the solution propose a general or special purpose money?; (8) Is privacy seen as a static or one-off solution to a problem or is it a dynamic/processual phenomenon worthy of ongoing consideration and revisionist development?

The selected white papers were scrutinized in two ways. First, we used the aforementioned questions to analyze each whitepaper and use *a priori* coding to generate preliminary answers in a spreadsheet (See Table 1). The results were then used to guide the identification of emergent themes in relation to the broader privacy as politics literature. Second, we carefully examined the selected white papers to gather in-depth inductive insights into the political motivations expressed in the whitepaper authors' own terms. These results provided the basis for examining the corpus across (1) privacy as politics themes within the whitepapers, which indicated convergent/divergent motivations for developing and fostering privacy; (2) identify tensions in the way privacy is framed epistemically and ethically in relation to politics; and (3) develop an agenda for future research based on issues that emerged from the analysis that indicate worthiness of further inquiry.

PRIVACY COINS AS POLITICAL BRANDS

Following the questions outlined in the data analysis section, we identified a number of political themes around privacy. These are shown explicitly for the cryptocurrency whitepapers examined in Table 1. The table shows that allegiance to distinct political ideologies is present in many of the whitepapers and can be seen in the championing of ideals such as '*Economic Liberalism'* (DigitalNote, 2018), '*Libertarianism'* (e.g. Horizen,-Viglione et al., 2017; CloakCoin, 2018) '*Egalitarian*' (Bytecoin - Van Saberhagen, 2013), '*Democracy'* (e.g. Aion – Spoke, 2017; Stakenet, 2018), '*Sovereignty'* (Mainframe - Clarke et al. 2018), '*Empowerment'* (Pura, 2018) and '*Revolution*' (Aeon, 2014).

Despite the variety of political positions expressed, privacy coin whitepapers are almost always ambitious too, as the vast majority aim to become a general purpose money rather than special purpose within a limited domain. Privacy is overwhelmingly seen as an end in itself, but there is some variation in the corpus over whether privacy should be seen as a right or commodity, and whether privacy requires a static or dynamic evaluation. Though the political justifications for privacy coins are varied, the *state* of privacy which privacy coins aim to protect according to Westin's definitions is, almost always, *anonymity*. Indeed a keyword search across all documents reveals that 31 of the 40 white papers included even use the same terminology explicitly as 'anonymous' or 'anonymity' in order to justify their existence.

Cryptocurrency designers have a wide range of political beliefs, but perhaps the common feature mentioned in the majority of whitepapers are variants of freedom. Freedom, however is a multi-faceted concept, and one can find references to freedom from governments, freedom from banks, freedom from multi-national companies, freedom from financial enslavement, freedom from exploitative charges, and freedom from surveillance. These claims for freedom are spread with inconsistent application throughout the corpus and depend largely on the domain specific aims of the designers.

Though the *functions* of privacy described in the whitepapers are primarily to protect communication and personal autonomy we find reasons that go beyond Westin's (1967) categories. The politics of 'privacy' claims are, generally speaking, less explicit than the broader and more common political aim of seizing the productive capacity of money from existing institutions. That said, there are a number of obvious convergent themes within privacy coin whitepapers that identify shared motivations for a range of societal stakeholders. Different motivations for privacy emerged from our review of cryptocurrency white papers. Although existing research indicates the need for brands to think about ways to protect and compete on privacy, scholars have neglected this approach (Ohm, 2012), which is salient when approaching cryptocurrencies as political brands as their motivations manifest in different ways. We now discuss each of them in turn:

Table 1: Privacy coins and associated whitepapers included within the corpus for further analysis

Currency Name	Ranking (#1-#500)	Market Capitalization	General or Special purpose money?	An end or a means?	A right or a commodity?	Is privacy protection static or dynamic?	States of privacy protected	Function of Privacy	Allegiance to Political Philosophy?
Monero (Noether 2018 - though multiple papers written)	10th	$1,773,363,977	General	End	Right	Dynamic	Yes - Anonymity	Protect users in a court of law	No
Dash (Duffield and Diaz 2018)	11th	$1,652,700,450	General	End	Commodity	Static	Yes - Anonymity	Protected communication	No
Zcash (Sasson et al. 2014)	21st	$561,792,867	General	End	Commodity	Static	Yes - Anonymity	Protected communication	No
Bytecoin (Van Saberhagen 2013)	24th	$375,452,075	General	End	Commodity	Static	Yes - Anonymity	Protected communication	Egalitarian
Verge (Verge 2018)	41st	$195,109,417	General	End	Commodity	Static	Yes - Anonymity	Protected communication	Libertarian
Basic Attention Token (Basic Attention Token 2018)	46th	$155,687,403	Special	End	Commodity	Static	Yes - Anonymity	Protected communication	Libertarian
Komodo (Komodo 2018)	53rd	$116,249,238	General	End	Commodity	Dynamic	Yes -Anonymity, Reserve	To protect freedom	Libertarian
Cryptonex (Cryptonex 2017)	54th	$113,665,784	General	End	Commodity	Static	Yes - Anonymity	Protected communication	No
Wanchain (Wanchain 2017)	62nd	$93,891,052	Special	End	Commodity	Dynamic	Yes - Anonymity	Protected communication	No
Aion (Spoke and Nuco Engineering Team 2017)	64th	$90,866,325	General	End	Commodity	Static	Yes - Anonymity	Protected communication	No
Bitcoin Dark (Lee 2014)	72nd	$78,689,089	General	End	Commodity	Static	Yes - Reserve	Protected communication	No
Horizen (Viglione et al. 2017)	76th	$72,210,878	General	End	Commodity	Static	Yes - Anonymity	Protected communication	Libertarian
Ark (Ark 2018)	82nd	$65,281,755	General	End	Commodity	Dynamic	Yes - Anonymity	Protected communication	No
Bitcoin Private (Brutman et al.	87th	$61,856,082	General	End	Commodity	Static	Yes - Anonymity	Protected communication	No
ZCoin (Miers et al.2018)	92nd	$57,576,857	General	End	Commodity	Static	Not Explicit	Protected communication	No
PIVX (Pivx 2018)	97th	$53,540,561	General	End	Right	Static	Yes - Anonymity	Protected communication	Libertarian
Enigma (Zyskind et al. 2018)	108th	$43,749,692	General	End	Commodity	Static	Yes - Anonymity	Protected communication	No
Aurora (Aurora Labs 2018)	112th	$41,548,918	General	End	Commodity	Static	Yes - Anonymity	Protected communication	Libertarian
Civic (Civic Technologies 2017)	119th	$37,923,916	General	End	Commodity	Static	Not explicit	Protected communication	No
Skycoin (Skycoin 2017)	131st	$32,744,135	General	Means	Commodity	Dynamic	Yes Anonymity	Protected communication	No
Storj (Wilkinson et al. 2016)	133rd	$32,500,268	General	End	Commodity	Static	Yes - Reserve	Protected communication	No
Particl (Kaiser 2017)	179th	$22,874,281	General	End	Commodity	Dynamic:	Yes - Anonymity	Protected communication Personal autonomy Consumer protection	No
Digital Note (Digital Note 2018)	194th	$20,677,499	General	End	Commodity	Static	Yes- Anonymity	Protected communication	Libertarian
ZClassic (Creighton 2018)	196th	$20,061,237	General	End	Commodity	Dynamic	Yes-Anonymity	Protected communication	Democracy
NIX (NIX 2018)	230th	$16,005,206	General	Means	Right	Dynamic:	Yes - Anonymity	Protected communication Personal security	'Empowering'
Quantum Resistance (Waterland 2016)	233rd	$15,927,975	General	End	Commodity	Static	Yes - Anonymity	Protected communication Business protection	No
Pura (Pura 2018)	242th	$14,907,661	General	Means	Right	Static	Not explicit	Protected communication	Democracy
Mainframe (Clarke et al., 2018)	247th	$14,647,533	Special	End	Right	Static	Yes - Anonymity	Protected communication Compliance	Sovereignty
IOTeX (IoTex Team 2018)	248th	$14,488,970	General	End	Commodity	Dynamic	Yes- Anonymity	Protected communication Safe acquisition	No
ION (Matlack et al. 2016)	255th	$14,111,834	General	End	Commodity	Static	Yes - Anonymity	Protected communication Consumer protection	No
NavCoin (Navcoin 2018)	257th	$13,959,244	General	End	Commodity	Static	Yes - Anonymity	Protected communication Business Protection	Democracy
CPChain (CPChain Team 2018)	266th	$12,864,672	General	End	Commodity	Static	Yes - Anonymity	Personal autonomy, Safe acquisition	No
TokenPay (Capo el al. 2017)	269th	$12,723,732	General	End	Commodity	Static	Yes-Anonymity	Protected communication Business Protection	No
PACcoin (Pac coin 2018)	276th	$12,012,093	General	End	Commodity	Dynamic	Yes - Anonymity	Protected communication	No
Aeon (Aeon 2014)	284th	$11,528,314	General	End	Commodity	Dynamic	Yes - Anonymity	Not explicit	Join the
Stakenet (Stakenet 2018)	285th	$11,484,925	General	End	Commodity	Dynamic	Yes - Anonymity	Personal autonomy, Safe transaction	No
Bulwark (Bulwark 2018)	310th	$9,970,454	General	End	Commodity	Dynamic	Yes - Anonymity	Personal autonomy	Libertarian
BitNewChain (Bitnew-Chain 2018)	318th	$9,761,978	General	End	Commodity	Dynamic	Yes - Anonymity	Protected comms/trans. Consumer protection	No
CloakCoin (Cloakcoin 2018)	320th	$9,671,115	General	End	Commodity	Dynamic	Yes - Anonymity	Protected communication	Libertarian
WABnetwork (Wab 2018)	331st	$9,089,798	General	End	Commodity	Static	Yes - Anonymity	Safe transactions	No

Privacy as a guarantor of fungibility

'*Fungibility is an attribute of money that dictates that all units of a currency should remain equal. When you receive money within a currency, it should not come with any history from the previous users of the currency or the users should have an easy way to disassociate themselves from that history, thus keeping all coins equal. At the same time, any user should be able to act as an auditor to guarantee the financial integrity of the public ledger without compromising others privacy.' (*Dash, 2018)

'Fungibility is a core component of money, it requires that all the pieces of a currency remain equal. For example, when you get coins via Private$PAC, these coins should not have any fingerprints from their previous transactions or users.' (PAC, 2018)

Money is used for all sorts of purposes, some of which are deemed illegitimate or criminal by governments. As money passes between people it can become tainted by the actions of previous owners, for example through illicit transactions involving drugs, weapons, stolen goods, money laundering, or perhaps more worryingly as a consequence of the subjective whims of a dictatorial regime. 'Dirty' money is therefore potentially at risk of being expropriated or seized by the state. By obfuscating the history of coin transactions some privacy coins (e.g. Dash - Duffield and Diaz, 2018; PAC Coin, 2018; Komodo, 2018; Stakenet, 2018) pursue the goal of a truly fungible money, wherein all coins are equally valued regardless of their historical trajectories and associated owners. In this respect, privacy coins try to attain the quality of fungibility already possessed by offline cash in the form of physical coins and banknotes. A further consequence of expropriated money is price instability for the rest of the market. As expropriation may become increasingly commonplace as governments resist the integration of cryptocurrency into wider society, designers have recognized that these instances do not happen in isolation from the rest of the financial system, and that fungibility can help to support financial resilience for the broader currency implementation.

Privacy as personal security

'To protect their privacy, users thus need an instant, risk-free, and, most importantly, automatic guarantee that data revealing their spending habits and account balances is not publicly accessible by their neighbors, co-workers, and merchants.' (Zerocash - Ben-Sasson *et al*, 2014)

If a malicious agent doesn't know how much money you own, it becomes harder to target potential victims. Privacy thus provides a safeguard through hiding resources. But the broader claims made by coins like Zerocash (2014), Particl (2017), and CPChain (2018) is that personal security is also the responsibility of the network. This is particularly a problem when consumers are not in a position to be sufficiently aware of potential privacy leaks or threats and thus are unable to provide informed consent. Personal security then is not just a matter of individuals ensuring they have the resources to defend and protect themselves, it is a much broader claim about the incomplete knowledge users possess and a political motivation to ensure maintenance of fiscal standards regardless. This judgment about user knowledge is not just a claim about the present moment, it is also extended into the future in recognition that all people are in a process of developmental learning, as can be seen in the quote below:

Many of humanity's most meaningful advancements in art, technology, and other human endeavors began in situations where the creator had the security of privacy in which to explore, to discover, to make mistakes, and to learn thereby. (Komodo, 2018)

Although issues relating to Westin's privacy state of *reserve* are only rarely discussed in the white papers, there is nonetheless evidence that some designers see privacy as a safeguard for ensuring the future personal growth of their users. This is a more sophisticated account of privacy than a static understanding permits, instead recognising that the acquiescence of others is a necessary precondition for the maturation of any person, and as such should be defended.

Privacy as consumer protection

'Consumers expect a certain level of convenience when it comes to transferring value in exchange for goods and services, and this is why payment processing on the web has become commonplace. Along with this expectation of convenience, there is an assumed level of privacy that comes with such a transaction. Unfortunately, over the past two decades there have been entities who profit off of creating an online 'profile' of a consumer by tracking online credit card transactions. This is incredibly invasive and serves as a large supporting premise for why a consumer would want to transact online with cryptocurrency.' (Bitcoin Private, 2018).

Commercial intrusion into consumers' lives is widely cited in the privacy coin literature as something to be resisted, for example:

'The online services we use are increasingly demanding more of our personal data, a disturbing trend that threatens the privacy of users on a global scale. Entities such as Google, Facebook and Yahoo have grown into colossal, seemingly unaccountable corporations by monetizing their users' personal data' (Particl 2018).

Multiple privacy coins (e.g. Aurora, 2018; Bitcoin Private, 2018; Particl, 2018; TokenPay – Capo *et al,* 2017; Enigma – Zyskind *et al,* 2018) explicitly comment on the use of privacy measures to protect consumers now and in imagined future scenarios. These arguments rely heavily on protecting the privacy state of *anonymity* (i.e. freedom from surveillance in public places) and the function of *protected communications.* For instance, if an account balance and behavior is unknown it is impossible to serve targeted advertisements based on behavioral segmentation. Behavioral advertising is now the norm across the Web, but it hinges on measuring, monitoring and updating a record of identity. Similarly, if an account balance is closely followed by companies it becomes possible to use that information for dynamic or differential pricing i.e. charging you more because of who are or based on the increased likelihood that you will pay more at particular moments. This thread in the privacy literature is thus an attempt to develop consumer sovereignty in the marketplace.

Privacy as business protection

'Meet Randal. As an entrepreneur, he is very aware of the importance of protecting the identities and finances of his clients safe. This is especially true as he provides anonymous genetic screening for diseases such as Parkinson's disease and Dementia. A breach of client data could ruin the lives of his clients, not only his business. After realizing that typical

financial solutions provided no actual guarantee that leaks and breaches would not affect his business or his client, he began to use Verge to transact business' (Verge 2018).

Privacy aims are widely extended to focus on businesses in many of the whitepapers in the corpus (e.g. BitNew Chain, 2018; CPChain, 2018; Verge, 2018; Skycoin, 2017; Ark, 2018; Bitcoin Dark – Lee, 2014; Wanchain, 2017; Iotex Team, 2018). Concealed transactions can help mask the relations between buyer and seller. Transactions up and downstream in supply chains can therefore be concealed from prying eyes. This is particularly important where a breach of privacy may jeopardize the lives of vulnerable clients, but it is also a means of maintaining competitive advantage. 3rd party financial intermediaries such as banks and credit providers have unprecedented access to transaction information of businesses across the globe. Although many consumers are increasingly vigilant with their privacy in the post-Snowden world we now inhabit, there is perhaps far less scrutiny given to the surveillance of corporate entities who are often seen as those adversaries being fought against. Organizations are especially vulnerable to privacy invasion. The obfuscation of supply chain relations is a defensive mechanism against competitors, but it is also potentially a means to deliberately hide information from consumers who may boycott a product when an organization fails to deliver on supply chain moral expectations.

Privacy as safe acquisition/transaction

The majority of discussion around privacy in relation to cryptocurrencies focuses on maintaining privacy before, during and after currency has been spent. But the acquisition process is similarly important for maintaining user privacy. The way that people acquire cryptocurrencies varies widely depending on their circumstance. Some people earn currencies as networks reward miners or 'masternodes' for validating transactions, while others directly exchange their fiat money for cryptocurrencies on 3rd party websites, and some are also the beneficiaries of direct payments, gifts, donations or anonymous tips. In each of these use cases people acquire cryptocurrencies through different means and each carry their own respective privacy risks. A range of whitepapers (e.g. CPCChain, 2018; Bulwark, 2018; Verge, 2018; Basic Attention Token, 2018; Komodo, 2018; Digital Note, 2018) draw attention to maintaining privacy during acquisition *and* transactions for a variety of reasons. For example, as discussed earlier, if a user is linked to a wallet address or ID then it becomes potentially fruitful for attackers to direct unwanted attention at that same address for malicious reasons. During the mining process for instance, miners can group together and censor transactions by actively not adding transactions to the proposed block. As more people become involved in hosting nodes for remuneration within these networks privacy may evolve to become more focused on guaranteed earnings than maintaining discretion when spending. If cryptocurrency is ever to become widely used for paying wages it is likely that privacy measures that manage coin acquisition would also need to be widely adopted.

Privacy as compliance

'The General Data Protection Regulation (GDPR) passed by the EU in 2016 requires enterprise IT practices to comply with strict privacy measures. Granting IT Admins a platform focused on user sovereignty, corporations can design streamlined systems without the risk of leaking information in transit. Liability is reduced when sensitive data is isolated within a secure system' (Clarke et al. 2018, Mainframe).

The media commentary around privacy coins has almost invariably drawn attention to what society loses when financial transactions become hidden. But this position loses sight of the already well-established legal frameworks surrounding interpersonal computing. A range of privacy coin whitepapers also draw attention to the need to act in accordance with preexisting standards and comply where necessary (Sasson *et al.,* 2014; Zerocoin –Miers *et al.,* 2018; TokenPay – Capo *et al,* 2017; Mainframe - Clarke et al. 2018). Privacy as compliance is likely to become increasingly important for those limited-domain projects which utilize blockchain, cryptocurrencies or tokens as a special-purpose money which can inadvertently reveal metadata about their users. Here privacy is less to do with a crusading moral purpose. Instead, it is *de jure* privacy, an adherence to a state of affairs in accordance with the law.

EPISTEMIC AND ETHICAL TENSIONS IN THE POLITICS OF PRIVACY COINS

Three clear political tensions emerged from the inductive analysis, these relate to: 1) an inherent conflict of political ideologies in maintaining privacy, 2) disagreement in the practical implementation of privacy, and 3) the ethics implications of conflicting privacy conceptualizations due to technical limitations in design.

Tension one: 'We the people' without the 'We'

'I don't believe we shall ever have a good money again before we take the thing out of the hands of government. That is, we can't take it violently out of the hands of government. All we can do is by some sly roundabout way introduce something they can't stop.' (Hayek quoted in Ammous (2018)).

Nakamoto recognized Bitcoin's sensibility to libertarian political philosophy and this remains a clear thread running through many privacy coins. The relation to libertarian ideas is clearest when privacy coin whitepaper authors cite the work of 'Austrian School' economists such as Friedrich Hayek. Indeed, in the prophetic statement shown above, Hayek recognized the practical issue of creating an ideal currency well before the advent of cryptocurrency or even the Internet. A good money in the eyes of this philosophy is a money not controlled by any one individual, and yet even if the money is not violently created, it nonetheless requires at worst coercion or at best a gentler form of persuasion. This echoes the work of Dodd (2017) cited earlier that draws attention to the implicit social structure involved in maintaining a trustless, decentralized currency. A typical argument made in favor of privacy coins can be seen below:

'I care about more than cryptocurrencies. In fact they are a means to an end, the end being political empowerment of individuals... Our goal is to create a backdrop that allows pioneers to forge a method of societal organization that politically empowers individuals to become their own bank and, eventually, their own government.' (Pura 2018).

Empowerment is a central theme in the literature, but this creates a tension when the political goal is also privacy. Pura (2018) cited above also discuss an aim to improve the 'common good' through enabling individuals rather than allowing central authorities to make decisions about intervening through capital projects. One evident tension here though is that without the knowledge of how money flows between different actors it is difficult to properly understand financial inequity through empirical means. Many of the rights granted to marginalized groups over the past hundred years were only guaranteed by a state after collective efforts drew attention and scrutiny to the mistreatment or corrosive power relations than exist between individuals. If all transactions between individuals become private, then it becomes impossible to trace the flows of capital and the associated structures of domination that potentially disempower marginalized groups.

Tension two: decisional privacy vs universal privacy

'The superior privacy layer that NIX offers solves many concerns in the cryptocurrency ecosystem. Because NIX believes that users should have the power of privacy, it is not a required feature, simply an optional one.' (NIX 2018).

How should privacy be practically embedded in privacy coins? All transactions by their nature include two parties. If both parties wish to reveal their interaction to other people should they be allowed to do so if they don't jeopardize the privacy of others? Some currencies are designed with modular privacy features that enable users to reveal details publicly when acting (e.g. NIX, Zcash). This has been criticized by privacy universalists such as Monero, who argue that the revelation of details by one user threatens the broader integrity of privacy for the rest of the network (sometimes called *networked privacy* – Boyd, 2012). The cherry-picked approach to privacy, is referred to as *decisional privacy*, and is criticized because it is seen as impinging on the rights of 3rd parties.

Decisional privacy is a well-established concept within the literature (e.g. Wacks 2015) and in this instance it refers to the right of an individual to choose what information is revealed during an interaction. The consequence of privacy coins that wish to facilitate decisional privacy is that the currencies will thus become special-purpose monies of limited domain, rather than a generally acceptable protocol, regardless of the privacy interest being defended. The likely outcome of this tension is that decisional and universal privacy coins are likely to coexist in the future and consequently eat the market share of each other, potentially precluding the positive network effects that could emerge if users privileged one design over the other.

Tension three: unlinkability or taint resistance?

Should designers aim to make technology which can make transactions unintelligible *or* invisible? This is the technical challenge, which privacy coin designers face and attempt to provide a solution to. Complete invisibility may be technically impossible as new technology continues to emerge and make robust protections become obsolete. This has important implications for user literacy too. If a user adopts a currency they are often confronted with a whitepaper or marketing material which promises anonymity, but this anonymity could come from invisibility of transactions or a technical intervention which makes behavioral traces become unintelligible. Both positions are seldom articulated as being distinct within the white paper corpus. Yet the anonymity claimed by so many privacy coins has been criticized as a kind of pseudonymity by many technical papers, and this is not well-reflected in whitepapers. Meiklejohn and Orlandi (2015) introduce the sophisticated notion of *taint resistance* when analyzing the claims made by privacy overlays. Existing notions of unlinkability for electronic cash require that a valid coin belonging to one user is indistinguishable from a valid coin belonging to another.

'In Bitcoin, it is impossible to satisfy this definition: a bitcoin essentially is its spending history, and it is thus trivial to distinguish two valid bitcoins. Any notion of anonymity that is useful for Bitcoin must therefore focus less on the coins themselves and more on ownership.'

Specifically, the concept ‘attempts to capture how well an adversary can discern the ownership of a bitcoin based on its previous spending history. Our definition has the advantage that we can not only provide proofs of security (i.e., prove that a protocol achieves optimal taint resistance), but that it also provides a concrete measurement of the degree to which a proposed solution is effective in improving anonymity.’ Though many of the coins make outlandish claims about the quality of privacy protection, and some speak as though their solution to privacy is static, there is nonetheless recognition within other papers that privacy requires vigilance. Taint resistance is clearly a different ethical standpoint on privacy to unlinkability (regardless of its potential future design possibility). The notion neatly captures the frailty of many existing uses of privacy when used in whitepapers to attract a broad audience. Expressing this ethic clearly is perhaps the single most important step to ensuring the possibility of informed consent. The failure to seek such consent will invariably lead to differences in understanding emerging between designers and users.

FUTURE DIRECTIONS FOR RESEARCH

Several issues became apparent when conducting the literature review, which warrant further attention. Though we can be confident in our assertions about designers’ intentions of privacy coins, we can be less sure about the motivations that are associated with user adoption. Most privacy coins treat privacy as an end in itself, which therefore means users may adopt the coins according to shared, different or even conflicting ultimate motivations. We suggest that further empirical scrutiny should be given to the following research questions:

(1) Who is using privacy coins? Is this the domain of a truly decentralized and egalitarian social project or does cryptocurrency, with its arsenal of jargon and technical barriers, actually preclude adoption from those marginalized or disenfranchised people who would benefit most from privacy features?

(2) Why do people use privacy coins? Scaremongering abounds in the media portrayal of privacy coins and yet this is often based on unsubstantiated claims about the actual use of the currencies. Though this is a tricky environment to conduct research in given that privacy coin users obviously want privacy, there is nonetheless a burgeoning community of users in online forums (e.g. Reddit, Bitcointalk, and Telegram) who have willingly expressed their views in public and on record. There are literally hundreds of thousands of people involved in these communities and many of them may be willing to disclose their views in person or in large-scale questionnaires.

(3) How does the relative prevalence of privacy coin adoption vary in relation to the broader political landscapes that people inhabit? Cryptocurrencies are a potentially subversive force for the existing monetary system in democratic countries, but they are potentially an emancipatory force for people living under the shadow of totalitarian regimes. Greater empirical scrutiny on the country-specific adoption rates of privacy coins would help to theorize the dynamics involved in their uptake as well as their revolutionary potential.

CONCLUSION

This paper contributes to the understanding of political branding by shedding light on how notions of politics emerge in privacy coins and uncovering different ways in which cryptocurrencies underpin political brands. The identification of political dimensions and ideologies in cryptocurrency challenges the idea that digital currency is removed from the influence of politicians (Dierksmeier and Seele 2016) and unveils a new context to research political branding.

Privacy often seems to be a secondary consideration in the world of cryptocurrency. Indeed, though Nakamoto paid lip service to the value of privacy their initial political aims seem more concerned with building a decentralized and resilient system that seizes the production of money from the state rather than guaranteeing the privacy of every individual user. As a consequence, the design of other cryptocurrencies since have largely echoed the ordering of these political points, the former being more urgent than the latter. One can readily find evidence of this in the claims made by cryptocurrency evangelists online that preventing governments from printing money will prevent war, genocide, poverty or other catastrophic events that blight human lives.

Privacy, though politically important, has historically been an add-on to the primary aim of decentralization. This has meant designers are now wrestling with the double-headed technical challenge of untraceability and unlinkability. We believe that many of these currencies already offer features that make tracking financial payments extremely difficult. How scrupulous those payments are is perhaps politically less important than what will happen to existing institutions. No amount of legislation is likely to prevent the growth of privacy coins in all areas of the economy in the next decade. Though many privacy coin designers would have us believe that transactions that don't involve us don't affect us, this clearly is not the case. As commerce becomes private debate must become public.

REFERENCES

Aeon, 2014. ‘AEON coin is the next generation of anonymous cryptocurrency’. Retrieved September 21 2018 from https://docs.google.com/document/d/11GxjLV8uszoCTRcPYmpXGYH7cUmHvriODD9lggu_gW8/edit

Ammous, S. 2018. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. John Wiley & Sons.

Ark 2018. ‘A Platform for Consumer Adoption’. Retrieved September 21 2018 from https://ark.io/Whitepaper.pdf

Aurora Labs 2018. ‘Aurora: A Decentralized Financial Institution Utilizing Distributed Computing and the Ethereum Network’. Retrieved September 21 2018 from https://auroradao.com/assets/Aurora-Labs-Whitepaper-V0.9.5.pdf

Basic Attention Token 2018. ‘Basic Attention Token (BAT) Blockchain Based Digital Advertising’. Retrieved September 21 2018 from https://basicattentiontoken.org/BasicAttentionTokenWhitePaper-4.pdf

Berentsen, A. and Schar, F. 2018. ‘The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies’. *Federal Reserve Bank of St. Louis Review*, 100 (2): 97-106.

Brutman, J. Layton, J. Sulmone, C. Stuto, G. Hopkins, G. and Creighton, R. 2018. ‘The Revolution of Privacy Fulfilling Satoshi’s Vision for 2018 and Beyond’. Retrieved September 21 2018 from https://btcprivate.org/whitepaper.pdf

Bitnew-Chain 2018. ‘Next-generation decentralized application platform for commercial applications’. Retrieved September 21 2018 from https://www.btn.org/download/BTN-Tec-white_paper_finalV1.1.pdf

Bohannon, J. 2016. ‘The bitcoin busts’. *Science*, 351 (6278): 1144-1146.

Boyd, D., 2012. Networked privacy. *Surveillance & Society*, *10*(3/4), p.348.

Bulwalk 2018. ‘Bulwark Cryptocurrency Whitepaper’. Retrieved September 21 2018 from https://bulwarkcrypto.com/docs/EN_-_Bulwark_Cryptocurrency_Whitepaper.pdf

Capo, D. Salazar, C. Pacetti, J. and Kalfoglou, Y. 2017. ‘TokenPay The World's’ Most Secure Coin’. Retrieved September 21 2018 from https://www.tokenpay.com/whitepaper.pdf

Civic Technologies 2017. ‘Civic White Paper’. Retrieved September 21 2018 from https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf

Chaum, D., 1985. ‘Security without identification: Transaction systems to make big brother obsolete’. *Communications of the ACM*, *28*(10):1030-1044.

Clarke, A. Craig, A. Hagen, B. Youngblood, C. Jaquier, C. Perillo, D. Tavazzani, L. Larson, M Hagen, M. Mosic, M. Le Cam, P. and Howley, S. (2018). ‘Mainframe: the web3 communications layer’. Retrieved September 21 2018 from https://mainframe.docsend.com/view/j39qpui

Cloakcoin 2018. ‘Enigma A Private Secure and Untraceable Transaction System for Cloakcoin’. Retrieved September 21 2018 from https://www.cloakcoin.com/user/themes/g5_cloak/resources/CloakCoin_Whitepaper_v2.1.pdf

Coinmarketcap.com 2018. ‘All Cryptocurrencies’ Retrieved September 11 2018 from https://coinmarketcap.com/all/views/all/

CPChain Team 2018. ‘Decentralized Infrastructure for Next Generation Internet of Things’. Retrieved September 21 2018 from https://www.cpchain.io/CPChain_Whitepaper_English.pdf

Creighton, R. 2018. ‘ZClassic’. Retrieved September 12 2018 from https://zclassic.org/pdfs/whitepaper.pdf

Crockett, D., and Pendarvis, N. 2017. ‘A Research Agenda on Political Ideology in Consumer Research: A Commentary on Jung et al.’s ‘Blue and Red Voices’’. *Journal of Consumer Research*, 44(3): 500-502.

Cryptonex 2017. ‘Privacy Policy’. Retrieved September 21 2018 from https://cryptonex.org/privacypolicy.pdf

Dierksmeier, C. and Seele, P. 2016. ‘Cryptocurrencies and business ethics’. *Journal of Business Ethics*, 152 (1): 1-14.

DigitalNote 2018. ‘DigitalNote XDN-project’. Retrieved September 21 2018 from https://digitalnote.biz/whitepaper_stake_award.pdf

Dodd, N. 2017. *The Politics of Bitcoin in Money in a Human Economy*, Hart, K. (Ed.). (Vol. 5). Berghahn Books.

Dodd, N. 2018. ‘The social life of Bitcoin’. *Theory, culture & society* (35, 3): 35-56.

Dostov, V. and Shust, P. 2014. ‘Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?’ *Journal of Financial Crime*, 21 (3): 249-263.

Duffield, E. and Diaz, D. 2018. ‘Dash: A Payments-Focused Cryptocurrency’ [White paper]. Retrieved September 21 2018, from https://github.com/dashpay/dash/wiki/Whitepaper

Goldfeder, S. Kalodner, H. Reisman, D. and Narayanan, A. 2018. ‘When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies’. *Proceedings on Privacy Enhancing Technologies*, 4: 179-199.

Hart, K. 2000. *The memory bank: Money in an unequal world*. London: Profile Books.

Harvey, J. Golightly, D. and Smith, A. 2014. ‘HCI as a means to prosociality in the economy’. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2955-2964). ACM.

Husted, E. Fredriksson, M. Moufahim, M. and Gronbaek P. J. (2018), ‘Political parties: Exploring the inner life of party organisations’, Theory and Politics in Organisation, ISSN 1473-2866, 1-7.

Hurlburt, G. 2017. ‘Shining Light on the Dark Web’. *IEEE Computer*, 50 (4): 100-105.

IoTex Team 2018. ‘Disclaimer for White Paper’. Retrieved September 21 2018 from https://iotex.io/white-paper

Kaiser, I. 2017. ‘A Decentralised Private Marketplace: DRAFT 0.1’ [Particle]. Retrieved September 21 2018 from https://github.com/particl/whitepaper/blob/master/decentralized-private-marketplace-draft-0.1.pdf

Karlstrøm, H., 2014. Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Scandinavian Journal of Social Theory*, *15*(1), pp.23-36.

Komodo 2018. ‘An Advanced Blockchain Technology, Focused on Freedom’. Retrieved September 21 2018, from https://komodoplatform.com/wp-content/uploads/2018/05/2018-05-09-Komodo-White-Paper-Full.pdf

Kranzbühler, A. M., Kleijnen, M. H., Morgan, R. E., and Teerling, M. 2018. ‘The multilevel nature of customer experience research: an integrative review and research agenda. *International Journal of Management Reviews*’, 20(2): 433-456.

Larios-Hernández, G. J. 2017. ‘Blockchain entrepreneurship opportunity in the practices of the unbanked’. *Business Horizons*, 60(6): 865-874.

Lee, J. 2014. ‘Teleport: anonymity through off-blockchain transaction information transfer - A Dark Paper for BTCD’. Retrieved September 21 2018 from https://whitepaperdatabase.com/bitcoindark-btcd-whitepaper/

Luger, E. and Rodden, T. 2013. ‘An informed view on consent for UbiComp’. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing* (pp. 529-538).

Matlack, A., Pfeiffer, M. and Nelson, R. 2016. ‘ION white paper v. 0.1’. Retrieved September 21 2018 from https://github.com/ionomy/ion/wiki/ION-Technical-Whitepaper

Maurer, B. Nelms, T.C. and Swartz, L. 2013. ‘When perhaps the real problem is money itself!’: the practical materiality of Bitcoin. *Social semiotics*, 23(2): 261-277.

Meiklejohn, S. and Orlandi, C. 2015. ‘Privacy-enhancing overlays in bitcoin’. In *International Conference on Financial Cryptography and Data Security* (pp. 127-141). Springer, Berlin, Heidelberg.

Miers, I. Garman, C. Green, M. and Rubin, A. D. 2018. ‘Zerocoin: Anonymous Distributed E-Cash from Bitcoin’. Retrieved September 21 2018 from http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

Nakamoto, S. 2008. ‘Bitcoin: A peer-to-peer electronic cash system’ [White paper]. Retrieved September 21 2018, from https://bitcoin.org/bitcoin.pdf

Navcoin 2018. ‘The Unbreakable Code Navtech Decentralisation Whitepaper’. Retrieved September 21 2018 from https://cryptorating.eu/whitepapers/NavCoin/NAV-Coin-Whitepaper.pdf

Needham C. and Smith G. 2015. ‘Introduction: political branding’. *Journal of Political Marketing*. 14(1-2):1-6.

Nielsen, S.W. 2016. ‘Measuring Political Brands: An Art and a Science of Mapping the Mind’. *Journal of Political Marketing*, 15 (1): 70-95.

Nielsen, S. W. (2017). ‘On political brands: A systematic review of the literature’. *Journal of Political Marketing*, 16(2): 118-146.

NIX 2018. ‘NIX Platform Whitepaper 2.0’. Retrieved September 21 2018 from https://nixplatform.io/docs/NIX-Platform-Whitepaper.pdf

Noether, S. 2018. ‘Review of cryptonote white paper’ [Monero]. Retrieved September 21 2018 from https://downloads.getmonero.org/whitepaper_review.pdf

Ober, M. Katzenbeisser, S. and Hamacher, K. 2013. ‘Structure and anonymity of the bitcoin transaction graph’. *Future internet*, 5 (2): 237-250.

Ohm, P. (2012). ‘Branding privacy’. *Minnesota Law Review*, volume 97: 907–989.

Okamoto, T. and Ohta, K. 1991 ‘Universal electronic cash. In Annual international cryptology conference’ (pp.324-337). Springer, Berlin, Heidelberg.

O’Shaughnessy, N. J. and Baines, P. R. 2009. ‘Selling Terror: The symbolization and positioning of Jihad’, *Marketing Theory*, 9 (2): 227-241

Pac Coin, 2018. ‘A 3rd generation peer to peer cryptocurrency. Built for the people, lead by social governance’. Retrieved September 21 2018 from https://download.paccoin.net/PAC_White_Paper_2018_Final.pdf

Petro, 2018. ‘White Paper 1.0 Financial Proposal’. Retrieved September 21 2018 from https://whitepaperdatabase.com/venezuela-petro-cryptocurrency-ptr-english-whitepaper/

Pittman, A. 2016. ‘The Evolution of Giving: Considerations for Regulation of Cryptocurrency Donation Deductions’. *Duke L. & Tech. Rev*., 14, 48.

Pivx 2018. ‘PIVX Zerocoin Privacy’. Retrieved September 21 2018 from https://pivx.org/white-papers/

Pura 2018. ‘A Digital Cash Movement for the Common Good’. Retrieved September 21 2018 from https://mypura.io/wp-content/uploads/2018/08/Whitepaper_0.3.pdf

Recorded Future, 2018. ‘Litecoin emerges as the next dominant dark web currency’. Retrieved September 12 2018 from: https://go.recordedfuture.com/hubfs/reports/cta-2018-0208.pdf

Reid, F. and Harrigan, M. 2013. ‘An analysis of anonymity in the bitcoin system’. In *Security and privacy in social networks* (pp. 197-223). Springer, New York, NY.

Ron, D. and Shamir, A. 2013. ‘Quantitative analysis of the full bitcoin transaction graph’. In *International Conference on Financial Cryptography and Data Security* (pp. 6-24). Springer, Berlin, Heidelberg.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. (2014). ‘Zerocash: Decentralized anonymous payments from bitcoin’. In 2014 IEEE *Symposium on Security and Privacy* (SP) (pp. 459-474). DOI:10.1109/SP.2014.36

Scott, B. 2016. ‘How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?’ (No. 2016-1). UNRISD Working Paper.

Seele, P. 2018. 'Let us not forget: Crypto means secret. Cryptocurrencies as enabler of unethical and illegal business and the question of regulation'. *Humanistic Management Journal*, 3(1):133-139.

Smith, G., and French, A. 2009. 'The political brand: A consumer perspective'. *Marketing Theory*, 9(2): 209-226.

Speed, R., Butler, P., & Collins, N. 2015. Human branding in political marketing: Applying contemporary branding thought to political parties and their leaders. *Journal of Political Marketing*, 14(1-2): 129-151.

Skycoin 2017. 'Skycoin Business Whitepaper'. Retrieved September 18 2018 from https://downloads.skycoin.net/whitepapers/Skycoin-Whitepaper-v1.0.pdf

Shamseer, L., Moher, D., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P. and Stewart, L.A., 2015. 'Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015: elaboration and explanation'. BMJ, 349: 7647.

Smith, H. J. Dinev, T. and Xu, H. 2011. 'Information privacy research: an interdisciplinary review'. *MIS Quarterly*, 35 (4): 989-1016.

Spoke, M. and Nuco Engineering Team 2017. 'Aion: Enabling the decentralized Internet'. Retrieved September 18 2018 from https://aion.network/media/en-aion-network-technical-introduction.pdf

Stakenet 2018. Whitepaper Version: 3.0. Retrieved September 21 2018 from https://stakenet.io/Whitepaper_Stakenet_V3.0_EN.pdf

Storj Labs 2018. 'Storj: A Decentralized Cloud Storage Network Framework'. Retrieved September 18 2018 from https://storj.io/storj.pdf

Van Hout, M. C. and Bingham, T. 2013. ''Silk Road', the virtual drug marketplace: A single case study of user experiences'. *International Journal of Drug Policy*, 24 (5): 385-391.

Van Saberhagen, N. 2013. 'CryptoNote V2.0' [Bytecoin]. Retrieved September 17 2018 from https://bytecoin.org/old/whitepaper.pdf

Verge 2018. 'Verge: The Most Private Crytocurrency' [white paper]. Retrieved December 5 2018 from https://vergecurrency.com/static/blackpaper/Verge-Anonymity-Centric-CryptoCurrency.pdf

Viglione, R. Versluis, R. and Lippencott, J. 2017. 'Zen White Paper'. Retrieved September 21 2018 from https://www.horizen.global/assets/files/Zen-White-Paper.pdf 64. Wab, 2018. Whitepaper. Retrieved September 21 2018 from https://wab.network/Whitepaper-en.pdf

Wab 2018. 'WAB Whitepaper'. Retrieved September 19 2018 from https://wab.network/Whitepaper-en.pdf

Wacks, R. 2015. *Privacy: a very short introduction*. OUP: Oxford.

Walsh, D. Parisi, J. M., and Passerini, K. 2017. 'Privacy as a right or as a commodity in the online world: the limits of regulatory reform and self-regulation'. *Electronic Commerce Research*, 17 (2): 185-203.

Weimann, G. 2016. ‘Going dark: Terrorism on the dark Web. Studies in Conflict and Terrorism’, 39 (3): 195-206.

Wanchain 2017) ‘Wanchain: Building Super Financial Markets for the New Digital Economy’. Retrieved September 18 2018 from https://wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf

Waterland, P. 2016. ‘Quantum Resistant Ledger (QRL)’. Retrieved September 17 2018 from https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf

Westin, A. F. 1967. *Privacy and freedom* (Vol. 1). New York: Atheneum.

Westin, A.F. 2003. ‘Social and political dimensions of privacy’. *Journal of social issues*, 59(2): 431-453.

Wilkinson, S. Boshevski, T. Brandoff, J.Prestwich, J. Hall, G. Gerbes, P. Hutchins, P. and Pollard, C. 2016. ‘Storj A Peer-to-Peer Cloud Storage Network’. Retrieved September 21 2018 from https://storj.io/storj.pdf

Zulkarnine, A.T. Frank, R. Monk, B. Mitchell, J. and Davies, G. 2016, September. ‘Surfacing collaborated networks in dark web to find illicit and criminal content’. In *Intelligence and Security Informatics* (ISI), 2016 IEEE Conference on (pp. 109-114).

Zyskind, G. Nathan, O. and Pentland, A. 2018. Enigma: Decentralized Computation Platform with Guaranteed Privacy. Retrieved September 21 2018 from https://enigma.co/enigma_full.pdf