Guiding Principles for Ethical Cryptocurrency, Blockchain, and DLT Research

Quinn DuPont
University College Dublin
quinn.dupont@ucd.ie

Abstract

This article investigates ethical research risks associated with cryptocurrencies and the related family of digital "value" technologies. It provides an empirical analysis of innovation and recommends guiding principles for ethical research and development.

Ethical research risks are identified through 1) an analysis of research methods and ethics disclosure practices in published empirical research and 2) a survey of academic research practices and researcher opinions. These data identified multiple research ethics issues. It was discovered that most researchers have extensive and undisclosed industry relationships, have undisclosed conflicts of interest arising from token ownership, and report low use of institutional review or ethics guidelines, among other issues. Three novel research risks—conflicts of interest, risky methods, and disclosure—are then introduced and compared to the risks of conventional research. It is argued that these technologies introduce ethical risks and opportunities beyond their sector. These findings suggest a new class of ethical and normative research practice, comparable to fields such as bio- or nanotechnology ethics. Based on these analyses, eight principles for ethical research are described, with practical lessons for the researcher.

1 Introduction

Researching cryptocurrencies and blockchains is fraught with ethical quandaries. This kind of research combines the challenges of studying computer security, financial technologies, online and anonymous communities, and novel and emerging technologies. Due to their decentralized design and underlying financial value, cryptocurrencies and blockchains present novel research and development risks.[1]

The cryptocurrency and blockchain industry is a decade old and has generated significant private and public investment, attracted a large workforce, and is increasingly delivering software and hardware products into a growing market. There appear to be few limits on possible use cases or industry verticals. At this stage in development, however, impact is best measured in terms of corporate investment, which continues to reach into the billions of dollars annually [12, 65]. While many individuals remain skeptical about the promises offered by the technology (and they have good reason to do so), cryptocurrencies and blockchains have nonetheless emerged as prime movers in many global technology sectors. Moreover, through successive investment and hype cycles, these technologies have expanded in scope and have been integrated with existing information and management systems, in turn introducing social and ethical complexities that are not well understood.

This article explores this challenging ethical terrain with a two-step research design followed by an analysis of three areas of research, ultimately detailing eight principles for ethical cryptocurrency and blockchain research. First, a large-scale review of academic literature identifies research methods and the prevalence of ethics disclosure statements. This analysis found limited evidence of ethical deliberation and very few disclosure statements—as well, most seriously, an underreporting of financial conflicts of interest. Second, a survey of cryptocurrency and blockchain researchers reports on six themes: research methods, awareness of ethics guidelines, ethics and pedagogy, software vulnerability disclosure, token ownership and disclosure, and industry relations. This analysis found that nearly half of all researchers have worked for industry, and of those, only half have reported it. Three-quarters of all researchers reported being very actively recruited by industry for their expertise and personal or university reputation. Nearly half of all researchers have purchased tokens for research and personal investment, yet almost none reported these investments to academic journals or media. Finally, almost no researchers felt that the cryptocurrency and blockchain industry was ethical, yet only a third reported using institutional review for their own ethical research compliance, despite widespread awareness of such guidelines.

[1] In this article, "cryptocurrencies and blockchains" refers to the entire family of digital "value" technologies that emerged from Bitcoin, irrespective of particular technical architecture.

These findings suggest that cryptocurrencies and blockchains comprise a new class of ethical and normative research practice, comparable to fields such as bio- and nanotechnology ethics, and through technological innovation and adoption introduce risks to a broader technology landscape.

2 Cryptocurrency and Blockchain Research

Bitcoin is a system of digital "money" invented in 2008/2009 that later became the first of many cryptocurrencies [27]. Early on, the Bitcoin community was small and niche, mostly of interest to technologists aligned to the political and cultural values of libertarianism, anarchism, and neoclassical economic theory [40]. But, by 2013 Bitcoin had grown in popularity and price, and subsequently, academic research followed.

Technical developments to broaden and enhance the Bitcoin system soon emerged, leading to the proliferation of hundreds of Bitcoin clones known as "alt coins" and "cryptocurrencies," alongside the emergence of general "blockchain" technologies. In 2014-2015, a major shift occurred with the development of the Ethereum platform (and a few other smaller projects), which built on the technologies underlying Bitcoin (by then known as a "blockchain"). Ethereum extended Bitcoin but did so without being necessarily tied to conceptions of money and monetary instruments.

The emergence of blockchains reoriented much of the attention away from money and instead drew focus on new, general-purpose decentralized computing platforms. The development of these general-purpose decentralized computing platforms proved attractive to many industry verticals, including banking, insurance, gaming and gambling, social networking, digital content distribution, logistics, heavy and high-tech manufacturing, food safety, pharmaceutical management, and corporate governance. Practically every large technology company (from IBM to Facebook) either experimented with new cryptocurrency and blockchain-based information and management systems or retrofitted their existing systems. Today, many of these systems are in development, have launched, or have since shuttered as hype came and went.

Academic research followed the transition from Bitcoin to blockchain and flourished. By 2016, cryptocurrencies and blockchains had entered mainstream academic discourse. Today, published journal articles on cryptocurrencies and blockchain technologies number in the thousands, dozens of monographs and edited collections have been published, and hundreds of academic workshops and conferences have taken place.

2.1 Cryptocurrency and blockchain ethics literature

Despite the fact that the cryptocurrency and blockchain industry has a generally negative reputation, academic discussions about ethical behaviours and practices remain rare. Tang et al. [71] discuss the desired functionality of blockchains for ethical use; Lapointe and Fishbane [51] describe ethical design constraints as part of a practical framework for cryptocurrency and blockchain systems; Hughes [46] discusses the ethical impact of the adoption of cryptocurrencies in relation to the "digital divide;" Dierksmeier & Seele [23] survey business risks—commercial and ethical—imagining if cryptocurrencies were to be adopted broadly; Coeckelbergh & Reijers [18] develop a general normative theory of cryptocurrencies and blockchains; Angel & McCabe [3] discuss the ethics of using cryptocurrencies for payment in society; Clark et al. [16] discuss the ethical implications of using cryptocurrencies and blockchain technologies to implement new markets; and Guadamuz & Marsden [43] address the ethical challenges of researching a field characterized by anonymity. There are no prior publications addressing or assessing ethical practices for cryptocurrency and blockchain research.

There are also no specific guidelines for ethical cryptocurrency and blockchain research and few public discussions of the topic. The first and most significant discussion about ethical research and publication practices originated with journalists, who already have clear and robust guidelines. In late 2017, the journalist Felix Salmon broached the topic in a Nieman Lab blog post [67] addressing the lack of disclosures by journalists. He argued that the early experiments by journalists who bought cryptocurrencies as a way to playfully engage with the new technology were potentially serious breaches of journalistic ethics. Salmon reports that high-profile mainstream technology journalists like Farhad Manjoo, Kevin Roose, and Kashmir Hill bought and then sold Bitcoins that, if they held for more than a year, would have increased dramatically in price and put these journalists in possession of hundreds of thousands of dollars' worth of Bitcoin. Against these permissive practices, Salmon writes emphatically, "[t]oday, if you write about bitcoin [as a journalist], you can't ethically own it, any more than you can own shares directly in companies you write about" [67]. Indeed, The New York Times, which has voraciously covered cryptocurrency and blockchain news, has ethical guidelines that extend to prohibitions on buying cryptocurrencies for any journalist covering the field: "[n]o staff member may own stock or have any other financial interest in a company, enterprise or industry that figures or is likely to figure in coverage" [58]. The focus of Salmon's critique and the thrust of ethics guidelines for journalism suggests that if journalists have an economic relationship to their topic, they are unable to act impartially or write without bias (or at least they will appear as such). I argue that academic cryptocurrency

and blockchain researchers have similar issues of impartiality and disclosure but also a distinct set of challenges, which are more complex. Yet, academics have not grappled with the complexity of their research ethics.

3 Study 1: Review of Research Methods and Ethics Disclosures

It is commonly said about research that "our methods determine our ethics" [48]. To better understand this relationship, I conducted a literature review of cryptocurrency and blockchain research. This review has two goals: 1) understand what research methods are being used in cryptocurrency and blockchain research, and 2) assess the prevalence of ethics disclosures. This review found limited evidence of ethical deliberation and only a single substantial disclosure of financial conflicts of interest.

3.1 Method

Only 4% of published research on cryptocurrencies and blockchains describe a research methodology. Typically, only empirical research includes discussion of research methodology. Likewise, only empirical research methods discuss research ethics because empirical research methods have *a priori* greater risk of harm. Therefore, empirical research methods are the subject of ethical concern and oversight in ways that non-empirical methods are not.

Based on an initial exploration of the literature, the main methods for empirical research on cryptocurrencies and blockchains were found to be interviews, surveys, passive measurement, and active measurement (as well as a few other less prevalent or mixed methods). Of these, passive and active measurement are common in computer science but rare in other fields, and therefore require some explanation. Passive measurement is the observation of information in its naturalistic state, especially as it is transmitted across networks. A typical passive measurement study of cryptocurrencies and blockchains might, for example, graph transactions in an attempt to find clusters and correlations or statistically study cryptocurrency exchanges for activity. Active measurement is a non-naturalistic method that introduces or alters information, typically in a network and usually with the goal of producing or inducing the studied behaviour. For example, an active measurement study might perform cryptocurrency trades and study the resulting market changes, directly attack the blockchain network to test network resilience, or attempt to exploit software vulnerabilities (the latter also falls into the category of security analysis).

It is not possible to systematically study cryptocurrency and blockchain research. Not only is the research field now rather large and heterodox, it lacks common publication venues and accepted research norms. In fact, a great deal of high-value research on cryptocurrencies and blockchains is not formally published at all, and instead resides in e-print or self-archive repositories (such as arXiv, SSRN, and institutional repositories). For these reasons, conventional methods for systematic review are not available. Therefore, this sample of research includes published and publicly-available but unpublished documents. The source of literature was the Blockchain Research Network's publication database (http://blockchainresearchnetwork.org), which, at the time of analysis (November 27, 2018) included 2090 items (with 953 full-text files) and is the largest specialized database of cryptocurrency and blockchain research.

A full-text and metadata search of the publication database resulted in an initial long list of 488 publications (searching for research method, analysis, and related terms). Publications that did not clearly identify research methods were then eliminated, resulting in a final list of 79 publications. Each publication was then read and coded for both research method and ethics disclosure or statement type. Using a reflexive, iterative process, four codes for disclosure statements were developed: institutional review (e.g., IRB), informal discussion of ethical implications, disclosure of funding sources, and disclosure of conflicts of interest.

3.2 Results

58% of the selected publications make some kind of ethics disclosure (Table 1)—most of which are *pro forma*. For comparison, in management fields, 17% of journals require ethics disclosures for compliance with Committee on Publication Ethics (COPE) guidelines, but many COPE journals are non-compliant [42]; actual disclosures in public administration (3%) and political science (12%) are lower [48].

Method	IRB	Informal	Funding	Conf. Interest	Any Disclosure
Interview (5) (6%)	1	0	0	0	1
User experience testing (1) (1%)	0	0	0	0	0
Discourse analysis (2) (3%)	0	0	1	0	1
Ethnography (1) (1%)	1	0	0	0	1
Mixed method (5) (6%)	1	0	2	1	3
Survey (16) (20%)	2	0	1	1	4
Passive measurement (40) (51%)	1	2	18	5	19
Active measurement (7) (9%)	1	4	5	0	7
Security analysis (2) (3%)	0	0	0	0	0
Totals (79)	**7 (11%)**	**6 (9%)**	**27 (34%)**	**7 (9%)**	**46 (58%)**

Table 1: Survey of research methods and ethics disclosures made in empirical cryptocurrency and blockchain research.

As encouraging as it might seem that cryptocurrency and blockchain research disclosure practices are numerically better than other fields, a closer look at the data reveals a different story. Nearly half of all statements were for disclosing funding sources (27 publications), which is a practice commonly used to give credit to funders and has limited ethical utility. When this category of disclosure is omitted from analysis, empirical cryptocurrency and blockchain research with ethical disclosure statements drops to only 20 publications, or about 25%.

The few publications that included financial conflicts of interest statements were clearly obligatory. The one exception is Athey et al. [4], which included a link to an online conflict of interest disclosure (Athey was then at MIT and advisor for several cryptocurrency companies, including CoinCenter, an industry lobby and advocacy group). Similarly, the lack of engagement with formal (and typically obligatory) ethical research processes like institutional review (REBs/IRBs) is notable.

4 Study 2: Survey of Ethical Risks

To better understand the range of possible ethical research practices, including formal disclosures, informal and ad-hoc justifications, research practices that occur before and after the formal research period, and interactions with industry, I conducted a survey of cryptocurrency and blockchain researchers.

4.1 Method

Participants were recruited for an online questionnaire through email. 206 "active" researchers were identified from publication data on the Blockchain Research Network, where "active" was defined as any scholar with two or more publications. This resulted in 192 invitation emails sent on June 21, 2018. The survey closed on August 13, 2018.

The questionnaire received 32 complete responses (17% response rate). The questionnaire contained 37 questions, which were designed to collect researcher practices and opinions.

Over half (57%) of the respondents were affiliated with engineering and computer science; social sciences were the second most common affiliation (27%). Respondents' job status skewed towards those in senior positions. Most respondents had studied cryptocurrencies and blockchains for two to four years (32%), yet a considerable number reported studying the field for five-to-six years (29%) or more than six years (26%). Similarly, the largest proportion (44%) reported having more than five publications in the field. Most had received funding for their research (overall 70%; engineers and computer scientists: 93%), but only a minority (25%) were currently a lab director or principal investigator.

Results were analysed to identify patterns of research ethics awareness, knowledge, and behaviour. Since many of the survey questions were informed by prior analysis of literature and observed behaviour in the field, questions were designed to target particular ethical issues in an attempt to validate previously identified hypotheses ("validate" in the weak sense of convergent observations). This approach can be considered a form of "triangulation" [47], where the overall goal was a "holistic" and "contextual" portrayal of the data.

4.2 Results

The survey reports on six themes. I describe each theme individually and then identify and compare ethical research risks to draw out broader implications.

4.2.1 Research methods used

Survey participants reported using methods that roughly match the major dimensions of the publication analysis (compare Table 1 and Table 2; n.b., non-empirical methods were absent from publication analysis). Overall, survey participants used passive measurement methods the most (53%), followed by humanistic or philosophical inquiry (47%) and security analysis (40%) (participants could select more than one method) (Table 2).

Method	#	%
Humanistic or philosophical inquiry	14	47%
Qualitative social science methods	9	30%
Quantitative social science methods	8	27%
Passive computer & networking measurement	16	53%
Active computer & networking measurement	8	27%
Security analysis	12	40%

Table 2: Methods used by all participants (multiple selections possible).

4.2.2 Awareness of ethics guideline

Survey respondents were aware of their professional associations' and university's ethics guidelines, however, they tended to not use REBs/IRBs. Most survey respondents knew of the existence of their academic associations' codes of ethics (55%) and were aware of the contents (82% were "somewhat" or "very" aware). The professional associations with the most commonly cited guidelines were ACM, IEEE, USENIX, IACR, AoIR, and AAA, but these results are likely more representative of the type of respondent than true awareness or impact of guidelines. Indeed, Payne and Landry [62] report that for business and IT professionals, the diversity of extant codes is seen as confusing. Similarly, most respondents knew of the existence of their university's codes of ethics (69%) and were aware of the contents (96% were "somewhat" or "very" aware). Familiarity of ethics guidelines increases slightly with time spent researching in the field (Figure 1).

Despite the general awareness of ethics guidelines, respondents reported low use of REBs/IRBs (only 32% have "ever" submitted a REB/IRB application for cryptocurrency or blockchain research). A key factor for this low use of REBs/IRBs appears to be due to disciplinary and research norms. Specifically, the rate of use of REBs/IRBs reported by engineers and computer scientists alone (18%) is significantly

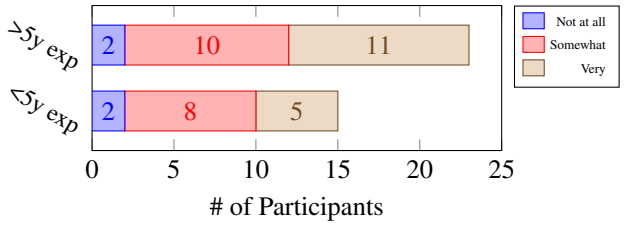

Figure 1: Familiarity with ethics guidelines (Q 5)

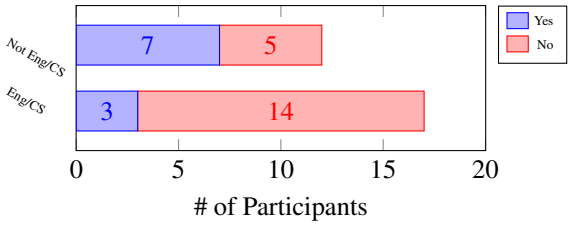

Figure 2: Have ever submitted REB/IRB application (Q 7)

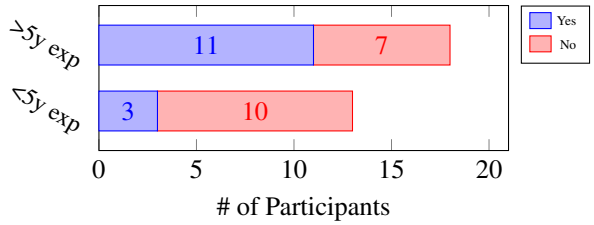

Figure 3: Purchased tokens for research (Q 18)

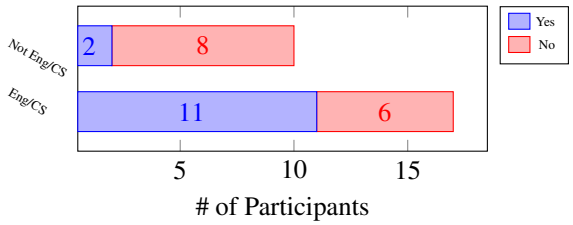

Figure 4: Purchased tokens for personal use (Q 19)

lower than those reported by all other (non-engineer/non-computer scientist) researchers (58%) (p: 0.04; Figure 2). This is hardly surprising given the views of many in the computer science and engineering fields, who tend to be unfamiliar with REB/IRB processes, find REBs/IRBs to be inadequately knowledgeable about typical engineering and computer science methods, and therefore tend to have a pessimistic outlook on the value of REBs/IRBs [34, 35].

4.2.3 Ethics and pedagogy

Most respondents taught students about cryptocurrencies or blockchains (88%), with about half of the respondents (54%) teaching engineering and computer science students. Of these, twice as many discussed ethical issues (66%), compared to those who did not (33%). But, only one in ten used a formal guideline or code of ethics when discussing ethical issues with students.

4.2.4 Software vulnerability disclosure

Most (65%) engineering and computer science respondents reported doing computer security analyses (such as intrusion testing or code analysis). Of these respondents, the majority (73%) found errors or vulnerabilities in cryptocurrency and blockchain software and all (100%) reported these issues to the software developers, yet the minority (38%) were compensated for their disclosures.

4.2.5 Token ownership and disclosure

Overall, about half of the respondents (47%) reported buying tokens for research purposes, which is a similar proportion of respondents who reported buying tokens for non-research (i.e., personal) purposes (52%). However, for researchers with more than five years of experience in the field, token purchasing for research was significantly higher (59%) than those with less than five years of experience in the field (29%) (the propensity to purchase tokens for *personal* use by researchers did not vary with experience) (Figure 3). One demographic segment, however, tells a different story: engineering and computer science researchers reported buying tokens for *personal* use much more often than those in other disciplines (61% and 23%, respectively) (p: 0.02; Figure 4).

Very few respondents reported disclosing their token holdings in academic publications (6%) or online (16%), despite the fact that many (38%) of the respondents who purchased tokens for either research or personal uses reported personally profiting from their token holdings. Similarly, while three-quarters (75%) of respondents have written about cryptocurrencies or blockchains online, only 8% made disclosures online about either token holdings or advisory roles with companies.

4.2.6 Industry relations

Slightly fewer than half of all respondents (44%) reported advising, consulting, or working for cryptocurrency and blockchain companies. Of those, just under half (43%) also reported being compensated for their work within industry. Researchers were commonly *solicited* for work within industry: of all respondents, three quarters (75%) reported being invited to advise, consult, or work for a company. Of those, all but one had been invited to work for a company in the last year, and a quarter (27%) reported being invited at least once in the last year. The reasons given by researchers for why they are being so actively recruited vary, but most cite their

expertise (93%), their reputation (64%), and their university's reputation (36%) (multiple selections possible).

Finally, respondents hold generally negative views about the ethical practices of the cryptocurrency and blockchain industry. Nearly half of the respondents reported feeling that the industry is "neither ethical nor unethical" (44%) (the term "neutral" was purposely avoided in the survey), but a sizable proportion reported feeling that the industry is "somewhat unethical" (36%) or "highly unethical" (16%). Only one respondent reported that the industry is "somewhat ethical" and none reported that the industry is "highly ethical."

5 Discussion: Cross-Domain Analysis of Research Ethics Risks

This article identified ethical research risks using a two-step study. Based on these findings, in the next section three areas of ethical risk are highlighted and comparisons are drawn between "conventional" research risks and emerging risks in cryptocurrency and blockchain research.

5.1 Conflicts of interest

When considering the risks of industry involvement in research, the most commonly cited issues stem from conflicts of interest, and especially financial conflicts of interest. This is particularly true for research that can be easily commercialized, such as biomedical and agricultural research. Conflicts of interest are defined as "a set of conditions in which professional judgment concerning a primary interest... tends to be unduly influenced by a secondary interest" [72]. Conflicts of interest include, for example, payment for consulting and services, stock and equity ownership, holding a position on a board of directors, and industry sponsorship of research. Many ethicists believe that contemporary research necessarily entails conflicts of interest and while it may seem like researchers ought to eliminate all conflicts of interest, such a goal is neither practical nor desirable [41, 66].

Financial conflicts of interest are extremely common but relatively straightforward to regulate. Guidelines are a key tool for regulation, which may be issued by institutions, professional associations, and funding agencies [66]. Institutions, such as laboratories and universities, typically require self-disclosure of financial conflicts of interest by researchers, but since it is not in the interest of institutions to prevent commercial activity [32], institutional prohibition is rare. Funding agencies, especially those responsible to the public, have somewhat more robust guidelines and enforcement mechanisms. For instance, the U.S. Department of Health and Human Services (HHS), Public Health Service (PHS), and the National Institutes of Health (NIH) issued guidelines stipulating that researchers must disclose personal financial interests in excess of $5,000. The National Science Foundation (NSF)—a dominant funder of cryptocurrency and blockchain research in the U.S.—mirrored the HHS/PHS guidelines [66], but opted for a $10,000 threshold. However, except for serious breaches of research ethics, often prompted by media coverage, government enforcement of conflicts of interest guidelines is rare [6].

While seldom included in regulatory guidelines, *non-financial* conflicts of interest are more common and potentially more deleterious than financial conflicts of interest [20, 52, 68]. For example, Saver [68] points out that none of the most-cited violations of research ethics involved financial conflicts of interest, including the Tuskegee Syphilis Study and the injection of live cancer cells into elderly patients, which led to the enactment of the National Research Act of 1974. Non-financial conflicts of interest include receiving gifts (e.g., lab equipment or access to datasets) and creating or maintaining personal relationships. These kinds of non-financial conflicts of interest have caused research violations that led to harm, faked and withheld scientific data, and biased and uncritical research [68]. By focusing regulations solely on simple *financial* conflicts of interest, many potentially deleterious research practices are being ignored.

Yet, conflicts of interest often result from the best of intentions. "People overestimate their willpower, objectivity, and ability to compartmentalize" Curzer and Santillanes [20] write, "while underestimating the strength of temptations, their tendency to rationalize, and ability to ignore the twinges of conscience." It is underappreciated that, in many cases, the *social* relationships between researchers and industry sponsors create the most serious conflicts of interest [68].

Conflicts of interest also degrade public trust in science [32, 52, 66]. The public's trust in science is essential for the adoption of science-based policy recommendations. Yet, universities often encourage entrepreneurial activities that potentially undermine research objectivity [32]. Entrepreneurial activities also undermine the educational mission of universities, since students [64] and the public [66] have been shown to be incapable of accurately identifying conflicts of interest and their real influence.

Conflicts of interest are a common and normal part of research. In biomedicine, Bekelman et al. [7] report that U.S. industry funding nearly doubled (from 32% to 62%) between 1980 and 2000, resulting in a quarter of biomedical researchers having industry affiliation and roughly two thirds of academic institutions holding equity in startups that sponsor research performed at the same institution. This has resulted in a measurable bias towards pro-industry conclusions, as well as the withholding of data and delay of publication [7, 20, 41]. Results are roughly similar for other research fields. From 1980-1999, 8% of all externally-funded researchers reported conflicts of interest, and almost twice as many reported conflicts of interest involving stock or stock options [36]. A study conducted in 2000 reported that the average value of industry sponsorship across all faculty was US $100,000, with many researchers receiving stock valued

at more than US $1 million [36]. More recently, Gottlieb [41] reports that half of all academic scientists are also consultants or have served on scientific advisory boards for industry. Yet, despite growing industry influence, biomedical research—and research more generally—has increasingly moved *away* from prohibition of financial conflicts of interest and instead moved towards risk-based models that manage conflicts of interest through disclosure.

Until recently, leading medical journals like the *New England Journal of Medicine* and the *British Medical Journal* banned publications from authors with ties to industry [15,26]. These bans were prompted by well-publicized exposés about the corrupting influence of industry-sponsored research, especially from the tobacco industry. While these publication bans provided a bright line for researchers (as do prohibitions against equity ownership for journalists, discussed above), "zero-tolerance" approaches proved misguided in their simplicity. Publication bans in biomedical research have since eased to accommodate a balance between research and industry and to broaden the potential pool of authors, since finding researchers with no ties to industry was becoming difficult and burdensome [39].

5.2 Conflicts of interest facing cryptocurrency and blockchain researchers

Cryptocurrency and blockchain researchers have many of the same kinds of conflicts of interest as other researchers—from compensation for consulting to personal bias—but, the prevalence of industry sponsorship and the unique technologies used for research present new and novel challenges.

The cryptocurrency and blockchain industry requires a steady stream of research to drive innovation, just like any other high technology industry, which necessarily introduces institutional conflicts of interest [60]. From 2015, when cryptocurrency and blockchain companies exploded into the mainstream, until the market downturn in 2018, industry-sponsored research had been generous (it still continues, but at lower rates). Recent examples of startups investing in sponsored-research are illustrative of this trend: Ripple created a US $54 million university research fund by partnering with 17 universities; Dash provided Arizona State University with US $350,000 to establish a research lab and award student scholarships; Tezos awarded research grants to Cornell University, the University of Beira Interior, the University of Illinois at Urbana-Champaign, and France-IOI; IOHK created a funded research chair at the Tokyo Institute of Technology and provided US $500,000 to the University of Edinburgh to set up a research lab; Brave recruited a "Visiting Researcher," and many university-based research labs (such as University of British Columbia and Cornell University) have "partnerships" with industry.

Startups often look for affiliation with name-brand universities to garner reputation, which is a valuable commodity for an industry marred by illegality and scams [45,73]. Sponsored research potentially creates a "halo" of positive press and the appearance of propriety. DuPont [27] found that investors highly value startups' research and development teams, even if in reality many of these relationships are little more than a thin attempt to leverage a university's sterling reputation. One of the key ways that startups "buy" a university's reputation is by recruiting university researchers as compensated "advisors" who do not necessarily provide expert guidance. Retaining Nobel Laureates as advisors—at least four are currently working with cryptocurrency and blockchain startups [74]—is a high profile example. Other researchers with top-tier credentials and reputations have helped launch notable startups and have taken advisory positions, usually accompanied by media attention but not formal disclosure.

In the best cases university researchers are positively contributing to company strategy and product development through their advisory roles [56, 63]. And, while any researcher is unlikely to be able to speak truly independently about a company or product when directly compensated, it must be stressed that financial conflicts of interest do not *necessarily* preclude unbiased and accurate research in general.

Finally, a novel source of conflict of interest arises for researchers who must purchase and use cryptocurrencies to conduct research. For many researchers and developers, cryptocurrencies or tokens must be purchased to conduct experiments, such as monitoring network performance, manipulating markets, and running security tests. However, ownership of valuable assets automatically creates conflicts of interest, which are also risks inherited by the infrastructures these assets are integrated into. With rapidly fluctuating price and no clear guidance for experiment lifecycle or protocols for disposal of tokens, researchers often find themselves in possession of very valuable assets at the conclusion of their research. It is a nearly-inescapable yet problematic feature of studying cryptocurrencies and blockchains that researchers often must "pay to play."

5.3 Risky research methods

The widespread adoption of information and communication technologies (ICTs) brought about new opportunities for research, but also introduced new research risks [11]. For the last two decades, ethicists have been puzzling over these new research challenges and developing guidelines, such as the AoIR and ACM codes of ethics [31, 53] and the Menlo Report [25]. Despite these advances, cutting-edge research methods and new and novel technologies have proliferated with little ethical debate. The field of computer and network security has been at the forefront of these developments—inventing controversial research techniques such as hacking, penetration testing, honey-potting, spoofing, and network manipulation [8, 24, 49, 54, 59, 61]. The intersection of controversial new computer and network security research methods and

the financial and monetary dimensions of cryptocurrencies further challenges research ethics.

For conventional research, institutional review in the form of IRBs/REBs, has been the first and often last line of defence against research abuses. Institutional review emerged out of recommendations from the Declaration of Helsinki (1964) and the Belmont Report (1979), which originally convened over concerns about high-profile cases of research abuse. Institutional review has since taken on a hybrid role in research ethics, "situated... somewhere in between administrative tribunals and administrative licensing boards" [52].

As effective as institutional review has been for ensuring safe research practices, some critics argue against the appropriateness and value of institutional review for situations that do not involve conventional notions of human subjects research [1, 11, 48]. This is particularly true for computer science and engineering fields [2, 5, 19, 34, 35]. Many scholars worry about "ethics creep" resulting from the increased scope and power of institutional review boards (a form of bureaucratic expansion) and institutionalized distrust of researchers [44]. On the other hand, a case can be made for institutional review to protect against new forms of research harm not typically associated with "human subjects" but that are no less harmful, such as "information risks" [22].

5.4 Risky cryptocurrency and blockchain research methods

While most cryptocurrency and blockchain research is conventional in design—using well-established protocols for surveys, interviews, ethnographies, and case studies—security analyses of cryptocurrencies and blockchains, in particular, introduces new, novel, and risky methods. Despite these risks, this research is also vitally important to ensure safe, effective, and error-free systems.

There are many controversial cryptocurrency and blockchain research methods, especially those that use deception, manipulation, system "attacks," and de-anonymization or personally-identifying account clustering. In computer and network security literature a distinction is usually made between methods that are "passive" and "active." Because passive measurement resembles traditional scientific practice, insofar as it measures computer and network phenomena naturalistically, it is less controversial. However, many passive studies have unintended consequences. Consider, for example, research that studies the activities of cryptocurrency investment algorithms. Stubbings [70] and Gandal et al. [33] each found evidence of illegal manipulation of cryptocurrency markets. By revealing illegal activities, their findings unwittingly put their research subjects at risk, who did not consent to be studied and were unaware of their participation in research.

Active measurement is controversial because it *creates* or *induces* the phenomena that is measured or studied. Active research often focuses on illegal and unethical activities, such as spam or manipulation. In some cases, active research sustains infrastructure services that are commonly used for illegal activities, entangling researchers with the activities of their research. Examples in computer and network security include creating virus honeypots, controlling botnets, and launching phishing attacks. Similar issues occur with cryptocurrency and blockchain research; consider the Bitcoin network research by Meiklejohn et al. [55]. To study activities on the Bitcoin network, Meiklejohn et al. [55] used Bitcoins to make hundreds of purchases, which included participation in gambling sites and the use of controversial "mixing" services. Mixing services are especially problematic, since they work by aggregating transactions to obfuscate buyers and sellers for the purpose of anonymous online commerce. Even though mixing services have legitimate uses (increased privacy), they are overwhelmingly associated with illegal activities, such as money laundering and drug dealing. Meiklejohn et al.'s research [55] is controversial because gambling and mixing services each *require* for their use active participation by a network of users (which, in this case, included the researchers).

Developing research methods capable of exploring anonymous networks can have wide-reaching and unintended effects beyond the scope of research. In particular, analysis techniques developed by researchers might also be used by criminals or law enforcement. This is not a speculative risk; there are several examples of social science researchers being legally forced to disclose methods or provide access to raw (un-anonymized) research data for use in police investigations [44]. Something similar has already happened with cryptocurrency and blockchain research: it appears that Bitcoin de-anonymization research has been provided to law enforcement [29].

Perhaps the most ethically fraught research practices are those that "attack" cryptocurrencies and blockchains, using techniques like hacking, penetration testing, and security code analysis. "Ethical" hacking (called "White Hat" hacking) and "ethical" penetration testing (called "Red Teaming") have always been controversial aspects of computer security research [8], but they are generally accepted practices so long as proper procedures are followed and disclosures are made. Computer security disclosure, a responsible research "best practice," also has, as I discuss below, myriad ethical issues, including controversial financial incentives for hacking and "bug markets" that encourage researchers to find and expose security exploits.

It is in the context of cryptocurrency and blockchain hacking that Philip Daian [21], a PhD student at Cornell University, conducted a non-scientific poll of the practitioner and academic community on Twitter. Daian asked the community whether they thought it was ethical to ask students to hack live smart contracts in the classroom (Figure 5). (A smart contract is quasi-legal automated code running on top of a blockchain that is often used to secure cryptocurrencies.) The

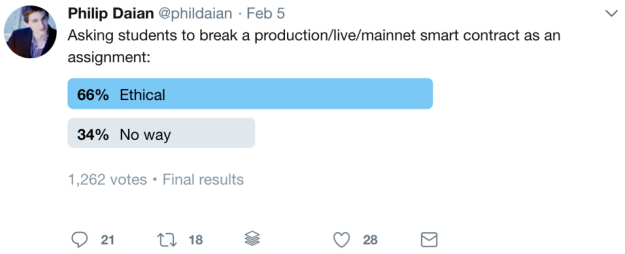

Figure 5: Philip Daian's Twitter poll.

general consensus from the community was that the practice is acceptable. From a normative perspective, these are notable results. In case there is any doubt, Daian's reply to his poll highlights the severity of the ethics at hand: he asked, "... if you find a $10M quick-cash exploit during... homework, do you take the 10 points or the [$]10M?" [21].

While teaching ethical hacking in classrooms is necessarily a controversial practice in any context, the fact that smart contracts directly protect valuable assets further complicates matters. Hacking a smart contract is functionally identical to accessing the cryptocurrency assets, which therefore relies *entirely* on the moral fortitude of students to not run off with the exfiltrated funds. Indeed, because most cryptocurrencies are pseudonymous, students learning the craft could make off with funds and nobody would know that the theft occurred or who perpetrated it. As students are increasingly exposed to these exercises, more and better ethics training and safeguarding needs to be introduced into the classroom.

5.5 Disclosure practices

Disclosure is the practice of informing stakeholders about relevant concerns. In research, disclosure is essential to the overarching goals of scientific publication. Typical disclosure practices range from optional to mandatory and include ethics disclosure (informing the readership that appropriate care was taken when conducting research), conflict of interest disclosure (informing the readership about potential biases so that conclusions can be exposed to appropriate skepticism), and specialized types, like software vulnerability disclosure (informing software producers about discovered vulnerabilities so that they can be fixed). While disclosure is not a perfect solution to the many issues facing research ethics, when performed openly and candidly it is generally considered best practice [9, 50].

Disclosure of financial conflicts of interest is perhaps the most common requirement because financial conflicts are among the easiest to regulate and the corrupting effects are so prevalent. Typically, institutions create guidelines for disclosing financial conflicts of interest that have clear rules (minimum values for reporting) and establish frameworks for monitoring compliance and punishment for non-compliance. As with all kinds of disclosure of bias, disclosure of financial conflicts of interest allows concerned parties to evaluate and monitor research and helps to prevent the erosion of public trust [36, 66]. However, despite being among the easiest forms of disclosure to regulate, actual compliance is rare. Even among journals with stated disclosure policies, Bekelman et al. [7] found that in the biomedical field—well known for its cozy relationship to industry—"few articles contained financial conflict disclosures."

Some research ethicists are critical of the overreliance on disclosure practices, finding that they are ineffective and inappropriate. Citing evidence on the lack of efficacy of disclosure practices, Capps [14] argues that a "funding effect" is visible even when direct financial ties are disclosed. Greenwood, on the other hand, argues that by requiring journals to monitor and discipline disclosure practices journals have to take on an inappropriate "policing role" [42].

More worrisome still, disclosure practices sometimes put researchers at risk. For instance, good-faith whistleblowers are often poorly protected by their institutions [57]. Even in the course of "normal" disclosure, as in the case of reporting adverse events, researchers may hesitate to act ethically out of fear of reprisal or due to the consequences of their disclosure. The well-known case of Nancy Olivieri, the University of Toronto hematologist who published results showing that an experimental drug's efficacy was declining and causing serious adverse effects, is illustrative. In response to the publication, the drug company attacked the integrity of Olivieri and her research. Both the university and the medical hospital worried that the drug company might withdraw research support and therefore allowed unsubstantiated misconduct allegations to be pursued [41].

5.6 Cryptocurrency and blockchain disclosure practices

Many of the same fears of industry retribution and lack of institutional protection are present in cryptocurrency and blockchain research. Yet, disclosure practices in cryptocurrency and blockchain research—as rare as they are—introduce novel kinds of risk due to their technical design and the social contexts they operate within.

In 2018, Cory Fields, a software developer working at the Massachusetts Institute of Technology, discovered a critical vulnerability in the widely used Bitcoin Cash client software. Upon discovering the vulnerability, Fields disclosed it to the software developers. But, Fields [30] felt that he had to make the disclosure anonymously. Fields recognized that in disclosing the vulnerability, which affected many thousands of running clients that were keeping secure billions of dollars' worth of cryptocurrency, he was also announcing that *he* was capable of exploiting the vulnerability. And, Fields knew that others—criminals—might have previously been aware of this vulnerability and already exploited it. Had Fields submitted

his vulnerability disclosure publicly, and had the vulnerability already been exploited, he would have been susceptible to claims that he was the one who had perpetrated the theft. In fact, due to the pseudonymous nature of Bitcoin Cash, he would have had no way to prove otherwise. Citing examples like this, Sirer [69] calls cryptocurrency and blockchain disclosure a "choose-your-own-security-disclosure-adventure" and argues that such practices are fundamentally inappropriate for cryptocurrencies and blockchains worth billions of dollars. Given the many ways that existing products and infrastructures are currently being "tokenized" by integrating cryptocurrency and blockchain technologies (from electricity distribution to home rentals), disclosure practices across the field of software engineering will need to change to accommodate these new ethical risks.

Fields' software vulnerability disclosure is not the only unique challenge facing cryptocurrency and blockchain research disclosure practices. As described above, cryptocurrency and blockchain researchers often have financial conflicts of interest due to the fact that their experimental material—cryptocurrency and blockchain tokens—are necessarily valuable. Due to this conflict of interest, some researchers have turned to a negative-disclosure practice as a potential solution—taking the firm stance of refusing to buy cryptocurrencies or blockchain tokens. These individuals are known, with some derision in the user community, as "nocoiners." While nocoiners have a simple solution and bright line for ethical research practice, much like medical journals that ban publications associated with industry funding, they draw these lines to the potential detriment of their own research. In many cases, active participation (which means "buying in") is the only way to truly understand a technology or a community. Nocoiners lose the privileged access and the deep understanding that participation and engagement produces.

6 Conclusion: Risks from a New Normative Class of Technology

In recent years there has been a nascent but encouraging move towards deeper ethical engagement across the industry, including efforts at standardization and the development of tools to align ethics and software development [28, 51]. Despite these encouraging signs, however, researchers and developers have yet to fully grasp the real risks involved in their work. To date, no specific guidelines or tools have been developed to support research in this field. Conflicts of interest, through association with industry or experimentation with valuable tokens, are rampant and underreported. Not engaging these conflicts of interest—the nocoiners solution—however, comes with significant drawbacks and while candid disclosure offers a way forward, it too introduces novel risks. Finally, many research methods, especially those associated with security research, are important and necessary to ensure the safe use and development of these technologies, but with few guidelines in place they also pose real risk to unwitting users who typically do not consent to be research subjects.

As these systems continue to develop and are further integrated into existing technologies, their research risks will become more pervasive. This risk of "ethical contagion" is much broader than typically realized and reaches beyond the weird and woolly world of cryptocurrencies and blockchains. Addressing these risks of contagion requires identifying site of intervention in the innovation value chain. Burt [13], for example, found that "structural equivalence" (the degree to which people occupy the same position in the social structure) rather than "coherence" (conversations with colleagues) was a better predictor of an innovation's adoption. Burt [13] also found that contagion in innovation arose "from people proximate in social structure using one another to manage the uncertainty of innovation." Extending Burt's findings to financial technologies helps explain why this study found cryptocurrency and blockchain researchers to be well informed about ethics but still engaged in risky behaviours, as a sector-wide norm. Such in-group dynamics remain underexplored in the cryptocurrency and blockchain sector, but as strong motivators for behaviour they also recommend potential solutions for ethical regulation.

Similarly, social network analysis has shown that the spread of ethical behaviour has to do more with *types* of relationships than mere exposure to deviance [10]. For example, Gino, Ayal, and Ariely [37] and Gino, Gu, and Zhong [38] found that in laboratory settings exposure to dishonest in-group members had a contagious effect, but the effect was modulated by out-group observation. Therefore, monitoring by, but especially *collaboration with*, norms-setting bodies, including IRB, ought to be strengthened throughout the sector, but with better aligned goals and less cross-disciplinary animosity. Norms-settings bodies might even begin to look at the nascent field as an opportunity—not a burden—for ways to explore working intensively with these kinds of fast-paced technology sectors.

Cryptocurrency and blockchain researchers and developers for their part *ought to seek ethics solutions from within their toolkit*, innovating for "ethics tech" in much the same way that "regtech" has become a key line of business in the industry. As is widely acknowledged, these powerful cryptoeconomic systems excel at producing designed human behaviours and their range of potential innovation far exceeds the traditional technology goals of efficiency, reliability, security, and profit. While this article identified ethical behaviour within the research and development community as a risk today, in the future ethical research and development *using* cryptocurrency and blockchain technologies may be an opportunity for growth.

Perhaps the most challenging ethical risk to overcome is that cryptocurrencies and blockchains are a unique class of ethical and normative activity, comparable to fields such as

bio- or nanotechnology ethics. Mark Coeckelbergh's pioneering work on "money machines" [17] has already introduced a general ethical principle for the development and adoption of such systems, arguing that they create moral "distance" among people and their relation to the world. This moral distance may result in diminished care for others and the environment. Extending Coeckelberg's analysis to the research and development context, the challenge of studying this technology is that it is not just *valuable* but *value* itself (*per se* value). While the de novo or "fiat" nature of money has long been studied, until recently—with Bitcoin's turn towards technicity and alegality—*per se* value has seldom been directly, that is, empirically, researched and developed. As *per se* value technologies, cryptocurrencies and blockchains are united as a class of ethical and normative activity, which demands *unique* ethical attention.

This comparison with living (bio-) and very small (nano-) technologies has deep social relevance but we are only at the beginning of understanding how to research "value" technologies. Nonetheless, while further study is required, some practical principles for guiding ethical research can be described.

7 Eight Guiding Principles of Ethical Cryptocurrency and Blockchain Research

1. **Develop a research lifecycle:** plan for acquisition and disposal of cryptocurrency and blockchain assets, ensuring that disposal does not further create conflicts of interest (charitable donation is an option).

2. **Use (and educate) IRBs:** don't depend on IRBs to understand the complexities of cryptocurrency and blockchain research, but take the opportunity to educate them and engage in a dialogue about ethical research.

3. **Disclose conflicts of interest:** include financial and non-financial disclosures of COIs when publishing research (especially when value exceeds US $5,000 or 5% ownership over the last 12 months), but also consider publishing a historically complete record online.

4. **Consider alternatives, testnets, and bright-line prohibitions:** conduct research (and education) using less ethically risky alternatives or testnets; in some cases, bright-line prohibitions should be established in advance to limit risk.

5. **Protect and dispose of dangerous methods:** avoid creating (executable) dual-use research methods (such as de-anonymizing methods) and otherwise protect methods and dispose of them immediately at the conclusion of the research lifecycle.

6. **Disclose software vulnerabilities:** current best-practice software vulnerability disclosure practices are not well-suited to cryptocurrency and blockchain research, but until better practices are developed, immediately disclose software vulnerabilities to software developers.

7. **Minimize value exchanges:** acquire or purchase the minimum value of assets necessary for research (none if possible).

8. **Develop lab guidelines:** work towards developing a usable set of internal research guidelines; consider engaging inter-disciplinary researchers outside of your research team.

Immediately and with some urgency, work is needed to establish robust guidelines for cryptocurrency and blockchain research and any future "value" technologies, ideally across academic, industry, and government stakeholders. In a gesture towards this future, this article investigated the prevalence of ethics disclosures in the literature, surveyed researchers about their ethical practices and opinions, and analysed the unique challenges facing the ethical research of cryptocurrencies and blockchains, warning of further risks as technologies are integrated across infrastructures.

Acknowledgments

I would like to thank Megan Finn and Katie Shilton for their support.

This research is supported by NSF grant #1634202

Availability

Appendix A: Publication data deposited at Mendeley Data: https://data.mendeley.com/datasets/cwzfpkpn67/1

Appendix B: Questionnaire response data deposited at Mendeley Data: https://data.mendeley.com/datasets/cwzfpkpn67/1

8 Declaration of Interests

I have small holdings of cryptocurrencies that change composition and value frequently, typically worth less than US $2,000. I work with a variety of cryptocurrency and blockchain companies and organizations and are compensated in USD or cryptocurrency for this work. My up-to-date declaration of interests can be found on my personal website: http://iqdupont.com

9 Ethical Approval

All procedures performed in this study involving human participants were in accordance with the ethical standards of the

institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards. Informed consent (where possible) was obtained from all individual participants included in the study.

This research was approved by University of Washington Institutional Review Board.

References

[1] Rachel Aldred. Ethical and Political Issues in Contemporary Research Relationships. *Sociology*, 42(5):887–903, October 2008.

[2] Mark Allman. What Ought a Program Committee to Do? In *Proceedings of the Conference on Organizing Workshops, Conferences, and Symposia for Computer Systems*, WOWCS'08, pages 3:1–3:5, Berkeley, CA, USA, 2008. USENIX Association.

[3] James J. Angel and Douglas McCabe. The Ethics of Payments: Paper, Plastic, or Bitcoin? *Journal of Business Ethics*, 132(3):603–611, 2015.

[4] Susan Athey, Christian Catalini, and Catherine Tucker. The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. Working Paper 23488, National Bureau Of Economic Research, Cambridge MA, June 2017.

[5] J. Aycock and J. Sullins. Why "No Worse Off" Is Worse Off. In *2013 IEEE Security and Privacy Workshops (SPW)*, pages 1–4, May 2013.

[6] Mark Barnes and Patrik S. Florencio. Investigator, IRB and Institutional Financial Conflicts of Interest in Human-Subjects Research: Past, Present and Future Symposium: New Directions in Human Subject Research: Looking beyond the Academic Medical Center. *Seton Hall Law Review*, 32:525–562, 2001.

[7] Justin E. Bekelman, Yan Li, and Cary P. Gross. Scope and Impact of Financial Conflicts of Interest in Biomedical Research: A Systematic Review. *JAMA*, 289(4):454–465, January 2003.

[8] M. Bishop. About Penetration Testing. *IEEE Security Privacy*, 5(6):84–87, November 2007.

[9] Jeff Bollinger. Economies of Disclosure. *SIGCAS Comput. Soc.*, 34(3):1–1, December 2004.

[10] Daniel J. Brass, Kenneth D. Butterfield, and Bruce C. Skaggs. Relationships and Unethical Behavior: A Social Network Perspective. *Academy of Management Review*, 23(1):14–31, January 1998.

[11] Elizabeth A. Buchanan and Charles Ess. Internet Research Ethics: The Field and Its Critical Issues. In *The Handbook of Information and Computer Ethics*, pages 273–292. John Wiley & Sons, Ltd, 2009.

[12] Matthew Budman, Blythe Hurley, Abrar Khan, and Nairita Gangopadhyay. 2019 Global Blockchain Survey: Blockchain Gets Down to Business. Technical report, Deloitte Insights, 2019.

[13] Ronald S. Burt. Social Contagion and Innovation: Cohesion versus Structural Equivalence. *American Journal of Sociology*, 92(6):1287–1335, May 1987.

[14] Benjamin Capps. Can a Good Tree Bring Forth Evil Fruit? The Funding of Medical Research by Industry. *British Medical Bulletin*, 118(1):5–15, June 2016.

[15] Mabel Chew, Catherine Brizzell, Kamran Abbasi, and Fiona Godlee. Medical Journals and Industry Ties. *British Medical Journal*, 349:g7197, November 2014.

[16] Jeremy Clark, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Miller, and Arvind Narayanan. On Decentralizing Prediction Markets and Order Books. In *Workshop on the Economics of Information Security*, State College, Pennsylvania, 2014.

[17] Mark Coeckelbergh. *Money Machines: Electronic Financial Technologies, Distancing, and Responsibility in Global Finance*. Ashgate, Farnham, Surrey ; Burlington, VT, 2015.

[18] Mark Coeckelbergh and Wessel Reijers. Cryptocurrencies as Narrative Technologies. *ACM SIGCAS Computers and Society*, 45(3):172–178, 2016.

[19] John Craynor. Ethical Concerns in Computer Security and Privacy Research Involving Human Subjects. In Radu Sion, Reza Curtmola, Sven Dietrich, Aggelos Kiayias, Josep M. Miret, Kazue Sako, and Francesc Sebe, editors, *Financial cryptography and data security: revised selected papers*, Lecture Notes in Computer Science, Tenerife, Canary Islands, Spain, January 2010.

[20] Howard J. Curzer and Gary Santillanes. Managing Conflict of Interest in Research: Some Suggestions for Investigators. *Accountability in Research*, 19(3):143–155, May 2012.

[21] Philip Daian. "Asking students to break a production/live/mainnet smart contract as an assignment:", February 2018.

[22] Norman K. Denzin. IRBs and the Turn to Indigenous Research Ethics. In *Access, a Zone of Comprehension, and Intrusion*, pages 97–123. Emerald Group Publishing Limited, 2008.

[23] Claus Dierksmeier and Peter Seele. Cryptocurrencies and Business Ethics. *Journal of Business Ethics*, August 2016.

[24] David Dittrich, Michael Bailey, and Sven Dietrich. Have we Crossed the Line? The Growing Ethical Debate in Modern Computer Security Research. In *16th ACM Conference on Computer and Communications Security (CCS 2009)*, 2009.

[25] David Dittrich and Erin Kenneally. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. Technical report, Department of Homeland Security, Washington DC, August 2012.

[26] Jeffrey M. Drazen and Gregory D. Curfman. Financial Associations of Authors. *New England Journal of Medicine*, 346(24):1901–1902, June 2002.

[27] Quinn DuPont. *Cryptocurrencies and Blockchains*. Digital Media and Society. Polity Press, Cambridge, UK, 2018.

[28] Quinn DuPont and Wessel Reijers. Ethical and Social Impacts of Blockchain Technologies, 2018.

[29] Dmitry Ermilov, Maxim Panov, and Yury Yanovich. Automatic Bitcoin Address Clustering. Cancun, Mexico, December 2017.

[30] Cory Fields. Responsible Disclosure in the Era of Cryptocurrencies, August 2018.

[31] ACM Code 2018 Task Force. ACM Code of Ethics and Professional Conduct, June 2018.

[32] Paul J. Friedman. The Impact of Conflict of Interest on Trust in Science. *Science and Engineering Ethics*, 8(3):413–420, September 2002.

[33] Neil Gandal, J. T. Hamrick, Tyler Moore, and Tali Oberman. Price Manipulation in the Bitcoin Ecosystem. 2017.

[34] Simson L. Garfinkel. IRBs and Security Research: Myths, Facts and Mission Creep. *Proceedings of the USENIX Usability, Psychology, and Security (UPSEC)*, 8:1–5, 2008.

[35] Simson L. Garfinkel and Lorrie Faith Cranor. Institutional Review Boards and Your Research. *Communications of the ACM*, 53(6):38–40, June 2010.

[36] Robert Gatter. Walking the Talk of Trust in Human Subjects Research: The Challenge of Regulating Financial Conflicts of Interest Human Subjects Research and Conflicts of Interest. *Emory Law Journal*, 52:327–402, 2003.

[37] Francesca Gino, Shahar Ayal, and Dan Ariely. Contagion and Differentiation in Unethical Behavior: The Effect of One Bad Apple on the Barrel. *Psychological Science*, 20(3):393–398, March 2009.

[38] Francesca Gino, Jun Gu, and Chen-Bo Zhong. Contagion or Restitution? When Bad Apples Can Motivate Ethical Behavior. *Journal of Experimental Social Psychology*, 45(6):1299–1302, November 2009.

[39] Fiona Godlee. Turning the Tide on Conflicts of Interest. *British Medical Journal*, 343:1, August 2011.

[40] David Golumbia. *The Politics of Bitcoin: Software as Right-Wing Extremism*. University Of Minnesota Press, Minneapolis MN, 2016.

[41] Julie D. Gottlieb. Chapter 10 - Financial Conflicts of Interest in Research. In Mark A. Suckow and Bill J. Yates, editors, *Research Regulatory Compliance*, pages 253–276. Academic Press, January 2015.

[42] Michelle Greenwood. Approving or Improving Research Ethics in Management Journals. *Journal of Business Ethics*, 137(3):507–520, September 2016.

[43] Andres Guadamuz and Christopher Marsden. Bitcoin: The Wrong Implementation of the Right Idea at the Right Time. 2014.

[44] Kevin D. Haggerty. Ethics Creep: Governing Social Science Research in the Name of Ethics. *Qualitative Sociology*, 27(4):391–414, December 2004.

[45] Laura Higgins. Initial coin offerings - Investment or scam. *Equity*, 31(11):19, December 2017.

[46] Kobina Hughes. Blockchain, The Greater Good, and Human and Civil Rights. *Metaphilosophy*, 48(5):654–665, October 2017.

[47] Todd D. Jick. Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative Science Quarterly*, 24(4):602–611, 1979.

[48] Sara R. Jordan and Phillip W. Gray. Reporting Ethics Committee Approval in Public Administration Research. *Science and Engineering Ethics*, 20(1):77–97, March 2014.

[49] Erin Kenneally, Michael Bailey, and Douglas Maughan. A Framework for Understanding and Applying Ethical Principles in Network and Security Research. In Radu Sion, Reza Curtmola, Sven Dietrich, Aggelos Kiayias, Josep M. Miret, Kazue Sako, and Francesc Sebe, editors, *Financial Cryptography and Data Security: Revised Selected Papers*, Lecture Notes in Computer Science, Tenerife, Canary Islands, Spain, January 2010.

[50] Andreas Kuehn and Milton Mueller. Shifts in the Cybersecurity Paradigm: Zero-Day Exploits, Discourse, and Emerging Institutions. In *Proceedings of the 2014 New Security Paradigms Workshop*, NSPW '14, pages 63–68, New York, NY, USA, 2014. ACM.

[51] Cara Lapointe and Lara Fishbane. The Blockchain Ethical Design Framework. *Innovations: Technology, Governance, Globalization*, 12(3-4):50–71, December 2018.

[52] Trudo Lemmens and Benjamin Freedman. Ethics Review for Sale? Conflict of Interest and Commercial Research Review Boards. *The Milbank Quarterly*, 78(4):547–584, December 2000.

[53] Annette Markham and Elizabeth Buchanan. Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee. Technical report, Association of Internet Researchers, 2012.

[54] Andrea M. Matwyshyn, Ang Cui, Angelos D. Keromytis, and Salvatore J. Stolfo. Ethics in Security Vulnerability Research. *IEEE Security and Privacy*, 8(2):67–72, 2010.

[55] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 127–140, New York, NY, USA, 2013. ACM.

[56] Fiona Murray. The Role of Academic Inventors in Entrepreneurial Firms: Sharing the Laboratory Life. *Research Policy*, 33(4):643–659, May 2004.

[57] National Academies of Sciences, Engineering, and Medicine (U.S.), editor. *Fostering Integrity in Research*. Consensus study report. The National Academies Press, Washington, DC, 2017.

[58] New York Times. Ethical Journalism: A Handbook of Values and Practices for the News and Editorial Departments. *The New York Times*, January 2018.

[59] C.C. Palmer. Ethical Hacking. *IBM Systems Journal*, 40(3):769–780, 2001.

[60] Krsto Pandza and Paul Ellwood. Strategic and Ethical Foundations for Responsible Innovation. *Research Policy*, 42(5):1112–1125, June 2013.

[61] Craig Partridge and Mark Allman. Ethical Considerations in Network Measurement Papers. *Communications of the ACM*, 59(10):58–64, September 2016.

[62] Dinah Payne and Brett J. L. Landry. Similarities in Business and IT Professional Ethics: The Need for and Development of A Comprehensive Code of Ethics. *Journal of Business Ethics*, 62(1):73–85, November 2005.

[63] Markus Perkmann, Valentina Tartari, Maureen McKelvey, Erkko Autio, Anders Broström, Pablo D'Este, Riccardo Fini, Aldo Geuna, Rosa Grimaldi, Alan Hughes, Stefan Krabel, Michael Kitson, Patrick Llerena, Franceso Lissoni, Ammon Salter, and Maurizio Sobrero. Academic Engagement and Commercialisation: A Review of the Literature on University–Industry Relations. *Research Policy*, 42(2):423–442, March 2013.

[64] Heather Brodie Perry. Undergraduates' Perceptions of Conflict of Interest in Industry-Sponsored Research. *portal: Libraries and the Academy*, 18(1):163–182, January 2018.

[65] Ian Pollari and Anton Ruddenklau. The Pulse of Fintech 2018. Technical report, KPMG, 2018.

[66] David B. Resnik. Conflicts of Interest in Science. *Perspectives on Science*, 6(4):381–408, December 1998.

[67] Felix Salmon. Covering Bitcoin While Owning Bitcoin, December 2017.

[68] Richard S. Saver. Is It Really all about the Money: Reconsidering Non-Financial Interests in Medical Research Conflicts of Interest in the Practice of Medicine. *Journal of Law, Medicine and Ethics*, 40:467–481, 2012.

[69] Emin Gün Sirer. Choose-Your-Own-Security-Disclosure-Adventure, May 2018.

[70] Phil Stubbings. Limit Order Book Visualisation, November 2014.

[71] Yong Tang, Jason Xiong, Rafael Becerril-Arreola, and Lakshmi Iyer. Blockchain Ethics Research: A Conceptual Model. In *Proceedings of the 2019 on Computers and People Research Conference*, SIGMIS-CPR '19, pages 43–49, New York, NY, USA, 2019. ACM.

[72] D. F. Thompson. Understanding Financial Conflicts of Interest. *The New England Journal of Medicine*, 329(8):573, 1993.

[73] Marie Vasek and Tyler Moore. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. pages 44–61, Puerto Rico, 2015. Springer.

[74] Eddie van der Walt and Agnieszka de Sousa. New Weapon for Blockchain Startups: Nobel Prize-Winning Brains. *Bloomberg*, September 2018.