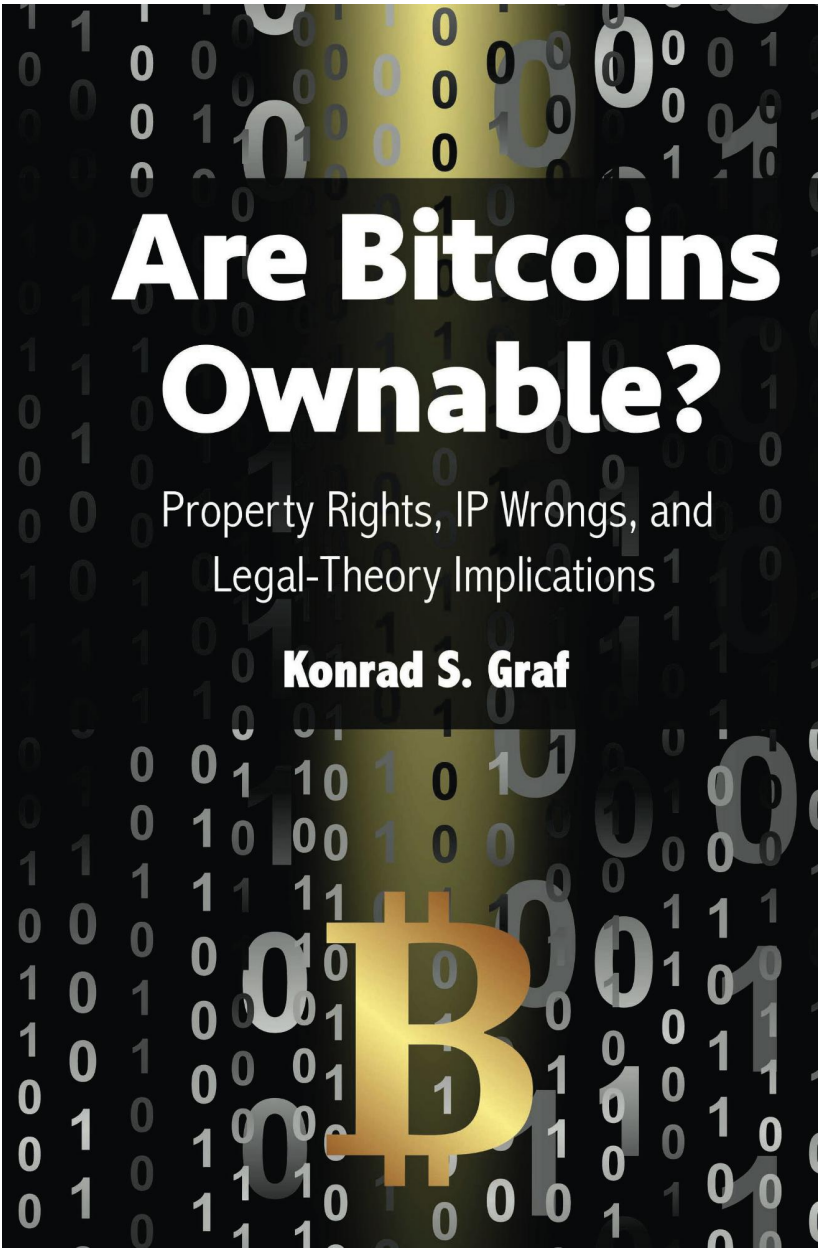
Are Bitcoins Ownable?
Property Rights, IP Wrongs, and Legal-Theory Implications
Konrad S. Graf

This edition, authored and published by Konrad S. Graf, is *author approved*. Agreed portions of any proceeds go to the author. The publisher may choose to make this content available in *multiple versions*, such as commercial paper versions, commercial ebook versions, and a PDF of the paper edition to facilitate sharing, text search, and citation.

Ways to support the author's work include recommending, reviewing, sharing copies, purchasing author-approved commercial editions, and donating bitcoin through his website.

Follow @KonradSGraf on Twitter. See other writings on bitcoin, legal theory, and other topics at konradsgraf.com

To pioneers of long-awaited next frontiers.

Contents

1

Facing the questions

Bitcoin raises questions about certain existing concepts and understandings in social theory. In economics: What is the nature of money and its origins? How do precise definitions of goods, scarcity, and commodity relate to bitcoin? How relevant is materiality and why?

The questions extend to legal theory as well, especially when legal theory, like economic theory, is viewed as mainly concerned with human acts, as I maintain it should be. To own, to sell, and to steal are all verbs with both economic and legal implications, not reducible to questions of technological form alone.

Is bitcoin[1] a type of thing that can be analyzed properly using legal concepts such as property rights and theft? Or would doing so be a category error, much like misapplying property concepts originating in the material world to intangible patterns, ideas, and methods in the style of intellectual-property legislation? Must property be measurable (matter, space, energy) if property rights are to remain an internally consistent and defensible concept? Bitcoin provides a fascinating and nuanced test case.

Although I have not addressed bitcoin ownability before, I have done related groundwork. My research and writing on what I have termed action-based jurisprudence[2]

[1] Upper-case Bitcoin can refer to software, protocol, or network. Lower-case bitcoin is reserved for the system's tradable units.

[2] Graf 2011, other links at konradsgraf.com/jurisprudence/

seeks to integrate action-theory approaches to law more explicitly under a Misesian framework[3] than had been thought possible before. I will use the term "action-based" jurisprudence, property theory, etc., in reference not only to my own work in formalizing and advancing this approach, but also more generally to existing works that mainly began to appear in the 2000s, which apply Misesian action analysis more or less explicitly to the nature and implications of property rights and related fields of legal thought such as contract and tort theory.[4] This project, my work on bitcoin and monetary theory, and my efforts to improve public understanding of how Bitcoin works at a technical level[5] now converge on the current topic.

On the question of whether bitcoin is properly ownable, legal theorist and patent attorney Stephan Kinsella has argued repeatedly that it is not, at least not under the approach to property theory he advocates.[6] More to the point, he claims that no suitable argument for bitcoin ownability has been advanced and that just assuming or asserting it by feeling or convention does not

[3] Praxeology and thymology as described in Mises 1998 and 2007.

[4] More references on action-theory and jurisprudence are in Graf 2011, but assuming a familiarity with Mises 1998 and 2007 and Rothbard 2002, 2002a, and 2004, I recommend the following study program: Barnett 1986 and 1998; Evers 1977; Hoppe 2004, 2006, and 2010; Hülsmann 2003 and 2004; Kinsella 1996, 2001, 2003, 2006, 2010, and 2011; Kinsella and Tinsley 2004; Sechrest 2004, Sima 2004, Tucker and Kinsella 2010; and Van Dun 2004 and 2009.

[5] See, for example, Graf 2013, 2014, and 2015 and other links at konradsgraf.com/bitcoin-theory/

[6] I am unaware of longer-form treatments and therefore reference social media discussions.

constitute a valid argument. Some bitcoin holders, meanwhile, naturally tend to have a strong intuition that they are indeed the owners of their bitcoins, quickly dismissing suggestions to the contrary. Yet mere assertion is indeed not a supported argument.

Kinsella's underlying approach to property theory is one I share. Hoppe (2006 and 2010) has elaborated it on a philosophical level and Kinsella has extended it to specific legal applications, most famously to a categorical opposition to intellectual property (IP) rights (2001). The current book references arguments in favor of property rights in controllable goods with physics-measurable properties, including material goods, spatially definable locations, and electromagnetic spectrum. It also references related arguments against IP rights that are derived by applying the same principles to these distinct cases. It considers bitcoin anew as a fresh case in terms of this existing discourse.

A central argument against IP rights is that they necessarily conflict with property rights in scarce goods and specifiable locations. A complete set of property rights in scarce resources is conceivable in a society such that no contradiction within the assignment of such rights exists. The addition of IP rights, such as rights to ideas, patterns, and methods, precludes any such non-contradictory rights arrangement even as a theoretical possibility.

Why is this so? An alleged ownership of an idea or abstract pattern conveys to the purported owner some partial rights to control the physical property and bodies of others. This conflicts with those others' rights and responsibilities to control themselves and their physical property. A potentially clear assignment of decision-making rights and responsibilities with regard to specific resources is thereby placed next to a vaguely overlapping

set of such assignments, requiring unending maintenance and litigation, and hobbling the potential scope of initiative, innovation, planning, and collaboration.

A copyright, for example, sets up a partial legal authority to limit what owners of printing presses may or may not print with them. This amounts to transferring a partial right to determine how a press is used from the press owner to the copyright holder and state agents. Having an exclusive and responsible decision maker with regard to the use of a given resource (the "owner") prevents conflict over its use. Having multiple decision makers, each with partial decision-making rights, introduces conflict and renders it intractable. This is the nature of the "political" world to which we are accustomed.

In contrast to a popular view that conflict is the essence of law, most famously exemplified by the popularly dramatized American version of the "adversary system," a sound legal system's value is in its efficacy at *preventing* conflict, and where that fails, most effectively resolving it. Introducing an irreconcilable contradiction into the concept of property rights itself, as support for IP rights does, represents a failure of legal theory to perform its central function.

In this context, considering whether bitcoin is or is not ownable could also potentially be of great importance. As with IP rights, a correct interpretation in terms of property theory could help prevent or alleviate conflict and injustice, while an incorrect interpretation could increase or even invite such conflict.

One notable flaw in discussions on bitcoin ownability is a tendency to shift with insufficient differentiation among several quite different perspectives: 1) a philosophical approach to property theory, 2) an everyday intuition about the nature of ownership as it may apply to

bitcoin, and 3) opinions on what a particular positive law jurisdiction happens to hold now, or may hold in the future, on bitcoin's legal classification. What follows belongs primarily to the first category, philosophical views on what is correct and defensible in terms of justice, rights, and procedures as they pertain to justifiable uses of force.

This book does not assess what any existing positive law jurisdiction might hold in legislative codes, administrative rulings, or court findings. It does not concern what any current regime says about bitcoin's local legal status this year or next, or what their respective agents are likely to do. Legal professionals, analysts, and institutes in various locales are already producing such analyses and forecasts with respect to such jurisdictions.

If one does wish to consider how bitcoin might best be treated within the context of bureaucratic classificationism, my personal understanding is that a categorization as "money" on a close analogy with foreign currency would likely be preferable for most users to a categorization as "property." But that is quite separate from the current topic.

Words should be used primarily as carriers of clear meaning. Words, however, can also be used as instruments of more efficient rule. Their meanings can become objects of political negotiation. Senses that words gain through such tactical uses tend to be less suitable for scientific employment, unless the subject matter is such tactical uses.

Bureaucratic classificationism, which insists that activities fall under a limited scope of legislatively defined and exploitable categories, has been powerful in history and its pervasive influence must be noted. With bitcoin, it takes the form of attempts to either call bitcoin illegal because it fits no existing official category or to construct

some new or modified category into which bitcoin is to fit—more or less.

Listing and categorizing elements of life reflects a worldview that "sees like a state." Administrators prioritize and channel activity into those aspects of life most "legible and hence appropriable by the state" (Scott 2009, 39). Among classificationism's other serious defects, however, it is anti-innovative and promotes fragility in society, in the sense Taleb (2012) contrasts with anti-fragility, including greater systemic vulnerability from reduced diversity of practices and methods and less "optionality" from the resulting narrowed scope of otherwise legitimately justifiable choices.

This book focuses on examples and implications for the most basic sense of ownership, having an enforceable right to retain or recover control of resources in response to others' acts. It concerns rightful control versus theft and non-rightful possession. It seeks to advance the discussion along some of the relevant lines. Other observers may see additional considerations to address for other aspects of law not discussed, and take up the baton of clarification.

Chapter 2 points out some wider contexts in which this issue is embedded, including the relationship between legal thinking and certain claims from within the crypto-anarchy movement that cryptography and other technologies can either partially or totally replace some legal methods (Chapter 6 picks up this theme in emphasizing the need to differentiate rightful ownership and mere possession). Chapter 2 also sets the stage further by reviewing the importance of differentiating legal from ethical fields, noting that legality as viewed under an action-based jurisprudence framework is a quite specific domain, far more delimited than ethical considerations of "right and wrong" in general, and why this is so important.

Chapters 3 and 4 examine ways in which bitcoin could be "stolen" (assuming as a placeholder that such a term, already rooted in an assumption of ownability, can be applied). The technical contexts of these methods are important for assessing the relevance of the ownability question to case judgment and response. This discussion emphasizes the distinction between property rights and IP claims and considers how this relates to bitcoin.

Chapter 5 considers, and critiques on factual and logical grounds, claims that if bitcoin were considered ownable, this could saddle network operators with additional justifiable legal obligations as an unintended consequence.

Chapters 6–8 are then positioned to dig into the main theoretical question directly. Are bitcoins ownable? This discussion proceeds by defining what bitcoin is and reviewing the theoretical foundations of the approach to property theory being applied, emphasizing the importance of differentiating rivalness as a social theory concept from physics-measurable characteristics of goods.

Chapter 9 summarizes and pulls the threads together.

2

Crypto-anarchism and conceptions of law and justice

One complication of the bitcoin ownability question is its embeddedness in a wider subject. Efficacy claims for Bitcoin and other products of the crypto-anarchy movement from which it sprang include improving upon and even replacing some institutions and practices understood under the domain "law." Aims include using cryptography and peer-to-peer networking to enable information security and transaction and event verification through software code such that *ex post* third-party external dispute resolution or court processes are rendered less necessary and less relevant—or in stronger formulations, unnecessary and irrelevant. Preferring "technological solutions over legal solutions," was already among the principles listed in Tim C. May's 1992 "The Crypto Anarchist Manifesto."[7]

One question such claims raise is whether bitcoin—as one such preferred technological rather than legalistic solution to the problem of digital cash—even needs to be treated under legal models that could be anachronistic in comparison. Is Bitcoin simply its own new realm? To what extent is it a self-contained participatory "law unto itself," in some ways superior to traditional trading and title-recording methods? Do all participants implicitly consent

[7] nakamotoinstitute.org/literature/crypto-anarchist-manifesto/

to use Bitcoin "as is," even if this includes some risk of unanticipated losses from what is ordinarily called "theft"?

Theft, however, is a wholly legal concept, perhaps the mother of all legal concepts. Is it inapplicable to this new domain of social life? If not, a proper role for law will have been readmitted in *some* form. If there is a scope for independence from conventional legal presumptions, and if this scope is not total, what are the new boundaries? What might remain useful from legal theory and practice next to this new crypto world order? Where, if anywhere, might there be legitimate contact surfaces between such worlds?

On the integrative side, a series of articles in the late '90s and early '00s by Szabo identified and drew on a variety of traditional legal principles and practices in informing the development of new, and potentially far superior, cryptographic solutions to extremely old problems of commercial law, corporate controls, payments, and contract fulfillment and verification.[8] Many of these insights begin from commercial practices of the kind often described as "evolved" through convention more than "enacted" from the top down by rulers. Szabo also advanced thinking on digital cash through the quest for digital "scarce objects" (2004) and then the description of "Bit Gold" (2005), which was among several key precursors of Bitcoin (Nakamoto 2008), the first large-scale digital-cash success.

Still, community hyperbole tends to complicate assessing relationships between the purported new crypto world order, existing legal institutions, and ideal legal practice. Some crypto-revolutionaries eager to witness the unholy state/bank alliance's crumbling tend to overstate

[8] See the collection at nakamotoinstitute.org/literature/

what can likely be "moved to the blockchain" in practice, leaving the impression that all legal approaches will inevitably become obsolete or less than worthless. In contrast, existing-order defenders tend to understate, or barely begin to ascertain, the scale and types of economic activities that can, do, and probably will take place through peer-to-peer cryptographic systems. Fortunately, valuable points from all such sides, and points in between, can be identified, extracted, and synthesized.

This book does not examine further the relationship between legal and crypto-anarchist models of transaction security, dispute resolution, and commercial practice. It focuses on applying a specific approach to legal reasoning to several types of what would appear to most people to be bitcoin thefts. It considers whether legal responses could be justified in such scenarios and on what grounds. It seeks to apply first principles to novel cases and consider what, if anything, institutions and actors identified under such principles as "legal" could do in such cases that might also be just. Finally, it considers how bitcoin might be viewed under the foundations of property theory as described in this approach.

The proper scope of the legal realm under action-based jurisprudence can be quite distinct from whatever existing positive law jurisdictions happen to be up to, whereas it is the latter that most people, under the sway of legal positivism, consider to simply *be* the legal realm. Others view law as almost exclusively an instrument of rule, with what justice it may happen to produce being more of a lucky and occasional byproduct.

This image of the fundamental corruption of observable positive law systems viewed from a strictly justice-oriented perspective, in addition to recognizing the oft-cited drawbacks of having to rely on "trusted third

parties," may partially explain some crypto-anarchist thinkers' instinct to distance from legalism. That approach, however, most likely assumes that the concept of law fits above all within positivist visions of it: that "law" amounts to the observable pronouncements and/or activities of existing positive law institutions and actors, while "justice" amounts to whatever these happen to mete out.

Justice as distinct from rule through law

In contrast, the action-based jurisprudence approach employed throughout this book considers the proper role of the legal realm to be the definition and promotion of justice, not of rule. Current and past forms of rule *through* law, as contrasted with the rule *of* law (and not of men) therefore provide only poor and rough reference points. If one's positivistic conception of justice finally amounts to whatever existing-order agents do (or have been mostly doing for some time), or whatever existing legislation and administrative rules specify, or whatever existing judges decide (or have been mostly deciding for some time) it provides no criteria for evaluating legal findings and acts other than reading the writ (or the precedents), watching the news, and nodding one's head.

The approach used here identifies and applies universal principles to assessing the justifiability of actions in terms of legal rights. These principles are universal in that they are derived from and pertain to necessary structural characteristics of action conducted in a social context. Some such action (or negligent omission) must be involved in any "legal" matter or it is not deemed such a matter. This approach is distinct from that of natural law/natural rights schools (though closer to them than to positivistic schools) in that it specifies rights more precisely as being necessary logical implications of the

analysis of action in a social context—including communicative action—rather than emerging from a more nebulously characterized "human nature." It also differentiates legal from ethical realms at a more precise level, as being distinct in methods, data types, and roles rather than as being more or less specialized versions of one another.[9]

The approach is also universal in that it does not admit status-based exceptions. Actions rather than actors are the primary locus of evaluation. This is related to the understanding that ideas and truth claims should be evaluated on content and evidence rather than on the identity or popularity of their current promoter. Applying the argument-from-authority fallacy test to evaluating legal-order practices, any legal system actor must be prepared to take personal responsibility for the results of his own acts.

In this view, "appeal to employment status" cannot successfully justify exceptions to general legal principles. False prosecutions ought to lead naturally to independent prosecutions of prosecutors, enforcement abuse ought to lead naturally to independent prosecutions of enforcers, and so on. Each judgment or enforcement step is a new action subject to the same sorts of evaluation and judgment as the alleged act being responded to. The neglect of such equality before legal principles promotes systematic abuses and injustices within a legal order.

Moreover, anyone, regardless of position, status, location, or even era, can employ these principles to independently evaluate the justifiability of actions taken by anyone else, likewise independent of position, status,

[9] Graf 2011, 13–19 and 21–25.

location, or era. This requires only an understanding of sound legal principles combined with acquiring a sufficient contextual knowledge of the case under evaluation, which is needed to apply those principles usefully.

It is in this broad sense that the unaccustomed term "judger" may be helpful in referring to anyone who undertakes such an evaluation. Knowledge of abstract legal-theory principles is accessible to anyone who learns it, in much the same sense as the principles of geometry. Though suitably useful degrees and certifications of knowledge and ability could aid as public recognition instruments, the principles themselves do not depend on any such certification or membership—much as the principles of geometry remain unaltered whether or not the one who happens to be applying them is a card-carrying member of the Pythagorean Society.

Sound legal principles are firm and universally applicable. It is the *practices* of case interpretation and enforcement that call for needed contextualization, flexibility, and moral judgment about what, if anything, ought to be done. The principles themselves are not altered or rendered unreliable merely by virtue of their actually being applied to interpretive and moral tasks, the latter tendency being the main error of a misplaced pragmatism.

In this sense, too, principles are apolitical. No political action, movement, party, opinion, or "reality" alters the principles of justice themselves in the slightest way, though these may certainly impact the details of their likely and best contextual applications and uses. Their bottom-line minimum application is to enable a single person anywhere and at any time to independently ascertain what is or is not a justifiable act and why.

This may seem to be both a useful form of knowledge and also in some ways "impractical." Yet in both the long

run of history and the ever-present interior gaze of moral conscience, such principles are among the most leveraged forms of knowledge. It is precisely this type of knowledge that is capable of producing multi-generation scale positive changes in society. It may also aid in informing more immediate choices, such as of which practices to advocate.

Consider, for example, abolitionist opposition to the formerly "legal" practice of slavery. This applied first principles to identifying slavery as categorically unjust regardless of any and all contemporaneous positive legal system treatments and opinions permitting it. It also did so regardless of worldly conventional wisdom of the time. Such insisted that slavery had always existed and therefore always would and as a practical matter must—adding that there are certain "necessarily evils" that practical men of the world understand (and choose to go along with). This example is not only idle ancient history: the second Fugitive Slave Act was passed *into* law in the United States Congress so recently as 1850.

A central action-based jurisprudence theme is differentiating legal theory, legal practice, and ethics based on field boundaries, functions, and methods. The legal, in this view, specifies the subject of property rights and the circumstances under which, and extent to which, force can be justified in response to their violation. It is therefore *extremely* specific in scope. Broader questions of "right and wrong" in general fall under the scope and methods of ethical and legal practice. Confusing these domains has been central to the real-life corruption of both legality and ethics (Graf 2011, Part IV). The logical endpoint of the unbridled extension of law into all questions of "right and wrong" is totalitarianism. An enforcement mechanism for a version of "moral" or "correct" behavior, according to the particular system in dominance, whether religious or secular, *displaces* the pursuit of justice.

Conversely, excusing state actors from personal responsibility for acts conducted in an official capacity likewise promotes and enables mass immoral action by state agents. "Just doing my job" and "just following orders" reflect an ideology that attempts to displace with law what is properly within the sphere of personal ethical responsibility. Both replacing law with ethics and replacing ethics with law (often done in a doubly-confused blend) fail utterly as constructive strategies, destroying useful functions of both and promoting the several police state variants across historical cycles.

With this distinction in mind, stealing bitcoins can be labeled "wrong" with relative ease, but establishing a *legal* claim that force is justified in response is a separate and much more rigorous task. Clear differentiation and healthy division of labor between law and ethics are part of the bedrock of civilization and are neglected at such civilization's peril. Legal questions must be met with legal approaches and ethical ones with ethical approaches.

The bitcoin ownability question is non-intuitive, rather specific, and could potentially have significant implications for evaluating the justifiability of certain acts in terms of property rights theory. If something is owned, a property rights violation could possibly justify legal force in remedy. The ownability question has implications for whether some legal response could possibly be justified vis-à-vis a bitcoin theft. In this light, the question seems somewhat less academic than it might at first. It could appear that if bitcoin is "property," guns might legitimately be drawn. If it is not "property," they might still be drawn, but their use in support of recovery acts might not be justifiable under these principles. We therefore turn to examining the question of bitcoin ownability primarily from the legal-theory perspective specified.

3

Trespass and trespass by hacking

Are there any imaginable situations in which it would matter whether bitcoin were ownable or not? If one is talking about "stealing" bitcoins, after all, they must be stolen *somehow*. The acts entailed in any such somehow could mean that certain types of cases may not necessarily turn on this issue at all.

How is this so? Any act involving bitcoin must *also* involve the use of some material and energy resources. This follows from what action is. Action interfaces between our dualistic understandings of the subjective and objective aspects of existence. Action must by its nature have *both* subjective and objective aspects, or in other terms, both 1) intentional elements, analyzable in terms of ends sought and means to pursue them, and 2) physical, spatial, or energetic elements of the kind that are subjectable to scientific measurement, or what I will call physics-measurable properties.

Objective elements are necessary for legal reasoning to be able to distinguish an implemented or even attempted action from a mere unrealized thought or wish. Intentional elements are necessary because action must be distinguished from mere observable behavior. Sound legal reasoning considers both objective and intentional elements and their interplay. These two elements can also be described in terms of causality and teleology:

> Human action involves two-fold causality. On the one hand, human action requires that time-invariant causal relations govern the physical world. Otherwise,

> a given means could not be said to achieve a desired result…And on the other hand, human action requires that those time-invariant causal relations can be understood and exploited by an individual whose actions are not themselves subject to time-invariant causal relations. Otherwise, there would be nothing to distinguish human action from blind natural forces. In such a world, laws would be pointless, because no one could be considered responsible for his actions. (Kinsella and Tinsley 2004, 98)

The main type of user act involving bitcoin is transferring control of bitcoin units from one or more addresses to one or more others. Transactions could also be automated or conducted by bots, but this only pushes back the questions to who is responsible for those, who programmed them to do what, who the beneficiaries are, and so on. We will stick with the base case of human users.

Sending a transaction requires certain objective physical events that have measurable elements expressed in physical movements and electromagnetic signals and states. A device running network-compatible software generates a signed transaction at a human user's behest. This transaction must be transmitted through data communication such that it begins to relay across the Bitcoin peer-to-peer network. It must then be incorporated into some of the various current candidate blocks, one of which must become the next link on the main chain for the transaction to become confirmed.

The culmination of this sequence creates changes to data on the blockchain ascertainable by anyone who examines it using proper methods, such as searching with a blockchain explorer. The state of these data is *universally verifiable*. Anyone who looks with suitable methods will see the same thing. By suitable methods, I mean, for example, that if one wants to see whether a given light in

the sky is a planet or an angel, one has to *look* through Galileo's telescope and not just keep explaining how "everyone knows" that it cannot be a planet. One must follow a suitable "learning injunction" to obtain the particular knowledge, but anyone who actually does so, that is, anyone who *looks*, arrives at the same result.[10]

However, even given the same universally verifiable technical components, the *social* nature of a transaction, including economic and legal facets, can differ based on other factors. A given transaction, otherwise identical on the blockchain, could be a payment, a gift, a theft, a gamble, or a mistake. Its universally verifiable components cannot establish which kind it is without evidence that is not only additional to but also different in kind from what the blockchain shows.

From economic and legal viewpoints, the intentional and socially contextualized aspects of the acts are of greater interest. Still, it must always be recalled that objective components must have *also* been present for there to have been an *act* at all, as contrasted with a mere dream, thought, or unrealized plan. This is a crucial distinction for legal causation. I have previously discussed the distinction between "objective" and "intersubjectively ascertainable" states of affairs and the need for *both* to establish legal causation (Graf 2011, 43–45). The "universally verifiable" concept above appears close to the borders of this division. That which is verified is still pure information independent of any *particular* material, spatial, or energetic instantiation. If the information lacks

[10] See Wilber 1998, 150–158 on learning injuctions and broad rather than narrow empiricism as the core of scientific method: "If you want to *know* this, you must *do* this (156)." Compare with the action-based epistemology in Hoppe 2006, 265–294.

at least one such instantiation, however, the pattern would be unrecoverably dissipated.

These concepts may also be viewed as dividing along fact and meaning. Even though machines can objectively verify a given key's identity as either *this* key or *that* one, assessment of associated meaning or significance of this fact requires a subjectivity capable of valuing.[11] At the same time, subjective does not equate to arbitrary. Intersubjectively ascertainable refers specifically to the phenomenon of multiple subjectivities *being able to* agree on a similar meaning with regard to the same events, such as whether Carl stole a bicycle or borrowed it. In both cases, the objective fact is Carl riding the bicycle, but the characterization of his actions that got him the bicycle can still differ in the intersubjectively ascertainable layer.

Given this dualistic nature of action, it is necessary to ask who owned the objective resources (computer equipment, paper backup, etc.) that must have been involved in a given bitcoin theft. Who had the right to control those resources? Did the person who made use of them have a right or permission to do so in that way?

With this in mind, what might stealing bitcoin entail at a practical level? The balance of this chapter covers direct action in person or by hacking. Chapter 4 covers the quite distinct case of brain-wallet sweeping.

A typical way a bitcoin balance is likely to be removed from its current possessor's control without his consent ("stolen") is through network-security breaches. The attacker needs to acquire signing keys to bitcoin addresses with balances. He must then use these keys to sign a transaction and send it to the Bitcoin network. This second

[11] Consider the discussion in Hoppe 2010, 136–142.

act transfers bitcoins in the victim's control to other addresses the attacker selects. As a direct result, the victim no longer controls bitcoins that he did prior to these acts.

It is tempting to exclaim, "Bitcoins were stolen!" and be done. However, some philosophers take a second look. They note that it should ordinarily not be possible to "steal" *a copy of a pattern* of ones and zeros, at least not in the same sense that one can steal a car. All that was "really stolen" was a copy of a particular sequence of digits. The keys needed to sign bitcoin transactions are a specific yet infinitely copiable pattern of pure information.

But more is at issue than an attacker obtaining a copy of signing keys. The attacker must obtain access to these signing keys in some particular way and how is he to do so? He might break into a physical structure, find a paper backup, and put the keys to use. He could also hack into computer equipment located in a home, business, or data center and thereby locate keys to a "hot wallet," one with keys stored on a machine connected to the internet.

Although he is physically present in one case, but not the other, the practical method and result is comparable in relevant senses. He uses another's physical property without consent[12] and for purposes to which they would not have consented if asked. There is no implied consent. If the attacker had asked the victim for signing keys, reasonable observers would agree that the answer would probably have been no, at least in the absence of duress. Nor could the attacker argue that computer users implicitly consent to unlimited, unauthorized, and detrimental use of

[12] A relevant common law doctrine is trespass to chattels en.wikipedia.org/wiki/Trespass_to_chattels. See this collection of discussions on trespass to chattels as applied to spam and hacking: stephankinsella.com/2010/01/why-spam-is-trespass/

their computers based merely on their decision to connect to the internet (although real user negligence might still be argued; discussed in Chapter 4).

Damages to victims that result from acts performed against or using the victim's property without consent are properly subject to enforceable and proportional restitution liabilities and possibly other punishment. What might such responses factor in? In principle, they should reflect damages to the victim that can be causally attributed to these rights-violating acts. The precise question, in applying the counterfactual reasoning method of action theory, is What damages would not have occurred in the absence of the rights-violating acts at issue?[13]

There are also several reasons why total restitution and/or punishment ought to exceed a simple nominal and purely physicalistic damage assessment. Among them, the contexts for the attacker and the victim are asymmetric in the attacker's favor. The attacker violated the victim's property rights at a time of the attacker's choosing. He then not only caused specific estimable damages, but also undermined the victim's sense of security and predictability in his possessions. The attacker could have struck at any time. The magnitude of the damage was uncertain to the victim. More or less could have been damaged. The victim could not know how much damage would be inflicted until after the initial events had concluded. Even then, the victim still awaits additional—necessarily uncertain—legal processes of investigation, judgment, and enforcement, none of which would have ensued without the attacker's initial acts.

[13] See Hülsmann 2003 and 2004 on the counterfactual method in economics and property theory.

A legitimate legal response is likely to be more orderly and predictable to the attacker than the crime was to the victim. The attacker can expect a result that is detrimental to him, but still likely to be roughly proportionate to what he had done. He is still the original mover and shaker; he remains a necessary cause of the entire sequence of events. He does not determine the entire sequence, but without his original acts, no part of the sequence would have ensued. The victim, in contrast, can only respond.

This contextual asymmetry implies an uncertainty premium in the victim's favor. As Kinsella explained, the total judgment,

> …may also be enhanced to take into account other damages such as interest, general costs of crime prevention, and also for putting the victim into a state of fear and uncertainty (1996, 70)…General bounds of proportionality are satisfied when the consequences and potential consequences to the victim that are caused by the aggression are taken into account. (69)

Moreover, the burden of proof in objecting to punishment details ought to be on the attacker, and the benefit of the doubt with the victim. With regard to punishment details for acts factually established:

> If there is a gray area, the aggressor ought not be allowed to throw his hands up in mock perplexity and escape liability; rather, the line ought to come down on the side of the gray that most favors the victim, unless the aggressor can further narrow the gray area with convincing theories and arguments, for the aggressor is the one who brings the gray into existence. (71)

Because repaying in kind can be cumbersome, imprecise, and more difficult for judgers and enforcers to monitor, a total restitution debt, possibly including such premiums as discussed above, is most efficiently estimated

as a total value, denominated and payable in money. This is particularly so with fungible items. Exceptions include requirements to return unique items such as paintings. Generally speaking, instead of, or in addition to, asking the offender to replace in kind, dispute resolvers in money-using societies have gravitated toward denominating total restitution debts in money terms.

Say a restitution finding requires a defendant Devon to pay plaintiff Parker for bitcoin losses resulting from trespass or similar acts. The particular bitcoin units that were stolen, though they might serve as evidence, need not be among the means of repayment. A restitution finding constitutes a monetary liability payable from Devon to Parker *somehow* from Devon's entire asset stock and present and future earnings. Whether Devon pays some of his debt to Parker funded with the same bitcoins at issue, or other ones, or some other wealth of his is immaterial. In most cases, the total restitution debt should also exceed the nominal amount stolen and therefore require the attacker in any case to transfer some amount in addition.

Just legal responses entail estimating the entire value loss that can be imputed to the attacker's rights-violating acts. This can reflect considerations such as market value, lost wages, and possibly even psychological or emotional damages. The key point is that not only physically defined damages, but also more intangible damages and value destruction can be estimated and factored into a total judgment, likely expressed as a single monetary debt owed to the victim, victim's assignee, or nearest relative.

Estimating legal damages thus differs from determining the ownability of any particular items with regard to whether legitimate property rights in those items can possibly exist and therefore also be violated. This leaves an important subtlety that is easy to miss. The case

would differ if the acts at issue *only* involved unownable items, but no ownable ones, or if only market *value* of property was involved.

Hypotheticals—Tim and Dan

A businessperson Dan sees rival Tim's more efficient work method by observing from across the road and then begins to emulate it. This increases Dan's competitiveness. Tim claims he has lost sales, market share, and business value due to this "idea theft." Tim had a reputation as the market leader. Now, he has been rendered one competitor among others, next to Dan, and it is Dan's fault. Not only has Tim's market share dropped, but also his reputation value.

Tim's legal claim would have to be dismissed according to principles of action-based property theory because the work method that Dan observed and then emulated is not *itself* ownable. An idea or opinion is not a rival good (explained below). Dan did not otherwise trespass or infringe on Tim's property. Dan observed from a location that Tim did not own and later emulated certain practices that he observed. None of these acts violated a valid property right of Tim's.

Consider a contrasting case. This time, Dan hauls away Tim's machine late one night, conceals its identity, and some time later starts using it. Dan's business gains and Tim's loses once again. Now Tim is reduced to working with inferior old machinery until a replacement is built and delivered. His reputation for quality and speed suffers. With that machine, meanwhile, Dan gains customers—and accumulating sales and contacts—at Tim's expense.

Tim's insurance investigators (representing the company that is mostly paying for that new machine being built) already suspected Dan and think they have forensic

evidence that Dan is using the stolen machine. Dan, having replaced identifying marks and falsified serial numbers, denies everything. A legal process ensues.

This time, though, the wider value Tim lost—including that attributed to intangibles—could be causally attributed through a valid legal process to a property-rights violation. Dan's action did violate a legitimate right in "ownable" property—Tim's factory site and machine. Any financial loss to Tim (and/or his insurer) reasonably attributable to Dan having hauled off Tim's machine is Dan's responsibility, not Tim's. Nor can such loss be explained away by coincidental market-price fluctuations. Dan caused losses. Those that can reasonably be attributed to Dan's rights-violating acts are subject to restitution.

As it turns out, the financial losses to Tim end up being similar in both cases. However, the legal status of the two cases differs entirely. In one, there was a property rights violation; in the other, none. This makes only the second case legally actionable under this approach.

Restitution liability is a separate matter from ownability. An act can cause damages to the victim. *Some* of those can involve unownable abstractions such as an estimated business value. Such intangibles could not be legitimate restitution objects *by themselves*, or just because Dan had raised his eyebrows the wrong way in an interview, but they could be causally attributed to some other action that *was* a property rights violation.

In the next case, Dan, again from across the road, photographs Tim getting drunk and partying after work behind Tim's factory. Dan publishes this to damage Tim's reputation and discredit his business. Tim argues he has a property right in his image and reputation and sues Dan. In this case again, though, Dan has violated no legitimate property right of Tim's. The photographs were

information. Dan used only his own property (self, camera) and stood on land where he was permitted.

Tim's "reputation value" is likewise not ownable, even though it is naturally of great interest to Tim. Reputation exists primarily as varied, subjective, and shifting assessments in the minds of dispersed others. It is as such impossible to subject to valid principles of control and ownership. The contents of others' minds would have to be monitored and repaired by the likes of Tim, Dan, or their respective agents. That would be a good subject for science fiction or totalitarian fantasy, but does not recommend itself for practical implementation.

Dan's action also says something about Dan and this may be negative for himself. Some people may not want to deal with Dan due to such behavior. After all, Tim might get drunk behind the factory, but Dan has demonstrated his underhandedness, and which is worse? All such things are properly cultural, social, and ethical matters, not legal ones.

Now another case. Tim has a side business. He purchased at auction a never-before-seen cache of old superstar photos. He digitized them and created a business that releases them to subscribers, one a week. Dan decides to break into Tim's office. He copies all the digitized photo data and just for spite dumps the files online, rendering them all irreversibly public.

The valuable items at issue were once again pure information, and therefore not ownable. This time, however, Dan *trespassed* to obtain the photo data. He entered Tim's site without permission and made unauthorized use of Tim's computer equipment as part of a sequence of acts that caused financial damages to Tim. As a result, Tim's weekly photo subscription business went under when his secret exclusive photo cache was released.

Dan owes Tim for this loss even though the images *themselves* are not ownable.

We next witness another round in this sad relationship, which the former cases should now aid in interpreting. Dan hacks Tim's business computer on which Tim's company accepts bitcoin payments from customers. Dan copies Tim's signing keys and uses them to transfer Tim's bitcoin balances to himself.

This results from Dan's trespass-by-hacking act. Without Tim's consent, neither explicit nor implied, Dan used Tim's property, his corporate servers. This use caused Tim to be deprived of his former control of the bitcoin balances at issue. In assessing the financial damage, the bitcoins of which Tim was deprived had a clear market price and are candidates for inclusion in a restitution finding against Dan. Once again, as with the photo business case, this causal attribution would hold *even if* bitcoins, as opposed to the material property Dan misused in obtaining them, were not considered ownable.

This loss of *bitcoin* contrasts with a loss of bitcoin *value*. If Dan deprived Tim of bitcoin that Tim had previous to Dan's actions, a dispute resolver could then reference the market value of this bitcoin in estimating reasonable restitution. However, this differs from a value loss due to a market price change. If Dan sells most of his substantial holdings of bitcoin and issues a press release adding that he now predicts the demise of Bitcoin, its price could drop as a result. Tim may suffer some unrealized losses on his own bitcoin holdings. However, no legal action by Tim against Dan could be justified. Even though there is a reasonably likely causal relationship between Dan's actions and the price drop—and therefore Tim's unrealized losses on his own bitcoin holdings—Tim still controls exactly the same bitcoin that he did before.

A value change in bitcoin, or in any other item of property, is not actionable. To be even possibly actionable, Dan must remove Tim's ability to control specific bitcoin units that Tim had controlled before. That these bitcoin units had a particular market value at the time of Tim's loss is a secondary fact for use in damage estimation.

As with reputation, an alleged owner of "market value" descriptively *cannot* exclusively control it, though he can try to influence it, as can potentially many others. Market prices, like reputation, change primarily along with complex constellations of *other people's* current opinions, whims, and priorities. These are far from controllable.

Not only can an alleged owner of the opinions and preferences of others, such as with regard to reputations and price preferences, *not* control these reflections of others' minds (though these others may be influenced to some degree), the degree to which these others can themselves control the shifting inclinations of their own hearts and minds is even questionable. If anyone can control such things at all, however, it is these other people who are the best candidates for attempting it in each of their own respective cases.

Hülsmann (2004, 51) specified several criteria for property-claim legitimacy, one of which is that a claimer should be "in a position to control the thing under consideration…one cannot be the owner of a thing if one cannot possibly control [it]." Note that under this criterion one does not have to *be controlling* the resource all the time once it is claimed. Instead, it must at least be *possible* for the claimer to exercise effective control, including through agents, such as within a company or other contractual structure. This is an outside limiter for a justifiable ownership claim. A specific agent *can* control bitcoin units, whereas such an agent *cannot* control

intangible outcomes of other people's judgments such as market prices and reputations.

Establishing causation and responsibility and estimating resulting value loss do not necessarily hinge on the ownability of each and every thing the value of which a trespass or other rights violation diminishes. The requirement is that the value loss is causally attributable to acts that violated *some* legitimate property right of the victim in an ownable thing, and then also inflicted a certain total estimated impact on this victim. In this important category of cases, bitcoin's ownability appears superfluous as a practical matter.

4

Double spending and brain-wallet sweeping

The previous chapter suggests that for a typical bitcoin theft that involves some form of trespass, the legal-theory question of bitcoin's ownability should have no practical impact on the justifiable scope of legal responses under action-based jurisprudence. If trespass is committed and bitcoin balances are lost as a result, bitcoin's ownability has no bearing on the damages the attacker caused the victim and the restitution that could be justified.

It may even be difficult to think of some method of stealing bitcoin that does not also involve some *other* less philosophically controversial rights violation. Fraud or duress might come to mind, but these are likewise rights-violating acts. For example, as Ranvier (2015) explains:

> There is a kind of fraud possible with cheque payments where the payer writes a cheque for more funds than they have available to spend. This is known as "check kiting" in the paper banking world and in many legal jurisdictions considered a felony, sometimes punishable by jail.
>
> Check kiting is possible in Bitcoin as well, where it is known as "double spending". A fraudulent payer can create and sign two transactions that consume the same inputs. Since only one of the transactions can be valid, and since ECDSA signatures are effectively impossible to forge (far more so than ink signatures on cheques), the existence of two signed Bitcoin

> transactions that spend the same inputs is prima facie evidence of fraudulent intent.

While much is made of double spending in the Bitcoin security-research literature, its practical importance to users remains low. The entire Bitcoin architecture can already be viewed as an invention to combat double spending. Still, there are a few cracks that can possibly be exploited under certain circumstances within narrow time windows. It is important to note that with double spending, no funds can be stolen directly. Only the fraudster's own funds can be directed in two or more mutually incompatible payments—until a short while later when the network confirms one of them, but not any of the others.

Where values are relatively high and double spending more tempting to the dishonest, receivers are also most likely to wait for more confirmations before releasing high-value and/or difficult to recover goods and services on the other side of the trade, defeating the strategy. Bitcoin escrow transactions could also be used.

Conversely, where values are low or the other side of the trade can simply be reversed later in response to the fraud (such as cancelling a subscription or reservation), the likelihood and meaningfulness of attempt is low, obviating the need to wait for confirmations. Moreover, costs to the receiver from lower-value transaction fraud is more easily written off as a quantifiable operating risk, much as with annual merchant costs from check and credit card fraud and the passing of counterfeit notes.

Double spending is therefore a form of payment fraud, which might be used to defraud someone out of other goods and services or monies. It thus 1) is *not* a method of stealing bitcoin held by other parties and 2) *does* involve other rights-violating acts.

The question, then, remains: Could bitcoin be stolen in some way that did not also involve some other rights violation in the process?

The candidate to consider next is brain-wallet sweeping, which differs substantially at a technical level from the cases considered so far. In the broadest sense, the concept of a brain wallet includes any method by which the information necessary to spend bitcoin can be memorized. However, there are critical differences in *how* a user can go about creating one.

A best-practice brain wallet begins with generating entropy, such as by recording a dice-roll series. These random data are converted into a word sequence, such as from a numbered word list, which the user can then memorize and/or securely record. These same data also serve as a cryptographic seed to create a wallet.[14] The same phrase always generates the same wallet with the same pairs of signing keys and addresses. If created properly, such a wallet can be sufficiently secure for its purpose.

A poorly generated brain wallet is a quite different matter. In the worst cases, it might be compromised in short order. Here, the user thinks up some phrase he feels would be both memorable to him and cleverly non-obvious to others. Alternatively, he selects some passage from an old text that he believes is sufficiently obscure that the particular sequence he choses could never be guessed.

Both approaches tend to result in poor entropy and therefore security. Brain-wallet sweeping software used in conjunction with ever-faster processing hardware is becoming increasingly adept at trying vast numbers of

[14] See *Entropic* github.com/bitstein/entropic and more generally *Diceware* world.std.com/~reinhold/diceware.html

possible "memorable phrases," as well as segments from any text in any language that has ever found its way into contact with the internet. Such software is also becoming ever better at defeating character-substitution methods, such as replacing a letter with a number that resembles it, and various abbreviation methods. The security value of such schemes is much more impressive to calculationally challenged human minds than it is to specialized software running on fast modern hardware. Any funds stored in brain wallets made with seeds created without sufficient entropy can be more and more readily removed as these capabilities progress.

Hypotheticals—Alice and Bob

Alice creates a brain wallet, transfers bitcoin into it, and then loses that bitcoin because Bob engaged in successful brain-wallet sweeping. In principle, we begin with no idea who Bob is or where on or near earth he may be, and he is also quite unlikely to have any idea whose bitcoin he is collecting. Moreover, his actions do not even really entail "cracking" anything. He bulk-generates key pairs from possible brain-wallet phrases, and scans the blockchain for any corresponding addresses with current balances. Any such addresses would have originally been generated using the same seed that he has now also used. He therefore also now has the signing keys for these addresses.

Bob thus starts by generating likely key pairs independently and only then looks for any existing balance that those signing keys could access. Bob happens to have generated the *same* key pair Alice also had. With high entropy, such convergence is so unlikely that it would effectively never occur, even over cosmic time scales. This fact is essential to understanding how Bitcoin address security is possible at all. Weak brain wallets, however, can

be compromised at any time. Preventative user education in secure wallet generation may well be the best response.

In an idealistic white-hat version of brain-wallet sweeping, when Bob removes a balance from such an address, he in effect picks up a valuable lost item from the sidewalk in hopes of returning it to whichever careless Alice left it out in public. Once Bob himself has discovered this address, it is plausible that some other brain-wallet sweeper is about to uncover it as well given the current state of the art, an art of which Bob is but one practitioner. If he does not pick up the balance first, someone else might, and that third person might wear a darker hat.

This white-hatted Bob, if discovered, could attempt to justify his address-sweeping behavior based on implied consent. If Alice could have been asked if she would like her bitcoin to be rescued from her own incompetence rather than stolen outright, reasonable observers would agree that she would most likely prefer the kindlier alternative. Consent can only be implied, not explicit, because there is no way to ask Alice in a timely way. It is hard to identify her at all and somebody else with less noble intent could be right behind white-hatted Bob in the race to vacuum up value from the next marginal crop of weak addresses.

Bob could seek to prove his hat color by demonstrating efforts to find relevant Alices and restore their funds when possible. If all white-hatted Bobs simply refrained from sweeping, it might at first appear morally laudable. However, this would also leave the field entirely to those with darker hats, excluding any possibility of lost funds being returned voluntarily.

However, trying to return Alice's lost bitcoin is neither simple nor costless. As with some physical lost and found situations, it may be quite difficult to identify and locate the

Alice in question. Somewhat like an unmarked dropped property item, the source bitcoin address alone cannot identify her. A traditional lost and found principle would expect Bob to make some reasonable effort to locate Alice to return her lost item. She might also be expected to announce the loss. She might by custom offer a reward for a civic-spirited return of her bitcoins. The respective notices might be posted on some relevant bulletin board.

Even upon locating the likely Alice, Bob should not simply return the amount to the same address. The next scanning sweeper might promptly empty it again. The return should go to some new address that the identified Alice generates (now with better entropy). Identity evidence might include proving possession of signing keys to the now compromised addresses. But if still others had independently discovered the keys, they could pretend to be the original Alice and collect her refund. For Bob, it could come down to balancing available evidence, assessing believability, and making a decision.

In the end, if Bob has no success identifying the real Alice, he could eventually claim the bitcoins were now "his" under legal principles (granting the ownability question itself for the moment). This could become a justifiable appropriation in that the item had become unowned, returned to a "state of nature," because the previous owner could not reasonably be identified in a timely way or at a suitable search cost relative to the lost item's estimated value. If this Bob were not only white-hatted, but also white-*winged*, he might donate some of the lost coins to an education campaign against weak brain-wallet use.

When can a lost item be considered conclusively lost for legal purposes, that is, subject to a new, justifiable claim of ownership by its subsequent first finder? Does the original owner eventually lose a legal claim to recovery,

such that the finder can put the item to some new use without indefinite fear of future legal action?

These are questions that fall under legal practice rather than legal theory. The answers must reference such things as the nature of the item and reasonable assessments of contextualized and relevant common sense, traditions, community standards, and customs.

Certain legal questions need to be determined *somehow* in each context, but a range of options may fall within theoretical framework requirements of justice and the rule of law (Graf 2011, Part III). In this context, Barnett (1998, 108–131) discussed what he termed legal precepts and specifying conventions, describing their roles: "A theory of justice is *underdeterminate* when it narrows down our choice of legal precepts but does not determine a unique precept to address the social problems at issue." *Some* precept may be needed, but a range of possibilities could fall within the general requirements of justifiability.

The next Bob is less generous, though he cites his reasons. He defends his grey-hat brain-wallet sweeping as a public service. He argues that systematically punishing poor wallet-generation practices reduces their future use as quickly as possible, bringing about a net increase in average user security as the weakest practices are weeded out in a Darwinian process.

Finally, unabashedly black-hatted Bob dispenses even with this attempt at justification. He just collects bitcoins from easy sources in a relatively secure form of the activity generally understood to be "theft." He preys, perhaps even "rationally" in a certain sense, on the most accessible and lowest-risk targets.

Implications and practice considerations

What are the implications for bitcoin ownability? A brain-wallet sweep can remove Alice's balance without trespassing and without fraud or duress. Such sweeping can likewise not be said to trespass on the Bitcoin protocol or the network that implements it because these are unowned and unownable. They are akin to an actively spoken global language and the totality of this language's speakers at any given moment.

Sweeping also does not appear to trespass on the computer and networking equipment of any of these infrastructure contributors, at least not in any actionable way. In running Bitcoin software, node operators and miners volunteer with no contractual context to relay technically valid transactions from peer to peer. Transactions are filtered on a purely technical basis as specified in the protocol. There is no way for node operators to distinguish the *legal* nature of given transactions. The network can only show that a transaction has been signed validly according to cryptographic specifications; it cannot show *who* did this signing, or with which economic and legal implications.

As a practical matter, Bobs of any hat are unlikely to have any idea who Alice is, and Bobs of some hats may not care. Any such Bobs see first of all a mathematical phenomenon—weak addresses with balances. What the various Bobs decide to do about this reflects a separate sequence of moral decisions.

Now what if a darkish-hatted Bob, one who had just pocketed the bitcoin, is later discovered and what if it is also provably clear who the relevant Alice was (or class-action Alices were)? In a physical lost property case, Bob may well have to return the item. What if Bob refuses to

refund the bitcoin or otherwise compensate Alice, claiming that these are just the breaks on the new frontier?

This Bob might counter that Alice was negligent in leaving her valuables out on the crypto street for anyone to pick up. *Somebody* in the world *was* going to pick them up, and it happened to be this Bob rather than some other who was in the right place at the right time. Moreover, he might argue that the time, expense, and uncertainty of even *trying* to locate the relevant Alice in every case did not seem worth it. Would there still now be a supportable *legal*—as opposed to a much broader potential moral—stance for Alice against Bob to recover her loss?

In other words, could the threat or use of force against Bob to compel him to compensate Alice possibly be justified in such a case? Would any judger issue such a finding? Could the clarity of and evidence for such a finding be viewed as sufficient to be relied on? Would anyone be willing to take on the risks and responsibilities of enforcing it? Doing so could invite costly and risky appeals and counterclaims if the judgment proves to have been weak in its evidence or logic.

If one argued that bitcoins are ownable due in part to properties of strong cryptography (discussed later), could weak keys—in effect, *weak* cryptography—invalidate such a basis in those cases? Could sufficient brain-wallet negligence undermine a claim to an enforceable remedy? Could it render an otherwise owned good into a good that does in effect sit out unattended in a "state of nature" on the crypto frontier? If a brain wallet is swept without trespassing due to substandard entropy, is presumed negligence enough to shield the sweeper from a potential future legal obligation to pay restitution to the victim?

The criterion noted from Hülsmann in Chapter 3 that for a thing to become subject to ownership, an owner

should be "in a position to control the thing under consideration" also implies the possibility of excluding others from exercising such control. It is unnecessary for a claimer to control an army capable of doing this successfully in any conceivable case. After all, any given crime victim has unfortunately in fact failed to successfully defend themselves or their property from a given alleged violation. For purposes of this minimum criterion, it need only be *possible* that the claimer could possibly exercise control of the resource and exclude others from also using it in relevant conflicting ways.

This criterion helps exclude absurd claims made using only words without any corresponding actions. For example, merely *saying*, "I own the moon," without so much as owning a single rocket for reaching a single patch of this claimed moon—let alone demonstrably making use of its entire surface in some recognizable way before anyone else—cannot qualify as a legitimate claim, which requires both action (first use) *and* contextually sufficient communicative action (first claim).

The strong cryptography and entropy of Bitcoin's signing-key/verification-key framework enables users to exercise exclusive control of bitcoin units. With a standard high-entropy address, a user controlling certain bitcoin units can exclude others from using them. With a low entropy address such as a weak brain wallet, however, the user is not in a comparable position to exclude others, and can do so *only* ineffectively.

Yet does this merely fall back on the above-rejected "strong-enough army" criterion? "The defense was too weak," does not *justify* in any legal or moral sense an invasion; it merely descriptively makes such a violation more of a practical possibility. Possible controllability, not

strength of defensibility, was the cited criterion and its function is to exclude arbitrary and baseless claims.

Considerations such as these could render making a successful claim for restitution for bitcoin lost from a weak brain wallet relatively challenging, particularly in the absence of any other act violating legitimate property rights (Chapter 3). Measures such as naming or boycotting might in some cases be *morally and socially* justified. White-hatted Bob's reputation and reasonable expectation of positive treatment in society could rise while black-hatted Bob's could suffer if he were identified and exposed, perhaps leading to ostracism. However, any necessarily risky, costly, and error-prone use of *legal force* against black-hatted Bob would be harder to justify than if he had engaged in some *other* rights violations in his process of depriving others of bitcoin.

Yet justifying theft based on a victim's weak security is problematic. "The door was unlocked," after all, does not justify burglary. This image applies to the theft by trespassing cases of Chapter 3. Even if hacking was easy due to poor security, it still entails a clearly non-consensual use of other's physical property and is therefore legally actionable. Dropping an unmarked item on the street, an image used for the cases of this chapter, is quite different from leaving the door unlocked. The respective acts are: 1) entering a structure without permission and leaving with an item and 2) picking up a dropped item off the street where *someone* was likely soon to pick it up. Moreover, neither image is a perfect analogy (there is no such thing).

Practical answers are not always fully or sufficiently determinable at the theoretical level or with malleable hypotheticals. There are matters, often including matters of degree, legitimately reserved for case interpretation—for legal practice and ethics. Overextended rationalism can

continue to emphasize theory even when the—necessarily situated and non-universal—domains of specific case interpretation and applied ethics need to be engaged. The armchair and the bench are quite different seats, yet both have their roles and are essential to the doing of justice. Doing bench business poorly from the armchair is problematic and so is doing theoretical work poorly from the bench, such as mangling clear principles so as to rationalize a weak, but convenient or preferred opinion.

Dilution and obfuscation of sound legal theory has resulted from taking the contextual judgment and ethics that are legitimate and necessary to case interpretation and enforcement decision-making and misapplying them such as to weaken the role of legal-theory principles themselves. This is comparable to trying to resolve a surveying miscalculation by creating an "exception" to the rules of trigonometry—instead of going out and finding the measurement error.

In the action-based jurisprudence model, a legitimate legal case is a dispute-resolution process between an aggrieved party or their representative and another party accused of a rights violation or their representative, mediated by a third party. Unlike universal action theory itself, each real case is contextually situated. Practical outcomes should not only be usefully interpretable under principles from legal theory, but also in terms of more imprecise factors such as balance-of-evidence judgments, local and otherwise relevant customs and expectations, and ethical stances and reputation considerations for dispute-resolvers, judgers, and enforcers.[15]

[15] Barnett 1998, Chap 6; Graf 2011, Parts III and IV.

In the absence of voluntary recognition and compliance from a defendant with regard to an adverse judgment, particular persons must actually decide whether to carry out any enforcement actions that this judgment approves. Each enforcer is naturally responsible for his own enforcement acts, if any, and as such must evaluate whether a judgment's defined scope of justifiable legal response has been sufficiently substantiated through process and evidence. To what extent can these findings stand up to future public scrutiny and possible countersuits for false accusations or disproportionality?[16]

Differentiating law from ethics, theory from practice and judgment from enforcement does not mean dispensing with or ignoring any of them; it means keeping each *in its proper roles* relative to the others. Whether bitcoin is ownable is a theoretical question, but it has first been necessary to establish a potential scope of application, if any, for answers to this question that may be arrived at. The question appeared inconsequential to the cases in Chapter 3. It appears possibly more relevant to the cases in this chapter, though these already appear to show notable signs of likely controversies of application in legal cases that actually could hinge on bitcoin ownability itself. This examination of possible case applicability is now in place to inform the direct theoretical discussions of ownability to follow, mainly in Chapters 6–7.

[16] Countersuits are also not free, however. They can be lost, ultimately at further cost to the countersuing party. This tends to reward making substantiated and clear claims and to dissuade making unsubstantiated, vague, or false claims.

5

Fungibility and third-party obligations

Before discussing rivalness in relation to bitcoin and ownability beginning in Chapter 6, this chapter addresses some additional issues. If bitcoins were ownable, it has been asked (in part rhetorically as an argument), would that also imply legal rights of bitcoin holders that could justify actions against Bitcoin infrastructure operators? Specifically, could miners be legally forced to reverse some transactions later found fraudulent? If so, would this be a net negative for Bitcoin, an unintended effect that spins additional justifications for legal interference?

The following passage argues that legal obligations for third-party Bitcoin infrastructure providers could follow from bitcoin ownability claims. In the apparent absence of more formal writings on this subject to date, the following has been selected from among several similar social media threads:

> Bitcoins are just ledger entries, and the ledger is stored on many people's private property—their computers/hard drives/servers. They own that property. How can the bitcoin "owner" have a right to their computers? Suppose A owns a bitcoin. B steals it and spends it on something. So now it's in C's hands. That means B's spending—[B] used A's private key to tell all the bitcoin users to switch the ownership of the bitcoin to C—and following the BTC protocol, the private owners hosting copies of the blockchain all changed the "ownership" of the bitcoin to C.

> Now if A owns the bitcoin and finds out that C "has" it—all this means is that all the users of the bitcoin protocol have some entry in the blockchain pointing to C. Does A have a legal "right" to force all the bitcoin users to change the entry on the blockchain to point it back to A? For it to have legal meaning for A to own a bitcoin would necessarily mean A has ownership rights in private property of the bitcoin network users.[17]

There are several difficulties with this line of reasoning and several technical and legal points to consider in relation to it. Let us proceed by reviewing and applying some general legal principles as grounded in the analysis of action and causation and continue with their application to relevant technical characteristics of Bitcoin.

The distinction between rightful ownership and mere possession is essential to sound legal theory. It implies that having mere possession, that is, being the one who descriptively has current effective control of a given good, may or may not map to legal ownership. Legal rights enable identifying *discrepancies* between ownership and possession. Legal processes are means of realigning rights and possession if they are identified to have been misaligned through the likes of theft or fraud.

In the above example, effective control changed from A to B to C due only to the actions of B. Only B's acts are legally causal. It is only B from whom any and all affected parties ought to seek restitution. An exception would arise if C can be established to be knowingly buying and reselling stolen property, acting as a "fence," in which case C's fraud victim D could pursue cases against both C and B.

[17] Stephan Kinsella, 31 Aug 2015 Facebook comment.

With bitcoin, the possessor is the party who has the descriptive ability to control the units at issue in a purely factual sense. This party was A before the theft, B after it, and finally C or D. But this alone cannot establish the identity of the rightful owner in a legal sense. The blockchain can only indicate a state of mere possession, not rightful ownership. Even if general ownability and specific rightful ownership *could* be established, the Bitcoin blockchain would still be incapable of showing such things directly. The blockchain can only show effective possession by any (pseudonymous) holder of the correct signing key; it cannot show whether each instance of such possession corresponds to any legal model of rightful ownership.

This is one reason rhetoric about blockchains replacing law can be overstretched. In the extreme, it can appear to support the claim that mere possession can replace the concept of rightful ownership entirely. But this implies, to use another image, that the current rider of a bicycle is thereby to be considered its rightful owner. However, such mere riding establishes no such thing. Although there is some statistical probability, which varies by location, of the current rider also being the rightful owner, the rider could in fact either be the owner (A), a thief (B), or even C, a subsequent fraud victim of B's, or perhaps even P, someone borrowing the bicycle with A's permission. Regardless of who is riding the bicycle, only A *owns* it in each instance.

Next, it is essential to trace specific acts and apply principles of legal causation, property rights, and ownership transfers. Let us first use a unique-property example, such as a painting. If C buys a stolen painting from B, C has a legal obligation to return it to A when this is discovered, regardless of whether C knew at the time of his purchase that B lacked valid title. This is because A remains the legitimate owner the whole time. B's theft does

not invalidate A's property right. If B had duped C, C would have to return the item to A and then sue B.

Even though C has engaged in no rights-violating acts, C can nevertheless not simply keep the stolen item. C has never acquired valid title. B's crimes have never transferred rightful ownership from A, only mere possession. In now having to return the item to A, C does not suffer due to the existence of A's property right, he suffers due only to B's serial acts of theft and fraud, and it is only B, not A, who ought to bear any and all related costs and consequences to the extent possible. C does have recourse: B has acquired two separate victims to face, A and C. Each is a victim of different crimes—A of B's theft and then C of B's fraud.

All this still only involves these parties. It is only B, or C, that must return the property to A. Beyond the painting being safely returned, B may well owe additional restitution to A and C as described in Chapter 3. However, this situation creates no justifiable legal obligation on producers of associated goods, services, and infrastructures, who have no relevant control or possession of the items at issue. Say B had sent the stolen item to C using FedEx under a fake name. If, during transit, FedEx became aware that the item actually belonged to A, it would have to halt its delivery to C and return the item to A (and sue B for the trouble). In this case, note that FedEx does have a descriptive ability to reroute the package.

After the delivery, though, even if C acquires a legal obligation to return the item to the still-current rightful owner A, FedEx does not thereby acquire any legal obligation to ship the item for free to A on C's behalf. All of A's and C's expenses, respectively, must be recovered from B, including the innocent C's cost of FedExing the stolen item back to A.

A key assumption in the sequence of arguments about bitcoin quoted near the beginning of this chapter regards the locus of unit control within the Bitcoin network. In contrast to the passage's implied assumption, however, miners and node operators cannot alter the constellation of bitcoin possession other than with regard to specific bitcoin under their own control. Likewise, none are positioned to reverse any past transaction. Unlike the FedEx example, *even if* node operators and miners faced some purported legally enforceable obligation to alter bitcoin possession, they have no way, practical or otherwise, to comply. Never do any of them, or even all of them together, acquire any capability to transfer bitcoins, the signing keys for which they do not possess.

They also have no practical way to identify any given party sending pseudonymous transactions to the network. The Bitcoin network in no way "points to C." C's identity is, in principle, unknown. It might be surmised through specific and costly processes of investigation whose outcome even then remains only probabilistic. There is no way for them to distinguish whether any given transaction is a payment, a theft, or something else.

Bitcoin was set up to create a form of digital cash. Certain cash qualities are undermined if each unit must be assessed for its historical pedigree before being accepted in payment. The absence of certain central features would also imply the absence of critical value propositions of the system for all users. These include censorship resistance, privacy, fungibility, and the reliability of bitcoin as a form of irreversible digital cash. Even if a certain node operator or miner might *wish* that brain-wallet sweeping transactions would not pass his way, by following the protocol and helping to make Bitcoin operate at all and for anyone, he accepts the absence of non-technical

discrimination as an essential part of the nature of the Bitcoin protocol.

There are additional conceptual problems with the idea that network contributors could possibly alter the constellation of bitcoin possession. Even if they could, which they cannot, on whom in particular should such a hypothetical obligation fall and why?

Thousands of globally dispersed and sometimes quasi-anonymous parties participate in providing bitcoin mining and node services on a no-obligation, volunteer basis. On which shoulders should fall any alleged obligation regarding a case otherwise involving only the parties A, B, and C? All who have ever contributed? Only those who were contributing in general at the time? Only those directly involved in relaying or mining the specific transactions at the time? Only those now currently participating, regardless of whether they had been participating at the time?

Any miner or node operator can drop in or out of the network at any time. None has any contractual or other obligation to either contribute to this network infrastructure or withdraw from such participation. Moreover, particular related acts by infrastructure providers cannot be causally attributed to specific transfers *ex ante*; their particular involvements with given transactions are random and unpredictable.

The economic or legal character of a given transaction cannot be ascertained from *within* the network. Such information as it does contain could only be used as one type of evidence among others from a larger case story. Such evidence must extend beyond the network to the human settings, identities, and contexts in which a transaction was sent.

Neither Bitcoin infrastructure providers, nor for that matter providers of general internet infrastructure over which Bitcoin peer-to-peer messages are relayed, took any action to support B's theft. And after the fact, they could not comply with any legal order to reverse a transaction. They never acquire any ability to transfer control of the bitcoin units at issue.

Transaction irreversibility is among Bitcoin's central value propositions and core characteristics. A hypothetical system in which some miners and node operators, or all of them collectively, could reverse specific transactions or otherwise alter possession is *not* Bitcoin and would constitute a separate topic.

If B is found liable for his acts, it is B who must take corrective steps and bear the consequences vis-à-vis A and C. If B is to repay bitcoin at issue to A directly in kind, he must initiate a new transaction that does so. No "reversal" exists, but nor is one required. Restitution findings concerning non-unique property are likely in any case to be estimated, denominated, and payable in money, and it is B's responsibility to pay A this amount from B's own assets or earnings (Chapter 3). This is all between A, the victim; B, the thief; and possibly also C or D, who were B's second and third discrete victims in his criminal sequence.

Unique vs. interchangeable items

With regard to unique items such as paintings, party A would not lose his original property right to re-acquire specific possession of that item even with some extension of the subsequent possession chain after an initial theft. A practical limit to such extension is that sufficient evidence is required to show that A has a title claim superior to that of the latest possessor.

This is the proper role of "possession is nine-tenths of the law," although I would modify the saying to state that law is concerned with the tenth of cases not already sufficiently covered by possession. Possession is presumptive evidence of ownership *unless* another's claim is found to be superior, as in "the better-claim test."[18] It must be demonstrated that a misalignment between ownership and possession has been brought about. If so, even party Z may have to return the item directly to A regardless of the entire intermediate possession sequence of C–Y, all of whom had bad title, but (we presume for simplicity) were unaware of this. Throughout this chain, party A never ceased to be the sole rightful owner.

The potential for complexity here is somewhat less than it may at first appear. If the final possessor Z had to return an item to A, Z and only Z would then have to deal with B for recovery of Z's losses. Parties C–Y are 1) no longer in possession of any property owned by A and therefore have no obligation to return it and 2) have committed no rights-violating acts themselves (assuming they were each unaware of the invalid title chain). The legal case may therefore simply reduce to the last holder of what turns out retrospectively to have been a hot potato—in this case that holder happens to be Z—having to seek redress from B. This still leaves only three parties, A, B, and one other party, the final possessor of A's stolen property at the time this property relationship is discovered and legally established for this purpose.

With a fungible item such as money, however, applying the same principle risks undermining fungibility if specific units are forever subject to direct return to an original victim, leading to potential absurdities and

[18] Described in Graf 2011, 19–21.

impracticalities the longer the subsequent chain of possession becomes. Each money user would then face an added uncertainty of having to return unexpected amount X to unknown and unrelated party A at any time in the future. This would greatly raise the general risk of using money in society.

Traditionally, specific money units were seldom sufficiently identifiable to make recovery of given units practical after they began to be passed on in varying amounts among widening circles of third parties. In a case of a stolen bag of 100 florins, at first, there was a single bag containing the coins. As soon as the thief was able to start passing them off, they started to become dispersed and lose their transient identities as "the coins that were in that bag." After a few rounds of circulation, a large number of unrelated parties with increasing geographic dispersion possessed some coins from the heist. This already freely multiplied the difficulty and cost of direct recoveries from final possessors as in a unique-property model.

The rapid multiplication of such complications helps explain why treating money as "property" for this purpose and in this way is soon unworkable. Yet this specific and practical exception does not generate grounds for not protecting A—rather than B—as being the rightful "owner" of the original bag of coins for the purpose of determining whether B is a thief.

With Bitcoin in its current state, a record of the history of each unit exists and could theoretically be traced. Still, with each transaction, some units (inputs) are broken up and reassembled into often differently sized other sets of units (outputs) with possibly multiple sets of sources and destinations. This is so provided only that the total outputs add up to the total inputs less transaction fee at each step. These differently sized outputs can be transferred at

varying times and stages to multiple other parties instead of one at a time as with a single non-divisible item. This is somewhat analogous to change-making, but unlike florins, there is not even any enduring and indivisible "coin" called a bitcoin that remains over time; only a history of variously sized and changing transaction inputs and outputs across time and addresses.

Fungible items may therefore be treated differently than specific unique property under various legal principles and practicalities. Bitcoin has fungibility characteristics, but also has some unit traceability. The likely solution in these cases, in which the practical identifiability of the stolen goods rapidly degrades with each subsequent transfer, is to restrict legal recourse directly between A and B, and possibly C. This could be a valid reason to call bitcoin "money" and not "property" for this particular application and context, to which certain implications of the word "property," as referring to specifiable unique items, cannot be usefully applied.

What remains clear across all such possible variations is that any parties wishing to recover damages for their losses under whatever other specific legal principles may apply, must all seek such recovery from B, not anyone else. It is only B's acts in these examples that are the unique causal factors back to which all subsequently established damages trace. Likewise, Bitcoin network contributors and other utility providers as such acquire or retain no factual ability or justifiable legal obligation to alter effective possession of any of the units in question.

6

Rival goods, property theory, and artificial scarcity

The scenarios in the foregoing chapters seem to limit the bitcoin ownability question's practical importance. Nevertheless, considering it closely might better clarify legal theory or raise additional questions. While unimportant in the most common trespass cases, it might still be a debatable point in certain brain-wallet sweeping cases that come to a legal process. Answers might also be important to some other types of cases, or areas of law not considered here.

Is it possible to "own" bitcoin or is this just the result of a poor analogy from the old legalistic/material age? What is a "bitcoin" anyway? Can such a thing even be located in reality? If not, how could "it" be "stolen"?

I examined economic-theory concepts such as goods, scarcity, commodity, and money in light of bitcoin in Graf 2015, providing definitions and step-by-step analyses. Here, I will list some of that paper's conclusions and consider how they may bear on ownability. It found that bitcoin is: 1) an economic good, 2) a rival good (which is a sub-type of scarce good), 3) a type of rival good known as a "commodity," 4) a new type of commodity called a "digital commodity," and 5) a "digital monetary commodity" (with unprecedented monetary characteristics).

In arriving at these findings, starting in early 2013, I returned to first principles, reread relevant classics, and applied methods and definitions. First, I researched to

understand what Bitcoin is and how it works in contextually sufficient technical detail. This is the single most neglected step among observers beginning from social-theory perspectives.[19] Second, I applied a strict Misesian action-based approach to the relevant social-theory concepts. Such concepts should, in this view, be grounded in action analysis, and only secondarily informed by characteristics of particular goods, services, or acts for specific interpretation.[20]

Third, I applied a sense of scarcity that is important to property theory—the rivalness of some types of goods. Under the approach to property theory on which this is based, were it not for scarcity of goods, there would be no reason for property rights to arise.[21] Given the existence of scarcity, however, property rights are a superior means for addressing it. If they did not exist in some form, they would have to be invented. Human societies are impoverished more or less in proportion to the unpredictability and insecurity of property rights.

Hoppe had explained the connection between scarcity in general and property rights this way:

> For a concept of property to arise, there must be a scarcity of goods. Should there be no scarcity, and should all goods be so-called "free goods" whose use by any one person for any one purpose would not in any way exclude (or interfere with or restrict) its use by any other person or for any other purpose, then there would be no need for property. If, let us say, due

[19] To help ease introductory technical pains, see Graf 2014.

[20] Mises 1998 and 2007.

[21] Hoppe 2004, 2006, and 2010; Kinsella 2001.

> to some paradisiac superabundance of bananas, my present consumption of bananas does not in any way reduce my own future supply (possible consumption) of bananas, nor the present or the future supply of bananas for any other person, then the assignment of property rights, here with respect to bananas, would be superfluous. To develop the concept of property, it is necessary for goods to be scarce, so that conflicts over the use of these goods can possibly arise. It is the function of property rights to avoid such possible clashes over the use of scarce resources by assigning rights of exclusive ownership. (Hoppe 2010, 18)

In economics, the word scarce can also be viewed as implied within the definition of what an economic good is. In that case, scarce could not distinguish some types of goods from others. In this view, goods are either "scarce" by definition or are not "goods" with respect to action, but mere background conditions of action (Rothbard 2004, 8). In shifting to property theory, something narrower would be useful to distinguish which *types* of goods should be considered ownable and which not.

After considering the treatment of IP rights under this approach (Kinsella 2001), I settled instead on *rivalness* to denote the more specific sense of scarce that is most essential to applying this type of property-theory reasoning. It is rivalness in particular that best distinguishes goods that qualify as ownable. This emerges most clearly in deconstructing the grounds for IP rights and in considering the phenomenon of artificial scarcity.[22]

Rival is also more specific than scarce, for example, in that it need *not* be contrasted with superabundant. Superabundant bananas are in this state only contingently

[22] Kinsella 2001, Tucker and Kinsella 2010, and Graf 2015, 56–57.

due to what surrounds them. Bananas, unlike, for example, personal opinions on bananas, could soon *become* scarce under other circumstances, such as if banana rot were to afflict this paradise.

Regardless of the current state of a particular banana's surroundings, however, that banana always has the characteristics needed to become a rival good as soon as human actors begin to treat it as an object of action. It can become subject to natural rivalry in that it is a material object. It could become legitimately owned through a claim made after superabundance ends. In contrast to this, the opinion statement, "bananas have too many carbs" could not ever become subject to legitimate ownership regardless of external conditions such as the number and sources of printed instances of this statement.

A banana can therefore already be distinguished as a type of object that is own*able* based on the criterion of rivalness alone. However, this cannot be said if the analysis is based on scarcity in general as contrasted with superabundance. Such scarcity is only a contingent descriptor that pertains to the environmental conditions surrounding the object, rather than to the nature of the object itself when considered in its potential or actual relation to human uses in social contexts.

IP rights, tradable claims, and fiat money

Property rights concepts have been subject to various corruptions and misapplications, foremost by rulers dispensing political favors in "legal" forms. For example, IP rights arose through misapplying otherwise correct basic property rights concepts to *nonrival* goods such as ideas and methods. This served censorship, favoritism, and economic cronyism.

Once such practices are established and then later spread more broadly, they can become self-feeding in a culture. Intellectual privilege laws are one category of law in which aristocratic forms of corruption were democratized—instead of being stamped out. In democratized forms, they now function as ongoing class subsidies, which quietly buy off and corrupt large numbers of intellectuals in general and cultural and economic innovators in particular in favor of the state as a seemingly indispensable source of rent-transfer largess to themselves (Hayek 1949).

Assigning legal rights to nonrival goods amounts to the legalistic creation of *artificial scarcity* through law. If an essential problem of human action is making trade-offs necessary due to the natural phenomenon of scarcity, the legal creation of artificial scarcity amounts to the political production of "bads." This contrasts with the economic production of "goods." The latter is the principle way to diminish, and the former to enhance, the pains of scarcity.

Such political production of artificial scarcity also sets up internal contradictions in operative legal principles, and this has further serious negative consequences such as net economic losses for society (Boldrin and Levine 2008) and a general rise in politicization and economic and legal unpredictability. This pervasive corruption of property rights concepts through their categorical misapplication, and the serious consequences that follow, give some legal theorists reasonable pause when hearing claims that an immaterial data construct such as a "bitcoin" is "ownable." That sounds identical to the IP category error.

The concept of artificial scarcity also explains why arguments in favor of considering bitcoin a rival good, as developed below, do not also apply to fiat money units. I discussed artificial versus natural scarcity in Graf 2015 in

the context of monetary theory. This particular natural/artificial dichotomy does not contrast artificial with natural in the sense of not touched by human hands, but rather with natural in the sense of being part of the essential and defining character of what a thing is. In this sense, bitcoin's rivalness is part of what defines it as being bitcoin, whereas this statement does not apply to fiat units. A unit without bitcoin's particular characteristics of rivalness would not *be* bitcoin. These characteristics are therefore "natural" to it, rather than being "artificial," or added onto it, as they are with fiat units:

> In monetary affairs, a similar blend of legalistic and technical artificial-scarcity measures [similar to copyright laws and DRM measures] are employed to combat the unauthorized replication of official paper slips (counterfeiting) and restrict to authorized members of national and supranational banking cartels the special legal privilege of issuing bank money, the private "fountain pen money" that flows from the pens of loan officers into upwardly revised digital account balances.
>
> How can bitcoin be interpreted in terms of such natural and artificial scarcity? The intuitive answer, that bitcoin is likewise "artificially" scarce, may not end up being entirely correct, but to argue this requires turning to a different concept—rivalry.
>
> A rival good is one that different parties *could not use* simultaneously for different incompatible purposes without coming into physical conflict. These are mainly physical goods as we most ordinarily think of them; they cannot be literally "copied," each one must be *produced*. A nonrival good, in contrast, is one—such as an idea, method, or digital file—that *can* be copied or emulated freely. Moreover, each copy or instance can be put to simultaneous parallel uses without direct mutual interference. The concept rival thus specifies a

> descriptive relationship between the nature of certain types of goods and their objective employability when used in a social context. (Graf 2015, 56)

Bitcoin units, by the inescapable nature what they are, exhibit rivalness, but this is not the case with fiat money units. Their scarcity is not an essential characteristic of their identities. It must be maintained through legal and technical artifices such as assigning special legal status, criminalizing counterfeiting, and selectively licensing and then closely regulating otherwise illegal fractional-reserve lending practices. As a factual, descriptive matter, fiat units *can* be copied and replicated *ad infinitum*. And in fact, only maintenance of some degree of artificial scarcity measures help prevent this from coming about. It only so happens, as a historical contingency, that fiat units are not so prolifically reproduced as they possibly could be, except during events leading to hyperinflations.

A fiat unit that is prolifically produced is still the same fiat unit, there is just more or less of it. Its identity and definition as a unit (though not necessarily its reputation and market value) remain unaltered. In contrast, a cryptocurrency, new units of which are produced at some schedule other than the one specified in the Bitcoin protocol is not bitcoin, but some other unit instead, a member of the vast club of hundreds of other altcoins.

Pieces of paper, including banknotes and various deeds and certificates, can be owned—in their capacity as physical objects. Thefts of such papers, such as via trespass and burglary, might entail wider losses and financial damages to the victim in excess of this literal paper value (Chapter 3). A certificate of stock or of title to real estate or a vehicle is likewise ownable in its capacity as a physical piece of paper. The significance of such documents,

however, is as a form of *evidence* to show ownership of the other real property to which they constitute formal titles.

A digital version of such titles and deeds could likewise be stolen through trespass by hacking, but this information *itself* would not be ownable. In both cases, though, some other ownable property would likely have to be employed without consent to obtain these documents, creating a separate basis for a legal case. The property to which the paper or digital deeds indicate evidence of ownership remains rightfully that of its owner. If the thief of the title information tries to use this in some type of fraudulent claim to such property, additional grounds for a legitimate legal case emerge.

Unlike fiat money notes viewed as pieces of paper, fiat bank account entries are not ownable goods, although bank computer systems are. The fiat account units themselves are merely arbitrarily constructed information blips of the same kind that bitcoin's detractors construe it also to be. Yet while both are indeed forms of information, the similarities stop there. As explained above, a key distinction between them is in the basis on which they are scarce. Fiat units are scarce only contingently. They are symbolic tickets issued and managed under alliances of states and banks.

Many users construed some direct ancestors of fiat units to be bearer certificates exchangeable for amounts of gold or silver. However deluded they may have been in doing so, users actually valued these paper slips as claims to specified amounts of precious metals. But a total of such goods corresponding to the total of such paper claims almost never existed in the relevant vaults. This might still be the case today in the form of "paper gold" investment funds with questionable correspondences to real instances of the specified metal. The last official remnants of the

always-tenuous association between monetary paper slips and metals were wholly and frankly repudiated in 1971.

Bitcoin has no such sad history. It has never been valued as anything other than itself (Graf 2013). It is not and never has been a title or claim to any other good.

One might argue that "colored coins" could be an exception. This refers to taking nominal bitcoin units and cryptographically marking them as claims to other goods to facilitate trade in those goods. A physical image for colored coins would be taking a penny and securely impressing it with additional unique information that entitled its bearer to one ounce of silver. The marked penny would then no longer be valued as a penny, but as a tradable claim to a silver ounce. However, this specific add-on use would not explain the original value of an unmarked penny *as* a penny.

A bitcoin unit that was later marked to function as a colored coin was not previously valued based on any such fixed substitution for something else. Bitcoin's value does not "trace back" to its having started life as a substitute for anything else. It is nothing other than the good itself, that which market actors have valued and traded directly from its first emergence as an economic good, born of a computer science project that had earlier gone live on 3 January 2009.[23]

Bitcoin only *later* became a digital monetary commodity when users began to employ it as one. In a previous publication,[24] I reviewed the history of bitcoin

[23]tradeblock.com/bitcoin/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

[24] Graf 2013, Appendix A, "Monetary interpretation by year."

price formation and trading types and arrived at the following rough characterizations: "2009: Technical experiment with no functioning monetary uses. 2010: Growing technical experiment with more organized trading of bitcoin as a novel digital investment good. 2011: First clear pattern of facilitating purchases of goods and services."

Bitcoins *were* just blips in a computer science project. This was the case well before they also later became economic goods and then a medium of exchange. These economic functions were able to *emerge* with time and trial and error on top of the original technical substrate (more on field layers in Chapter 8).

Although the experiment in this case *was* designed to provide just such a substrate, the process of creating it was quite separate from people later actually taking up the result to use in various economic functions. Monetary valuations of gold were able to emerge on top of an original chemical substrate forged in distant supernovas billions of years earlier. In that case, the exploding supernovas presumably did not manufacture the gold with any hopeful intent of possible future monetary applications by as-yet non-existent two-legged life forms. In both cases, however, certain people later found these technically describable pre-existing things, and then actually began using them in various ways that are explainable with economic theory.

7

Measurability and claim operationality

Since rivalness is a foundational concept in action-based property theory, applying such theory to bitcoin must entail determining whether bitcoin is a rival good. What counts for applying action-based concepts such as "good" and "rival" is that the objects of action that are under consideration either qualify or not under these terms' meanings. There is no rigorous way to define them without reference to action. A universe with no acting beings contains no economic goods, no economics, and no phenomena describable as "legal" or not.

When it comes to property rights, an actionable or "operational" system must include recognizable boundaries and claims if people are to know *ex ante* what they are or are not permitted to do within that rights system. The infamous vagaries of what persons may or may not do in relation to copyrights and patents provide examples of how to do this poorly.

What does or does not constitute "fair use" of copyrighted material? This can vary by year, country, interpretation, use, user, and formal *ex post* legal outcome by case. How long does a copyright remain in effect and why this length of time and not some other? This also varies by year and country, etc. and is periodically altered (almost always lengthened) by legislative decree.

But it is the patent-litigation industry that demonstrates best how utterly a confused property-rights

system can fail to provide clear and actionable *ex ante* advice as to what actions are or are not permitted in relation to rights as specified under that framework. It also illustrates how much wealth agents operating within legal systems based on confused legal theory can divert away from primary productive economic actors to themselves.

Hoppe has explained the need for clear boundaries and definitions of property, for example, as follows:

> In this [Lockean-Rothbardian] intellectual tradition, property is defined as tangible, physical objects which have been "visibly" lifted out of the state of nature of un-owned goods through acts of appropriation and production…Objectively ascertainable borders of property are established and specific objects connected to particular individuals. There are indicators of owned (as compared to unowned) objects and of who owns them (and who does not), for everyone to "read." Moreover, the theory fulfills perfectly the requirement of being operational in that it traces all present property back to acts of "original appropriation." (2004, 88)

This introduces a challenge to the thesis that bitcoins are rival goods, particularly with regard to property theory. They are clearly not "tangible, physical objects" as the above passage specifies. However, let us nevertheless examine the above criteria more closely in light of bitcoin.

Bitcoin units do not exist in a generalized, abstract, or undifferentiated state. They only exist as specific units, varied in size, called unspent transaction outputs (UTXOs). Only persons who possess the signing keys specified within each UTXO can sign and therefore spend them (which amounts to transferring their assignment to other addresses). This is closer to the passage's "specific objects" (UTXOs) connected to "particular individuals" (those in possession of the respective keys).

Moreover, each new bitcoin produced is discovered at a specific time by one particular miner and no other. When a new block is mined, the miner's own address is included for taking control of the corresponding block reward. The protocol thereby assigns effective control of each new bitcoin unit unequivocally and in a single publically recorded instant. This assignment, albeit pseudonymous, is still specified between object and controller, and as such is at least as clear as many first appropriations of physical goods and locations.

In this way, bitcoin assignment appears to go some significant way toward fulfilling "the requirement of being operational in that it traces all present property back to acts of 'original appropriation.'" As clarified in Chapter 5, only possessors of the specific requisite signing keys can send valid transactions, and infrastructure contributors in their capacities as node operators and miners cannot spend bitcoin assigned to addresses for which they lack signing keys, leaving no control ambiguity on this point.

A time-stamped, unforgeable public record of the appropriation and transaction history of every bitcoin unit exists. While this record can only indicate effective control and possession, not rightful ownership, in the vast majority of cases, such possession can be assumed to be rightful, unless it is established that some rights violation has led to a wrongful alignment of such control.

"'Visibly' lifted out of the state of nature of un-owned goods" refers to the need for markers that others can recognize, indicators "for everyone to 'read.'" It is impossible to respect a property right when one cannot ascertain its existence, such as when it is impossible to distinguish something that is owned from something that has been abandoned or was never claimed.

Although the blockchain does not directly reveal *who* controls each UTXO, it is clear that either some party controls each one or access has been lost, rendering the UTXO permanently unusable. Total signing key loss extinguishes the corresponding UTXOs from their former roles as economic goods.[25] With some extremely minor and technical exceptions, in principle, usable UTXOs do not exist in any unclaimed state of nature. The fact that someone else has possessed them first is clear.

The rivalness of economic goods has been understood largely through physics-measurable properties. This includes coordinate-definable spatial locations (such as "land"), material goods and resources, electromagnetic spectrum (due to signal interference), and even spatial locations as further specified in the "forth dimension" of time, such as air and shipping routes.

Bitcoins as tradable informational objects, however, lack such properties. Therefore, an observer defining rivalness in physics terms, rather than directly in terms of action, is likely to conclude that bitcoin must be nonrival.

However, rivalness itself is at issue and bitcoins cannot necessarily be excluded from action-defined categories merely due to an absence of physics-measurable characteristics. True, such characteristics have long served as reliable proxies for rivalness. Dominant factors such as the nature of materiality and the impossibility of two objects or persons occupying the same location at the same

[25] Single-key loss, including loss of all backups, would be unrecoverable. In the case of multi-signature wallets, loss of marginal keys could be tolerated. For example, in a 3-of-5 multisig wallet, any three keys would suffice for spending and any two keys could be lost without the funds becoming unrecoverable.

time had been mostly sufficient to explain which goods were rival.

Using physics properties as proxies for rivalness *was* a reliable intellectual shortcut, but this appears to fail when applied to bitcoin, which demonstrates a novel basis on which an economic good can exhibit rivalness. Bitcoins are rival goods *even without* being material or spatial. This rivalness is due to cryptographic and network properties that are part of the essential nature of what a bitcoin unit *is*. In other cases, such rivalness is due, for example, to physical and chemical properties that are part of the nature of what various physical objects *are*. This partly explains Bitcoin's magnitude as an innovation, the historic scale of which can be difficult to ascertain.

8

Some illusions of enlightened explanations

As important as it is to gain at least a basic technical understanding of Bitcoin, attempts to describe what its tradable units "really" are, as elaborated from some allegedly more enlightened perch, can sometimes distract more than aid when applying economic and legal concepts. For example, pundits discussing whether bitcoin falls under what they each consider to be "money" or not sometimes explain that bitcoin is really just a "ledger entry" or a "protocol token," a harmless technical artifact of a promising new "blockchain technology."

Whatever the root of or strategy behind such discourse, however, a bitcoin buyer does not in fact seek a "share in a distributed ledger" or any other such tortured monstrosity. He wants to *buy a bitcoin* in the same sense that he might want to buy a grapefruit. He in no way sets out toward the market to buy a share of a global orchard cooperative that also happens to entitle him to one grapefruit that day.

Nor is it relevant that a grapefruit is "really" organic molecules, water, and some other substances. For that matter, a physicist might go further and insist that a grapefruit is "really" nothing but some occasional quarks suspended in vast stretches of empty space. All such misused reductionism is irrelevant to understanding the buying and selling of grapefruit. It likewise has no bearing on whether grapefruits can be eaten without being paid for and how or if people ought to react if they are.

Economic theory and legal theory are fields concerned with human acts, such as acquiring, holding, trading, and stealing. Action is marked by verbs. If one is interested in understanding the grapefruit market, one does not seek first to master grapefruit-tree cellular biology, let alone quantum mechanics. It is sufficient for economics to view those grapefruits actually being traded as the relevant goods, the production, pricing, and distribution of which are to be examined using economics methods.

In this connection, note Hoppe's comment on the importance of distinguishing action analysis from a "quasi-mechanical model of causation" in legal reasoning:

> In addition to a physical appearance, actions also have an internal, subjective aspect. This aspect cannot be observed by our sense organs. Instead, it must be ascertained by means of understanding (*verstehen*). The task of the judge cannot—by the nature of things—be reduced to a simple decision rule based on a quasi-mechanical model of causation. Judges must observe the facts and understand the actors and actions involved in order to determine fault and liability. (2004, 94)

While distinguishing fields such as economics and law from natural sciences is essential, the attractions of misused reductionism even beckon within and among natural sciences. Anderson (1972) explained a possible reason. This is the temptation to shift the direction of analysis from "downward" toward more fundamental elements to "upward" by attempting to "model" greater complexity and layers of emergence using some of the identified parts:

> The reductionist hypothesis does not by any means imply a "constructionist" one: the ability to reduce everything to simple fundamental laws does not imply the ability to start from those laws and reconstruct the

> universe…The constructionist hypothesis breaks down when confronted with the twin difficulties of scale and complexity…At each level of complexity entirely new properties appear…Psychology is not applied biology, nor is biology applied chemistry (393)…The whole becomes not merely more, but very different from the sum of its parts (395).

This implies the importance of taking care in selecting which fields of knowledge, aspects of the phenomenon, and "layers" of reality are the most relevant to consider in understanding what bitcoin "really" is, including with regard to whether it is ownable.

One must also proceed with caution in applying analogies. For example, it is easy to view bitcoin as "just like" other digital blips buzzing around the internet. However, it should be emphasized that buying a bitcoin is *not* like buying other digital goods, such a copy of a song file. One does not buy *a copy of* a bitcoin, but a bitcoin itself. A bitcoin seller no longer possesses the bitcoin in question after the sale (and contextually sufficient confirmations). When one buys (a copy of) a song file, in contrast, the possessor retains copies from which to make more copies.

Most digital goods, such as documents and song files, are nonrival. They *can* be copied. Multiple people can use multiple copies simultaneously. "Stealing a copy" leaves the original as it was. It is not gone after being "stolen."

Likewise, not only can a whole blockchain be copied, but some key part of its value derives from its actually being so copied and distributed with redundancy to numerous independently operated locations. A signed bitcoin transaction is also a short digit string that can be copied, sent, and resent around the globe in fractions of seconds. These are nonrival goods, as are cryptographic signing keys. With nonrival goods, one person can have one

copy and another can have another and each can control these respective copies independently and simultaneously.

However, this is not the case with bitcoins. A bitcoin *cannot* be copied in any such way. It is rival in the same sense as a physical object or spatial location. In addition, a bitcoin cannot be sufficiently described as "just a ledger entry" because a ledger entry records *something*. This formulation does not explain *what* it is that is recorded.

From a unit perspective, bitcoins function as a digital monetary commodity according to strict economic-theory definitions. From an integral perspective, the units are inseparable aspects of the Bitcoin blockchain. They cannot exist without it and it does not exist without them. There is a nondualistic relationship between bitcoin units and the Bitcoin blockchain. While they are distinguishable conceptually, they are not separable in reality.

Abstract as contrasted with specified

One other argument against bitcoin ownability is formulated with a slightly different emphasis. This is that bitcoins are "abstract" and as such belong together with unownable ideas and methods, not with ownable scarce material goods and locations. While closely related to the argument from materiality, a pivotal issue for this approach is the relevant meaning of "abstract," an examination of which raises additional considerations regarding bitcoin vis-à-vis the binary model of material property rights versus IP rights.

The abstract idea "chair" exists in the realm of ideas and language, which is a realm of copiability and free emulation. However, no one can sit in an abstract chair. Property rights can prevent and settle conflicts only by specifying who has the recognized right to set conditions

on who gets to sit in *this or that* physical chair and when. If one misapplies property rights directly to an abstraction, such as by claiming to own the *idea* of a chair or a *method* for building one, one may then seek to delimit the behavior of everyone who builds or sits in any really existing chair anywhere, setting up an inexhaustible source of conflict.

An alleged owner of Platonic Chair Essence might seek injunctions against anyone who dares sit in any specific chair without prior written permission. More practically, this owner might seek to collect royalties on "chair-sitting instances," aided by some state agency that exists to facilitate the corresponding political wealth transfers.

The conceptual absurdities of applying property rights to abstractions and the resulting potential for *added*, rather than reduced, conflict in society is both clear in principle and documented in practice. [26] It introduces an irreconcilable contradiction into basic legal principles, as between, for example, owning actual chairs and owning the idea "chair" or some method of building chairs or some particular chair design.

Generating and multiplying conflict in society directly contradicts the central potential positive social function of the legal realm. That function is to prevent, reduce, alleviate, and resolve conflict. Viewed positively, such conflict-reduction facilitates dynamic, wide-ranging, and complex collaboration by raising predictability for all participants with ascertainable *ex ante* specification of decision-making rights, as well as their defense if infringed.

However, does this important "abstract" critique, so devastating to the grounds for IP rights, also apply to bitcoin ownability? An assumption that it does could easily

[26] Consider the historical review in Boldrin and Levine 2008.

follow from taking materiality as a proxy for rivalness, seeing no materiality, and concluding logically that rivalness must likewise be absent (Chapter 7).

The following considerations argue against this. No user can control any "abstract" bitcoin whatsoever. Bitcoin units are not abstract if abstract is understood to indicate a *type* of thing such as the idea "chair," rather than a specific instance of a chair that one can sit in. Bitcoin users can only control *specific* unspent transaction outputs (UTXOs) in particular, not an idea of bitcoins in general. The idea "bitcoin" cannot be spent. The most relevant opposite of abstract for this purpose may therefore be uncopiable and rival. Bitcoin is both.

UTXOs are rival goods in that they are *not copiable* for multiple parallel uses. In this way, they are not comparable to ideas or digital files, which are descriptively copiable, with each copy independently usable and reusable. Cryptographic keys are nonrival, *are* just data strings. However, keys do not equal bitcoins, and the ownability question concerns bitcoins. Bitcoin exists only as specific, unique UTXOs that can be spent successfully but once. Each is by nature specified rather than abstract.

9

Following the leads

Property rights understood with action theory are implications of the essential social functions of appropriating, holding, and trading rival goods. Such acts are defining characteristics of human social orders. The clarity and definition of the category rival goods is important to understanding and applying this approach. Bitcoins are novel instances.

Bitcoin fits many of the theoretical criteria that have been cited as necessary for ownability. It is realistically controllable, exclusively appropriable, and exists only as specified discrete units. Block-winning miners exclusively appropriate block reward coins and then hold or trade them. Additional trades proceed through subsequent holders of specific UTXOs. This is reflected in an unforgeable public record of effective possession. UTXOs can only be spent successfully once each. Each spend generates new UTXOs for subsequent unique uses. The replacements' sizes and numbers may freely vary from that of their sources, so long as the total of outputs equals the total of inputs less transaction fee.

However, even if bitcoin were *not* considered ownable, the practical consequences of such a finding appear quite limited. This is because a restitution judgment that includes liability for lost bitcoin may be justifiable just as well based on other rights violations. All that is required is to establish that an act infringed *some* property right of the victim in some ownable thing, and then to assess any and all damages reasonably and causally attributed to this.

Considering the main methods by which any purported property rights in bitcoin are likely to be violated, such as trespass, fraud, or duress, restitution findings in cases involving such acts need not hinge on bitcoin's ownability.

In brain-wallet sweeping, which entails no other rights violation, matters are much more complex. First off, even determining the identities involved is likely to be difficult. Then, even if both of the relevant identities could be established, an argument that weak brain-wallet use constitutes a form of user negligence might render it more difficult to make a successful legal claim that is also then actually enforced. Reputations hang in the balance and countersuits are possible. The case would most likely have to be relatively clear if it were to go in favor of sanctioning and then actually resulting in a forcible collection.

In a brain-wallet sweeping case in which the facts and identities have been established, the theoretical issue of bitcoin ownability could become important to deliberations. Among the types of cases examined in this book, in this one alone a judgment might arguably hinge on this point. A claim of general ownability, and of specific ownership based on it, could be used to counter arguments from user negligence. Deliberations might revolve around attempts to shift the operative legal analogy between "unlocked-door burglary" and "picking up an unmarked dropped item."

Criteria for assessing whether a good is ownable or not include whether it is possible for an owner to control it. In the case of intangibles such as market values and reputations, an alleged owner is descriptively incapable of exercising such control. Attempting it would amount to trying to control and alter the contents of the minds and emotions of others. In contrast, with standard bitcoin addresses, exclusive control of bitcoin units can, indeed, be

exercised. But does the use of a weak brain wallet with substandard entropy undermine this controllability criterion as a basis for an ownability claim case by case? A bitcoin is fully controllable in a strong address, but not in a weak one.

It should be recalled that while theoreticians have their roles, cases must be decided from the bench, not the armchair. Making a judgment in a given case is necessarily also a moral act and legal roles cannot negate individual moral responsibilities. The legal realm, properly understood, defines an outermost sphere of what uses of force can possibly be justified, but it creates no moral obligation to automatically employ the full justifiable extent of such force, or even any of it, in every case.

It should also be emphasized that even if bitcoin's ownability were granted, the blockchain itself is incapable of showing ownership directly. It can only show, at best, mere possession, which, from a legal perspective can be either rightful or wrongful. The blockchain can only show that a particular signing key enables the effective ability to control a given bitcoin unit. It cannot show whether the possessor of this key is the owner, a thief, a fraud victim, a brain-wallet sweeper, or a permitted borrower.

Tempting answers to the title question, "Are bitcoins ownable?" in the foregoing chapters might be summarized on balance as, "yes, but it does not seem to matter much." The qualifications and limitations seem far more significant than recurring apparent reasons for affirmation, such as the presence of native scarcity and rivalness.

This seemingly paradoxical outcome raises a final possibility. Perhaps what we have defined as physics-measurability, which brings together property classes based on materiality, measurable location, and electromagnetic spectrum, does indeed after all need to be

among the criteria for legal ownability. Bitcoin appears to strongly qualify as a rival and scarce good on theoretical grounds, yet in each of the types of cases examined in this book, this characteristic alone does not appear to decisively alter hypothetical just legal outcomes. Bitcoin ownability itself is either superfluous—as in trespass or duress cases in which restitution can be justified on other grounds—or, as in brain-wallet sweeping recovery suits, could produce judgments that appear controversial and arguable even before any given real case starts.

This could follow from the dualistic nature of action. Physics measurability may after all be needed to fulfill the objective (causality) side of this dualism. Even a universally verifiable state of information may not be wholly sufficient. This could explain the paradoxical outcomes that appear to result from using rivalness *alone* as a direct legal criterion for ownability in the novel case of bitcoin units, which exhibit rivalness without themselves having any physics-measurable properties.

That said, the active Bitcoin *network* can be described in physics-measurable terms as a specific set of interconnected computers (and their linking infrastructures) running the Bitcoin protocol. The inseparability of bitcoin units and the Bitcoin blockchain that is shared among these computers (rival imitation blockchains on other networks are irrelevant) means that these units are in fact an aspect of this specific network, which *does* have objective measurable features. Nevertheless, as noted, bitcoin traders deal in bitcoin units themselves and do not seek shares in a Bitcoin cooperative. From an action-theory point of view, the units traded are the primary goods to be considered and these units as such lack physics-measurable properties.

This unexpected sequence of conclusions illustrates the value of process-orientated research. Instead of taking up an intuitive position and then locating evidence in favor of it, which would tend to lead to the reinforcement of one or another initial intuition, new insights are more likely to emerge from beginning with questions, assembling and applying relevant principles and facts, and then following the resulting leads, even when—perhaps especially when—different elements *appear* for a time to point in different directions simultaneously.

Further considerations may be raised, including possible implications from, and for, other areas of law not discussed. It is hoped that the foregoing has better differentiated the several issues, advanced the state of the debate, and above all further indicated the usefulness and clarity of basing legal reasoning directly on the analysis of human action.

References and readings

Anderson, P.W. 1972. "More is Different: Broken Symmetry and the Nature of the Hierarchical Structure of Science." *Science* 177 (4047): 393–396.

Barnett, Randy E. 1986. "A Consent Theory of Contract." *Columbia Law Review* 86: 269–321.

———. 1998. *The Structure of Liberty: Justice and the Rule of Law*. Oxford: Oxford University Press.

Evers, Williamson M. 1977. "Toward a Reformulation of the Law of Contracts." *Journal of Libertarian Studies* 1 (1): 3–13.

Graf, Konrad. 2011. "Action-Based Jurisprudence: Praxeological Legal Theory in Relation to Economic Theory, Ethics, and Legal Practice," *Libertarian Papers* 3, 19.

———. 11 Nov 2013. *On the origins of bitcoin: Stages of monetary evolution.* konradsgraf.com.

———. 19 Sep 2014. "Bitcoin: Magic, fraud, or 'sufficiently advanced technology'?" *konradsgraf.com.*

———. Winter 2015. "Commodity, scarcity, and monetary value theory in light of bitcoin." *The Journal of Prices and Markets*, Volume 3, Issue 3.

Hayek, Frederick von. 1949. "The Intellectuals and Socialism." *The University of Chicago Law Review* (Spring): 417–33.

Hoppe, Hans-Hermann. 2004. "Property, Causality, and Liability." *The Quarterly Journal of Austrian Economics* 7 (4): 87–95.

———. 2006 [1993]. *The Economics and Ethics of Private Property, 2nd Ed.* Auburn, Alabama: Mises Institute.

———. 2010 [1989]. *A Theory of Socialism and Capitalism.* Auburn, Alabama: Mises Institute.

Hülsmann, Jörg Guido. 2003. "Facts and Counterfactuals in Economic Law." *Journal of Libertarian Studies* 17 (1): 57–102.

———. 2004. "The A Priori Foundations of Property Economics." *The Quarterly Journal of Austrian Economics* 7 (4): 41–68.

Kinsella, Stephan. 1996. "Punishment and Proportionality: The Estoppel Approach." *Journal of Libertarian Studies* 12 (1): 51–73.

———. 2001. "Against Intellectual Property." *Journal of Libertarian Studies* 15 (2): 1–53.

———. 2003. "Toward a Libertarian Theory of Contract: Title Transfer, Binding Promises, and Inalienability." *Journal of Libertarian Studies* 17 (2): 11–37.

———. 27 Jul 2006. "The Limits of Armchair Theorizing: The Case of Threats." *Mises Economics Blog.*

———. 5 Jan 2010. "Intellectual Property and the Structure of Human Action." *Mises Economics Blog*.

———. 2011. "Intellectual Freedom and Learning Versus Patent and Copyright." *Economic Notes* No. 113. London: Libertarian Alliance.

Kinsella, Stephan, and Patrick Tinsley. 2004. "Causation and Aggression." *The Quarterly Journal of Austrian Economics* 7 (4): 97–112.

Mises, Ludwig von. 1998 [1949]. *Human Action: A Treatise on Economics.* The Scholar's Edition. Auburn, Alabama: Mises Institute.

———. 2007 [1957]. *Theory and History: An Interpretation of Social and Economic Evolution.* Auburn, Alabama: Mises Institute.

Nakamoto, Satoshi. 31 Oct 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." nakamotoinstitute.org/bitcoin

Ranvier, Justus. 26 Jun 2015. "What is mining, why do we need it, and how much is enough?" *bitcoinism.liberty.me.*

Rothbard, Murray N. 2002 [1982]. *The Ethics of Liberty.* New York: New York University Press.

———. 2004 [1962, 1970]. *Man, Economy, and State, with Power and Market.* The Scholar's Edition. Auburn, Alabama: Mises Institute.

———. 2010 [1988]. "Beyond Is and Ought." *Mises Daily*. August 24. Originally from *Liberty* Nov 1988.

Scott, James C. 2009. *The Art of Not Being Governed: An Anarchist History of Upland Southeast Asia*. New Haven: Yale University Press.

Sechrest, Larry J. 2004. "Praxeology, Economics, and Law: Issues and Implications." *The Quarterly Journal of Austrian Economics* 7 (4): 19–40.

Sima, Josef. 2004. "Praxeology as Law & Economics." *Journal of Libertarian Studies* 18 (2): 73–89.

Szabo, Nick. 2004. "Scarce Objects." nakamotoinstitute.org/scarce-objects

———. 29 Dec 2005. "Bit Gold." nakamotoinstitute.org/bit-gold

Taleb, Nassim Nicholas. 2012. *Antifragile: Things that Gain from Disorder.* New York: Random House.

Tucker, Jeffrey A., and Stephan Kinsella. 25 Aug 2010. "Goods, Scarce and Nonscarce." *Mises Daily.*

Van Dun, Frank. 2004. "Natural Law and the Jurisprudence of Freedom." *Journal of Libertarian Studies* 18 (2): 31–54.

———. 2009. "Argumentation Ethics and the Philosophy of Freedom," *Libertarian Papers* 1 (19).

Wilber, Ken. 1998. *The Marriage of Sense and Soul: Integrating Science and Religion*. New York: Broadway Books.

About the author

Konrad S. Graf has written groundbreaking articles on the new field of Bitcoin monetary theory, and created the *Bitcoin Decrypted* introductory video lecture series. He also formulated and is developing the action-based jurisprudence framework, which argues for more explicit applications of action theory in an integral approach to legal philosophy. He has spoken on bitcoin and on legal theory at conferences in Europe and Australia. In addition to his independent research and writing activities, he has worked as a professional Japanese-to-English translator since 1998.