2015

Cryptoinsurance

Michael B. Abramowicz
George Washington University Law School, abramowicz@law.gwu.edu

Recommended Citation

Abramowicz, Michael B., Cryptoinsurance (2015). Cryptoinsurance, 50 Wake Forest L. Rev. 671 (2015).; GWU Law School Public Law Research Paper No. 2019-17; GWU Legal Studies Research Paper No. 2019-17. Available at SSRN: https://ssrn.com/abstract=3366634

CRYPTOINSURANCE

Michael Abramowicz[*]

INTRODUCTION

The sharing economy has begun to make inroads in finance. Peer-to-peer lending is growing substantially in volume[1] and in academic attention,[2] though it remains less than a rounding error in comparison to more traditional sources of loans. Meanwhile, Congress passed the Jumpstart Our Business Startups ("JOBS") Act,[3] which directed the Securities and Exchange Commission ("SEC") to create regulations allowing crowdfunding in at least some circumstances.[4] The SEC, as of yet, has published only proposed rules,[5] ignoring a congressional deadline,[6] but state regulators have begun to create their own rules for intrastate crowdfunding.[7] Yet, one area of finance has resisted even these tentative first steps: insurance.

[*] Professor of Law, George Washington University. I am grateful to David Abrams, Omri Marian, and Peter Siegelman for helpful comments and to participants in workshops at Boston College and George Washington University, as well as at the symposium. All errors are my own.

[1] *See* Dean Grazioisi, *Peer-to-Peer Lending Is Growing in Popularity with Investors*, HUFFINGTON POST (Mar. 13, 2015, 11:23 AM), http://www.huffingtonpost.com/dean-graziosi/peertopeer-lending-is-gro_b_6856490.html.

[2] *See, e.g.*, Garry Bruton et al., *New Financial Alternatives in Seeding Entrepreneurship: Microfinance, Crowdfunding, and Peer-to-Peer Innovations*, 39 ENTREPRENEURSHIP THEORY & PRAC. 9, 9–10 (2015).

[3] Jumpstart Our Business Startups Act, Pub. L. No. 112-106, 126 Stat. 306 (codified as amended in scattered sections of 15 U.S.C. (2012)).

[4] *See id.* § 302(c).

[5] *See* Crowdfunding, 78 Fed. Reg. 66,427 (proposed Nov. 5, 2013) (to be codified at 17 C.F.R. pts. 200, 227, 232, 239, 240 and 249).

[6] *See* Rory Eakin, *The JOBS Act Is Progress but Much Remains To Be Done*, TECHCRUNCH (Mar. 29, 2015), http://techcrunch.com/2015/03/29/the-jobs-act-is-progress-but-much-remains-to-be-done/.

[7] Steven Davidoff Solomon, *S.E.C.'s Delay on Crowdfunding May Just Save It*, N.Y. TIMES: DEALBOOK (Nov. 18, 2014, 2:56 PM), http://dealbook.nytimes.com/2014/11/18/s-e-c-s-delay-on-crowdfunding-may-just-save-it-2/.

As a trillion dollar industry,[8] insurance might appear to be at least a tempting target for would-be disrupters. And indeed, the Internet has disrupted established insurance business models with price-comparison sites, including a new entrant by Google, which poses a substantial challenge to insurance agents.[9] But this disintermediation has merely facilitated the purchase of insurance from insurers; it has not allowed individuals to compete with insurance companies. This Article argues that cryptocurrencies could enable a new form of unregulated competition for traditional insurers. This new form of competition could occur simply through an offshore insurer that uses cryptocurrency transactions to avoid regulation. A more transformative possibility, however, is that the insurance mechanism could be built into a cryptocurrency, with transactions on that cryptocurrency's block chain used to determine whether insureds have suffered losses and how much they should be paid.

The obstacle to individuals, or to some new business models, of competing with traditionally structured insurance companies is formidable, perhaps so formidable as to appear insurmountable. Insurance is a heavily regulated industry.[10] Banks are highly regulated too, but there is a long tradition of friends making loans to one another with simple contracts or contributing funding to others' business ventures.[11] Peer-to-peer lending can arise on the theory that such lending is *not* banking, and crowdfunding could perhaps be legitimized on the theory that such contracts are *not* securities. Individuals, in principle, could enter into individual contracts of insurance, but coordination or aggregation of many such contracts seems likely to trigger regulatory scrutiny. Meanwhile, individual contracts do not provide much economic benefit. Insurance is a mechanism for pooling risk.[12] Individual contracts of insurance can only transfer risk.

[8] *Industry Overview*, INS. INFO. INST., http://www.iii.org/fact-statistic/industry-overview (last visited Sept. 10, 2015) (reporting that total industry premiums totaled $1 trillion in 2013).

[9] Conor Dougherty, *Insurance via Internet Is Squeezing Agents*, N.Y. TIMES (Jan. 18, 2015), http://www.nytimes.com/2015/01/19/technology/insurance-via-internet-is-squeezing-agents.html?_r=0.

[10] JOHN L. MAGINN ET AL., MANAGING INVESTMENT PORTFOLIOS: A DYNAMIC PROCESS 108 (3d ed. 2007).

[11] *See, e.g.*, Daniel Bortz, *How to Lend Money to Family and Friends*, U.S. NEWS & WORLD REP. (Aug. 22, 2012, 9:15 AM), http://money.usnews.com/money/personal-finance/articles/2012/08/22/how-to-lend-money-to-family-and-friends.

[12] *See generally* KENNETH S. ABRAHAM, DISTRIBUTING RISK: INSURANCE, LEGAL THEORY, AND PUBLIC POLICY (1986) (explaining the method behind and the purpose of insurance).

While it might be possible for a wealthy individual to underwrite a personal insurance contract for a less wealthy individual, for the risk-pooling benefits to approach those that an insurance company can provide, the individual would have to be so wealthy that the individual would likely not want to spend time underwriting personal insurance contracts. To be a viable economic rival to the insurance industry, an upstart business model must provide a mechanism for pooling risk, but it is hard to see how that can happen without triggering the requirements of insurance regulation. The economic significance of risk pooling makes a simple extension of the peer-to-peer lending and crowdfunding concepts to insurance seem unlikely.

Nonetheless, this Article will argue that radical financial disintermediation in insurance is possible—perhaps not in the next decade, though possibly in the next half century. By "radical financial disintermediation," I mean a form of insurance in which the insurers are not regulated insurance companies, at least as regulated insurance companies are traditionally understood. For this to occur the upstart business model cannot play by the rules, for existing insurance regulation presumes that the insurers are insurance companies. Rather, the model must be one in which the upstart model evades regulation, flouting the law but using technology to escape repercussions, at least in the short term while legal institutions evolve to address the challenge. The initial appeal of this business model may, in part, be its avoidance of regulatory restrictions, which saves transaction costs associated with legal compliance and provides products to some insurance consumers at lower rates than they would be able to obtain elsewhere. But the ultimate appeal of the business model will depend on whether it can produce a product that is inherently more attractive than existing alternatives.

We can think of the competition that such a business model produces as "unregulated competition"—that is, competition that established industry participants might face from an unregulated (possibly illegal) product. The sharing economy has already illustrated this form of competition. For example, critics argue that Airbnb has disrupted the hotel industry by ignoring regulations applicable to the renting of rooms.[13] Similarly, Uber has disrupted the taxi market by competing aggressively even in the face of legal declarations that its service is illegal.[14] Similarly, VizEat seeks to disrupt the restaurant industry by providing meals without

[13] *See* Brittany McNamara, Note, *Airbnb: A Not-So-Safe Resting Place*, 13 COLO. TECH. L.J. 149, 150 (2015).

[14] *See, e.g.*, Bos. Cab Dispatch, Inc. v. Uber Techs., Inc., No. 13-10769-NMG, 2014 WL 1338148 (D. Mass. Mar. 27, 2014).

complying with local restaurant regulations.[15] In all of these cases the goal seems to be to illustrate to consumers the benefit of a new type of product, which provides political momentum for legalization, or at least political momentum for adapting the regulatory framework to allow these new services subject to relatively minor limitations. Incumbents may initially respond by urging officials to apply existing rules to the upstarts—effectively barring them—but eventually, incumbents may shift tactics, seeking relaxation of the rules that put them at a competitive disadvantage with the upstarts.

Unregulated competition can be helpful by providing legal experiments that test whether existing regulatory restrictions are beneficial; of course, to the extent that those restrictions are beneficial and are evaded, it can be harmful. Several factors may determine the susceptibility of an industry to disruption from unregulated competition. First, disruption is more likely when the new unregulated business model is legal, or at least when substantial uncertainty exists about whether existing regulations apply to the new business model. Uncertainty about whether those renting rooms or driving cars are subject to hotel or taxi regulation gave Airbnb and Uber plausible deniability that allowed them to continue their business practices in the short term. Second, if existing regulation entails high regulatory costs there is a greater benefit to a disruptive technology. With Uber, for example, artificial limits on the number of taxicabs boosted fare prices and provided a strong incentive for market entry.[16] Third, unregulated competition is a greater danger when the service can be provided in a decentralized way, with central activities conducted remotely, because this makes it more difficult to enforce judicial or administrative decisions. Authorities may, for example, be able to arrest individual Uber drivers,[17] but they appear unable to shut down the servers and bank accounts that make Uber work,[18] and therefore they can only disable a small part of the Uber network.

[15] *FAQ*, VIZEAT, https://www.vizeat.com/pages/faq (last visited Sept. 10, 2015).

[16] Unsurprisingly, the value of taxi medallions has fallen substantially since the advent of Uber. *See* Josh Barro, *Under Pressure from Uber, Taxi Medallion Prices Are Plummeting*, N.Y. TIMES (Nov. 27, 2014), http://www.nytimes.com/2014/11/28/upshot/under-pressure-from-uber-taxi-medallion-prices-are-plummeting.html?abt=0002&abg=0.

[17] Tim Worstall, *This Is Why We Can't Have Nice Things: Uber and Lyft Drivers Being Arrested*, FORBES (Aug. 3, 2013, 11:14 AM), http://www.forbes.com/sites/timworstall/2013/08/03/this-is-why-we-cant-have-nice-things-uber-and-lyft-drivers-being-arrested/.

[18] *See* Pranesh Prakash, *Why It Is Almost Impossible to Ban Uber and Ola in India*, QUARTZ INDIA (Dec. 9, 2014), http://qz.com/308879/why-it-is-almost-impossible-to-ban-uber-and-ola-in-india/.

The claim of this Article is that this set of criteria suggests the possibility of unregulated competition in insurance and thus of radical insurance disintermediation. This might occur in one of two ways, each taking advantage of cryptocurrency as a means of payment of premiums and payout of claims. The first, less radical possibility is that an insurance company, located in a jurisdiction where it is beyond the long arm of regulation, will offer insurance to individuals in other jurisdictions. Cryptocurrency can help such a company do business without access to the global banking system, and it can help establish at least a minimum degree of operational transparency that might provide consumers some assurance. This assurance, however, may be inadequate, as consumers will worry that an unregulated company might simply steal its premiums.

The second, more radical possibility is that the insurance mechanism would be built into the cryptocurrency itself. The mechanism would be an insurance fund whose payouts would be based on a set of decentralized decisions made via the cryptocurrency's block chain ledger. There are three essential elements to this proposal. First, all payments (premiums and payments for losses) will be in a cryptocurrency, like Bitcoin. Cryptocurrencies are themselves a financial product that is difficult to regulate,[19] and such payments will make it more difficult for authorities to interfere with insurance contracts. Second, determinations of whether a loss has occurred will be made in a decentralized way facilitated by the cryptocurrency. Third, premiums will be placed into a fund, which will be used entirely to fund claim payouts and to compensate individuals for participating in the claim resolution process.

Part II focuses on the first of these mechanisms and outlines an evolutionary path toward the second. It imagines a simple insurance product offered by an offshore insurer that merely uses a cryptocurrency as a means of receiving and making payments, and it explains how such transactions could largely protect the privacy of insurance customers while providing sufficient assurance that the insurers were processing claims in a legitimate way. It then details how this simple cryptoinsurance scheme could be improved, by building security protections into the cryptocurrency itself. One approach to improve the scheme would be to require that trusted third-party intermediaries approve of spending to be made by the insurer, as a means of blocking the insurer from absconding with the insureds' funds. A more advanced approach would decide questions such as whether claims should be paid out peer-to-

[19] *See generally* EUROPEAN CENT. BANK, VIRTUAL CURRENCY SCHEMES (2012) (discussing Bitcoin and other virtual currency schemes and their impact on banking regulation).

peer. The cryptocurrency protocol would include rules explaining how to aggregate decision making by cryptocurrency participants, so there would be no need for trusted intermediaries. Part II explains how formal tacit coordination games can structure a decision-making process that gives all participants the incentives to resolve assessments according to consensus normative standards.

Part III builds on this in two ways. First, it describes a simple mechanism that could be built into a cryptocurrency that would allow for provision of insurance without the need for an insurance company. Insurers would place their money into a fund and proposed payouts from the fund would be assessed with the peer-to-peer decision-making mechanism. The peer-to-peer decision makers—anyone who wishes to participate—would be charged with assessing what portion of an insurer's premium was allocated to a loss of the type suffered and what the ex ante probability of such a loss was. At the end of a year, or other designated period, all money from the fund would be distributed directly in proportion to the portion of premiums allocated to the loss and inversely in proportion to the ex ante probability. This simple mechanism is unlike traditional insurance but builds on some features of known insurance schemes, such as a mutual insurance scheme known as La Crema. The cryptoinsurance fund would provide users a guarantee that all premiums would be repaid to insurers, but it would have the disadvantage of not providing ex ante certainty about the level of claim payouts.

Secondly, Part III considers whether cryptoinsurance could feature traditional ex ante insurance contracts while still taking advantage of the security features and assurances provided by the cryptoinsurance fund. It considers both the possibility that a cryptoinsurance fund might evolve additional features, and whether an insurance company using cryptocurrency might be able to take advantage of some of the protections of the fund while still offering ex ante contracts.

Part IV concludes this Article by considering both the private and social benefits of cryptoinsurance. The simplest reason is that it could provide a means of evading various forms of insurance regulation that at least some consumers might not want. A consumer of traditional insurance must pay for the legal costs incurred by the insurance company because our existing system of courts is used to ensure that the insurance company will abide by regulations and will pay claims according to its contracts.[20] There are benefits to this, of course, but costs as well, and it is possible

[20] *See* Philip J. Hermann, *Legal Costs to Insurance Companies and How They Can Be Reduced*, 1964 INS. L.J. 133, 133 (noting that legal fees are the second-highest expense for most insurance companies).

that an insurer might be able to establish a sufficiently good reputation for assessing claims without adjudication. An insurer can also avoid the costs associated with rate regulation, perhaps ultimately to the benefit of the consumer. Meanwhile, the insurance consumer and the insurer can avoid regulation of what must be provided in the insurance contract. This would be of obvious benefit to some consumers (and cost to others) where insurance rate regulation cross subsidizes some consumers at the expense of others—for example, by requiring that insurers cannot discriminate on the basis of sex. This establishes that even if cryptoinsurance benefits some consumers, it is not necessarily socially desirable. Part IV will consider the social benefits and costs that might come with cryptoinsurance, and will assess how regulation might respond to cryptoinsurance in the long term.

II. HOW CRYPTOINSURANCE WOULD WORK

A. *Cryptoinsurance with Existing Cryptocurrencies*

A cryptocurrency like Bitcoin could facilitate cryptoinsurance by making it possible for a party beyond the geographic scope of regulation to accept payments. A full description of how cryptocurrencies work is beyond the scope of this Article, but cryptocurrencies generally do not require a person making payments to identify himself or herself.[21] Rather, the owner of cryptocurrency registered to a particular address simply uses a digital signature to validate transactions that send cryptocurrency to another.[22] A digital signature proves to the world that the person authorizing the transaction used the private key corresponding to the cryptocurrency address, which serves as the public key.[23] Cryptography makes it simple to perform such verifications, but virtually impossible to guess the private key that was used to digitally sign a document.[24] The result is that cryptocurrency transactions are public yet difficult to trace if the recipients of payments do not reveal the source of those payments. Moreover,

[21] Aleksandra Bal, *How to Tax Bitcoin?*, *in* HANDBOOK OF DIGITAL CURRENCY: BITCOIN, INNOVATION, FINANCIAL INSTRUMENTS, AND BIG DATA 267, 272 (David Lee Kuo Chuen ed., 2015).

[22] Alex Hern, *Bitcoin: What You Need to Know*, GUARDIAN (Oct. 4, 2013, 6:49 AM), http://www.theguardian.com/technology/2013/oct/04/bitcoin-what-you-need-to-know-silk-road.

[23] CGI, PUBLIC KEY ENCRYPTION AND DIGITAL SIGNATURE: HOW DO THEY WORK? 3–4 (2004), http://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf.

[24] *See, e.g.*, Mihir Bellare & Bennet Yee, Forward-Security in Private-Key Cryptography (Nov. 2000) (unpublished manuscript), https://cseweb.ucsd.edu/~mihir/papers/fspkc.pdf (describing the cryptographing process and its use).

cryptocurrency transactions are difficult to block. A means by which the United States and the international community have exerted control over rogue financial institutions in other countries has been to threaten those institutions with economic isolation, including lack of access to the international banking system.[25] But if those institutions can receive funds outside the traditional banking system, then they need not fear the long arm of US regulation.

At the same time, cryptocurrency transactions are public and preserved in ledgers that cannot easily be manipulated and are stored in a database that government cannot easily disable.[26] Digital signatures predated Bitcoin, so even before Bitcoin it was possible for individuals to communicate authoritative approval of transactions.[27] The chief innovation of Bitcoin is that it provided a mechanism to ensure that all such authoritative approvals would be kept in a public database not under the control of any single party.[28] There are many copies of this ledger database, known as the block chain.[29] Each block in the chain consists of a list of transactions and includes a "hash value," which is essentially a digital fingerprint that depends on all previous values in the block chain.[30] Any party can add a block to the block chain and receive a reward of new Bitcoins if he can arrange the transactions (along with a field containing a random number) in such a way that the block's hash value is sufficiently small;[31] the threshold changes over time to ensure that a new block is added on average once every ten minutes.[32] Achieving this requires trillions of random guesses and thus a great deal of computer time. While some have attacked this

[25] *See, e.g.*, Gracielle R. Cabungcal, Note, *Paradise Lost? Searching for New (Off) Shores: The State of Bank Secrecy, Fiduciary Mistrust, and International Estate Planning After the Financial Crisis*, 25 QUINNIPIAC PROB. L.J. 67, 83–84 (2011) (discussing international pressure exerted on Lichtenstein and Switzerland); Mike Kelsey, *The USA Patriot Act: Compliance with the Anti-Money Laundering Provisions*, 21 DEL. LAW., 22, 22–23 (2003) (describing the requirements imposed by the Patriot Act on banks doing business in the United States to help combat money laundering).

[26] Lan Pak Nian & David Lee Kuo Chen, *Introduction to Bitcoin*, *in* HANDBOOK OF DIGITAL CURRENCY, *supra* note 21, at 5, 15–16.

[27] *Id.* at 21–22.

[28] *See* Jaume Barcelo, *User Privacy in the Public Bitcoin Blockchain*, 6 J. LATEX CLASS FILES 1, 1 (2007), http://www.dtic.upf.edu/~jbarcelo/papers/20140704_User_Privacy_in_the_Public_Bitcoin_Blockchain/paper.pdf.

[29] *Id.*

[30] *Id.*

[31] L.S., *How Bitcoin Mining Works*, ECONOMIST (Jan. 20, 2015, 11:50 PM), http://www.economist.com/blogs/economist-explains/2015/01/economist-explains-11.

[32] *Id.*

feature of Bitcoin as wasteful,[33] it underlies the convention that Bitcoin establishes for identifying the authentic, authoritative version of the block chain. Given two block chains, each containing legitimate hashes, the authoritative block chain is the one that required more work to create.[34] Removing one copy of the block chain is futile, for others will survive, and removing a block from the block chain will create a version of the block chain viewed as inauthentic.[35] One could manipulate the block .chain to keep transactions off it only by producing new blocks faster than everyone else combined, but the cost of mounting such a "51% attack" is estimated to be in the hundreds of millions of dollars.[36]

The combination of these features means that it would be possible for an insurer to accept money from the public in a way that could be publicly observed and make payouts to the public with equal transparency. The result is that an insurer could be located anywhere in the world—and thus beyond the reach of regulators—but still able to act in a transparent way. Transparency is especially important in the absence of regulation. Potential purchasers of insurance will want to know that the provider of insurance is likely to make payments if the purchasers have a legitimate claim. Of course, observing that the insurance company has received money and has paid out money is insufficient; the public will want to see that the company has paid out money on legitimate insurance claims. (Otherwise, the insurer might simply be making payments to itself.) The insurer could meet this obligation by publicly releasing information on claim payouts.

It might appear that this would sacrifice the privacy of insurance customers, but this need not be so. An insurance customer might consult with an insurer through an encrypted communication, and then both parties might digitally sign a document that indicates the coverages being purchased, including a hash of this document in metadata on the cryptocurrency purchase transaction. This would be a variation on existing services that make very small Bitcoin transactions as a means of providing proof that a particular document existed at a particular point in

[33] *See, e.g.*, Hass McCook, *Under the Microscope: Economic and Environmental Costs of Bitcoin Mining*, COINDESK (June 21, 2014, 6:02 AM), http://www.coindesk.com/microscope-economic-environmental-costs-bitcoin-mining/.

[34] Gavin Wood & Aeron Buchanan, *Advancing Egalitarianism*, *in* HANDBOOK OF DIGITAL CURRENCY, *supra* note 21, at 385, 393–94.

[35] *Id.*

[36] *See* Ali Mohammadian, *Why Bitcoin Will Not Be Attacked*, PANTURE (Apr. 17, 2014), http://www.panture.com/why-bitcoin-will-not-be-attacked/.

time.[37] When making a claim, the insured would need to reveal the contract and information supporting the claim at least to the insurer through an encrypted communication. Even if the possibility of losing privacy when a claim is made was problematic, the insurer could hire one or more reputable third-party auditors to evaluate its handling of a random sample of claims. The claimant would need to place metadata on the block chain indicating that it was making a claim, but it would not need to publicize its claim.

My claim is not that insurance purchased in this way is just as efficient as insurance purchased from a local vendor. To be sure, there are obvious limitations. The insurer would not be able to perform any in-person, ex ante checks to determine whether the individual in fact is eligible to purchase insurance. How important this is, and the extent to which telepresence could adjust for it, would vary from one type of insurance to another. Possibly, it might rely on third parties to perform ex ante inspections, though such individuals would risk being the subject of regulatory enforcement actions, or it might simply rely on paper documentation, such as the medical records of a candidate for life insurance. Meanwhile, the insurer similarly would need to rely on photographs and documents supporting a claim, instead of conducting an in-person inspection. This might increase the danger of fraud, and the insurer might expect that the state would be less likely to prosecute individuals perpetuating frauds against rogue insurers. It would be difficult to measure the costs of these limitations and to weigh them against the benefits of avoiding regulation, which will be discussed later.[38] My point for now is simply that a payment mechanism beyond the control of government makes unregulated offshore insurance seem much more plausible than it otherwise would be.

There is, however, a much more serious obstacle to insurance based on cryptocurrencies as described so far. The problem is that even the transparency that the block chain provides might be insufficient to make customers sufficiently confident to trust the insurer with their money. The ultimate concern is that the insurer might simply decide to take all of the premiums deposited with it and close up shop, perhaps claiming to have lost the deposits due to a third party's theft. Indeed, depositors in what was then the largest Bitcoin bank, Mt. Gox, lost virtually all of their deposits after an alleged theft, amid rumors that perhaps the owners of Mt. Gox simply stole the money deposited.[39] Of course, if Mt. Gox was in

[37] *See Trusted Timestamping on the Bitcoin Blockchain*, BTPROOF, https://www.btproof.com/ (last visited Sept. 10, 2015).

[38] *See infra* Part IV.

[39] Nirupama Devi Bhaskar & David Lee Kuo Chen, *Bitcoin Exchanges*, *in* HANDBOOK OF DIGITAL CURRENCY, *supra* note 21, at 559, 564.

fact the victim of theft, that is hardly reassuring, as a cryptoinsurer might face a similar theft. To be sure, if an insurer is profitable, it might well make more sense for the insurer to maintain its reputation than to pocket the premiums, especially as it would face the inevitability of investigations and the possibility of criminal liability if it sought to perpetuate a massive fraud.

Provision of offshore insurance through cryptocurrencies will thus require further improvements to the cryptocurrency infrastructure. Over time, best practices that could likely avoid theft may become established. For example, cryptocurrency holders can maintain their private keys offline, ideally split into multiple pieces stored in different locations.[40] Further, if reputable cryptocurrency banks are established, an insurer might store its funds in those banks. Of course, other improvements to cryptocurrency might also make an insurance business that uses cryptocurrency more plausible. Most obviously, a cryptoinsurance needs to have a mechanism for overcoming the high volatility of Bitcoin. An emerging cryptocurrency, Bitshares, facilitates this by creating a marketplace allowing its cryptocurrency to be traded with other cryptocurrencies that are pegged to real currencies, such as the dollar.[41] Alternatively, an insurer might immediately exchange Bitcoin deposits for dollars, performing the reverse conversion when paying a claim, but this would invite further concern about the insurer's solvency.

B. Cryptocurrency with Inherent Security Protections

A more powerful means of instilling trust in an insurer using cryptoinsurance would be to build security measures using the cryptocurrency itself. Use of a cryptocurrency itself requires a leap of faith, an expectation that the block chain will truly record a transaction in which one spends cryptocurrency and that the cryptocurrency cannot be stolen by third parties. In fact, as described above, the genius of Bitcoin is that the block chain is so tamperproof. There are no documented cases of anyone stealing Bitcoin except by stealing the private key corresponding to the public key.[42] This level of security stands in contrast with credit

[40] *Store Your CryptoCurrency Using Digital Wallets*, COINPURSUIT, https://www.coinpursuit.com/pages/bitcoin-altcoin-wallets/ (last visited Sept. 10, 2015).

[41] *Price-Stable Cryptocurrencies*, BITSHARES.ORG, https://bitshares.org /technology/price-stable-cryptocurrencies/ (last visited Sept 10, 2015).

[42] *See, e.g.*, Adrianne Jeffries, *How to Steal Bitcoin in Three Easy Steps*, VERGE (Dec. 19, 2013, 1:10 PM), http://www.theverge.com/2013/12/19/5183356 /how-to-steal-bitcoin-in-three-easy-steps (discussing the process behind Bitcoin theft).

cards, where a cybercriminal might be able to place unauthorized charges simply by stealing the credit card number. Credit card companies are beginning to respond to this danger by building encryption into credit cards, but this protection applies only to in-person transactions.[43] The inherent security of cryptography and of the block chain, along with the small transaction costs needed to make cryptocurrency transactions, are in fact drivers of cryptocurrency growth. However, lack of knowledge of cryptocurrency and legitimate concerns about volatility principal impediments cause difficulties for cryptocurrency growth.[44] If a cryptocurrency mechanism could further extend security to reduce the danger of third parties stealing currency entrusted to them, that would in the long run support the growth of cryptocurrency-based institutions such as cryptoinsurance.

A simple possibility would be for a cryptoinsurer to use trusted third parties as escrow agents, preventing the insurer from releasing the funds without the digital signatures of a sufficient number of these agents and enabling the escrow agents to refund premiums if the insurer ceased to perform the task entrusted to it. A rudimentary version of this is already possible, though cumbersome, with Bitcoin.[45] That cryptocurrency includes a "scripting" language that can, for example, require multiple digital signatures to make a cryptocurrency payment.[46] Complex rules encumbering payments, however, might not easily be achieved with Bitcoin. A proposed cryptocurrency called Ethereum goes considerably beyond this, allowing complicated conditions embedded in computer code to be attached to cryptocurrency.[47] For example, Ethereum could be used to facilitate gambling contracts; so long as the code can determine the winner of a bet, it can ensure that winners are compensated.[48] The founders of Ethereum have also argued that it could facilitate "smart contracts," with payments mechanistically determined by computer code.[49]

[43] Marco Santana, *Encrypted Chips Help Fight Credit Card Fraud*, USA TODAY (Jan. 9, 2014, 10:22 PM), http://www.usatoday.com/story/news/nation/2014/01/09/encrypted-chips-help-fight-credit-card-fraud/4400347/.

[44] *See, e.g.*, ALEX TAPSCOTT, A BITCOIN GOVERNANCE NETWORK: THE MULTI-STAKEHOLDER SOLUTION TO THE CHALLENGES OF CRYPTOCURRENCY 4–9 (2014), http://gsnetworks.org/wp-content/uploads/DigitalCurrencies.pdf (discussing the inherent challenges to cryptocurrencies).

[45] Nian & Chen, *supra* note 26, at 13.

[46] *Id.* at 15–16.

[47] Robert Sams, *Ethereum: Turing-Complete, Programmable Money*, CRYPTONOMICS (Feb. 1, 2014), http://cryptonomics.org/2014/02/01/ethereum-turing-complete-programmable-money/.

[48] *Id.*

[49] John Weru Maina, *Cryptocurrency Burst Makes Smart Contracts A Reality, What Happened to Ethereum?*, CRYPTOCOINSNEWS.COM (Jan. 27, 2015),

Insurance provides an example of a context in which a technology like Ethereum, should it become sufficiently developed, could enable cryptocurrency-based transactions. If the cryptocurrency itself can ensure that a payout will be made on a valid claim, perhaps with complex exceptions handling situations such as the possibility that total claims might exceed the available insurance fund, then consumers will be more comfortable purchasing insurance with cryptocurrency. At least this argument applies to consumers who understand the protection that the cryptocurrency provides, just as cryptocurrency growth in general may be fueled by those who understand cryptocurrency's security model. But Ethereum has a significant limitation. The cryptocurrency programs themselves cannot ascertain facts about the outside world, and so they must rely on trusted third parties, dubbed "oracles" by the Ethereum founders.[50] These oracles would make assessments such as whether an insured is in fact entitled to a payout, and more complex arrangements might be constructed in which a decision depended on multiple oracles or allowed for some sort of appeal.

For this system to inspire consumer confidence, consumers will need to trust the oracles. This might be especially problematic if publishing the names of the oracles would leave them open to legal action for promoting unregulated insurance. Even if the individuals did not face the danger of legal prosecution, insurance consumers might not trust them. Trust would require that the oracles have sufficient incentives to make careful decisions, and it is not obvious how Ethereum could provide such incentives. Whether a particular oracle is trustworthy might depend on that individual's reputation, but insurance consumers will likely not wish to investigate the oracles who might assess their claims. In the end, a system dependent on trusted intermediaries is antithetical to the core objectives of a cryptocurrency. After all, precursors to Bitcoin depended on trusted intermediaries to store databases of transactions.[51] The point of Bitcoin is that it is peer-to-peer, meaning that there are *no* specially designated trusted intermediaries. The cryptocurrency protocol itself provides incentives to maintain and identify accurate copies of the block

https://www.cryptocoinsnews.com/cryptocurrency-burst-makes-smart-contracts-reality-happened-ethereum/.

[50] Vitalik Buterin, *Ethereum and Oracles*, ETHEREUM BLOG (July 22, 2014), https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/.

[51] Katherine Sagona-Stophel, *Bitcoin 101: How to Get Started with the New Trend in Virtual Currencies*, THOMSON REUTERS, http://site.thomsonreuters.com/business-unit/legal/digital-economy/bitcoin-101.pdf (last visited Sept. 10, 2015).

chain. If trusted intermediaries are necessary to make cryptocurrency based insurance work, then much of the benefit of using a cryptocurrency is lost.

C. *Cryptocurrency with Built-In Decision-Making Capabilities*

It is possible, however, to imagine a cryptocurrency that could secure funds provided by insurance customers and ensure that payments are made on valid claims without relying on designated third parties. Human judgment is still required, but the cryptocurrency protocol could provide a mechanism for aggregating human judgment. If potential insurance customers trust the mechanism, then they need not trust any individual person. This can be seen as the broader strategy for encouraging trust in cryptocurrencies. Bitcoin and most other cryptocurrencies do not rely on the designation of trusted intermediaries,[52] and individual participants do not need to trust those who are engaging in cryptocurrency mining. The system provides incentives for transactions to be included in the block chain, and even if one participant sought to exclude a transaction in a particular block,[53] others would have incentives to include the transaction in another block. Since no one has a monopoly on creating blocks, each transaction will be included eventually, and so long as one waits to be sure a transaction is included in the authoritative block chain, one need not worry that the money being transferred has already been spent.

The Bitcoin mechanism works because it is a protocol that provides a simple rule for tacit coordination in determining what counts as the correct block chain. Because it is easy to confirm that a block chain meets applicable requirements—the hash of each block connects it to the previous one—and to compare two block chains to determine which one represents more work, there is no room for subjective judgment or for arguments about which block chain is the "correct" one. Of course, one could imagine alternative hypothetical conventions for determining the correct block chain. If one suddenly expected everyone else to switch to some alternative convention, then it would be in one's interest to switch as well; just as if one expected everyone else in the United States to start driving on the left side of the street, it would be in one's interest to drive on the left side too. But there is no reason to expect either convention to

[52] An exception is Ripple. Each client node includes a list of other trusted nodes, and distributed consensus about the correct state of the ledger is obtained through a voting mechanism. *See* Bryant Gehring, *How Ripple Works*, RIPPLE (Oct. 16, 2014), https://ripple.com/knowledge_center/how-ripple-works/.

[53] *See Beginner's FAQ*, BLOCKCHAIN INFO, https://blockchain.info/wallet/bitcoin-faq (last visited Sept. 10, 2015).

change suddenly, and so the existing tacit coordination convention in both cases is powerfully stable. Perhaps one can imagine some scenarios in which an alternative convention might emerge and compete with the existing Bitcoin convention, but Bitcoin is an illustration of how a convention can provide stability without the appointment of trusted intermediaries. Bitcoin's convention resolves the question of how much Bitcoin each person owns.

It might appear that the Bitcoin convention works only because it is entirely deterministic, and thus the same underlying principles can not be used to resolve questions requiring the exercise of subjective judgment, such as whether a person who purchased a cryptoinsurance policy has a valid claim and is thus entitled to a payout, let alone what the payout should be. For cryptoinsurance to overcome concerns about the need to rely on trusted intermediaries, and thus the broader obstacle facing an offshore insurer not subject to regulation, some such mechanism must be built into the cryptocurrency itself, along with the usual security guarantees preventing the insurer from manipulating the cryptocurrency. That is, the cryptocurrency itself must provide a mechanism for aggregating human judgment that would bind the cryptoinsurer. We have seen that a cryptocurrency like Ethereum could do this, but only by selecting trusted intermediaries. The challenge is to do this without selecting intermediaries.

In an in-progress paper, *Peer-to-Peer Law, Built on Bitcoin*,[54] I explain how this could be done, even without software that exhibits general artificial intelligence. The key is for the cryptocurrency convention to include a deterministic mechanism for aggregating human judgment about whether cryptocurrency ownership should be reassigned.[55] That is, the convention need not determine precisely how to make difficult legal judgments, but must determine (if the convention is to be sufficiently stable) how individuals can register their judgments by making cryptocurrency transactions and how these judgments can be aggregated. Such a mechanism could be built on top of a cryptocurrency with programming capabilities like Ethereum, but it could also be built into the protocol of some other cryptocurrency.

To explain how this works, let us first start with a simple example of the system. This simple example has serious problems, but it at least successfully demonstrates the possibility of having a mechanistic approach to aggregating judgments that can be seen on a cryptocurrency block chain. We might allow anyone to put a claim on some existing cryptocurrency (such as some amount owned by the

[54] Michael Abramowicz, Peer-to-Peer Law, Built on Bitcoin 10–11 (Mar. 4, 2015) (unpublished manuscript), http://ssrn.com/abstract=2573788.

[55] *Id.* at 4.

insurer) by creating a very small transaction with metadata establishing the claim. We might then have some period of time in which individuals can "vote" by sending money to accounts in support or in opposition to the claim for this cryptocurrency to be transferred. By convention, cryptocurrency sent to these accounts would simply cease to exist. If the "yes" account receives more money than the "no" account in a particular amount of time (an entirely mechanical assessment), then the cryptocurrency transfer would be approved. Because the cryptocurrency convention, and thus software, would recognize such transactions, the money would be available to be spent by the insured, and no longer by the insurer.

As explained in more detail in the forthcoming article, that is not a good system; it would simply allow those with the most resources to make decisions.[56] But a simple variation on it can make for a drastic improvement. The core extension, elaborated on and formalized in the forthcoming paper, is that those who contribute to the winning resolution receive money contributed to the losing resolution, with the first contributors to the winning resolution receiving funds first.[57] The insured, applying the system to our example, would initiate the decision-making process by putting at least a certain amount of money—presumably, a function of the insurance claim—at stake. This initiation fee provides an incentive for others to investigate the claim and to counter it if they think that it will fail. In deciding whether to counter it, by placing at least as much money on the opposing proposition, participants must anticipate what still further players might do in the next stage, recognizing that they in turn will try to anticipate what others will do after that, and so on. As demonstrated in the article mentioned earlier, a risk-neutral participant's incentive in this game is to counter a move by putting enough money on the opposing position to switch the balance. If the participant is confident that there is further participation, then the further participants will more likely than not take the counter position.[58] That is, each person will have an incentive to correct a wrong decision to make an insurance payout if the person believes that subsequent players would agree that no payment should be made, and the same applies to a wrong decision to refuse an insurance payout.

It might appear that this system is entirely circular. Each participant's incentive is to anticipate what hypothetical future participants might decide. So, if each participant anticipated that others would resolve the question of whether an insured receives an insurance payout by looking for a particular constellation in the

[56] *See id.* at 4–5.

[57] *See id.* at 34.

[58] *Id.*

night sky, then each participant's incentive would be to do so as well, rather than to consider the underlying normative case for the payout. But the question of whether the insured should receive a payout provides a powerful focal point, because that is the question that participants are supposed to be considering, and there is no particular reason to expect participants to use any particular other approach to resolve the question. Just as Bitcoin depends on tacit coordination by participants who realize that there is no reason to expect others to suddenly switch to some alternative convention for the cryptocurrency, so too would this system seek tacit coordination along two dimensions: first, around the principle that the rules of the game determine whether money is transferred; and second, around the normative question that the participants are supposed to address.

That people can coordinate around non-mechanical solutions to problems is not a novel insight. The game theorist Thomas Schelling introduced the concept of tacit coordination games by posing the following problem: Suppose two people must meet tomorrow in New York, but with no communication as to when or where. In his survey, a high percentage of respondents said that they would go to the information booth at Grand Central Terminal at noon.[59] This is the solution that appears most salient for complex reasons that, particularly along the place dimension, cannot be seen as entirely mathematical. Thus, if participants in our insurance game expect others to play the same game then their best strategy will be to determine what is most salient, and the sensible normative solution, all things considered, will generally be most salient, even if that solution may sometimes be controversial or hard to identify. Meanwhile, participants will have good reason to play the same game, since playing any other game, such as the astrological one, would mean that the system would fail and that all would lose. Thus, there is likely to be tacit coordination around the general principle of resolving normative questions and then around the specific perceived resolutions to particular normative questions.

What does all of this mean? It is possible, at least in principle, to have a cryptocurrency that can serve an adjudicative function and can thus serve as the backbone of an insurance scheme. The person buying cryptoinsurance need not trust the insurer. The premiums could be placed into an account that, by convention, the insurer could not spend without approval. The person thus need only trust the system and the distributed aggregated judgment of those participating in it. To be sure, that will still be a challenge for

[59] Thomas C. Schelling, *Bargaining, Communication, and Limited War*, 1 CONFLICT RESOL. 19, 20 (1957).

many, especially when this system is immature. Most would probably want to wait for empirical evidence, or at least anecdotal evidence, that such a system in fact works before committing their own money. Of course, the same general problem exists for any cryptocurrency. Individuals are willing to purchase any particular cryptocurrency only because there is perceived to be some value for that cryptocurrency—a higher-level tacit coordination problem. For cryptoinsurance with built-in decision making to evolve, first a cryptocurrency that has the relevant support for formal tacit coordination games would have to not only merely exist but be viewed as stable and likely to succeed, and then the insurance could be built on top of this mechanism, if it too obtained sufficient agreement. My purpose here is not to predict that cryptoinsurance will emerge despite these obstacles, but rather to demonstrate that cryptoinsurance would be a powerful application for a cryptocurrency, and thus, that formal tacit coordination games might be a useful feature for a cryptocurrency seeking to differentiate itself from competitors.

II. BUILDING CRYPTOINSURANCE

The last Part has suggested that cryptocurrencies could facilitate offshore provision of insurance and that the effectiveness of the insurance business models might depend on the features offered by the cryptocurrencies. Cryptocurrencies in their current form might facilitate insurance sales because they would make it difficult for regulators to block the sales or impose other legal rules, while simultaneously providing at least some means of transparency that could help insurers assure customers that they are in fact making payouts on claims. If cryptocurrencies were integrated with smart contracts that could provide further assurance through trusted intermediaries, customers would know that their money could not be stolen without these intermediaries' assistance. And cryptocurrencies with built-in decisionmaking could provide the greatest level of customer confidence, because customers would not even need to know who the trusted intermediaries are. Of course, all of this presupposes that other problems with cryptocurrencies, including their high volatility, can be overcome and that customers over time can learn about the benefits of the new business model.

So far, though, this has been much more of a description of cryptocurrency innovation than of insurance innovation. Even if a cryptocurrency can perform adjudication, insurance companies are considerably more complex than that. How is a decision-making mechanism alone sufficient to transform a currency into an insurance company? This Part aims to answer that in two ways. First, Subpart III.A will argue that, in fact, an ex post decision-making mechanism alone could be sufficient to build a working system of insurance. Under this system, insurance claimants would receive a stake in the insurance fund proportional to premiums paid and inversely proportional to the adjudication system participants' estimate of the probability of loss. Surely, an argument against this system is that it is not what we do today. But what we do today may be a function of the legal regulatory environment; the insurance company's expectation that it might be sued leads to detailed ex ante contracts. Moreover, even if this ex post system is imperfect, it bears some resemblance to insurance schemes that have worked in the past, and the advantages to some consumers of avoiding regulation (to be discussed in Part IV) may be sufficient to overcome these imperfections.

Subpart III.B, meanwhile, will ask whether cryptoinsurance could be structured to be, in some or all ways, much more similar to traditional insurance, with ex ante contracts, reinsurance, and so forth. That is certainly possible. The cryptocurrency decision mechanism described previously can be used to craft rules, to enter into ex ante agreements, to hire specific individuals to handle and assess claims, and to structure complex institutions. All of this additional institutional complexity, however, means that if cryptoinsurance functions like an ordinary insurance company, then it is unlikely to incorporate built-in decision making. A cryptoinsurance system with built-in decision making could develop complexity over time, but the simple insurance-fund system is more plausible as an initial means for credibly providing insurance through cryptocurrencies.

A. An Insurance Fund with Ex Post Evaluation

1. Historical Analogies

Before describing in more detail how the cryptoinsurance fund might work, it is worth looking at some real-world institutions that have some of the features of the cryptoinsurance fund. First, existing insurance contracts often impose ex post examination to ensure that the insured in fact was eligible to purchase the contract.[60] The doctrine of *uberrima fides* illustrates that ex post assessment can have a significant and beneficial role in insurance contracting.[61] Second, an insurance mechanism from Andorra known as La Crema allows insureds to pay whatever premiums they

[60] Dudi Schwartz, *Interpretation and Disclosure in Insurance Contracts*, 21 LOY. CONSUMER L. REV. 105, 105–06 (2008).

[61] *See* Patrick J.S. Griggs, *Coverage, Warranties, Concealment, Disclosure, Exclusions, Misrepresentations, and Bad Faith*, 66 TUL. L. REV. 423, 443 (1991) (explaining the origins and theory behind *uberrima fides*).

like, with premium amounts then tied to the level of the premium.[62] This considerably reduces the need for ex ante contracting and provides some incentive for honest self-valuation, subject to considerations of moral hazard. Third, a nascent insurance business model is peer-to-peer insurance, which attempts to incorporate information from acquaintances of an insured.[63] This element, like the others, could easily be incorporated into a cryptoinsurance mechanism.

a. The Doctrine of Uberrima Fides

The principal problem of insurance contracting is that of asymmetric information. In many contexts, the insured may have a better idea of its relative riskiness than the insurer. Information asymmetry can lead to adverse selection, where only those with relatively high risk buy insurance, and particularly serious cases of adverse selection can lead to a death spiral, in which progressively higher insurance prices scare off all but the highest risk buyers until there are no customers left. In the canonical model of how insurance companies may overcome the adverse selection problem, Rothschild and Stiglitz suggest that insurance companies offer different insurance policies to obtain a "separating equilibrium," that is, one in which individuals have an incentive to purchase an insurance policy tailored to their risk.[64] In particular, one type of insurance is cheaper but includes only partial coverage, so that it will still be appealing to those with relatively low risk, while another type of insurance provides more comprehensive coverage but is more expensive, appealing to those who have relatively high risk.[65] Such mechanisms, however, are hardly perfect. The low risk types end up purchasing less insurance than they would have if it were possible to determine someone's risk type perfectly, and the high risk types may end up with even more coverage than they would desire with full information. Moreover, a separating equilibrium may not always be possible, and information asymmetry may mean that some types of potentially useful insurance—such as divorce insurance—simply will not exist.

[62] *See generally* Antonio Cabrales et al., La Crema*: A Case Study of Mutual Fire Insurance*, 111 J. POL. ECON. 425 (2003) (analyzing Andorra's mutual fire insurance mechanism).

[63] Paula Newton, *Guide to Collaborative Finance—Part 4*, INTELLIGENTHQ (Jan. 10, 2014), http://www.intelligenthq.com/finance/guide-to-collaborative-finance-part-4/.

[64] Michael Rothschild & Joseph Stiglitz, *Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information*, 90 Q.J. ECON. 629, 638, 643 (1976).

[65] *Id.* at 640.

In some contexts, insurance companies may also be able to address information asymmetry through ex ante investigation of the insured. For example, with health insurance or life insurance a medical examination of the insured may help the insurance company overcome at least some of the information asymmetry. But ex ante investigation is expensive. Thus, in some situations it may be optimal for the insurance company to rely instead, at least partially, on ex post investigation. For example, the insurance company might check the medical records of someone who has incurred large medical bills or who has died after the relevant insurance claims are filed. The feasibility of this will depend on the effectiveness of an ex post investigation and its relative cost.

Professor Avinash Dixit emphasized this point on ex post investigation in a paper on the doctrine of *uberrima fides*, Latin for "utmost good faith."[66] This common law doctrine requires insureds to make accurate disclosures on the insurance application, and "if the answers are found to be false, the company can refuse to pay the claim on the grounds that the customer has not made the requisite disclosures."[67] Professor Dixit offers a mathematical model to examine the equilibrium under a doctrine of *uberrima fides*, in comparison to a Rothschild-Stiglitz equilibrium based entirely on ex ante contracting.[68] Under certain assumptions, he identifies two potential benefits of *uberrima fides*: first, that there will be a larger range of situations in which a separating equilibrium exists and that insurance contracting is therefore possible, and second, that this will be a Pareto improvement, with no loss to those with high risk and substantial expected utility gains to those with low risk.[69]

As Dixit notes, however, "[d]ifferent countries apply *uberrima fides* with different degrees of strictness," and not strictly at all in the United States.[70] One possible explanation for this is that, in practice, ex post investigation is much more expensive than ex ante investigation (so much so as to compensate for the lessened need to apply it), or perhaps, it is much less reliable. But there is another possibility: that the legal system imposes restrictions that prevent optimal insurance contracting. Consumer protection doctrines such as insurance incontestability, which prevent insurance companies from voiding a policy for a misstatement by an insured after a

[66] Avinash Dixit, *Adverse Selection and Insurance with* Uberrima Fides, *in* INCENTIVES, ORGANIZATION, AND PUBLIC ECONOMICS: PAPERS IN HONOUR OF SIR JAMES MIRRLEES 41 (Peter J. Hammond & Gareth D. Myles eds., 2000).

[67] Avinash Dixit & Pierre Picard, On the Role of Good Faith in Insurance Contracting 42 (Jan. 25, 2002) (unpublished manuscript) (on file with Princeton University).

[68] *Id.*

[69] *Id.* at 47.

[70] *Id.* at 43.

specific amount of time,[71] may reflect political concerns or desires to transfer wealth from insurance companies to consumers, rather than attempts to create an optimal contracting environment. Meanwhile, whatever the legal regime, insurance cases are ultimately decided by real people—judges and juries—who may be sympathetic to an insured, especially an individual insured, regardless of the applicable legal requirements.

In short, our existing practice of relying heavily on ex ante contracting rather than ex post investigation may reflect political and legal constraints, rather than solely economic efficiency. Meanwhile, insurance policies may be relatively rigid, containing broad exclusions. This helps the insurer segment pools of consumers, consistent with the Rothschild-Stiglitz model, while also avoiding ambiguous contractual terms. Ambiguous contracts are read against the insurer,[72] and so an insurer may exclude coverage in broad classes of situations, even though it might seem that the broad excluded class contains at least some situations in which the ability to purchase insurance would be desirable. If there were a more reliable, or at least less biased, adjudicative system, this might be less of a concern.

b. Mutual Insurance

While customers may have better information about their own riskiness than insurance companies, the companies may have better information about the companies' riskiness, and thus about their ability to pay claims. Historically, a distinctive aspect of the insurance market is that many companies are mutual insurance companies. That is, they are owned by their policyholders. As Professor Henry Hansmann notes, "the annual volume of business done by the mutual life insurance companies, which are formally organized as policyholders' cooperatives, far outweighs the volume of business done by consumer cooperatives in any other line of business."[73] Hansmann explains this in part by noting that life insurance contracts are written under conditions of great uncertainty, and it may be difficult for customers to assess whether companies maintain sufficient reserves.[74] Even if a customer can be confident that a company currently maintains sufficient reserves, it is difficult for a contract to guarantee that the company will

[71] Robert E. Keeton, *Insurance Law Rights at Variance with Policy Provisions: Part Two*, 83 HARV. L. REV. 1281, 1312–13 (1970).

[72] *See, e.g.*, ABRAHAM, *supra* note 12, at 121; VINCENT R. MARTORANA, A GUIDE TO CONTRACT INTERPRETATION 9 (2014), http://www.reedsmith.com/files/uploads/miscellany/A_Guide_to_Contract_Interpretation__July_2014_.pdf.

[73] HENRY HANSMANN, THE OWNERSHIP OF ENTERPRISE 265 (1996).

[74] *Id.* at 267.

maintain sufficient reserves in the future. Because it is owned by customers, a mutual insurance company is less likely to take large risks at the customer's expense. This advantage of the mutual form may sometimes be sufficient to overcome the disadvantages—such as, in practice, a full separation of ownership from control and reduced access to capital markets.[75]

The mutual insurance form, however, has receded somewhat in popularity, and Hansmann attributes that in part to increased regulation of reserves.[76] With greater assurance that the government will require insurance companies to maintain sufficient reserves, there is less need for the mutual form.[77] This highlights that mutual organization and regulation may be substitutes for one another. This may mean that mutual organization is unnecessary given sufficiently high-quality regulation, but it is also possible that regulation can be excessive, or that some aspects of regulation may be welcome while others are not. If cryptoinsurance is unregulated, the costs of this absence of regulation may, to some extent, be compensated with mutual mechanisms and other assurances that prevent exploitation of consumers, while cryptoinsurance can avoid those aspects of regulation that are not part of the economically optimal insurance contract.

c. La Crema

One form of mutual insurance deserves special attention, even though it is quite rare. Even with *uberrima fides*, the insurance company and the insured must arrive at contract terms, which include the cost of the insurance and the amount that it will be paid out given an insurable event.[78] A system of mutual insurance called La Crema, however, shows that it may be possible to have an insurance contract in which insureds may pay whatever they like for the insurance.[79] Under this system, each household in a village annually announces the value of the property in the village that the household owns.[80] If any household burns down, then the homeowners receive the value that they announced, and this funding is paid by all the other homeowners, in proportion to the

[75] *Id.* at 270, 272–73.

[76] *Id.* at 271–72.

[77] *Id.* at 267–68.

[78] *See generally* Richard E. Kihlstrom & Alvin E. Roth, *Risk Aversion and the Negotiation of Insurance Contracts, in* FOUNDATIONS OF INSURANCE ECONOMICS 264 (Georges Dionne & Scott E. Harrington eds., 1991) (studying risk aversion and its relationship with the bargaining of terms in an insurance contract).

[79] *See* Cabrales et al., *supra* note 62, at 427.

[80] *Id.*

values that they themselves announced for their households.[81] In effect, each homeowner decides how much to pay for insurance, with larger payments receiving larger payouts in the event that a claim materializes.

In a mathematical analysis of this system, Antonio Cabrales and his colleagues assessed the efficiency properties of La Crema.[82] As the number of households becomes arbitrarily large, under certain assumptions, each household has an incentive to announce the true valuation, including subjective components of the valuation such as emotional attachment,[83] and there is no need to determine the real valuations. If one is risk averse and there is no administrative cost to insurance, one should want to purchase insurance that will make one indifferent about whether an insurable event occurs. One would not want to announce a lower than truthful valuation, for then one would be underinsured, and one would not want to announce a higher than truthful valuation, for then one's utility would decline should someone else suffer a loss. Interestingly, the mechanism does not perfectly align incentives,[84] but it can lead to near perfect valuation incentives with large numbers of households.

Of course, La Crema is not in common use, and there may be good reasons for that. A significant problem is moral hazard. In the extreme, moral hazard amounts to arson. If someone anticipates committing arson, then that person has an incentive to overvalue the property. Cabrales and his colleagues note that this is limited by the possibility of criminal prosecution, and the fact that those paying are the neighbors of the party with the insured loss may make it harder to cover up arson.[85] This suggests a difficulty in applying a similar mechanism to pools of heterogeneous insureds that may not know one another very well. Moral hazard short of arson could be a problem as well; each insured will have a reduced incentive to take care to avoid fire. This is a general problem with any insurance mechanism, but if moral hazard varies from one insured to another, it could distort incentives to announce honest valuations. Nonetheless, La Crema reveals that in principle it is possible to have an insurance system in which insureds choose what to pay, so long as those payments are tied to the amount that claimants receive. With a system of ex post evaluation of claims, some of the difficulties of self-assessment might be overcome.

[81] *Id.*

[82] *Id.* at 436–38.

[83] *Id.*

[84] *Id.* at 427.

[85] *Id.* at 432–33.

d. Peer-to-Peer Insurance

A nascent development that deserves some attention is peer-to-peer insurance. A German startup, called friendsurance,[86] offers insurance via a crowdsourcing mechanism in which individuals and their social media friends all purchase insurance.[87] The insurance premiums are placed in escrow and are paid out in the event of a claim.[88] The insurance company then offers additional insurance on top of this, and it is this portion of the insurance that requires regulation.[89] There are two theories underlying peer-to-peer insurance. First, the fact that friends are willing to invest in one's insurance claim provides information to the insurance company that one is a relatively good risk. A more elaborate version of the mechanism might allow friends to withdraw their support in a way that would alert the insurance company but without a report to the friend (who would not know how many had withdrawn support, only that the insurance price was increased or insurance was rejected). Second, the requirement that one first obtain coverage from friends reduces the chance of fraud.

These are substantial informational benefits, but the friends themselves do not receive the benefit of the insurance protection. It appears that an insured can trigger payment from friends, while the insurer can resist paying additional insurance on the grounds that it is not warranted. While friendship may reduce such opportunistic behavior, it sometimes may not; friends might use this as an opportunity to obtain a loan or simply to take their friends' money. Even if friendship adequately protected against this, the requirement that the friends themselves purchase insurance may be a limitation. In theory, this could ultimately lead to powerful network benefits (and perhaps antitrust concerns), but in the short term, the need for one's friends to sign onto the same insurance plan severely limits the insurer's attractiveness. Nonetheless, it is useful as a principle and proof of concept. In theory, one's ability to obtain insurance for a portion of a risk through one's friends should provide the insurer information and assurance and could reduce information asymmetries associated with cryptoinsurance.

2. *The Cryptocurrency Fund*

All of these antecedents could serve as precedents for a simple cryptoinsurance mechanism based on a fund. Anyone would be

[86] *See About Friendsurance*, FRIENDSURANCE, http://friendsurance.com (last visited Sept. 10, 2015).

[87] *How It Works*, FRIENDSURANCE, http://www.friendsurance.com/about.html (last visited Sept. 10, 2015).

[88] *Id.*

[89] *Id.*

permitted to purchase cryptoinsurance simply by sending money to the fund. Metadata for the transaction would include a hash of a document indicating what the person was purchasing insurance for—life, health, personal possessions, and so forth. The fund would cover a certain period of time. At any point during or shortly after the coverage period, the person could file a claim. There would be some cost to filing a claim, perhaps five percent of the amount sought, and one would initiate the claim by sending that sum to a designated address. In the metadata for that transaction one would include the hash of a document containing all information relevant to the insurance claim. The document itself could be listed somewhere else on the Internet so that anyone could search for it by its hash.

The filing of the claim would initiate a process of decision making concerning the claim, pursuant to the approach described above and in more detail in *Peer-to-Peer Law*.[90] The money spent to initiate the claim, intended to deter frivolous claims, serves the additional role of providing an incentive for third parties to investigate the validity of the claim. This initial fee is in effect a payment on behalf of the proposition that the claimant should be paid. A third party who determines that others likely would agree that the claim should be denied would have an incentive to counter this by placing at least as much money on the proposition that the claimant should be denied. Participants might well put questions or additional information concerning the claim on the Internet, including the hash so that it is searchable. Someone taking a particular position does not merely need to passively predict that others will come to the same conclusion, but can seek to persuade others with evidence or analysis. Thus, the process of deciding the claim becomes a kind of adjudication, bringing forth opposing arguments, albeit without formal rules of evidence and procedure, other than simple rules for determining when the final decision on a claim should be made.

Ideally, the adjudication would produce not merely a binary determination of whether the claim should be denied, but a determination of how much money, if any, the claimant ideally would receive. This does not mean that every claimant would receive some recovery; to the contrary, if the evidence is quite weak that a loss has occurred, participants in the adjudication process would probably give no recovery at all. Perhaps participants would decide to give no recovery if a preponderance of the evidence indicates that the claimant did not suffer a loss (perhaps with the

[90] *See* Abramowicz, *supra* note 54, at 41–42; *see also supra* text accompanying notes 54–58.

burden placed on the claimant), and full recovery if the claimant meets its burden. There is a normative argument that adjudication recoveries generally should be all or nothing[91] (i.e., that plaintiffs should either recover damages or not, and that they should not recover partial damages proportional to uncertainty).[92] But there is also a normative argument, particularly powerful in the insurance context since the argument itself is based on the insurance function of adjudication, that partial recoveries should be allowed where the probability that a claimant should recover is somewhere near the middle of the probability spectrum.[93] Participants in the focal point coordination game would need to weigh the relative merits of these arguments to determine what proportion of a claim to honor when there is some probability that the plaintiff indeed is entitled to a payout.

Whether the claimant has suffered a loss, however, is only one consideration in determining how much the claimant should receive. Even assuming that a loss has occurred, the amount that the claimant should receive must relate to the amount of money that the claimant contributed to the fund.[94] A claimant, after all, who contributes $1 to the fund and then claims a loss of $1,000,000 should not receive nearly that much, unless perhaps the loss was (a) the only loss that the contribution was intended to recover; and (b) the ex ante probability of loss was one in a million. As this analysis suggests, assuming that the claimant has indeed suffered a loss, the payout should depend on three factors: (1) how much the claimant put into the fund (m), (2) the proportion of the amount put into the fund that would have been devoted to a loss of this type (t), and (3) the ex ante probability of a loss of this type (p). The total ideal recovery according to this theory would then be mt/p.

If there are normative arguments for other theories, those might be in competition with this analysis in determining the coordination focal point, but this approach seems consistent with the broad concept that insurance payments should be greater the more money that the insured has paid to cover a particular type of loss and the less likely this loss was to occur. A possible extension would be to impose some deductible or coinsurance requirement, for the same reason that these exist with existing insurance: to reduce the

[91] *See e.g.*, David Kaye, *The Limits of the Preponderance of the Evidence Standard: Justifiably Naked Statistical Evidence and Multiple Causation*, 7 AM. B. FOUND. RES. J. 487, 495–97 (1982).

[92] *Id.*

[93] *See* Michael Abramowicz, *A Compromise Approach to Compromise Verdicts*, 89 CAL. L. REV. 231, 237 (2001).

[94] *Peer-to-Peer Law, Built on Bitcoin* explains how a formal tacit coordination game can be used to make quantity determinations as well as binary assessments. *See* Abramowicz, *supra* note 54, at 16.

moral hazard effect of insurance and to reduce the transactions costs associated with processing relatively small insurance claims.[95] The adjudicators would thus determine what deductible the insured would have negotiated for the relevant type of loss in negotiating the contract. Of course, the insured could specify in the initial document purchasing insurance that it wanted relatively high or low deductible coverage; choosing a high deductible would decrease the probability of loss and increase the payouts above the deductible amount if a claim in fact occurred.

This system thus closely resembles the La Crema system discussed above.[96] In La Crema, insureds can allocate the money they put in across different parts of their property, and so too here insureds might have an incentive to specify when purchasing insurance what different portions of the insurance amount is intended to cover different losses.[97] If an insured fails to specify whether the insurance is for life or for a boat, participants would have to determine ex post what the insured would have preferred ex ante, so the insured has some incentive to be precise. But there is some optimal degree of precision; it may not make sense to break down a payment for auto insurance into the muffler, the window, the roof, and so on, because that would require substantial research into the relative value of these and the relative risks of loss. It may make more sense for the ex post evaluators, who may become specialized in this type of analysis, to figure out below some level of specificity how to allocate whatever premium was paid and what level of deductibles should be inferred.

The system is also similar to La Crema in that there is no need to value the property being insured, at least as a general matter.[98] The payouts are proportional to the contributions for the relevant type of loss. A risk-averse participant in this insurance scheme—and it is of course in the nature of insureds to be risk averse—would have an incentive to allocate an amount that would smooth out the insured's utility in the event of a loss. To be sure, participants might consider the size of the loss in certain circumstances, for example in assessing whether the insured might intentionally have caused a loss. One reason that insurance companies ex ante investigate to make sure that insured property is worth no more than it is being insured for is to discourage moral

[95] ABRAHAM, *supra* note 12, at 15; Mark V. Pauly, *The Economics of Moral Hazard*, 58 AM. ECON. REV. 531, 535–37 (1968).

[96] *See supra Sub*part II.A.1.c.

[97] *See* Cabrales et al., *supra* note 62, at 431.

[98] *Id.* at 426.

hazard or deliberate destruction of the property.[99] But this type of consideration can be analyzed ex post. If there is a determination that the insured likely destroyed property intentionally, one can infer that the ex ante probability of a loss was high and therefore that the payout should be low. The ex post need to determine ex ante probabilities makes this system one that reflects the logic underlying *uberrima fides*, but with the twist that because there is no underlying contract, misrepresentations and intentional destruction affect the probability estimates. There may be an argument that those who are found to have deceived should receive even less than the probability estimates would suggest, or perhaps nothing at all, as a means of deterring such behavior.[100]

One significant difference from La Crema is that in that system there are no premiums; each person contributes only once a loss occurs. That will not work so well in this context, since there would be no way of making anonymous insurance customers pay other than when those customers file a claim. With a cryptoinsurance fund, premiums would be paid at the time the insurance was purchased. This also means, however, that only those premiums would be available to pay claims. Thus, the fund could promise payout of the entire pool in proportion to the ideal claim amounts determined by the validation process. Thus, if there were more claims than expected by chance or if decision makers were systematically too generous with claims, then each claim would be proportionately reduced, and vice versa if there were fewer claims or if decision makers were too stingy. The pool approach thus compensates for the danger that decision makers might make systematic errors in assessing ex ante probabilities, a challenging assessment to make in hindsight.[101] Over repeated cycles, this system would provide feedback to decision makers about ex ante probabilities, and if the number of independent insurance purchases grew to a high number, the claim payouts likely would exhaust the fund.

The five percent fee to initiate a claim would not be part of the pool but claimants would be reimbursed this amount in accordance with the rules of the decision-making process if their claims are determined to be valid. Because the claimant is in effect the first

[99] *See* Steven Shavell, *On Moral Hazard and Insurance*, 93 Q.J. ECON. 541, 542 (1979).

[100] *Cf.* A. Mitchell Polinsky & Steven Shavell, *Punitive Damages: An Economic Analysis*, 111 HARV. L. REV. 869 (1998) (arguing that punitive damages can help compensate for low probabilities of detection).

[101] *See generally* Jeffrey J. Rachlinski, *A Positive Psychological Theory of Judging in Hindsight*, 65 U. CHI. L. REV. 571 (1998) (discussing judicial hindsight bias).

participant in the formal coordination game, the claimant also could receive money from someone who took a position against the claim, assuming the claim nonetheless was approved. The denial of claims, in whole or in part, will pay for the services of the adjudicators. The fees submitted by those with denied claims, along with payments by adjudicators or others in support of the claim, are given entirely to those who bet against the claim. Of course, some participants in the formal coordination game might decide to back a claim, and they might earn money at the expense of participants opposing the claim. But the total profit of all participants excluding the claimants themselves will be equal to the claim fees of the rejected claims. This profit is divided effectively based on the skill of participants in forecasting how others will make decisions and in convincing others as to their positions.

The more prevalent the practice of submitting claims deemed to be valid, the greater incentive there will be to invest in trying to identify bad claims. This is as it should be. In a world where everyone is honest there would be no need to pay for adjudicators' services, but in a world of dishonesty, or where claimants may be overestimating the amount they should be paid, the adjudicators' services are more important, and it is thus worth investing greater resources on them. There is nothing magic, of course, about the five percent number. This number would reflect a determination that it makes sense to spend $0.05 in resources for each $1 claim that the adjudication process rejects. If precision were more important, then a higher percentage should be demanded of claimants. Because claimants who are sure that their claims will be honored lose nothing, the ultimate trade-off affects claimants with fully or partially denied claims. A higher percentage would indicate that it is worth it to spend more money on claim processing to ensure greater accuracy, while a lower percentage would indicate that the cost imposed on someone who files a bad or inflated claim, which might reflect miscalculation more than malice in some cases, should be reduced. The percentage is the minimum amount that a claimant must invest and reflects the desire to affect other insureds in their interest in the pool. A claimant can always act as a participant in the decision-making process and place more money in favor of its position, thus giving greater incentive for accurate determinations.

This system guarantees that the total revenues of the insurance company equal the total expenses. The promise that all amounts contributed will be paid out, either to insureds or to decision-making participants, is guaranteed by the cryptocurrency itself. As this suggests, the insurance company is not really a company at all, or if it is to be conceived as a company, it should be conceived as a mutual insurance company in its most extreme form. This arrangement has both benefits and costs. The obvious benefits are that insureds do not need to pay for expenses that a traditional insurance company would bear, such as marketing, legal services, or real estate expenses. The costs are that insureds do not obtain the benefits and assurances that they would get from more conventional insurance. Ordinarily, insureds benefit ex ante from the actuarial expertise of the insurer because the insured knows precisely how much coverage will be provided in exchange for the premiums.[102] Moreover, if insurance contracts are efficient, then insureds benefit, at least ex ante, from insurers' decisions on what to include and exclude.[103] Perhaps the cryptoinsurance fund participants will ex post be somewhat able to reconstruct the hypothetical contract that would have been entered into ex ante, by looking at actual insurance contracts and also by looking at the guidance that the insured provided when purchasing the contract. But this is an imperfect substitute for the traditional process in which individuals shop for insurance and enter into an actual contract that fits the parties' needs.

B. *Ex Ante Cryptoinsurance*

It might seem that if the cryptoinsurance fund was a sensible arrangement it would already exist, albeit without cryptocurrency. The existing insurance industry would offer funds like that described above, committing only to paying a set percentage of premiums in the aggregate according to their own discretionary estimates of ex ante probabilities, instead of ex ante contracts with predictable payments in the event of a claim. An insurer could emphasize a chief benefit of this approach, namely that because the total claim payouts are fixed, the insurer has no inherent bias against validating a claim. There are at least two possible explanations for the dominance of the current system. One possibility is that the current system is efficient given the legal environment. Insurance companies may have concluded that they cannot create a fund in which they retain full discretion to assess how much to pay off on claims. Insureds would sue, which would cost money regardless of the result, and the courts might ignore a contract allowing the insurance company full discretion to determine how much the insurers should pay ex post. Insureds today can always sue insurers, and it is not clear whether the courts would tolerate a regime in which insureds gave up this right by contract. At least there would be litigation about whether such an arrangement is acceptable. The second possibility is that conventional ex ante insurance contracts are in fact more efficient

[102] *See* Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 203 (2012).

[103] *Id.* at 206–07.

than the fund approach described above, because insureds value the certainty that ex ante contracts provide. The truth, of course, may be somewhere in the middle.

The question then becomes whether it is possible to imagine a form of cryptoinsurance that looks more like conventional insurance than the insurance fund described above—that is, that takes advantage of cryptocurrency's ability to escape regulation and perhaps of mechanisms that would prevent the insurance company from taking premiums and not making payouts, but that uses ex ante contracts. We have already seen in Part I that one possibility is to have the insurer be an actual company rather than just a creature of advanced cryptocurrency protocols. The advantage of such a company is that it can use any process that it likes, without worrying about how to implement those processes through the cryptocurrency mechanism. The difficulty facing such a company, we saw, is to assure consumers that it cannot be regulated while simultaneously assuring customers that it will not simply take their money. The cryptoinsurance fund that we described in Subpart II.A is a radical response to this problem, organizing the entire insurance mechanism around a simple arrangement that allows insurance to be provided in an entirely peer-to-peer way, no insurance company needed.

There may be two possibilities between these extremes. On one hand, we can imagine a cryptoinsurer—that is, an actual company—using smart contracts embedded in cryptocurrency to restrict its freedom in some ways. In effect, the smart contracts could serve as a regulatory mechanism that would prevent the cryptoinsurer from simply taking participants' deposits. Such a smart contract could, most importantly, prevent the insurer from spending money without the approval of an adjudicative process based on a formal tacit coordination game. For example, if the cryptoinsurer wanted to invest some of the money, that would need to be approved by the participants in such a game, who could seek to ensure that investments were legitimate (rather than attempts to appropriate money by the cryptoinsurer) and sufficiently diversified. Similarly, formal tacit coordination games could be a required step before any claim was paid out. This does not mean that the games would be used as described in Subpart II.A, to decide whether the claim in fact had merit, but simply as a means of providing a check on the cryptoinsurer's ability to steal money on the guise of paying claims. The formal tacit coordination games serve in this model not as a routine method of making decisions but as a mechanism of self-control and customer assurance in a regime that deliberatively avoids regulatory oversight.

The alternative possibility is that the fund embedded in cryptocurrency might itself develop additional features that would make the insurance offered through it more conventional, but still offered in an entirely peer-to-peer way without a company serving as an insurer. In *Peer-to-Peer Law, Built on Bitcoin,* I explain how cryptocurrency could be used to create rules or regulations, using the same formal tacit coordination games that would underlie the adjudication mechanism described above.[104] And so, a process could exist for standardizing insurance contracts. Rules could also be provided to require a certain minimum amount of reserves and to pay interest to those who provide the reserves. These reserves could be crowdfunded; that is, individual investors might provide these reserves to the cryptoinsurance mechanism in much the same way as individual investors put their money in catastrophe bonds that will pay them high interest rates unless a catastrophe occurs.[105] Placing all of these elements together could allow for ex ante contracts with high transparency and, depending on the reserve levels, high confidence that payments could be made in the event of loss.

What is much trickier for insurance embedded in a cryptocurrency is to invest the reserves. This is important in part as a means of increasing the size of the insurance pool and thus decreasing the cost of insurance. But it is especially important with cryptocurrency because of high volatility. At the least, insureds would want their cryptoinsurance premiums to be changed into dollars (or other local currency) to avoid risk from exchange rate volatility. A cryptoinsurance company could simply exchange cryptocurrency for dollars or other currency, possibly subject to the constraints above, and then purchase investments in its own name. But if the cryptoinsurance mechanism is entirely embedded in the cryptocurrency, there is no company and thus no entity that can own investments. In *Peer-to-Peer Law, Built on Bitcoin,* I note that this could change: if a single jurisdiction permitted a cryptocurrency to own assets, then it could do so.[106] If not, an alternative would be for the cryptoinsurance pool to rely on third-party borrowers. An adjudicative process could.be used to approve specific borrowers, who would be expected to return the borrowed cryptocurrency, making adjustments for changes in the cryptocurrency value and for interest.

The cryptocurrency might be sold in exchange for a virtual asset pegged to a real currency. An innovative cryptocurrency called

[104] Abramowicz, *supra* note 54, at 5–6.

[105] *See generally* Joshua D. Coval, Jurek W. Jakub, & Erik Stafford, *Economic Catastrophe Bonds*, 99 AM. ECON. REV. 628 (2009) (discussing economic catastrophe bonds and their comparison to other structured finance instruments). The similarity would be even stronger if the cryptoinsurance is used to insure against highly correlated events such as hurricanes.

[106] Abramowicz, *supra* note 54, at 56.

Bitshares attempts to overcome concerns about volatility in cryptocurrency by allowing exchange between the main Bitshares currency "BTS" and other virtual currencies that are pegged to real currencies, such as the dollar.[107] Suppose Jane holds BTS but wishes to purchase 1 bitUSD, which is pegged to the dollar. The bitUSD is created when John agrees to take Jane's BTS in exchange for a promise to pay back in the future the amount of BTS corresponding to the future BTS-bitUSD exchange rate. John is also required to put additional BTS aside as collateral, and if the value of BTS falls, this collateral may automatically be sold to ensure that Jane will be able to recover the bitUSD. Given the collateral requirements, only a drastic fall in Bitshares could cause Jane to lose value. A cryptocurrency that embeds a cryptoinsurance scheme could also provide a mechanism similar to Bitshares, so that premiums are held in a stable currency. Or, Bitshares could be extended to include the features of a cryptoinsurance pool.

Bitshares is worth discussing not merely because it provides a mechanism for overcoming cryptocurrency price volatility, though that is critical to a cryptocurrency, but because Bitshares is in a sense performing an insurance function. The purchaser of bitUSD (Jane in the example above) is buying insurance against the possible fall in the value of BTS, and the person taking the other side of the transaction (John) is serving a function akin to parties providing reserves to a cryptocurrency. Cryptoinsurance can be analogized to an extension of Bitshares to purchaser-specific virtual currencies.[108] Jane, instead of buying bitUSD, can buy bitJanesLife, where the amount of BTS that bitJanesLife is worth is dependent on both the value of BTS and on whether Jane is still alive, so that she can be promised a specific amount of money in the event of her death. Bitshares has a voting mechanism for determining the current BTS-dollar exchange rate, but no mechanism for assessing whether Jane is still alive or other states of the world that might require some degree of interpretation.[109] The peer-to-peer insurance adjudication mechanism developed here could provide that.

[107] *See Price-Stable Cryptocurrencies*, *supra* note 41.

[108] A version of insurance powered by BitShares has already been created. *See* bytemaster, *BitShares Insurance—Insure Anything (Almost)*, BITSHARES FORUM (Mar. 4, 2014, 7:31 AM), https://bitsharestalk.org/index.php?topic=3387.0. This version, however, requires that a specific insurance adjustor be selected in advance to determine whether a claim should be paid, instead of relying on a peer-to-peer decision-making mechanism.

[109] *See Price-Stable Cryptocurrencies*, *supra* note 41.

CONCLUSION: CRYPTOINSURANCE AND REGULATION

Bitcoin is perhaps the most prominent example of financial disintermediation; yet, to date it has not enabled meaningful competition with established financial institutions. This Article has sought to explain how cryptocurrencies might facilitate the development of an unregulated insurance market in competition with established insurance business models. Cryptocurrencies facilitate unregulated payments and provide some degree of financial transparency, thus making plausible an insurer that has no physical presence in the insureds' jurisdiction. In their current form, however, they also might make it too easy for an insurer to steal insureds' money, much as some early cryptocurrency banks have either stolen or lost deposits. A feature that might help consumers to have sufficient confidence in unregulated cryptoinsurance would be for the cryptoinsurance itself to build in security features that would guarantee the safety of insureds' funds.

Smart contracts, a feature of the cryptocurrency Ethereum, could provide some limited protections of this sort, by specifying third-party intermediaries who would need to approve of particular transactions or by specifying more complex voting protocols.[110] Cryptoinsurance can become more flexible, however, if a system of peer-to-peer decision making is built into the cryptocurrency. Formal tacit coordination games can be used to make decision-making unambiguous, even where those decisions require normative judgment. The games are structured in such a way so that each player must anticipate what hypothetical future players would think the best resolution is to the normative questions posed, looking themselves to still future players for their incentives.[111] Only with peer-to-peer decision making can a system of cryptoinsurance be truly peer-to-peer. Just as Bitcoin is built in a way that ensures that its users do not need to trust anyone who participates in the process of maintaining the Bitcoin block chain ledger, so too could a cryptocurrency be established so that individuals would not need to trust any particular decision maker.[112]

This Article has suggested that cryptoinsurance might arise in either of two ways. The first possibility is that a company could sell insurance using cryptocurrency, and to the extent that the cryptocurrency supports smart contracts or focal point tacit coordination games, it could provide users assurance that their

[110] *See* Vitalik Buterin, *Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform*, BITCOIN MAGAZINE (Jan. 23, 2014), https://bitcoinmagazine.com/9671/ethereum-next-generation-cryptocurrency-decentralized-application-platform/.

[111] *Id.*

[112] *See* Nian & Chen, *supra* note 26, at 5.

claims will be processed in accordance with a particular decision-making procedure that the insurer cannot control. The alternative possibility is that the insurance mechanism could be built into the cryptocurrency itself. A simple version of this would be a pool that would be paid out in its entirety to claimants, with additional claim fees used to fund the claim adjudication process. A more elaborate process could allow for approval of ex ante contracts with fixed payout rules. Third parties who provide insurance reserves could earn interest for doing so if their reserves were not needed, and the premiums and the reserves might be invested or at least transferred to an asset pegged to the dollar to eliminate exchange rate risk. The rules governing these processes could be determined by the same tacit coordination games used to adjudicate individual claims, and so some form of insurance regulation could emerge from unregulated competition.

My intent in this Article has not been to argue that cryptoinsurance would be an unmitigated good. Insurance regulation may be largely socially beneficial. To some extent, insurance regulation is designed as a form of consumer protection, and it is not clear that cryptoinsurance, especially at first, would provide the same degree of consumer protection.[113] The legal infrastructure for ensuring that insurers will have sufficient funds to pay legitimate claims is complex, and it may be quite difficult for a comparable degree of protection to arise from private ordering. Insurance regulation is also designed to achieve a number of other goals, including cross-subsidizing rates.[114] For example, many laws ban genetic discrimination.[115] Assuming that these laws are justified,[116] cryptoinsurance can be condemned for undermining them. In seeking to ascertain the ex ante probability of a loss, cryptoinsurance adjudication participants plausibly might be interested in the genetic profile of the insured.

The law could take at least three strategies to combat cryptoinsurance and its undermining of regulations. The first would be to directly attack, with civil or criminal penalties, those who provide cryptoinsurance or who otherwise support it, for example by participating in the adjudication process. But this type of regulation may be frustrated for the same reasons that regulation of

[113] *See, e.g.*, Daniel Schwarcz, *Transparently Opaque: Understanding the Lack of Transparency in Insurance Consumer Protection*, 61 UCLA L. REV. 394 (2014) (describing the realm of insurance-related consumer protection).

[114] *See id.*

[115] *See* Henry T. Greely, *Banning Genetic Discrimination*, 9 NEW ENG. J. MED. 895 (2015).

[116] *See* Marvin R. Natowicz et al., *Genetic Discrimination and the Law*, 50 AM. J. HUM. GENETICS 465, 468 (1992).

cryptocurrencies themselves may be frustrated. It is difficult—though not necessarily impossible—for the government to discover who those people are, and they may be beyond the long-arm-of-law enforcement. The goal of combating money laundering is laudable, and thus so is the goal of regulating cryptocurrencies to reduce this potential. But as long as cryptocurrencies exist somewhere in the world, efforts to regulate cryptocurrencies for money laundering are likely to fail; it will be much easier to find someone who will exchange cash for Bitcoin on the black market than to launder suitcases of cash or gold in traditional ways, regardless of the regulation. And similarly, so long as cryptoinsurance exists anywhere in the world, it will be difficult for the law, deprived of its ability to threaten to block access to the international financial system, to ban it.

The second strategy for combatting cryptoinsurance would be to target the purchasers of the cryptoinsurance directly. We have seen that one challenge in establishing cryptoinsurance is maintaining the privacy of the insureds,[117] and this can work to the regulator's advantage. Even if insurance policies remain private until a claim is filed, the legal system could confiscate payouts under cryptoinsurance policies once the claims become public. It is possible that cryptoinsurance could devise elaborate protections against this—for example, by designating only a set of adjudicators trusted to keep information confidential, as those authorized to participate in the formal tacit coordination games used to approve claims. But the more fundamental problem is that targeting purchasers of insurance may be politically implausible. Even in financial realms such as securities regulation, targeting purchasers has never been seen as an enforcement tool, in part because regulation is styled as being for the protection of the public.[118] This form of regulation would at least involve a change in mindset—for example, recognition that those who undermine a cross-subsidization scheme by purchasing cryptoinsurance are akin to tax evaders or thieves.

The third strategy would be to make cryptoinsurance unnecessary or redundant. The most obvious way to do this would be to make insurance mandatory and to exclude cryptoinsurance from counting as satisfying the regulatory requirement. Of course, many forms of insurance are already mandatory, and in these realms, cryptoinsurance is less likely to develop. For example, drivers are generally required to have auto insurance,[119] at least if

[117] *See supra* Part II.

[118] *See* Schwarcz, *supra* note 113.

[119] Jennifer B. Wriggins, *Mandates, Markets, and Risk: Auto Insurance and the Affordable Care Act*, 19 CONN. INS. L.J. 275, 280 n.13 (2012).

they are not bonded.[120] Perhaps cryptoinsurance could be designed to serve drivers who want more than the minimum coverage, perhaps including collision coverage, but drivers desiring to obtain all of their auto coverage from a single supplier would likely avoid cryptoinsurance. Meanwhile, under the Affordable Care Act,[121] those who do not carry health insurance must pay a tax.[122] In principle, the law could require greater insurance coverage as a means of discouraging individuals from obtaining any of their health coverage through cryptoinsurance. Similarly, the legal system could mandate life insurance or property insurance or disability insurance. A case can be made independent of cryptoinsurance for such insurance requirements, and cryptoinsurance would strengthen the case. Nonetheless, in most situations, requiring purchase of insurance would likely be seen as an infringement of individual autonomy.

In sum, I am not optimistic that the legal system would be successful in any attempt to regulate cryptoinsurance should it arise. But the legal system's ability to do so would depend on the popular reaction to cryptoinsurance, and, if there were a widespread sense that cryptoinsurance was causing social damage by enabling private choice, then some form of regulation might well be feasible. In the meantime, even one who believes that insurance regulations are justified might see some benefit in a cryptoinsurance experiment. Whatever the ultimate merits of forms of unregulated competition in the sharing economy from the likes of Uber and Airbnb, these new business models at least have forced a rethinking of the need for regulation.[123] These experiments can thus be seen as having effects analogous to those of sunset laws, forcing legal decision makers to ask anew whether regulation is desirable and if so how it can best be achieved.[124]

A number of obstacles must be overcome for any form of cryptoinsurance to develop, including the development and validation of a cryptocurrency that supports formal tacit coordination games. Moreover, it may be difficult for any private party to capture the benefits of a new insurance model. If

[120] *See, e.g.*, Robert K. Lewis, Note, *The Physical Contact Rule for Uninsured Motorist Coverage in Arizona: Where We Were, Where We Are, and Where We Ought to Be*, 36 ARIZ. L. REV. 1033, 1036–39 (1994).

[121] Affordable Care Act of 2010, Pub. L. No. 111-1148, 124 Stat. 119-24.

[122] 26 U.S.C. § 5000A (2012).

[123] *See* Emily Badger, *What Happens When Uber and Airbnb Become Their Own Regulators*, WASH. POST (Feb. 4, 2015), http://www.washingtonpost.com/blogs/wonkblog/wp/2015/02/04/what-happens-when-uber-and-airbnb-become-their-own-regulators/.

[124] Sofia Ranchordas, *Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy*, 16 MINN. J. L. SCI. & TECH. 413, 450–51 (2015).

cryptoinsurance is to be embedded in the cryptocurrency itself, the motivation to create cryptoinsurance would have to come from holders of the cryptocurrency, but if these holders are sufficiently diffused, they may not have adequate incentive. It is possible, however, that cryptoinsurance, should it be available, might be favored by some consumers. For those consumers, whatever extra protection the courts provide over the form of peer-to-peer adjudication that we have described here may not be worth the expense, which ultimately is paid in insurance premiums. And similarly, even if the consumer protection provided by existing regulation of insurance is better than the cryptocurrency substitutes that might develop, some consumers might conclude that the amount of protection provided is excessive. In the long term, it is likely to be the market rather than the government that determines whether such a form of radical financial disintermediation serves a useful function.