THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW

THE GREAT DECENTRALIZATION: HOW WEB 3.0 WILL WEAKEN COPYRIGHTS

NICK VOGEL

ABSTRACT

Bitcoin's popularity increased as its value increased and people became excited about the prospect of a trustless, decentralized currency that could be used on the Internet. Within the last two years, however, people and organizations began exploiting the potential of the block chain that powers the bitcoin network. These people realized that the block chain—a transparent public ledger that cannot be altered—can be used for more than digital currency. One such organization calls itself Ethereum and its developers plan to use block chains to allow decentralized autonomous applications to operate free of government censorship or corruption. While such a network would have a profound effect on society—allowing trustless voting, uncensored social networking and the like—its impact on copyrights could be devastating. This paper argues that the emerging, decentralized Internet (also known as Web 3.0) will be the straw that breaks the copyright owner's back. This paper argues that, with block chain technology and decentralized applications, those buying and selling unauthorized copies of copyrighted material cannot be subject to court injunctions; making enforcement of copyrights nearly impossible on a decentralized Internet. This paper then proposes that copyright holders get out in front of the problem by embracing a decentralized Internet. This can only be done by drastically reducing the price of copyright licenses. In other words, by offering cheap licenses at the dawn of Web 3.0, copyright holders can instill a sense that it's better to be safe than sorry when it comes to the ongoing struggle between technology and copyrights.

THE GREAT DECENTRALIZATION: HOW WEB 3.0 WILL WEAKEN COPYRIGHTS

NICK VOGEL

THE GREAT DECENTRALIZATION: HOW WEB 3.0 WILL WEAKEN COPYRIGHTS

NICK VOGEL[*]

I. INTRODUCTION

Imagine starting over. Imagine a new Internet. Imagine that this time, however, there is no Amazon, no Google, no Apple, no Yahoo or any of the other wealthy, influential and ambitious corporations around which the Internet's significant market activity orbit. Imagine an Internet where no centralized corporation or government has control over the content shared between users. Imagine an Internet where no one is in charge and no one can be held responsible when something goes wrong. What impact would such an environment have on artists' copyrights? What impact would this decentralized Internet have on copyright law and attorneys? Some commenters believe the Internet faces a great movement to decentralize most online services.[1] This article will attempt to illustrate this decentralization's likely impact on copyright law.

Part II of this comment discusses the technological advance known as a block chain and gives examples of some cutting edge companies that plan to maximize the block chain's potential.

Part II A of this comment focuses in on one particular initiative known as Ethereum and discusses the Ethereum Foundation's plan to decentralize the Internet. Part II B of this comment looks at how the courts historically handled file sharing over the Internet and the misappropriation of copyrighted material.

Part III of this comment discusses the impact decentralized applications may have on copyrights.

Part IV proposes that creators of copyrightable material embrace a decentralized Internet as soon as possible and offer licensing at a hyper competitive price.

The comment briefly concludes in Part V with a warning that copyrights will have less legal effect in the realm of a decentralized Internet.

II. BACKGROUND

This section discusses the new technology allowing software applications to run independent of any authority or centralized government or company. This section will also discuss which parties or entities courts have traditionally held liable for copyright infringement via the Internet.

---

[1] Jamie Bartlett, *Soon, the Internet will be impossible to control,* THE TELEGRAPH (Dec. 10, 2014) (http://www.telegraph.co.uk/technology/internet/11284538/Soon-the-internet-will-be-impossible-to-control.html) (reporting that, "among the hacker community an alternative way of running the internet is being built already: an internet where no one is in control, where no one can shut you down, where no one can manipulate your content. A decentralised internet.").

Before diving into this topic it is important for the reader to become familiar with Bitcoin and the novel software technology that powers it. Bitcoin is a decentralized digital currency that cannot be counterfeited, so to speak.[2] This means that a Bitcoin can be transferred from one person to another, or, one computer to another, or one smartphone to another in order to securely and confidently facilitate trade.[3] While a digital currency holds promise for the future of commerce, most commentators recognize the technology *behind* Bitcoin will revolutionize the way we social network, trade corporate stock and even vote.[4]

The technology that makes Bitcoin work is called the block chain (sometimes written as one word 'blockchain').[5] This is how an organization called the Bitcoin Foundation explains what a block chain is:

> The block chain is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.[6]

---

[2] Michael Sivy, *The Real Significance of the Bitcoin Boom (and Bust)*, TIME (April 12, 2013) (http://business.time.com/2013/04/12/the-real-significance-of-the-bitcoin-boom-and-bust/) (reporting that "to prevent counterfeiting, (Bitcoin's creator) attached a history of transactions to each currency unit—but allowed users to keep their transactions nearly anonymous. Counterfeiting is hard because fake Bitcoins would need an authenticated history to pass muster.").

[3]   BITCOIN,   https://bitcoin.org/en/faq#who-created-bitcoin   (last   visited   March   29, 2015)(hereinafter "bitcoin.org").

[4] *Exclusive: IBM Looking at Adopting Bitcoin Technology for Major Currencies*, NEW YORK TIMES (March   15,   2015)   (http://www.nytimes.com/reuters/2015/03/12/business/12reuters-bitcoin-ibm.html?_r=0) (explaining that the technology behind Bitcoin is "viewed as bitcoin's main technological innovation, allowing users to make payments anonymously, instantly, and without government regulation.").   Dominic Frisby, *The Incredible Technology behind Bitcoin is About to Change the World,* BUSINESS INSIDER (Jan. 21, 2015) (http://www.businessinsider.com/bitcoin-blockchain-technology-dominic-frisby-2015-1) (claiming that companies are using the technology behind Bitcoin for "finding new ways to communicate and socially network without third-party providers (the likes of Gmail, Apple, Facebook or Twitter). They're finding ways to draft and enforce contracts without the need for lawyers (these are known as 'smart contracts'). They're finding ways to issue and trade shares – without the need for traditional stock exchanges and financiers."); Meghan Neal, *Bitcoin could change voting the way it's Changed Money*, MOTHERBOARD (June 6, 2014) (http://motherboard.vice.com/read/bitcoin-could-change-voting-the-way-its-changed-money) (reporting that "Political groups and tech startups are beginning to experiment with digital voting systems based on the bitcoin and its technological protocol.").

[5] Bitcoin.org, https://bitcoin.org/en/how-it-works (last visited May 1, 2015).

[6] *Id*. The Bitcoin Foundation explains how private keys are used to facilitate exchanges on the block chain,
> A transaction is a transfer of value between Bitcoin wallets that gets included in the block chain. Bitcoin wallets keep a secret piece of data called a *private key* or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The *signature* also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast between users and usually begin to be confirmed by the network in the following 10 minutes, through a process called *mining*.

Id.

   In other words, because everyone can see the block chain, anyone can spot a
duplicate or fraudulent transaction.[7] This solves the problem of an individual merely
making a digital copy of a bitcoin and holding onto it after sending the original bitcoin
to another person.[8] Another way to understand the block chain is to look at it as a
large, public spreadsheet in which everyone has the ability to check that each digital
exchange is unique.[9]
   Bitcoin has emerged from obscurity over the past few years, and has gained
acceptance by some mainstream financiers.[10] And as bitcoin became popular for its
potential to disrupt the way we think of currency, enterprising individuals and groups
realized the potential hidden within bitcoin's novel block chain technology.[11] These
tech savvy individuals saw that society could use the block chain to transfer and secure
more than digital currency.[12] Contracts, domain name registration, a vote for a
politician, land titles, the mining and market history of a diamond; the limit is yet
unknown.[13] One example is a company called Namecoin. Rather than transfer digital

---

[7] Larry Greenenmeier, *Bitcoin-Based Blockchain Breaks Out*, SCIENTIFIC AMERICAN, (April 1,
2015) (explaining that "[o]nce a transaction is entered into the blockchain ledger, it cannot be deleted
or changed.").
   [8] Rob Wile, *SATOSHI'S REVOLUTION: How The Creator Of Bitcoin May Have Stumbled Onto
Something   Much,   Much   Bigger*,   BUSINESS   INSIDER   (April   22,   2014)
(http://www.businessinsider.com/the-future-of-the-blockchain-2014-4) (describing what is known as
the Byzantine General's Problem, which is a challenge "to send and receive money online without the
need for a trusted third party, such as PayPal, ensuring that the same digital credit standing in for
the amount being exchanged isn't being spent twice.") (hereinafter "Wile").
   [9] Wile (describing the blockchain as "a ledger of all transactions owned and monitored by everyone
but ultimately controlled by none. It's like a giant interactive spreadsheet everyone has access to and
updates to confirm each digital credit is unique.").
   [10] *E.g.* Jacob Pramuk, *Bitcoin Exchange Gemini Safe and Legal: Founders*, CNBC (Oct. 8, 2015)
(http://www.cnbc.com/2015/10/08/bitcoin-exchange-gemini-safe-and-legal-founders.html)   (reporting
the launch of a Bitcoin called Gemini. The exchange was founded by Cameron and Tyler Winklevoss.
The Winklevoss twins are reported saying that, "their platform gives hedge funds and market makers
a secure platform to dive into the digital currency.").
   [11] Mathew Sparkes, *The coming digital anarchy*, THE TELEGRAPH (June 9, 2014)
(http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html) (reporting
that "[i]n time, blockchains will power many radical, disruptive technologies that smart people are
working on right now," and that the, "hidden power of the Facebooks, Twitters and Googles of this
world is inspiring digital anarchists to destroy the smug, jargon-infested giants of Silicon Valley," and
that society's first experience with "this decentralised power happened to be a currency, Bitcoin, but
it could equally have been a stock exchange, a social network or an electronic voting system.").
   [12] Andy Extance, *Entrepreneur's Explore Bitcoin's Future*, SCIENTIFIC AMERICA, (Sept. 30, 2015)
(reporting that "[m]any people see this block-chain architecture as the template for a host of other
applications, including self-enforcing contracts and secure systems for online voting and
crowdfunding.").
   [13]   *E.g.*,   IC3:   INITIATIVE   FOR   CRYPTOCURRENCIES   AND   CONTRACTS
(http://www.initc3.org/projects.html) (last viewed Oct. 8, 2015). It is the mission of IC3 to research the
possibilities of the blockchain architecture. The initiative's Website does a good job describing the
potential of a "smart contract" on the blockchain, writing that,
         Smart contracts hold great promise for the creation of new financial and legal
      instruments. But they also offer new opportunities for criminal behavior.
      Autonomously executing contracts for key theft, document leakage, and a variety
      of real-world crimes (e.g., assassination) become a possibility. We are exploring the
      risks of new criminal ecosystems arising in decentralized smart contract systems
      to inform policymakers and to devise countermeasures that can be deployed in a
      timely way.

currency on Bitcoin's block chain, Namecoin uses the block chain to register domain names.[14] By downloading Namecoin's software, a user can then use a namecoin to obtain a domain name with the extension ".bit."[15] A user's claim to that name is then preserved on the Bitcoin block chain where no one can steal it, or use it.[16] The cost comes out to about $.10 U.S.D.[17]

Consider, also, the story of Leanne Kemp, an Australian. Kemp has come up with a way she says diamonds can be tracked on a block chain.[18] Kemp's plan is to create digital certificates detailing a diamond's history.[19] These certificates would then be "mapped" onto a diamond. Buyers and retailers could then use this digital certificate to help recognize the identity of a diamond and its true value.[20]

A. Decentralization Becomes a Reality

Then, there is Ethereum. First conceptualized by a 19-year-old Canadian, Ethereum stands to become the driving force behind the looming decentralization of the Internet.[21] That 19-year-old was Vitalik Buterin and in 2011 he came up with the idea of creating a block chain and using it to support a whole new programming language, rather than a currency like Bitcoin.[22] Ethereum launched, officially, on July 30, 2015.[23] The team of people behind Ethereum created a new operating system upon which new applications can be created.[24] Ethereum even plans to have its own

---

[ ] *Id.*

[14] NAMECOIN (https://wiki.namecoin.info/index.php?title=FAQ#How_does_Namecoin_work.3F) (last viewed Oct. 9, 2015).

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] Sally Davies, *Bitcoin: possible bane of the diamond thief*, THE FINANCIAL TIMES (Feb. 3, 2015) (http://www.ft.com/intl/cms/s/0/f2b0b2ee-9012-11e4-a0e5-00144feabdc0.html#axzz3X0JPOTZE).

[19] *Id.*

[20] *Id.*

[21] Ilya Pozin, *The Three Platforms that will Decentralize the Web*, FORBES (Apr. 10, 2015) (http://www.forbes.com/sites/ilyapozin/2015/04/10/meet-the-3-platforms-that-will-decentralize-the-web/2/).

[22] Alexander Leishman, *A Next-Generation Smart Contract and Decentralized Application Platform*, Ethereum White Paper, (https://github.com/ethereum/wiki/wiki/White-Paper) (last visited April 14, 2015) (hereinafter "The White Paper") (explaining that Ethereum "intends to provide a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create 'contracts' that can be used to encode arbitrary state transition functions, allowing users to create [decentralized autonomous organizations, crypto-currencies, digital assets to represent custom currencies and financial instruments and complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules], as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.")

[23] Stephan Tual, Ethereum Launches, Ethereum Blog (July 30, 2015) https://blog.ethereum.org/2015/07/30/ethereum-launches/ (writing that the first live release of Ethereum became available on July 30, 2015) (hereinafter "Tual").

[24] Primavera De Filippi, *Tomorrow's Apps Will Come From Brilliant (and Risky) Bitcoin Code*, WIRED (March 8, 2014) (http://www.wired.com/2014/03/decentralized-applications-built-bitcoin-great-except-whos-responsible-outcomes/) (explaining that "Ethereum is a contract validating and enforcing system based on a more sophisticated platform than other derivative cryptocurrencies (it features an internal Turing-complete scripting language that can be used to encode advanced transaction types directly into the blockchain).") (hereinafter "De Fillippi"). According to her biography, De Fillippi is

decentralized application browser, similar to Google Chrome or Apple's App store.[25] Rather than use a block chain to support a digital currency like bitcoin, Ethereum's block chain will contain distributed autonomous companies (also referred to as decentralized autonomous applications)—software programs that once started, cannot be stopped.[26] With Ethereum, programs will use "smart contracts" to execute agreements between two users, between a user and an application or between two applications.[27] Rather than rely on a court to enforce a contract, a smart contract can enforce itself via lines of code.[28] A prediction market called Augur provides an example of how a smart contract can be used on the Ethereum network. With Augur, users bet money predicting future events.[29] That money is placed on the Ethereum network where it cannot be released until the terms of the smart contract are satisfied or when the event predicted comes to fruition.[30] Essentially, the users trust their money to the software application existing on the Ethereum network to deliver the money when the result of the bet is revealed.[31] The plan for Ethereum is to use a cryptocurrency like Bitcoin to power the smart contracts.[32]

Since the Ethereum network is decentralized, existing in the aggregate on the computers of those who use the network, the only logical way to "stop" a smart contract is to take complete control over the Ethereum network.[33] Doing this would require one

---

"currently a research fellow at the Berkman Center for Internet & Society at Harvard Law School, where she is investigating the legal challenges of "governance-by-design" in online distributed architectures, such as Bitcoin, Ethereum etc." *See* Primavera De Filippi, https://cyber.law.harvard.edu/people/pdefilippi) (last viewed Oct. 9, 2015).

[25] *See* Ethereum, *Ethereum Presents Mist*, YOUTUBE (Nov. 12, 2014), https://www.youtube.com/watch?v=IgNjs_WaFSc.

[26] De Fillippi (reporting that software programs will function on the blockchain "with an autonomy of their own."); Tual, writing in his blog that Ethereum's vision was to create a "censorship-proof 'world computer' that anyone can program."

[27] *See generally*, The White Paper (explaining how Ethereum uses smart contracts).

[28] Vitalik Buterin, *DAOs Are Not Scary, Part 1: Self-Enforcing Contracts And Factum Law*, ETHEREUM BLOG (Feb. 24, 2014) https://blog.ethereum.org/2014/02/24/daos-are-not-scary-part-1-self-enforcing-contracts-and-factum-law/ (hereinafter "DAOs Are Not Scary"). Buterin provides the following hypothetical to show how a smart contract would work on Ethereum: "[I]magine a world where everyone has their own private key on a smartphone, and there is a car such that when you pay $100 to a certain address the car automatically starts responding commands signed by your private key for a day." *Id.*

[29] *See* Augur, *Augur - How A Decentralized Prediction Market Works* YOUTUBE (May 20, 2015), https://www.youtube.com/watch?v=yegyih591Jo.

[30] *Id.*

[31] Klint Finley, *Out in the Open: Teenage Hacker Transforms Web into One Giant Bitcoin Network*, WIRED (Jan. 27, 2014) (http://www.wired.com/2014/01/ethereum/) (using a simple betting system as an example of a smart contract) (hereinafter "Finley").

[32] DAOs Are Not Scary (writing that "with [digital cryptocurrencies], we have created a way for contracts, and perhaps even law in general, to work, and be effective, without relying on any kind of mechanism whatsoever to enforce it.").

[33] *Blythe Masters Says a Bitcoin Technology Will Revolutionize Finance*, BLOOMBERG NEWS, (Sept. 1, 2015) (http://www.crainsnewyork.com/article/20150901/FINANCE/150909984/blythe-masters-says-a-bitcoin-technology-will-revolutionize-finance) (explaining that "[e]very new block is connected to every prior one in a digital chain. So the record of every Bitcoin transaction lives on the computers of the miners and is updated with each new entry. That's why the blockchain is also called a distributed or a decentralized ledger. This replication makes the blockchain secure. The only way to tamper with it would be to seize control of most of the computers holding the blockchain in their

to gain control over the cryptocurrency that fuels the smart contract and change the public ledger on the Ethereum block chain.[34] Gaining control over a cryptocurrency is incredibly difficult.[35] Former Ethereum spokesperson Stephan Tual says gaining this kind of control is virtually impossible.[36] In an interview, Tual said building something like The Silk Road or Wikileaks on Ethereum is possible, "(a)nd if somebody wanted to take it down it wouldn't be able to shut the server, because there's no server . . . The only thing they could do is chase every single user. Or shut down the internet—that would work."[37]

Hypothetically, with Ethereum, someone can create a social networking application like Facebook and, rather than send advertising revenue to a Facebook Inc., the autonomous software could send individual users advertising revenue for the number of times their homepage has been viewed by other users.[38]

One could argue that Ethereum is attempting to create a new, decentralized Internet.[39]

B. Legal Liability for Copyright Infringement

This paper's thesis is that once the Internet is decentralized, copyright holders will have no party to sue in order to stop infringement. Since the Great Decentralization[40] has yet to occur in ways warranting significant legal action, legal research is confined to comparisons to similar technology and analysis is confined to theoretical conclusions.

Thus, before asking whom to sue for infringement that takes place on a decentralized network via block chain technology, it is worth discussing how the law has already reacted to the next closest thing: peer-to-peer file sharing.

This section of the paper explains copyright holders' attempts to stop copyright infringement via peer-to-peer file sharing. In the case of Ethereum and other

---

memories, which miners call the "51% attack." Such an assault has a better chance of materializing in the next Bond flick than in reality.").

[34] *Id.*

[35] *See generally* Fran Berkman, *What is a 51 percent attack, and why are Bitcoin users freaking out about it now?*, THE DAILY DOT (Jan. 13, 2014) (http://www.dailydot.com/business/bitcoin-51-percent-attack/) (explaining that in order for one entity to steal or double spend Bitcoins, that entity would have to control more than 51% of all the computing power of the bitcoin network. Given the massive amount of computing power in the Bitcoin Network, such a situation is not likely).

[36] Gian Volpicelli, *Smart Contracts Sound Boring, But They're More Disruptive Than Bitcoin*, MOTHERBOARD (Feb. 16, 2015) (http://motherboard.vice.com/read/smart-contracts-sound-boring-but-theyre-more-disruptive-than-bitcoin).

[37] *Id.*

[38] De Fillippi, (explaining that Distributed Autonomous Organizations "are autonomous entities that subsist independently from any legal or moral entity. After they have been created and deployed onto the internet, they no longer need (nor heed) their creators.").

[39] Taylor Gerring, *Building The Centralized Web 3.0*, ETHEREUM BLOG (2014) https://blog.ethereum.org/2014/08/18/building-decentralized-web/ (writing on behalf of Ethereum's developers that "Ethereum sets the stage for an [sic] total sharding of traditional [Internet] infrastructure as we know it.").

[40] My phrase.

platforms actualizing a decentralized Internet, the block chain's closest technological relative is peer-to-peer networking (commonly expressed using the initialism "P2P").[41]

Our modern, connected and technologically advanced society presents various challenges for copyright owners. One such challenge exists in determining who to sue for copyright infringement that takes place via file sharing on the Internet. In the early days of the Internet, Internet Service Providers (ISPs) were targeted under a theory of strict liability.[42] Much has changed, as will be explained *infra*.

1. Liability of Software Developers for P2P Traffic

Peer-to-peer networks have traditionally enabled individuals to connect their computers directly to other specific computers.[43] Typically, people use these connections, or networks, to share files with one another.[44] A user first installs a free software program that helps find specific files (like mp3s) and then downloads the files.[45] Users also share their own files with other users.[46]

In *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, the Supreme Court had to decide whether companies that distributed peer-to-peer software applications enabling copyright infringement were liable to copyright holders.[47] MGM sued Grokster and the other defendants because they distributed "free software products that allow computer users to share electronic files through peer-to-peer networks, so called because users' computers communicate directly with each other, not through central servers."[48] The court looked at Grokster's intent, which was to attract users who downloaded unauthorized, illegal content.[49] The court held that Grokster could be held liable for third-party copyright infringement.[50] The case was remanded and ended up back at the District Court. Before the case returned to trial, however, two of the parties named in the suit, Grokster and Sharman Networks, settled with MGM.[51] The final hold out was a company called StreamCast, which tried to continue its

---

[41] De Fillippi (writing that, "blockchain-based applications also present legal, technical, and social challenges similar to those raised by other P2P applications that came before them, such as BitTorrent, Tor, or Freenet.").

[42] Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, NYU J.L.P.P. 15, 42 (2005) (hereinafter "Elkin-Koren") (positing that "ISPs became a favorite target of lawsuits by copyright owners during the mid-1990's.").

[43] FBI, *Risk of Peer-to-Peer systems*, http://www.fbi.gov/scams-safety/peertopeer (last viewed Oct. 9, 2015).

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[48] *Id.* at 919-20 (2005).

[49] *Id.* At 938 (reasoning that "anyone whose Napster or free file-sharing searches turned up a link to Grokster would have understood Grokster to be offering the same file-sharing ability as Napster, and to the same people who probably used Napster for infringing downloads; that would also have been the understanding of anyone offered Grokster's suggestively named Swaptor software.").

[50] *Id.* (holding that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.").

[51] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 971 (C.D. Cal. 2006).

defense against MGM.[52] StreamCast lost.[53] A glance at the original motions filed by MGM show that MGM's main goal was an injunction.[54] MGM argued that "[w]hile the award of damages for past infringement will be appropriate, there is no *adequate* remedy at law in this case. Damages cannot begin to compensate Plaintiffs adequately for the harm caused by StreamCast."[55]

2. Liability of Internet Service Providers for Copyright infringement

Can an Internet Service Provider (ISP) be held vicariously liable for copyright infringement that takes place over a peer-to-peer network? A court's[56] first reaction to this legal issue was to say yes.[57] In *Playboy Enterprises, Inc. v. Frena*, the court held that an online bulletin board service (BBS) infringed Playboy's copyrights by allowing users to upload and download Playboy's photos.[58] The Defendant, Frena, argued that he did not know the users were uploading and downloading these photos.[59] The court said that did not matter, holding that since, "direct evidence of copying is rarely available in a copyright infringement action, copying may be inferentially proven by showing that Defendant Frena had access to the allegedly infringed work, that the allegedly infringing work is substantially similar to the copyrighted work, and that one of the rights statutorily guaranteed to copyright owners is implicated by Frena's actions."[60]

Courts later changed course and saw that bulletin board services (BBS) did not face vicarious liability for the acts of another on the BBS network.[61] In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, a company called Netcom provided an electronic bulletin board service.[62] Users were able to upload and share files to that bulletin.[63] One of those users was a former minister of Scientology turned vocal critic of the church.[64] This minister used the bulletin board service to

---

[52] *Id.*

[53] *Id.*

[54] *See* 454 F. Supp. 2d 966.

[55] Notice of Motion and Motion for a Permanent Injunction Against Streamcast Networks, Inc. and Musiccity Networks, Inc. at 6, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, No. 01-08541 (C.D. Cal. 2006).

[56] In terms of jurisdiction, this paper assumes any copyright claims related to decentralized systems will be dealt with in Federal court. *See, e.g.* 28 U.S.C. § 1338 (2012) (stating that "[t]he district courts shall have original jurisdiction of any civil action arising under any Act of Congress relating to patents, plant variety protection, copyrights and trademarks. No State court shall have jurisdiction over any claim for relief arising under any Act of Congress relating to patents, plant variety protection, or copyrights.").

[57] Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993).

[58] *Id.* at 1554.

[59] *Id.*

[60] *Id.*

[61] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1382 (N.D. Cal. 1995) (holding that a theory of vicarious liability against a BBS operator "fails as a matter of law because there are insufficient factual allegations to support it.").

[62] *Id.* at 1368.

[63] *Id.* at 1367.

[64] *Id.* at 1365.

create a public, online forum to criticize the church.[65] The Church sued both the BBS and the forum's creator when the forum began posting portions of the church's copyrighted materials.[66] The legal issue facing the court was, "whether the operator of a computer bulletin board service . . . and the large Internet access provider that allows that BBS to reach the Internet, should be liable for copyright infringement committed by a subscriber of the BBS.[67] The court held that it was "not entirely convinced that the mere possession of a digital copy on a BBS that is accessible to some members of the public constitutes direct infringement by the BBS operator."[68] This case is seen as the turning point for law concerning the strict liability of ISPs for copyright infringement.[69] *Religious Technology Center* allowed ISPs to escape strict liability because—although no knowledge of the infringement is needed for copyright law—actionable conduct is not present when a company "simply owns a system that others use to make copies."[70] This decision is the way courts generally allow ISPs to escape liability for online copyright infringement.

Recognizing a need to protect innovation on the Internet, in 1998 Congress passed the Online Copyright Infringement Liability Act (ILA), which is Title II of the Digital Millennium Copyright Act.[71] The act specifically protects ISPs from copyright infringement suits concerning unauthorized file sharing of copyrighted material.[72] The ILA states that

> A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections . . . .[73]

The ILA does give copyright holders a method of working with ISPs when a copyright infringement is detected.[74] If a copyright holder spots unauthorized file sharing, that copyright holder can contact the ISP and request action be taken.[75] Upon notification, the ISP must quickly "remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[76]

---

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Religious Tech. Ctr.* 907 F. Supp. at 1372 (further holding that, "[o]nly the subscriber should be liable for causing the distribution of plaintiffs' work, as the contributing actions of the BBS provider are automatic and indiscriminate.").

[69] *See* Elkin-Koren at 42.

[70] *Id.*

[71] Lateef Mtima, *Whom the Gods Would Destroy: Why Congress Prioritized Copyright Protection over Internet Privacy in Passing the Digital Millennium Copyright Act*, 61 RUTGERS L. REV. 627 (2009).

[72] *Id.*

[73] 17 U.S.C. § 512 (2012).

[74] *Id.*

[75] *Id.*

[76] *Id.*

3. Holding the Individual Liable

Because of the way that peer-to-peer file sharing works, it is difficult to hold a single, identifiable source liable for copyright infringement.[77] Thus, with a peer-to-peer copyright infringement case, the copyright holder's best opportunity to stop infringement is to sue the party that downloads the infringing files.[78] The Liability Limitation Act gives copyright holders the power to obtain the identity of an individual it believes to be downloading unauthorized files containing copyrighted material.[79] The Act says that a copyright owner may request the court issue a subpoena to an ISP "for identification of an alleged infringer."[80] Further, ISPs, "shall expeditiously disclose to the copyright owner . . . the information required by the subpoena."[81]

In 2010, a total of 119 potential plaintiffs received letters from their ISPs indicating that they stand to be sued for downloading unauthorized copies of the movie "The Hurt Locker."[82] The plaintiff, Voltage Pictures, LLC., claimed the defendants had downloaded the movie via the peer-to-peer file sharing program BitTorrent.[83] The defendants' various ISPs provided identifying information for the defendants in response to subpoenas from Voltage Pictures.[84]

How, exactly, Voltage Pictures was able to connect ISPs to individuals who actually downloaded the Hurt Locker is unknown. In their opposition to Defendants' motion to quash, Voltage Pictures claims they discovered the date and time of the unauthorized downloads, the ISP that provided Internet access to each defendant and the unique, Internet protocol (IP) address assigned to each defendant.[85] The method for obtaining this information is a "proprietary tracing software program" provide by a company called Guardaley, Limited.[86]

III. ANALYSIS

We see from examples provided by peer-to-peer litigation that the interests of copyright owners and the advance of technology will continue to conflict with one another.[87] As challenging as technology has been, however, copyright holders still win cases alleging infringement liability—be it secondary liability or vicarious liability—against some party. With block chain technology and Ethereum, software programs

---

[77] *See* Elkin-Koren at 35.

[78] *Id.*

[79] 17 U.S.C. § 512(h)(1).

[80] *Id.*

[81] *Id.*

[82] Voltage Pictures, LLC v. Does 1-5,000, 818 F. Supp. 2d 28, 31 (D.D.C. 2011).

[83] *Id.*

[84] *Id.*

[85] Plaintiff's Opposition to Motions to Quash at 8, Voltage Pictures, LLC v. Does 1-5,000, No. 1:10-cv-00873-BAH (D.D.C. 2011) (hereinafter "Voltage Motion to Quash").

[86] Voltage Motion to Quash at 8.

[87] *E.g.* Jacqueline D. Lipton, *Solving the Digital Piracy Puzzle: Disaggregating Fair Use from the Dmca's Anti-Device Provisions*, 19 HARV. J.L. & TECH. 111, 112 (2005) (writing that "[o]verzealous enforcement of copyright laws could impede technological innovation in cryptography and file-sharing, while under-enforcement could impede artistic innovation."

will exist and run across thousands of machines around the world.[88] Once software programmers have a network like Ethereum to upload their programs to, there will be no one left upon which to pin the liability.[89] This is best illustrated with a hypothetical. For instance, a software programmer can create a simple autonomous software program on the Ethereum network that allows users to exchange anonymous digital currency—like Darkcoin—for a complete PDF copy of *The Hunger Games* (novel). This program, by way of its "smart contract," can collect money and distribute unauthorized PDFs without need for further human interaction. Because the programmer loaded the smart contract software onto Ethereum's peer-to-peer network, (which is distributed among the thousands of computers connected to the network) it cannot be shut down. Similar to the way Bitcoin's block chain protects bitcoins from being double spent, Ethereum's block chain will keep software programs out of the reach of governments, courts and corporations.

    The program distributing unauthorized editions of *The Hunger Games* merely exists. There is no reason to believe the original programmer would have to attach any kind of self-identifying traces to the program, so he or she never faces liability.[90] No centralized organization runs Ethereum (there is an Ethereum Foundation, which constitutes the men and women who envisioned and built it, but once those individuals launched the Ethereum network, they technically surrendered control).[91] And because block chain technology enables cryptographically protected exchanges, it is entirely possible for an individual to send digital currency to the program and receive the PDF to an encrypted server, without being traced. This leaves no close ties of liability.

    Copyright holders could try to sue hardware makers for allowing these transactions to take place on their computers, but it seems likely the courts would shoot this down, saying that computers are used for much more than illegal file sharing.[92]

    Copyright holders cannot necessarily work with ISPs the same way they do when a P2P infringement transpires. And the type of protection ISPs will get from the LLA is unclear. Due to the cryptography protecting the identity of individual users, it is not likely the ISPs will have the ability to trace individual users or provide the kind of information subpoenaed in peer-to-peer cases.[93]

    Recall that in in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, Plaintiff MGM chiefly wanted the successful issuance of an injunction against the entities

---

[88] Finley; De Fillippi (reporting that "[i]nstead of being run locally, blockchain-based applications operate globally.").

[89] De Filippi (reporting that "[e]ven though the blockchain is inherently transparent (as every transaction is recorded on a public ledger), users can have multiple identities that don't necessarily relate to their real persona.").

[90] *Supra* note 89.

[91] Ethereum, *Foundation*, https://www.ethereum.org/foundation (last viewed Oct. 9, 2015) (stating that the "Ethereum Foundation is a non-profit organization registered in Switzerland, and has the purpose of managing the funds that were raised from the Ether Sale in order to best serve the Ethereum and decentralized technology ecosystem.").

[92] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 446 (1984) (holding that the business of supplying the equipment that makes copying of television programs feasible "should not be stifled simply because the equipment is used by some individuals to make unauthorized reproductions of respondents' works.").

[93] *Supra* note 89.

enabling unauthorized copying of MGM's property.[94] In a decentralized environment such as Ethereum, a software programmer can upload a decentralized autonomous program such as the one hypothesized about *Supra*, and hide his identity behind cryptography.[95] This makes an injunction feckless for it would be against an unknown party. Additionally, an injunction would not be enforceable because the program would exist on thousands of machines dispersed throughout the world. So, theoretically, you can destroy one machine hosting the hypothetical *Hunger Games*-selling program, but the program will exist on thousands of other machines.

IV. CONCLUSION AND PROPOSAL

To conclude, it appears as though a future, decentralized Web might prove challenging for copyright lawyers. Some may argue in favor of such dramatic social change, claiming that copyright laws tend to prohibit the spread of culture and knowledge.[96] Others, however, would point out that unregulated online copyright infringement would discourage artists and scholars from creating and producing.[97]

The uncertainties spawned by technological advances are inescapable. As has been suggested *supra*, the potential for copyright abuse is very real with the implementation of a decentralized Internet. Additionally, the absence of any realistic method of enjoining an infringer on a decentralized Internet poses new challenges for copyright holders and IP attorneys.[98]

I propose that copyright holders take advantage of the new technology. By offering licensing at an attractive price, copyright holders could inspire a culture that encourages software developers working in a decentralized regime to embrace the legal use of protected materials. By openly encouraging the authorized use of copyrighted materials, copyright holders will also encourage the growth of decentralized autonomous software programs that they support.[99] By definition, a decentralized

---

[94] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 913 (2005) (summarizing that "[s]eeking damages and an injunction, a group of movie studios and other copyright holders . . . sued respondents for their users' copyright infringements.").

[95] *Supra* note 89.

[96] *See Generally* MICHELE BOLDRIN & DAVID K. LEVINE, AGAINST INTELLECTUAL MONOPOLY (Cambridge University Press, 2008) (arguing that the "monopoly over useful inventions creates intellectual inefficiency because it also blocks the development of other potentially useful inventions.").

[97] Elliot M. Abramson, *How Much Copying Under Copyright? Contradictions, Paradoxes, Inconsistencies*, 61 TEMP. L. REV. 133, 134-35 (1988) (arguing that the "underlying premise of copyright law is that progress of the arts is promoted by granting talented creators exclusive control over their creations, and the economic rewards they generate.").

[98] *Cf.* Ben Depoorter, *Technology and Uncertainty: The Shaping Effect on Copyright Law*, 157 U. PA. L. REV. 1831, 1835 (2009) (opining that "copyright law is greatly influenced by technological change.").

[99] James Gibson, *Risk Aversion and Rights Accretion in Intellectual Property Law*, 116 YALE L.J. 882, 887 (2007) (laying out a theory that "the players in key copyright industries tend to be risk-averse, a tendency exacerbated by high upfront investments and the need to satisfy conservative insurers and downstream distributors," that "these factors cause copyright users to seek licenses even when they have a good fair use claim—i.e., even when proceeding unlicensed would probably result in no liability" and that the "result is a steady, incremental, and unintended expansion of copyright, caused by nothing more than ambiguous doctrine and prudent behavior on the part of copyright users.").

network is self-regulating. By instilling, early on, the notion that use licenses can be obtained at a reasonable cost to developers of decentralized applications, copyright holders may stand to influence the decentralized culture in their favor. If they wait and miss out on the opportunity to embrace and profit from a decentralized network, copyright holders may be reduced to disgruntled entities seeking feckless injunctions; portrayed as mean spirited, centralized corporations hunting down potential claims on a property right rendered ethereal by new technology.