



# Cryptocurrency and the BlockChain:

## Technical Overview and Potential Impact on Commercial Child Sexual Exploitation

Prepared for the Financial Coalition Against Child Pornography (FCACP)  
and the International Centre for Missing & Exploited Children (ICMEC)  
by Eric Olson and Jonathan Tomek, May 2017

## Foreword

The International Centre for Missing & Exploited Children (ICMEC) advocates, trains and collaborates to eradicate child abduction, sexual abuse and exploitation around the globe.

Collaboration – one of the pillars of our work – is uniquely demonstrated by the Financial Coalition Against Child Pornography (FCACP), which was launched in 2006 by ICMEC and the National Center for Missing & Exploited Children. The FCACP was created when it became evident that people were using their credit cards to buy images of children being sexually abused online. Working alongside law enforcement, the FCACP followed the money to disrupt the economics of the child pornography business, resulting in the virtual elimination of the use of credit cards in the United States for the purchase of child sexual abuse content online.

And while that is a stunning accomplishment, ICMEC and the FCACP are mindful of the need to stay vigilant and continue to fight those who seek to profit from the sexual exploitation of children.

It is with this in mind that we sought to research cryptocurrencies and the role they play in commercial sexual exploitation of children. This paper examines several cryptocurrencies, including Bitcoin, and the Blockchain architecture that supports them. It provides a summary of the underground and illicit uses of the currencies, as well as the ramifications for law enforcement and industry.

ICMEC is extremely grateful to the authors of this paper – Eric Olson and Jonathan Tomek of LookingGlass Cyber Solutions. When the FCACP proposed an examination of cryptocurrencies and their use in commercial child sexual exploitation, Eric and Jonathan immediately volunteered to take on the challenge. They brought their outstanding expertise and superb skills to the task and the result is a paper that will advance the FCACP in its mission and will be an excellent addition to ICMEC's research library.

Critical to the study of cryptocurrencies and commercial sexual exploitation of children is building an understanding of current laws and regulations that address the topic. That subject will be covered in a series of papers, with the first – reviewing the laws and regulations in the United States (at the federal and state levels) – to be released later in 2017. Future papers will look at laws and regulations in other countries and regions of the world.

ICMEC is proud of the FCACP and applauds its members for the role they play in helping to keep children safe. It is our hope that the financial industry, law enforcement and NGOs around the world will use this paper as a resource in their efforts to keep children safe from commercial sexual exploitation.



Ambassador Maura Harty, *ret.*  
*President & and Chief Executive Officer*  
International Centre for Missing & Exploited Children

## Acknowledgements

ICMEC wishes to thank the following individuals and organizations for their assistance and guidance related to this report:

- Eric Olson and Jonathan Tomek of LookingGlass Cyber Solutions, who are the authors of this paper and have brought their considerable talents and expertise to address this important aspect of keeping children safe from sexual exploitation.
- The reviewers of the paper, including Europol, FCACP Steering Committee members, the National Center for Missing & Exploited Children (NCMEC), and the New Zealand Department of Internal Affairs.

ICMEC extends a special thank you to American Express for its financial support of this effort.

## Executive Summary

As stated in the title, this report is meant to provide members of the Financial Coalition Against Child Pornography (FCACP), the International Centre for Missing & Exploited Children (ICMEC) and other interested parties and stakeholders with a primer on cryptocurrencies such as Bitcoin, Ethereum and Monero, as well as their underlying technologies, and the implications of these technologies for commercial child sexual exploitation. It is intentionally written in informal and non-technical terms in order to provide a basic background in this rapidly-advancing and technical field, and assumes that most readers have limited or no familiarity with the inner workings, risks, benefits and implications of cryptocurrency.

Cryptocurrencies, in their modern form, appeared on the scene in 2009 with the first release of the Bitcoin core. Bitcoin is by far the world's largest, best known and most widely traded digital currency. However, it has since been joined by a host of smaller players, some based closely on the Bitcoin architecture, but others which differ markedly in attempts to solve specific technical and privacy challenges. Nearly all of them do rely on a common foundational underpinning that is also helpful to understand. This common foundation is known as the blockchain.

At the simplest level, the blockchain is a distributed and decentralized database in which every member of the network retains a complete, verified and synchronized copy of all transactions. The architecture combines advanced cryptography, a complex incentive-and-reward system and a distributed-consensus model that ensures the integrity of the data in the complete absence of a central authority. The result is a system with a truly remarkable set of characteristics:

1. It is immutable, i.e. it *can't* be falsified or edited
2. It is "trustless," i.e. it ensures absolute trustworthiness in the system while requiring no trust at all in the honesty of the participants
3. It is "censorship resistant," which means while there may be consequences *after* a transaction has been made, if two users desire to engage in a transaction, it is *impossible* to prevent
4. Near-zero settlement times: Instantaneous final and verified settlement increases liquidity and capital velocity enormously.

These characteristics mean the blockchain will likely have broad and far-reaching implications for a wide range of industries beyond currency or finance, which we explore briefly in order to provide some context around the potential scope of the disruption these systems will bring.

They likewise of course have significant implications for criminal activity and for its investigation, analysis and prosecution as well. In that criminal realm, there is clear evidence that Bitcoin has made significant inroads into commercial sexual abuse material, the sex trade and in the exploitation and



trafficking of minors and adults alike. While Bitcoin does provide significant barriers to identification of individuals, it is not, contrary to the misinformation common in media reports, completely anonymous. In fact it is far from it.

At least in its current implementation, Bitcoin, the de facto standard digital currency for illicit activity, is neither as anonymous nor as opaque as many of its users and proponents believe. The overwhelming majority of Bitcoin information, from timestamps to dollar amounts to transaction history, nearly everything *except* the real-world identity of the users, is by design completely public, and any user can, and in fact “full” network nodes such as miners (covered below) *must*, download a copy of the entire data set to fully participate in the system. This data set is easily explorable using a variety of free and commercial off-the-shelf tools.

Moreover, the utility of Bitcoin and its even-less-widely-used cousins is still quite limited outside the borders of the Bitcoin universe. This means that, sooner or later, many users will attempt to spend their bitcoins with a mainstream online or brick-and-mortar merchant that accepts them, or convert them into more easily-spent fiat currency such as dollars or euros. At these connection points between the Bitcoin universe and the “real world” there is an informational and investigative choke point that can reveal or point the way toward the one key datum not available from the blockchain: the user’s identity. These chokepoints should be seen as a key opportunity for the investigation and prosecution of child exploitation that involves the use of Bitcoin and the blockchain.

Finally, in looking specifically at the use of Bitcoin and its ilk in commercial child sexual exploitation, we find definite, and of course deeply disturbing, examples of its use, some of which are highlighted. However, in a surprising turn, at least to the authors, there is actually some evidence that use of cryptocurrencies is quite limited for a variety of both economic and security-related reasons. Even Bitcoin, vastly more adopted than all its alternatives combined, is, in fact, both far too illiquid and (as criminals are learning, and the press and police should continue to publicize) not nearly as anonymous or as infallible as its proponents would have us believe.

Cryptocurrencies do make the job of battling commercial child sexual exploitation a bit different and a bit more challenging than in the past, but the same was true of e-Gold, PayPal and a dozen other payment systems when they first emerged. Some, like e-Gold, fought the law, and the law won. Some, like PayPal, aggressively took the fight to offenders and are now recognized as world leaders in this effort. If leading organizations like ICMEC continue to engage with the industry through the FCACP and other outreach groups, there is absolutely a body of data, tools, expertise, goodwill and willing volunteers that can continue to bring the fight to abusers.

## CONTENTS

Introduction: A Bit of History (and Mystery).....	4
A Primer on the Blockchain.....	6
What is the Blockchain? .....	6
So what? Why is this architecture so powerful? .....	9
1. Immutability .....	9
2. Zero Trust, Absolute Trustworthiness .....	9
3. Censorship Resistance .....	10
4. Near-Instantaneous Settlement.....	10
Disruptive Potential across a Wide Range of Industries .....	11
Bitcoin and Other Cryptocurrencies .....	13
Bitcoin: Blockchain-Based Money .....	13
Bitcoin is Not Alone .....	15
Underground and Illicit Uses .....	17
Investigation and Law Enforcement.....	18
Use in Commercial Child Sexual Exploitation .....	27
Content Production and Distribution .....	27
Trafficking and In-Person “Services” .....	28
Use Remains Limited .....	29
What Can Industry Do? .....	31
Conclusions .....	33

## Introduction: A Bit of History (and Mystery)

In order to understand the blockchain, cryptocurrencies, and the potential impact of both on commercial child sexual exploitation, it is worth a few minutes to review some history. Unlike many transformative technological trends that emerged gradually, the blockchain and cryptocurrency in its current form can actually be traced to a specific moment in time.

At exactly 18:10 GMT on October 31, 2008, a user named Satoshi Nakamoto posted a White Paper to a cryptography mailing list entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*.

In an amazingly concise eight pages, Nakamoto outlined a system for creating and exchanging a new form of digital money called Bitcoin<sup>1</sup> that brought together four complimentary characteristics.

**Digital signatures and encryption ensure security and clarity of ownership.** The proposal was very explicitly for a system of digital *cash*, not a digital *payment system*. In other words, you can be absolutely sure that someone offering you a bitcoin actually owns the bitcoin, and when you take possession of it, it is irrevocably and instantaneously yours. It is not stored as a balance in a bank that you can access, or, for example, during a run on a bank, be *denied* access to. It is, in this way, akin to cash more than it is to simply having a digital balance in a third-party bank's computer. The appeal of absolute possession, and in an alternate, non-national currency, is enormous, especially (just as one example) in unstable economies. This absolute possession was true in some past experimental attempts at digital cash as well, but they suffered from another problem that Bitcoin successfully addresses.

```
From: Satoshi Nakamoto <satoshi<at>vistomail.com>
Subject: Bitcoin P2P e-cash paper
Newsgroups: gmane.comp.encryption.general
Date: Friday 31st October 2008 18:10:00 UTC (over 8 years ago)

I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the
network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would
allow online payments to be sent directly from one party to another
without the burdens of going through a financial institution.
Digital signatures provide part of the solution, but the main
benefits are lost if a trusted party is still required to prevent
double-spending. We propose a solution to the double-spending
problem using a peer-to-peer network. The network timestamps
transactions by hashing them into an ongoing chain of hash-based
proof-of-work, forming a record that cannot be changed without
redoing the proof-of-work. The longest chain not only serves as
proof of the sequence of events witnessed, but proof that it came
from the largest pool of CPU power. As long as honest nodes control
the most CPU power on the network, they can generate the longest
chain and outpace any attackers. The network itself requires
minimal structure. Messages are broadcasted on a best effort basis,
and nodes can leave and rejoin the network at will, accepting the
longest proof-of-work chain as proof of what happened while they
were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

-----
The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to majordomo@metzdowd.com
```

---

<sup>1</sup> By convention, Bitcoin (capital B) refers to the system, network, mining and wallet software and so on, and bitcoin (small b) refers to the "coins" or any fractional variant thereof, i.e. the units of currency within the Bitcoin network.

**Bitcoin solves the so-called “double spend” problem.** Unlike physical money, electronic files can be easily duplicated. If each coin or unit in a digital currency is just a file, there must be a mechanism to prevent a user from sending the same digital coin or unit to multiple recipients. This traditionally required a central authority to verify that units of value offered to a seller had not already been spent elsewhere by the buyer via a centralized ledger or clearinghouse. The bitcoin architecture uses a mechanism called proof-of-work (more on this later) that makes it impossible to spend the same coin twice.

**The solution to the double-spend problem requires no central authority** such as a bank or government. Bitcoin not only solves the double-spend problem, but specifically does so in a way that explicitly eliminates that need for a trusted central authority or market-maker. It is, as the title of the paper says, a *peer-to-peer* system; it is totally distributed.

Most currencies are issued by an authorized entity such as a national treasury or central bank. Bitcoin is purely peer-to-peer, and new units are essentially generated out of thin air by the participants in the ecosystem themselves. While this might lead one to question the utility or value of this “made up Internet money,” it is actually less nonsensical than it sounds.

Bitcoin is, in this way at least, no different than the US dollar. Both are instruments with no inherent value of their own that can be traded for goods and services based purely on a mutually-agreed convention among the users. The only reason one American provides real goods or services in trade for green ink printed on cotton is the shared belief that another user down the line will similarly accept that dollar bill as a token of value when offered in trade for something else.

The innovation in Nakamoto’s approach negated the need to have any one central power issue the money. Because it solves the double-spend problem among the participants themselves, the Bitcoin proposal essentially asked *and answered* the question, “If money is just a mutually-agreed convention that can be traded for real goods and services, why do we, the users of this network, need someone else to create money for us?” Answer? They don’t. They can, and do, create their own money, purely by mutual acceptance of the conditions built into the network’s design.

**Value requires scarcity, and Bitcoin ensures a known, bounded volume of currency in circulation.** By setting clear rules, limits and timetables for block and coin generation (again, more on this shortly), the scarcity of the currency, the volume of coins in circulation at any moment in time and safeguards against counterfeiting are built right into the core Bitcoin protocol itself.

In 2009, the theory behind Bitcoin became real with the first release of Bitcoin software, which put into actual practice all the elements of the original architecture. The system, with various software upgrades, has been in continuous operation since, with approximately 16 million bitcoins (each worth north of \$1,000 USD as of this writing) now in circulation.

Finally, there is one more unusual fact about this potentially globally-disruptive technology...

**No one knows who created it.**

The 2008 paper was published by a person or persons unknown. Satoshi Nakamoto is a pseudonym. While there have been several people put forth as possible candidates, and one who eventually claimed (but explicitly failed to prove) that he was Nakamoto, the creator's actual identity is still a mystery. This is all the more remarkable because, as of this writing in early 2017, Nakamoto's personal store of bitcoins is now worth approximately one *billion* US dollars.

Let us now dive deeper into how cryptocurrencies like Bitcoin (there are now many others as well) actually work in order to frame their potential impact on commercial sexual child exploitation, and for that matter, other forms of cyber and physical crime.

## A Primer on the Blockchain

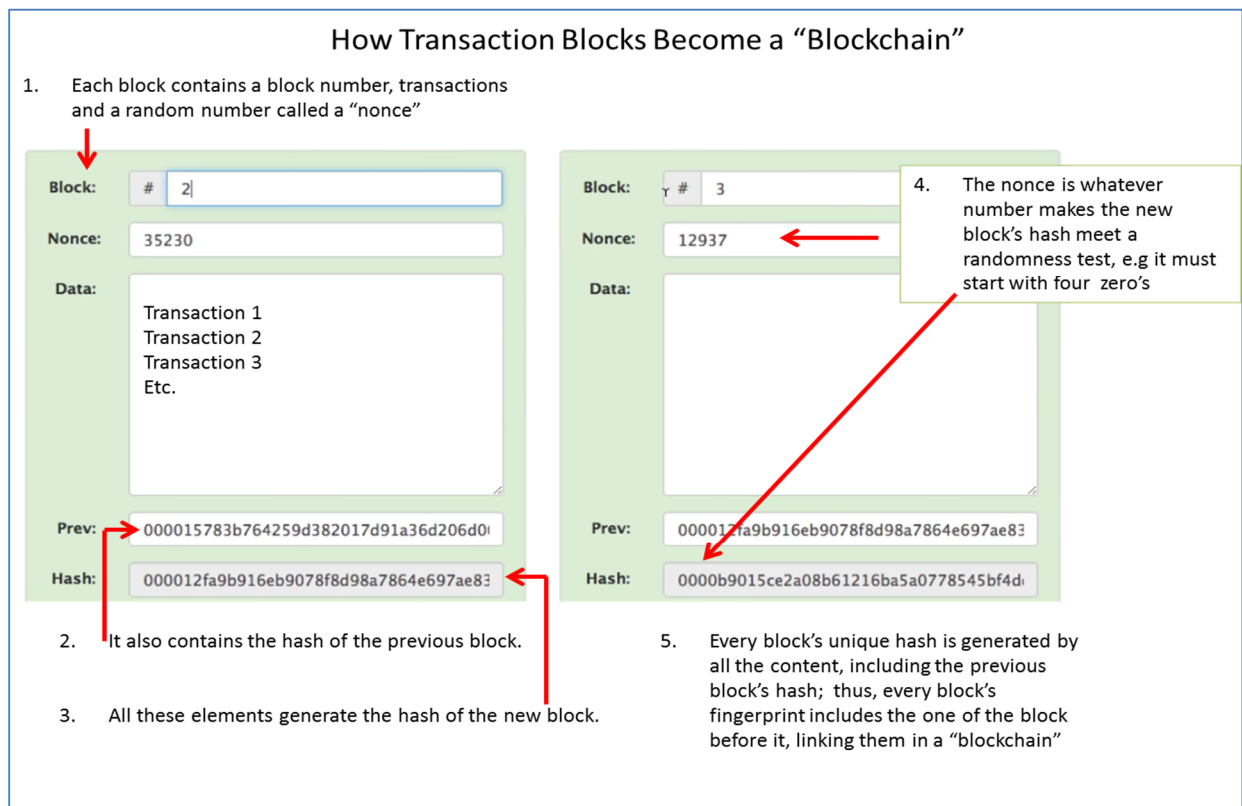
### What is the Blockchain?

In order to understand Bitcoin or similar cryptocurrencies, it is first necessary to understand the underlying database, which is called the blockchain. In fact, the true innovation of Bitcoin is not really the digital money at all, which has existed in many forms for decades. Rather, it is the underlying system that makes a distributed, peer-to-peer currency possible. Think of this as an analog to the early days of the Internet. The first thing the Internet enabled of value to common everyday users was email. This was followed years later by the World Wide Web. Both are remarkable innovations that have changed how we live, work and communicate, but they are applications on top of a more foundational underpinning. For either application to exist, the enabling infrastructure of the Internet and the transmission of data over a protocol called TCP/IP had to exist first, and these have since enabled many other useful applications as well. The blockchain similarly undergirds the currency application that is layered on top.

So what is the blockchain? At the most basic level, a blockchain is a distributed system in which a bunch of computers all store copies of a database. More specifically, it is a ledger, i.e. a record of a series of transaction events, but a ledger with a very specific set of properties.

1. **Events are recorded chronologically:** Transactions have time stamps, and transactions are grouped into "blocks" and the blocks are then added to the "official" version of the ledger in sequential order. This may not sound unique; however, it is critical because it is also true that...

2. **Each block can only be created by incorporating information from the previous block:** In a blockchain, each transaction is recorded into a “block” of transactions that become part of the permanent record, and generating a block requires specific inputs, some of which are markers derived from the previous block. This linkage between each block and the one that preceded it, which leverages a technique called cryptographic hashing, essentially “chains” the event sequence together in a clear and unalterable chronological order (hence the name blockchain). As a result, the ledger must, by design, contain a complete record of *everything* that has happened in the system since the very first or “genesis” block. To make this easier to understand, let’s look at a diagram of how a single block is added to the blockchain.



3. **The blockchain is distributed:** Everyone who participates in the network has a copy of the ledger. Given point #2 above, this means that everyone *in* the system has a copy of the entire history *of* the system. It also means that no one party is the owner or keeper of any “master” copy. There is no central authority or clearinghouse that can manipulate or withhold the data.
4. **Encryption is built into every aspect of the process:** The creator(s) of the blockchain learned a great deal from the early mistakes in the creation of the Internet. Unlike the earlier system, which took many years to retroactively resolve the fact that it did little to ensure privacy or security, the blockchain incorporates strong encryption, security and privacy in its basic DNA.



5. **The system automates consensus:** Perhaps the most remarkable innovation of the blockchain is that, by some very sophisticated methods, it essentially forces all participants to agree on one definition of “the truth.” The system identifies and resolves discrepancies in the data automatically if the network nodes start to disagree about entries in the ledger.
6. **Adding records to the database incurs a cost:** The mechanisms are quite technical, but simply put, in order to add a new block to the blockchain, certain participating systems in the network (known as “miners” in the Bitcoin world), must perform some very expensive brute-force calculations to solve a math problem. They have to spend electricity and labor and computing power to solve these problems, and to thereby be allowed to add records to the officially and mutually sanctioned version of the ledger. This requirement to perform expensive calculations, known as Proof-of-Work, is intentionally designed to drive costs *up* for miners.
7. **Participants are incentivized to compete for the right to add records to the database:** Miners voluntarily incur these costs because they are motivated with a potential reward. When a new block of transactions is ready to be added to the authoritative shared ledger, many miners will have the transaction data, but they must compete to be the first miner to solve one of these costly math problems in order to be the miner authorized to add it to the official ledger. The first miner who successfully completes the math problem, and thus wins the right to add the new block to the chain, is rewarded with some value. In the case of the Bitcoin implementation of blockchain, the reward (as of this writing) is 12.5 newly-created bitcoins worth approximately \$12,000, which are essentially created “out of thin air” by the rules of the Bitcoin network itself. With minor variations, new blocks are added to the chain roughly every ten minutes.

This means that there is a bounty of approximately \$1.8mm per day, or more than half a billion dollars per year, up for grabs to the miners who participate in helping add and verify blocks to the database. In other words, the right to create new bitcoins is the incentive that motivates miners to compete in the Proof-of-Work contests that, through their collective efforts, ensure the safety, validity and security of the shared ledger. In exchange for a shot at huge payoffs every few minutes, the miners essentially keep the entire system trustworthy for themselves and everyone else.

In summary, the blockchain is a secure, distributed, chronological ledger in which participants compete and are rewarded for ensuring the security and consistency of the ledger. Now let us look at why this structure is so innovative and what the practical implications are.

## So what? Why is this architecture so powerful?

Taken together, this built-in combination of features, methods and characteristics results in a system that might seem peculiar to the casual observer. It is a system where no one owns the data and you can't edit the records once they've been saved. Taken together, these two facts mean, among many other things, if you ever lose or are scammed out of a bitcoin, or store them in an unbacked-up computer that crashes, they are gone forever. There is absolutely no recourse and no central authority to appeal to or petition for a refund. Moreover, to add data to the system, large numbers of participants voluntarily incur huge costs. So why would anyone want such a thing? Because this mix of attributes results in a system with a number of truly remarkable characteristics.

### 1. Immutability

A system that is encrypted, distributed, and consensus-based, a system in which every block incorporates, and cannot exist without, elements of the previous block, and in which each block can only be added to the official ledger after costly Proof-of-Work, is for all practical purposes, immutable. Put simply:

**You *can't* falsify the data. The blockchain is essentially immune to hacking, fraud or unauthorized modification.**

Once a block has been added to the chain and distributed out to the network, the only way you could edit, falsify or change a record would be to get everyone on the entire network to go back and agree to change every copy of the database. The cryptography aspect of the process makes this falsification (nearly) impossible mathematically. More importantly, the Proof-of-Work element makes it impracticable economically. Remember that every block is inextricably linked to the one that preceded it, and generating each block requires lots of competing miners to all incur lots of cost. This means that to get the entire network to accept a falsified block, you would have to regenerate the entire ledger from that point forward, *and* get the whole network to accept your altered version of the truth. To do this would require you to re-expend the equivalent of *all* the costs incurred by *everyone* in the system since the block you seek to modify was logged.

### 2. Zero Trust, Absolute Trustworthiness

The second remarkable innovation in Nakamoto's design was merging a range of existing concepts from game theory, computer science, mathematics and other disciplines into a system that enabled "distributed trustless consensus." In most traditional transaction systems, we must inherently place trust in some central authority or entity, whether that is a central bank that issues sovereign currency, a broker transacting equities on our behalf, or a government body issuing title to some property or asset. The system only works if we all agree and assume that the central party is an honest broker (and that their computer systems are accurate and secure, which is all too often not the case).

By removing any central processor, broker, owner or market-maker from the data stream, by ensuring that everyone must agree to the record for the record to be valid, and by giving everyone in the network a copy of the same data, the blockchain *structurally* doesn't require trust. In other words, blockchain data is not only, for all practical purposes, impossible to falsify as noted above, but it thereby enables complete trust in the integrity of the process even in the absence of trust in any of the participants. Thanks to the decentralized, forced-consensus model of the blockchain, you can believe absolutely that every other participant would rob you blind if they had the chance, and yet you can still transact with them in complete confidence. Given the potential lack of "honor among thieves," the potential utility of such a system in the criminal world is obvious, but it also offers advantages over the traditional payment systems used by the general public for decades.

### 3. Censorship Resistance

In this context, "Censorship Resistance" is a term of art referring to a very specific characteristic of the blockchain network, at least in its current Bitcoin implementation. Because it is permissionless and decentralized, anyone can join it anonymously and no central authority logs or controls who comes and goes. Put simply, this means that while authorities or other parties may impose a penalty, fine or prosecution for having made a transaction, there is no way to prevent it from happening in the first place. This has significant implications we will explore later.

### 4. Near-Instantaneous Settlement

The other potentially seismic change this system enables is nearly instantaneous final settlement of transactions. This might seem like "no big deal" to the average consumer, but for the commercial sector the implications are enormous. Consider just a few examples.

If a consumer walks into a café and buys a latte with their credit card, from the consumer's perspective, that charge appears on their account within, perhaps, one day. So if it appeared within seconds, would that materially change the experience? Not really. However, the merchant has a very different experience. By the time the money in question has been passed from the consumer's bank to the payment processor to the credit card company to the merchant's bank to the merchant's account as payment, two things have happened.

First, somewhere between three and seven percent of the price of goods sold has been taken off the top as fees, costs and profit margins for all the middlemen handling the money. Second, the money may have taken as long as 30 days to arrive in the merchant's account. In other words, the merchant has essentially loaned their working capital to all the middlemen for up to a month, allowing them to earn interest on the "float," while the merchant, who has bills to pay out of what is already in their account, is paying interest or opportunity cost on the missing working capital.

Now imagine the exact same transaction for a café that accepts bitcoin. The consumer walks in and buys a latte. The money is received in the merchant's account five to ten *seconds* later, ready to be spent on costs and purchases, and the fee incurred is less than a penny. In many retail businesses, net

profit margins are often razor thin, sometimes as little as two or three percent. If a meaningful portion of their revenues suddenly changed from minus-five-percent-in-fees to essentially free, the extra few points of margin could literally change the viability of many small businesses.

More broadly, near-zero settlement times have dramatic implications for liquidity in all kinds of markets. Today, suppose that a US “day trader” logs onto their brokerage Web site and, let’s say, buys and sells 100 shares of a stock through a Web browser, completing both transactions within five minutes, making a small profit on the moment-by-moment swings in the stock’s market price. While those transactions actually take three days to legally settle in the back-office computers of a settlement clearinghouse, the user experience in the stock market is one of instantaneous liquidity. The user can sell an asset seconds after purchasing it if they so desire.

Transactions using Bitcoin, or a Bitcoin-like system, essentially could bring this type of liquidity and velocity to entirely new asset classes. Imagine a world where land, vehicles, buildings, artwork, collectibles or other assets could be traded electronically, securely and with absolute certainty of ownership with the speed and ease of trading stocks on E-Trade.

## Disruptive Potential across a Wide Range of Industries

The implications of this are mind-boggling. As with any disruptive new technology, those implications may be good or bad for one’s personal interests, depending on his or her role in the status quo. However, while any one party may be a winner or loser in the future, writ large, consider just a few of the other potential areas outside of money and finance that could potentially be impacted by some future system that features completely transparent ledgers, unimpeachable ownership and unfalsifiability. We offer the following as three simple illustrative examples to get the reader’s mind thinking about just how big a disruption this may represent.

**Title Insurance:** Anyone who has bought a home in the US is familiar with the line on the settlement statement that tacks on a fee, usually several hundred dollars, for some company to provide research into, and documented history of, the ownership and title of the property they are buying. This not only ensures that the seller actually has the right to sell the asset in question, but the buyer will have clear title to it, and the service provides insurance against future risks should someone come forward and attempt to put a claim on the title. Worse still, when the buyer later sells the house, the entire process is repeated and the fee charged again, even though the title was researched and verified at the last change of ownership.

Now imagine that municipalities have put the entire ownership history of each property in a blockchain database. There is no need for title insurance because the ownership, history and rights of the seller and buyer are guaranteed and immutable. This could potentially wipe out the need for

residential title insurance services entirely, and (at a conservative estimate of \$300 per sale on 4.5 million US home sales per year) put \$1.35 billion dollars back in the hands of consumers to spend on other things.

**Energy:** This is a somewhat speculative example, but one which exemplifies how the blockchain might be combined with other innovations to utterly transform an industry that has remained largely unchanged for decades. Imagine the implications if consumers who produce their own energy, e.g. via wind, solar or geothermal micro-generation on their own property, could directly sell, buy and transmit energy with their neighbors. This might not only alter the dynamics in developed economies from their traditional model of large generators and distributors in regulated markets, but could be a complete “leapfrog” step in the developing world where an established, robust grid may not exist yet.

As renewable and personal power generation explodes, nascent energy markets could develop without a central authority in the same way that many countries leapt directly from no phones to ubiquitous cellular without ever implementing traditional, nationally-controlled copper-wire phone systems. A remote village in rural Africa, for example, could go directly from no electricity to solar power that is counted, bought, sold and recorded on a blockchain directly between those neighbors with excess to sell and those neighbors without solar panels ready to buy. Neither the financial transaction, nor the micro-grid between houses would require any central authority or outside regulation. In *both* cases (i.e. the generation of power and the financial trading of it), the members of the network themselves negotiate, price, agree and transact without need of higher authority.

**Elections:** A blockchain-based system uses cryptographic keys to anonymize, but itemize, every user in the system, and in this use case, the details of their “transactions,” i.e. their votes, are otherwise public, documented and immutable. For countries struggling with, or concerned about, vote-rigging, corruption or other improper influences on the electoral process, a blockchain-based voting system, perhaps tied to biometric user accounts that ensure every voter is one, and only one, real human being, might offer a path to absolute clarity, verifiability and accountability in the democratic process.

These three are just simple examples to help communicate the vast implications of distributed, public, immutable ledgers on a wide range of industries and processes. Many, many more, from escrow services to global remittances to the fine art market could be fundamentally rewritten by the capabilities of some future implementation of a blockchain.

# Bitcoin and Other Cryptocurrencies

## Bitcoin: Blockchain-Based Money

As discussed in the Introduction, Bitcoin is an application on top of the blockchain architecture. Many experts have compared the blockchain to the fundamental protocols and standards that enable the public Internet. The Internet, the comparison says, is a design optimized for the free transmission of information. The blockchain is a design optimized for the secure transmission of value. If the blockchain provides secure, immutable and instant transmission of value, then money is the obvious first, but far from the only, potential application. Digital cash is simply the first compelling application to build on, prove and drive evolution of the underlying architecture, much as email and then the Web did for the Internet.

So how does it work? It's actually quite simple. Users acquire bitcoins, and use the Bitcoin network to trade bitcoins for goods and services with other users or commercial merchants who agree to accept bitcoins as payment. A user can acquire bitcoins in one of three ways. First, they can purchase them on an exchange for fiat money such as dollars. You simply log onto an exchange Web site, create an account and link it to a checking account or credit card, then use dollars or Euros or other common currency to purchase bitcoins like you would acquire Sterling before visiting the UK or yen before flying to Japan. Your bitcoins are then stored in your "wallet," a software app that holds your public and private crypto keys and allows you to transact with other Bitcoin users. There are now even Bitcoin ATM machines where you can put in your cash or bank card and have bitcoins transferred into your Bitcoin wallet in seconds. These often appear in unlikely locations, including the one shown here which was installed in, of all places, a Shell gas station less than ten minutes from the headquarters of ICMEC.



The second way to acquire bitcoins is to create an account and install wallet software, then provide real goods or services to a bitcoin holder and accept bitcoins as payment. If you offer services likely to be of interest to the types of users who hold bitcoin, e.g., design, freelance coding, etc. it is entirely possible that some of your customers would be willing to pay in Bitcoin if asked.

The third option is to become a miner by downloading mining software and adding your computer to the global network of machines trying to solve the complex math problems that award you bitcoins for being the first to randomly generate a winning hash to add a block to the chain. Mining has



become so fast and hyper-competitive, however, that this method is not really practical for all but dedicated professional miners.

In order to be reasonably profitable, professional miners run vast server farms of custom-built specialized machines optimized for the brute-force hashing that enables successful mining. In fact, this industry has become so large, and so competitive, that the profits available justify not just custom machines, but custom *chips*, known as Application-Specific Integrated Circuits or “ASICs,” despite the enormous initial costs of tooling up a chip fabrication process. They are also beginning to cluster in regions that have either or both of two specific characteristics: they are either in places with extremely low-cost or subsidized electricity, since power is by far the largest on-going expense (e.g., China, where the power companies themselves have begun to run mining operations), and/or in places with cooler climates such as Sweden, since the specialized mining computers produce enormous amounts of heat and cooling consumes as much power as running the machines.



Image: Inside view of a Swedish mining farm<sup>2</sup>.

This does not mean, however, that the individual user cannot participate in mining. Average users can join a “mining pool” where they essentially pay for a small fractional share of the expenses of running a mining farm, and receive a pro rata share of the coins that are successfully won by the farm.

By any or all of these methods, you end up with a bitcoin, or a fraction thereof (bitcoins are actually divisible down to the eighth decimal place, a fraction whimsically known as a “Satoshi”) in your Bitcoin wallet. You can then transact with any other user for goods or services in the real world, or spend your bitcoins at a merchant or Web site. The number of “mainstream” merchants accepting bitcoins has

---

<sup>2</sup> <http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic>

grown exponentially in the last few years, and now includes Overstock.com, Dell Computers, Expedia and PayPal, among many others. If you acquired your bitcoins by mining or received them in payment rather than buying them, you can also of course just use the same exchanges or ATM machines to exchange them back into fiat currency such as dollars and put them in your pocket or bank account.

## Bitcoin is Not Alone

While Bitcoin is by far the largest and best-known of the cryptocurrencies currently in circulation, it is by no means alone. Despite its many creative, indeed revolutionary, innovations, Bitcoin is beset with problems and limitations. Some alternative coin systems will develop solutions that may be folded back into the Bitcoin code later. Others explicitly seek to dethrone Bitcoin and take its place by addressing some of its flaws and limits. Here is just a sampling of how busy the space has become in a few short years.

**Ethereum:** Ethereum is the brainchild of Vitalik Buterin, a programmer who was originally heavily involved in the Bitcoin software code. The problem Buterin sought to solve was that he saw how Bitcoin and the blockchain could actually support a wide range of broader applications if a fully robust scripting language could be built into the Bitcoin core code. Failing to gain a consensus among the Bitcoin developer community, Buterin created a new cryptocurrency that incorporated many of the improvements and broader capabilities he envisioned.

**Litecoin:** Litecoin is a close cousin to Bitcoin, and technically very similar. Created by a former Google engineer, Charles Lee, it is actually based on the core Bitcoin software, but incorporates a few key differences. The maximum number of coins to be issued is four times larger, the blocks are added to the blockchain in 2-3 minute increments vs. around ten minutes for Bitcoin, and some technical differences are built in to change how the hard math of the Proof-of-Work is accomplished.

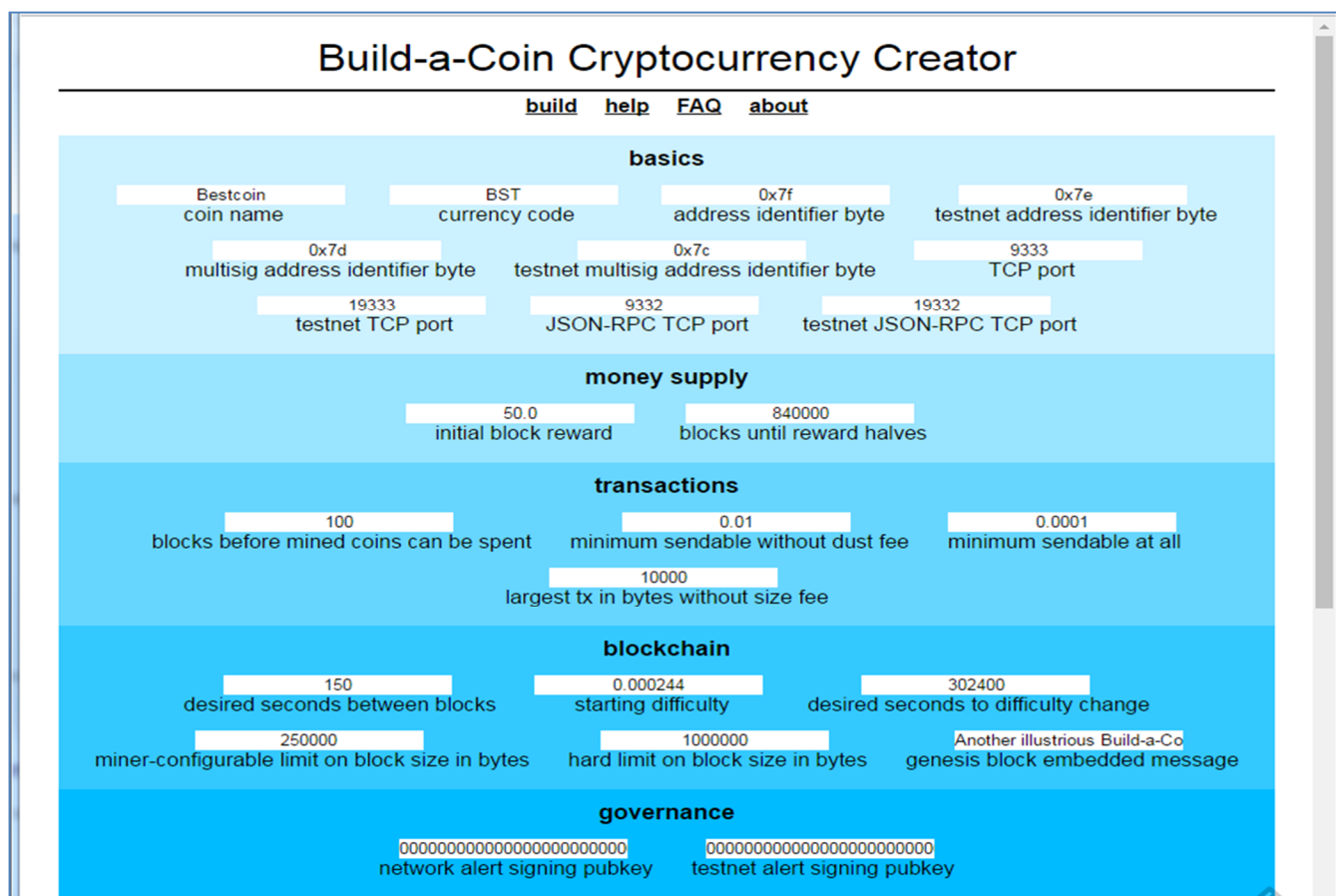
**Monero:** Monero is an open-source cryptocurrency created in 2014 that explicitly attempts to radically increase the privacy and anonymity for users relative to the many cryptocurrencies that are derivatives of Bitcoin. Monero is based on the CryptoNote protocol and incorporates significant algorithmic differences, an obscured blockchain, one-time wallet addresses for each transaction and the inclusion of an I2P (anonymizing Darknet) router directly in the application. In other words, Monero is explicitly designed to be many levels more difficult to investigate, track or explore than the Bitcoin blockchain, which has led to its rapid adoption in the last year by both online and offline sellers of illicit materials, drugs and other contraband.

**Ripple:** Ripple was started in 2012 and is a peculiar hybrid in the space. It is both a currency and a payment network that allows for instant conversion into different currencies. You can convert bitcoin to Ripple, and vice-versa, serving (at least in its own eyes) not as a competitor to Bitcoin, but rather a compliment to it. By making currency conversions easy, Ripple attempts to provide more liquid access

to traditional currencies and help make cryptocurrencies easier for the mainstream consumer to adopt.

These are just a few of the best known examples. From a single player just a couple of years ago, Bitcoin, Litecoin, Ripple and Ethereum have been joined by a host of others, including Dogecoin, Steem, Dash, Peercoin, Primecoin and Anoncoin, just to name a few, each with their own purported advantages, niche markets or specialized functions.

Perhaps the most astonishing evidence of how fast this technology is evolving, and commoditizing, is the appearance in the last year of Web sites that will take a variety of user inputs (e.g. name, proof-of-work method, hashing preference) and auto-generate your own blockchain-based coin with a few mouse clicks.



**Build-a-Coin Cryptocurrency Creator**

[build](#) [help](#) [FAQ](#) [about](#)

**basics**

Bestcoin coin name BST currency code 0x7f address identifier byte 0x7e testnet address identifier byte

0x7d multisig address identifier byte 0x7c testnet multisig address identifier byte 9333 TCP port

19333 testnet TCP port 9332 JSON-RPC TCP port 19332 testnet JSON-RPC TCP port

**money supply**

50.0 initial block reward 840000 blocks until reward halves

**transactions**

100 blocks before mined coins can be spent 0.01 minimum sendable without dust fee 0.0001 minimum sendable at all

10000 largest tx in bytes without size fee

**blockchain**

150 desired seconds between blocks 0.000244 starting difficulty 302400 desired seconds to difficulty change

250000 miner-configurable limit on block size in bytes 1000000 hard limit on block size in bytes Another illustrious Build-a-Co genesis block embedded message

**governance**

00000000000000000000000000000000 network alert signing pubkey 00000000000000000000000000000000 testnet alert signing pubkey

Image: [www.build-a-co.in](http://www.build-a-co.in)

Certainly, “JohnSmithCoin” might not have much appeal or utility to a global user base, and never acquire monetary value. Nonetheless, as shown in the “Build-a-Coin” Web site example above, this is evidence that this revolutionary technology has gone from something that only its advocates and devotees can operate, to something that a user with no more knowledge of its inner workings than they have of their Web browser can now begin to leverage.

## Underground and Illicit Uses

Outside of technology, law enforcement and a few other specific verticals, general public familiarity with Bitcoin, in name if not in particulars, is largely due to its association with the Silk Road marketplace. Bitcoin was, and remains, the principal method of payment used on Silk Road and many other black and gray market Web sites. Thus, the much-publicized takedown of the Silk Road and its founder by US law enforcement not only put Bitcoin into every mainstream newspaper, but headlines like “The Secret Web: Where Drugs, Porn and Murder Live Online” inextricably linked Bitcoin in the public imagination to online drug dealers, pedophiles and murder-for-hire.

Bitcoin and its relatives obviously would hold great appeal for criminals. It is perceived as totally anonymous (though as we will discuss, this is not entirely true), it is instantaneous, passes through no regulated authority or institution, and is borderless and censorship-resistant. In other words, the things that make Bitcoin Bitcoin, which we have explored above, are exactly why it would be an appealing medium for the exchange of value among criminals.

In fact, as one interesting measure of the expansion of Bitcoin and the like in the criminal world, consider this data point provided by online intelligence firm and fellow FCACP member G2, which tracks millions of surface Web sites suspected to be involved in transaction laundering. Referring to Web sites engaged in some illegal or violating activity, G2 observed Bitcoin or other cryptocurrency available 11% of the time in 2016, nearly triple the 4% seen the previous year and the under-3% level observed in 2014.

When combined and used in concert with sites on the so-called “Dark Web” that run on non-HTTP networks like Tor, I2P, Freenet and Zeronet, the difficulty in locating, attributing or identifying any actor or even Web site/marketplace operator make a powerful mix to enable cybercrime that is hard to detect, and harder still to investigate and prosecute.

As of this writing in early 2017, even the casual and non-technical observer will hear regularly about criminal uses of cryptocurrencies. Not only are they commonly reported in the media as the preferred method for purchase of goods and services in online criminal markets, but they are, for example, the almost-exclusive way to pay criminals who attack via ransomware, a virus that locks your computer and demands bitcoins to release control back to the user. It is also true that Darknet marketplaces such as Alphabay, Valhalla and Dream Market that offer a wide range of criminal goods and services do thrive on Bitcoin and, to a lesser extent, other cryptocurrencies.

The results of these widespread associations between Bitcoin and crime, and discussion of Bitcoin’s anonymity, are two-fold. First, the perception that Bitcoin is totally anonymous engenders the belief among criminals, as well as some investigators and legislators, that its use is entirely anonymous.

Second, and closely related, is the perception that commercial child sexual exploitation has, as a result, rapidly shifted to Bitcoin for payment.

While there is certainly some truth to both of these perceptions in specific cases, the reality is much more nuanced and both these perceptions are only true within fairly specific limits, especially in the very specific case of child sexual exploitation, which is so anathema to so many, that even criminals who accept all other forms of illegal commerce will often band together to combat it. We will now briefly explore each of these areas in turn.

## Investigation and Law Enforcement

The perception that Bitcoin is totally anonymous is both practically and by definition incorrect. Properly described, Bitcoin is pseudonymous. Much like email, it hides the real-world identity of the user behind an address, though with Bitcoin it is admittedly a human-unfriendly address typically made up of an unreadable string of characters. However, it is, in all other ways, vastly *more* transparent, explorable and accessible than email, cash exchanges or other private communications. But if encryption and security are built right into the architecture of Bitcoin, how can this be so?

First, recall from the overview of the blockchain that one of the key foundations of the system is a *public* ledger. You may not know who `8u4hufhehr28dhehrjdhed884kd92` is by name, but you do know the complete history of every transaction they have been party to, exactly what parties (by address) were involved, how much changed hands and the time, down to the second that the transaction took place. You also know the history of every bitcoin involved from the second it was mined. You know every pair of hands the bitcoin has gone through, and every transaction every one of those people has ever done.

This is far *more* visibility than traditional cash provides, and it is engendered by the fact that not only is the ledger public, but every full participant in the network has a complete copy of the entire history back to the very first transaction. A host of academics, computer scientists and, more recently, startup companies are taking advantage of this reality to demonstrate how the nature of the blockchain actually can provide extraordinary insights into transaction patterns, flows and even user identities for criminal investigators and governmental authorities.

For example, Sarah Meiklejohn, a leading expert on the topic, co-authored a 2013 study<sup>3</sup> specifically on investigative analysis of Bitcoin transaction data. She found that by applying advanced clustering

---

<sup>3</sup> A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, S. Meiklejohn et al, University of California, San Diego and George Mason University, October 2013

and heuristics techniques to Blockchain data, often based on small innocuous purchases she made on Silk Road herself, she could conclusively link hundreds of thousands of transactions together, and reduce almost 12 million unique addresses to a much smaller cadre of actual users. (See the four-minute video at <http://cacm.acm.org/magazines/2016/4/200174-a-fistful-of-bitcoins/abstract> for a concise explanation of how this was accomplished.)

While Bitcoin certainly poses some additional hurdles to investigation relative to well-established payment systems such as credit cards and money-transfer services, the study in fact specifically states as one of its goals, to explain “the challenges for those seeking to use Bitcoin for criminal or fraudulent purposes at scale.” Rather than lament the opacity of the Bitcoin blockchain as hopeless for effective investigation, Meiklejohn states rather that, “an agency with subpoena power would be well placed to identify who is paying money to whom.”

This fact poses two potential benefits to investigators, prosecutors and law enforcement professionals. The first is the hope, based on comments from experts such as these, that the anonymity of Bitcoin and other cryptocurrencies is, given some investigative effort, not nearly as complete or impenetrable as it might otherwise seem.

The second is more nuanced, and was summed up in an insightful observation made in his 2013 U.S. Senate testimony by Ernie Allen, then the President and CEO of ICMEC, who said, “the attractiveness of Tor and Bitcoin for child pornography is based upon a perception of anonymity... Thus, if the perception of anonymity diminishes, we believe the criminal use will diminish with it.”

As the members of the FCACP know well from past experience engaging with PayPal, MoneyGram, Western Union and the major credit card companies, every obstacle, speed bump or increase in transparency that can be added to a particular payment method used by criminals contributes directly to their migration to some alternate method. Given that Bitcoin’s reach and acceptance dwarfs that of all other current cryptocurrencies combined, if criminals gain the *perception* that it is no longer safe to use, they will be driven to even more obscure and less established alternatives, which increases friction, reduces the buyer pool and most importantly, reduces liquidity of the payments received, which we will discuss further in the section on Child Exploitation below.

Thus, one possible prescription for potentially reducing the utility of Bitcoin for criminals is to aggressively publicize and highlight cases where criminals are successfully identified, arrested and prosecuted despite their use of Bitcoin. And as we discuss below, there are in fact a number of tools and “chokepoints” that make identifying criminal Bitcoin users possible despite the advertised anonymity of Bitcoin.

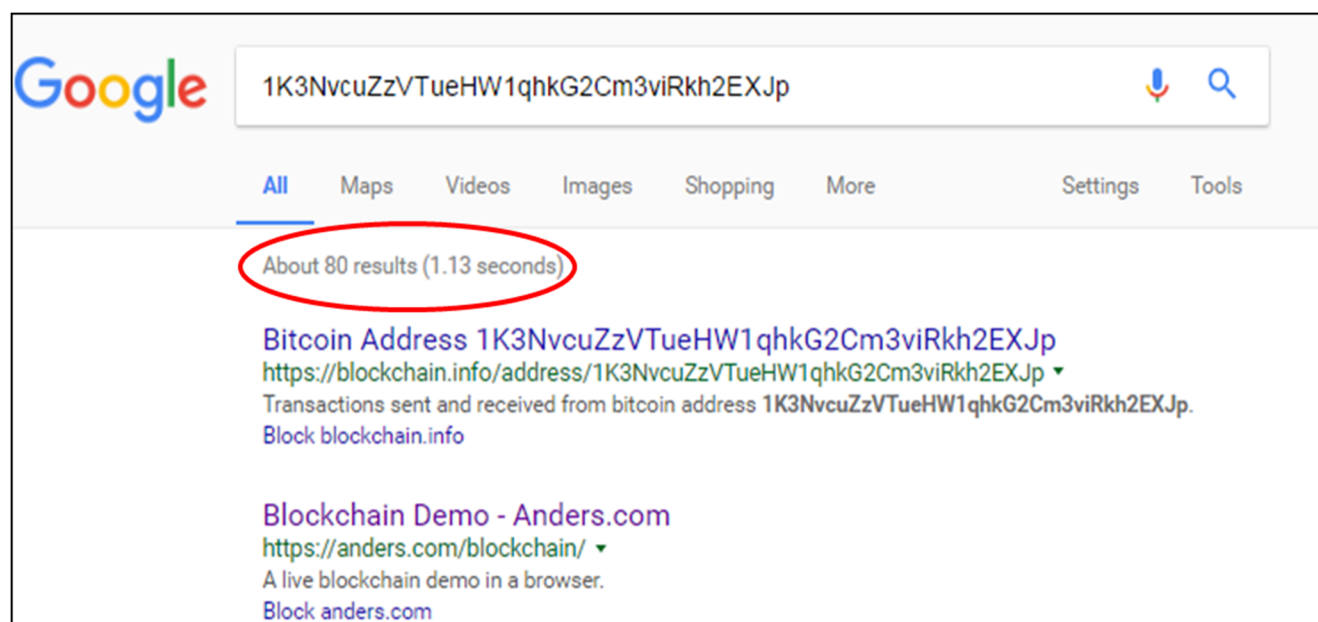
To assist investigators in exploring and exploiting data from the Bitcoin blockchain, a whole new ecosystem of tools and services has emerged in the past several years, and most dramatically reduce the amount of technical skill required to understand and make use of blockchain data. At least as



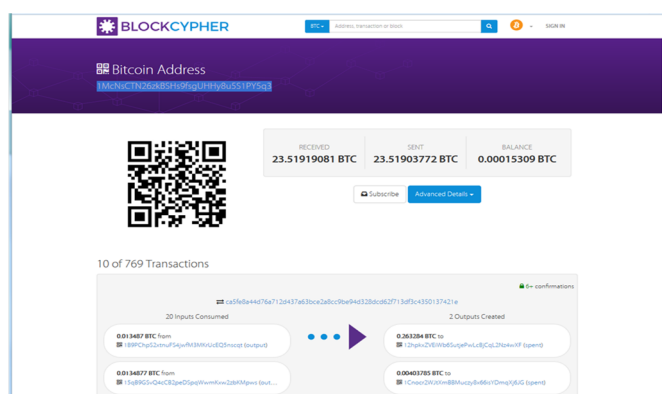
early as 2012, individual users were posting tools, scripts and homebrewed programs like “Blockviewer” which launched in August of that year<sup>4</sup>.

Today, an array of easy-to-use methods is available to investigators. The most straightforward is to simply plug the Bitcoin address of interest into a range of search engines. Many users who post or sell goods (illicit or otherwise) online will include their Bitcoin address in forum posting, advertisements or even just in their signature or profile in order to trumpet their standing among the digerati.

You may find live or archived pages that reveal identity information, email addresses, past activities or social connections simply by putting the address into Google, Yahoo, Yandex and the like. For example, Anders Brownworth, a technology professional who also blogs about (among other things) Bitcoin and blockchains, uses the Bitcoin address 1K3NvcuZzVTueHW1qhkG2Cm3viRkh2EXJp. A simple Google search on this address produces 80 distinct matches on the easily-searchable “surface Web”.



To delve more specifically into transaction history, a second option includes various free “Blockchain explorer” tools for the Bitcoin database, such as Blocktrail or the explorer on blockchain.info. Blockcypher.com (shown here) offers a similar tool that works for Bitcoin and also for Litecoin and Dogecoin,



<sup>4</sup> <http://www.bitcointrading.com/forum/bitcoin-specific/blockviewer-com-visualize-the-bitcoin-block-chain/>

and etherscan.io and etherchain.org offer similar tools for the Ethereum blockchain.

Obviously, transaction histories may be helpful, but in investigative processes, the ability to link blockchain data to a real person or enterprise would obviously be a powerful shortcut. According to research from Europol's Cyber Crime Center<sup>5</sup>, "Walletexplorer remains the best publicly available free resource that links several million Bitcoin addresses to wallets managed by hundreds of large entities, such as exchanges, mixers, Dark Web sites or gambling Web sites." Walletexplorer (shown below) also offers a convenient CSV file export for easy ingestion of the data into other tools.

**Wallet** [000001e522] [\(show wallet addresses\)](#)

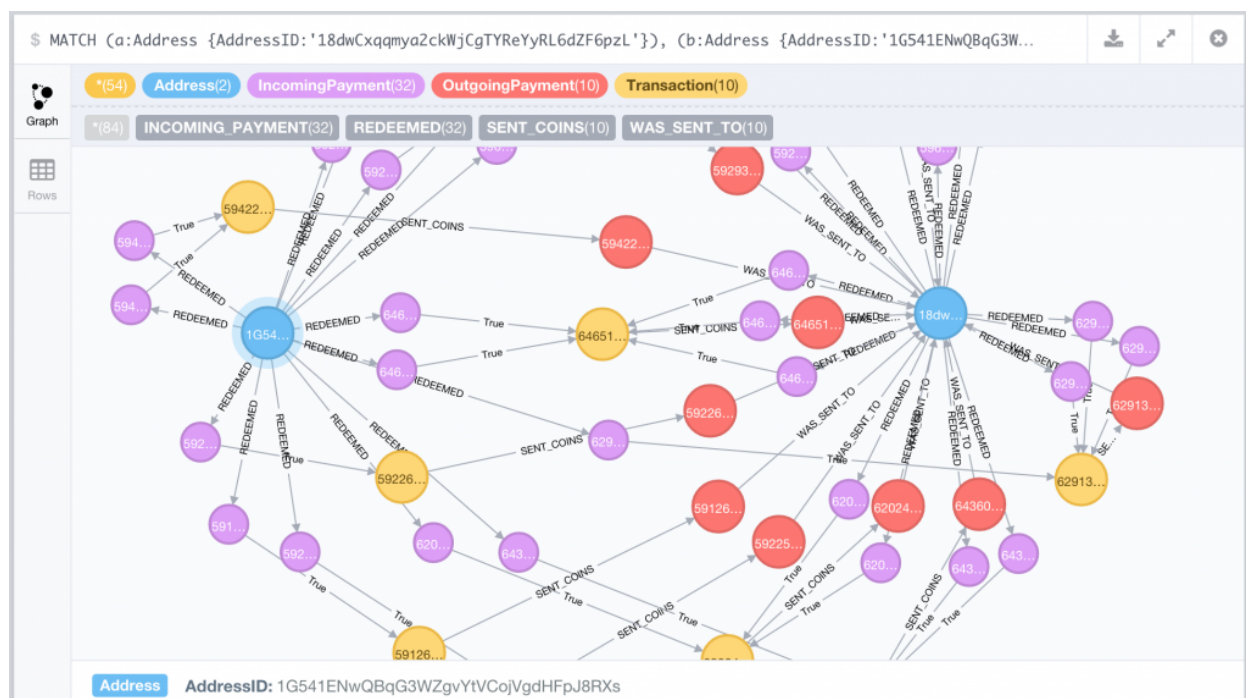
Displaying wallet [000001e522], of which part is address 1MhuCTH26xk85ru9fugU0ny8u51PY5q3. [Show only address 375](#)

Page 1 / 95684 [Next](#) [Last](#) (total transactions: 9,568,323) [Download as CSV](#)

date		received/sent	balance	transaction
2017-02-21 01:12:27	<span style="background-color: #ff00ff; padding: 2px;">[a73276ba7e]</span>	+0.01162277	5440.9173525	<a href="#">8ef8d4f4f4f77a0b0b...</a>
2017-02-21 01:12:27	<span style="background-color: #ff00ff; padding: 2px;">[6d6f2455da]</span>	+0.026	5440.90572973	<a href="#">15de3c0c10e7f7f7f7...</a>
2017-02-21 01:12:27	<span style="background-color: #ff00ff; padding: 2px;">[ecae04879f1]</span>	+0.00890245	5440.87972973	<a href="#">808a0fae0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.00237588	5440.87082728	<a href="#">810d0f0c0c0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.02728414	5440.8684514	<a href="#">7a0f0a0f0a0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0039932c85]</span>	+0.00570004	5440.84116726	<a href="#">1500b0b0f0f0f0f0...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.00098121	5440.83546722	<a href="#">0f0f0a0f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.00597746	5440.83448601	<a href="#">0f0f0d0f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.0012264	5440.82850855	<a href="#">0f0f0c0f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.01707785	5440.82728215	<a href="#">0f0f0b0f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #ff00ff; padding: 2px;">[0607056b3e]</span>	+0.00181658	5440.8102043	<a href="#">0f0f0a0f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.00253618	5440.80838772	<a href="#">0f0f090f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.00020947	5440.80585154	<a href="#">0f0f080f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #ff00ff; padding: 2px;">[73c2ed0e709]</span>	+0.00406864	5440.80546187	<a href="#">0f0f070f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[5ab0bae40e1]</span>	+0.00490771	5440.80157323	<a href="#">0f0f060f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[6666122611]</span>	+0.05218754	5440.79466552	<a href="#">1570f0f0f0f0f0f0...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.12707883	5440.74247798	<a href="#">0f0f050f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[20407996d7]</span>	+0.00417041	5440.61539915	<a href="#">1570f0f0f0f0f0f0...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.02797193	5440.60922874	<a href="#">0f0f040f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[0000152fc2]</span>	+0.00791335	5440.58125481	<a href="#">0f0f030f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #ff00ff; padding: 2px;">[756e91b7ae]</span>	+0.05543888	5440.57334346	<a href="#">0f0f020f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #0000ff; padding: 2px;">[b04d97678e]</span>	+0.004256	5440.51770458	<a href="#">0f0f010f0f0f0f0f...</a>
2017-02-21 01:12:27	<span style="background-color: #ff00ff; padding: 2px;">[84d0c0e8289]</span>	+0.1882791	5440.51144858	<a href="#">0f0f000f0f0f0f0f...</a>

To go a step further, a variety of commercial software applications add powerful features, better visualization and other benefits, and may be worth exploring if budgets permit. Some of the options included Elliptic, Chainalysis, BitAnalysis, Neo4J (shown below) and QLUe from the Blockchain Intelligence Group.

<sup>5</sup> Europol EC3 "Cyber Bits" Intelligence Notification 21/2016 (Unclassified), July 2016



The availability of these tools is only half the solution, of course. The knowledge to understand and use them effectively is also a critical component, and a gap that is being filled slower than the software options, which scale much faster than skills and training. This is actually the much bigger problem, says Colm Gannon, a Senior Inspector with the New Zealand Department of Internal Affairs who specializes in Digital Child Exploitation and works closely with ICMEC's Asia Pacific FCACP. "The data is all available, it's public," says Gannon, "but there's not enough knowledge or skills in the government sector."

This sentiment was echoed by Shone Anstey, President and co-founder of the Blockchain Intelligence Group, maker of the QLUe analysis software. "We work quite regularly with the IWF [Internet Watch Foundation] in the UK. They'll send us information or ask what we know about an address or a wallet or bitcoin." Like many commercial firms, his company readily volunteers data, time or assistance and knowledge to aid in child exploitation cases, and they are often called upon by the IWF or other groups including law enforcement in Canada (where the firm is based) because many investigators simply don't have the knowledge to effectively exploit blockchain data in their investigations.

An added challenge is that sophisticated criminals have a number of methods available to make this process more difficult. One of the most common is the employment of "mixers" or "tumblers" who will take in bitcoins from a range of users and privately mix and split and redistribute them back out, making it more difficult to trace them from one user or transaction to another. However, as pointed

out by Europol<sup>6</sup>, there are still several risks to even a criminal employing a mixer. First, should the mixer be compromised “and the record of the mixing process revealed, a user’s bitcoins would once again be traceable. One way to reduce this risk is to use multiple mixers.” In this case, as long as any one mixer in the chain remains secure, the linkage between coins and users will remain obfuscated. However, it conversely increases the risk for the criminal. Each time you use a mixer, you gamble that your mixer will not simply “make off with your bitcoins”, as one recently did to the tune of several million dollars, according to the Blockchain Group’s Anstey. This makes the risks and benefits of mixing your ill-gotten gains a bit more of a balancing act.

That said, in the criminal world as in any other population, the most sophisticated actors are a minority, or, as Officer Nick Selby, a cybercrime expert with the Midlothian, Texas police department put it, “most of these guys aren’t ninjas.” The fact that such complex obfuscation measures are available to criminals should not prevent investigators from exploring every available tool and option. For these reasons, the odds are that in more cases than not, investigators will find some value in the explicitly-transparent history available from the blockchain.

Finally, **there is an important “chokepoint” in the entire process which every investigator or law enforcement officer should keep in mind**, especially in longer-term activities where patience is possible. Recall our earlier discussion of how a user comes into possession of bitcoins:

1. They buy them on an exchange or via Bitcoin ATM;
2. They receive bitcoins as payment for goods or services; or
3. Bitcoin mining

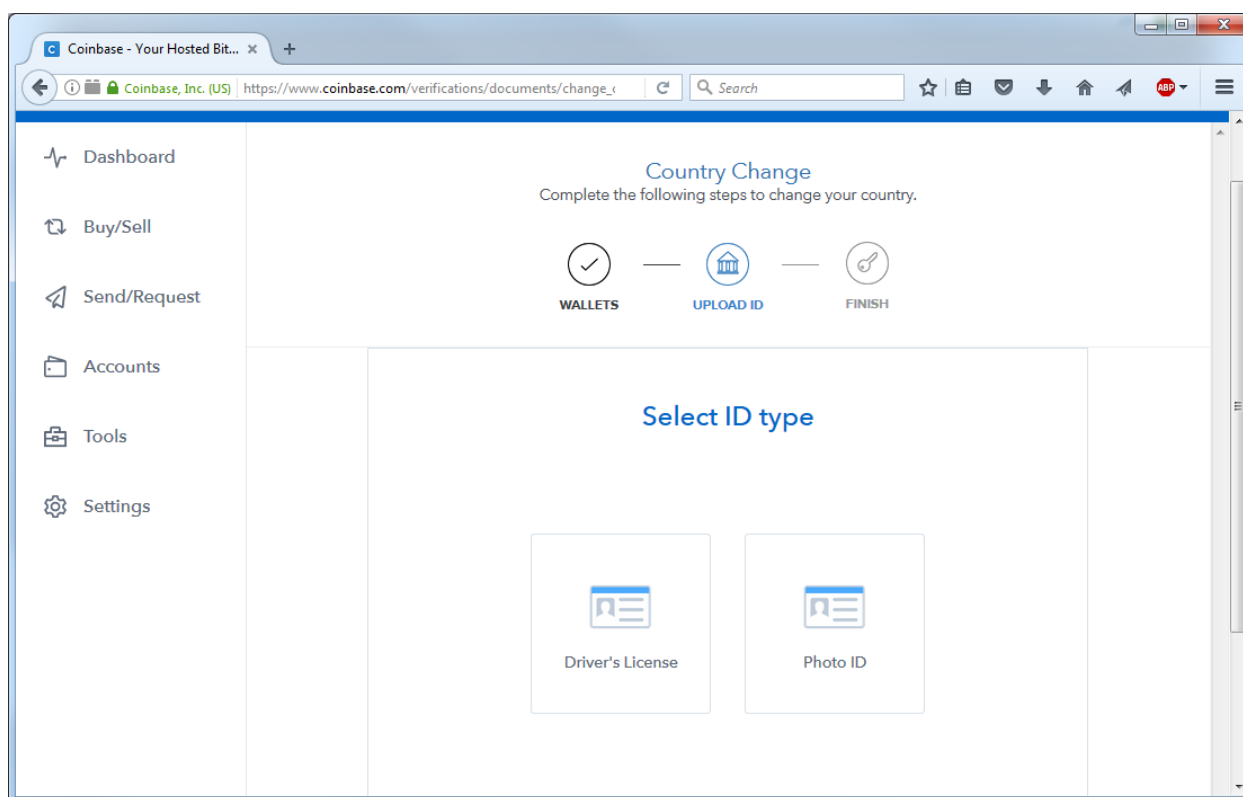
While a criminal or Person-of-Interest (POI) could conceivably acquire and use bitcoins solely to transact with other bitcoin users *inside* the Bitcoin universe, many will, sooner or later, cross the boundary between Bitcoin and the traditional financial system or between Bitcoin and the “real world.”

If a POI is associated with, or can through the methods mentioned above be tied to, a specific wallet, then if that wallet ever transacts with an exchange or makes a purchase from a legitimate “real world” merchant like Dell or Expedia, that touchpoint between Bitcoin and the real world is a weak point for the criminal. Sooner or later, some POIs will try to turn their ill-gotten bitcoins into “real” money on one of the major exchanges (many of which are based in the US or Europe and subject to significant regulation), or into goods and services from a legitimate business.

---

<sup>6</sup> Europol EC3 “Cyber Bits” Intelligence Notification 18/2016 (Unclassified), July 2016

When they do, you have an above-board commercial concern that keeps records, ships goods to real names and addresses, or connects to the traditional banking system. These parties, unlike the Bitcoin universe, *are* subject to Anti Money Laundering (AML), Know-Your-Customer (KYC) and other standard regulations and requirements that can link the transaction to a party in the real world. For example, to purchase *just \$100 worth* of Bitcoin or Ethereum, Coinbase, one of the largest Bitcoin exchanges in the world, requires personally identifiable details including date of birth, a photo of your driver's license or other government issued identification, *and* a real time Web cam photo of your face that it compares to the photo on your ID.



There is still a very finite universe of things a bitcoin holder can buy or obtain with bitcoins, which is the most widely accepted cryptocurrency in the world. Other "alt-coins" are even more limited in what they can do or buy. So whether it is a purchase on a legitimate site, currency trade on an exchange or even the camera on a Bitcoin ATM machine, the inherent limits on a bitcoin's utility beyond the Bitcoin universe mean that, more often than not, a user will eventually try to exchange their bitcoin for something tangible or fungible, and that is where their identity is most likely to be revealed.

Inspector Gannon from New Zealand put it bluntly: "They have to be on guard all the time. If they make *one* mistake, we've got them. Because once we can tie one transaction to that individual," everything they've ever done on the blockchain becomes immediately, and indisputably, tied to them. And, to quote Gannon again, "no one is infallible in the long run. Just ask Ross Ulbricht," the now-

imprisoned founder of the notorious Silk Road Dark Web marketplace, whose minor carelessness in leaving traces of his real identity in emails and web sites led to his capture.

In addition to the expanding range of software tools, there are other potential opportunities and access points that can potentially make Bitcoin users far less anonymous than they think they are (assuming proper use under appropriate authorities, of course).

For example, several hackers and academics have posted papers or proof-of-concept data theorizing, or in some cases proving, that Bitcoin users can in fact be identified through the correlation of meta data. For example, three researchers at the University of Luxembourg published a 2014 paper<sup>7</sup> that demonstrably showed methods to gather IP address information as a user, or technically a wallet, initiates a Bitcoin transaction.

**Deanonymisation of clients in Bitcoin P2P network**

Alex Biryukov  
University of Luxembourg  
alex.biryukov@uni.lu

Dmitry Khovratovich  
University of Luxembourg  
dmitry.khovratovich@uni.lu

Ivan Pustogarov  
University of Luxembourg  
ivan.pustogarov@uni.lu

**Abstract**

Bitcoin is a digital currency which relies on a distributed set of miners to mint coins and on a peer-to-peer network to broadcast transactions. The identities of Bitcoin users are hidden behind pseudonyms (public keys) which are recommended to be changed frequently in order to increase transaction unlinkability.

We present an efficient method to deanonymize Bitcoin users, which allows to link user pseudonyms to the IP addresses where the transactions are generated. Our techniques work for the most common and the most challenging

about 100,000 nowadays. The vast majority of these peers (we call them *clients*), about 90%, are located behind NAT and do not allow any incoming connections, whereas they choose 8 outgoing connections to *servers* (Bitcoin peers with public IP).

In a Bitcoin transaction, the address of money sender(s) or receiver(s) is a hash of his public key. We call such address a *pseudonym* to avoid confusion with the IP address of the host where transactions are generated, and the latter will be called just *address* throughout the text. In the current Bitcoin protocol the entire transaction history

15 Jul 2014

By correlating the data over time to localize the user's location, this method can, in theory, localize the machine not just of an individual user, but of a significant portion of the entire user network. Most interestingly, according to one of the study's authors, the whole thing can be accomplished with a couple of laptops and a 2,000 EURO budget<sup>8</sup>.

Finally, there are other points in the data transmission chain from user to Bitcoin network to recipient that may allow law enforcement or other authorities to capture data leading to the identification of real world actors. Here are just a few:

<sup>7</sup> Deanonymisation of clients in Bitcoin P2P network, Biryukov, Khovratovich and Pustogarov, University of Luxembourg, 2014 (<https://arxiv.org/pdf/1405.7418.pdf>)

<sup>8</sup> Ivan Pustogarov, <http://www.coindesk.com/eavesdropping-attack-can-unmask-60-bitcoin-clients/>



1. **Traditional merchants:** Obviously, if a wallet associated with past criminal activity, such as the purchase or sale of drugs, guns or other contraband on a Dark Web market, were to then transact with a legitimate merchant such as Dell or Expedia, their purchase, identity and address information would all be available to subpoena. The IP address they used would also be logged and, while it *might* be anonymized by use of a proxy or Tor browser, in many cases it will not, and can provide clues to the user's location and identity.
2. **Exchanges:** As noted above, most legitimate exchanges (at least in the Western democracies) are actually subject to significant KYC and AML controls and have detailed information on their users. Identity data, IP addresses and exchange histories can all provide avenues to locate and identify the user. This is not just a theoretical access point for useful data. In the "Fistful of Bitcoins" study discussed earlier, Meiklejohn et al. traced the funds in a number of bitcoin-thefts and criminal acts and found that, "for the thieves that did not [use sophisticated mixing and evasion techniques] there seemed to be ample opportunity to track the stolen money directly to an exchange."

As seen in the hack that destroyed Mt. Gox, a former Bitcoin exchange, these sites are also (literally) rich targets for hackers, who may release the user information once it has been exfiltrated. It is then not only available in raw form, but typically many large and interesting breaches are then "pre-digested" by the security community, with detailed results and analysis often posted freely online, as in the *Willy Report* analysis of the Mt. Gox data<sup>9</sup>.

3. **ISPs:** Before a user transacts with the Bitcoin network, they must first connect to it, and that requires an Internet connection. As the specialists at 99bitcoins.com explained it succinctly:

*Bitcoin does not have any built-in encryption when it comes to broadcasting transactions across its P2P network. When your client relays transactions over the network, they pass through your ISP's gateway servers in plain text. Your ISP can intercept and analyze this traffic, and then determine which of these transactions belong to your IP address (versus those transactions which you are only relaying). The transactions that belong to you will first appear on the network via your IP address, differentiating them from transactions that have already been propagated by other nodes. And then your IP address can be used by your ISP to lookup your personal identity — they have it on file from when you subscribed to their service.*

---

<sup>9</sup> <https://willyreport.wordpress.com/2014/05/25/the-willy-report-proof-of-massive-fraudulent-trading-activity-at-mt-gox-and-how-it-has-affected-the-price-of-bitcoin/>

This technical detail may have important implications for, as Meiklejohn et al. phrased it, “an agency with subpoena power” to gain access to data that significantly increases the likelihood of identifying individual users in the course of an investigation.

In summary, then, while the Bitcoin network offers the average user convenient and relatively easy anonymity, or rather pseudonymity, the combination of public ledger data in the blockchain, an expanding universe of tools and vendors, and the application of focused technical capabilities can, at least in some and specific cases, pierce this perceived shield. If the user of interest is even the slightest bit careless in their interactions between the Bitcoin network and the “real world,” many of these complex and technical measures may even become unnecessary.

## Use in Commercial Child Sexual Exploitation<sup>10</sup>

Taken in total, the various technical and investigative (though not-always-insurmountable) challenges of cryptocurrencies covered so far indicate an obvious, and unfortunate, potential boon to those engaged in the production, sale or consumption of commercial Child Abuse Material (CAM) or those engaged in paid, in-person sexual engagements with minors. Put simply, the difficulty (relative to more regulated payment systems) of investigating Bitcoin users would seem to offer an obvious appeal to both sellers and buyers of commercial child sexual exploitation. While this is certainly true to some degree, the reality *so far* is that the evidence available (though admittedly anecdotal) indicates that it is true to a surprisingly limited extent. First, let us examine the specific ways in which cryptocurrency *is* being used, and then why the evidence appears so limited.

At a macro level, various investigators and researchers have identified several specific ways in which Bitcoin (and to a lesser degree other digital and cryptocurrencies) is being used. Inspector Gannon from New Zealand specifically identified several that his team has observed.

### Content Production and Distribution

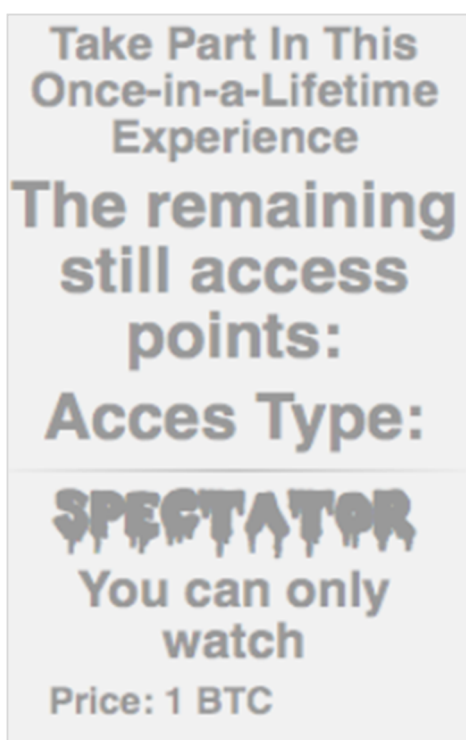
First, there are various surface- and Dark-Web sites that offer static content such as large photo sets and video libraries for purchase or access. Gannon notes, however, that these are relatively few, for

---

<sup>10</sup> The term “child pornography” is used for the purposes of this report as it is the expression most readily recognized by the public at large, at this point in time, to describe this form of child sexual exploitation. In addition, “child pornography” is the term most frequently used in legislation around the world addressing the issue. It should not be taken to imply that children “consented” to any sexual acts depicted in any images. The term “child abuse material” is increasingly being used to replace the term “child pornography” as it more clearly highlights the exploitation that occurs. The two terms are used interchangeably in this report. See also, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Jan. 28, 2016, Terminology and Semantics Interagency Working Group on Sexual Exploitation of Children, ECPAT International, at <http://luxembourguidelines.org/> (last visited Jan. 27, 2017) (on file with the International Centre for Missing & Exploited Children).

simple economic reasons – supply and demand. “It’s kind of like adult pornography,” says Gannon, “there are always a few people willing to pay for something that’s completely new, but there’s so much of it already out there that most people just don’t need to pay for it.”

The most common type of commercial, i.e. paid, digital exploitation Gannon’s team investigates, by far the majority of cases, is for live streaming “events.” These involve live sessions that abusers schedule and market ahead of time, and customers pre-pay for a link or access code that allows them to watch the abuse happening live. Even more disturbing are events where the role of “director” is auctioned off or charged at a significant premium, giving one user the right to “control the action” as Gannon puts it. The LookingGlass research team was able (with depressing ease) to find examples of just such a scenario on a Dark Web site called Red Room, which showed bitcoins as the accepted payment method. Note in the screenshots below the 10x difference between the spectator and “commander” roles. When this screenshot was taken in March 2017, a single bitcoin was trading at approximately \$1,000 US dollars.



## Trafficking and In-Person “Services”

Even more horrifying, New Zealand’s Gannon identified one case in which bitcoins were required as the payment method for what amounted to nothing less than a modern slave auction, in which

children were quite literally bought and paid for, with bitcoin used for both the “purchase” and transportation fees.

The other obvious potential use for cryptocurrencies is the payment for individual encounters. However, Gannon says that, in his department of 16 investigators, he has, “never seen that”. This sentiment was echoed by several others we spoke to in U.S. law enforcement. “It makes for good TV,” says Texas police detective Selby, “but I’ve never actually seen it”.

Given the lack of available data, the impact of Bitcoin and similar currencies on in-person services involving exploitation of children is at this time more difficult to gauge. Certainly, there is evidence that those in the sex trade are gradually adopting Bitcoin as a payment option. (In fact, some adult sex workers in the US who voluntarily work in the trade praise the alternative to cash and credit cards as better for their physical safety [no cash to rob] and their freedom from prosecution, as bitcoin creates a much harder trail to follow than Visa or Mastercard).<sup>11</sup>

However, it is also true that Backpage, the notorious Web site familiar to most FCACP members that was repeatedly investigated for facilitating sex trafficking of minors, moved to taking bitcoin exclusively for its paid ads. The result, according to the owner of one Bitcoin exchange was a measurable uptick in business<sup>12</sup>. In other words, the efforts of, among others, the FCACP members to shut down “traditional” methods of payment, appear to have actively precipitated increased adoption of cryptocurrency as an alternative<sup>13</sup>.

## Use Remains Limited

Other data mirrors these observations regarding the gradual adoption of bitcoin for payment in the child sexual exploitation area. For instance, the Internet Watch Foundation’s 2016 Annual Report itemized an increase of roughly 10x in child exploitation sites the organization identified as accepting Bitcoin in 2016 vs. 2015, but that increase was from 4 to 42. This is relative to the 2,416 domain and 50,000+ URLs found on the “surface” web in the same year<sup>14</sup>. Gannon echoes this trend in the cases investigated by his team. “It took a dive from 2015 to 2016, though it’s come back a bit, I think because of the value,” he says, referring to the meteoric rise in the value of one bitcoin in the interim, from around \$200 US to more than \$1,000. Still, Gannon pointed out in mid-March 2017 that the last time his team had done an investigation involving bitcoin was “back in February” meaning more than a month prior. This in an office that handles approximately 2,500 cases or leads per month.

---

<sup>11</sup> For Sex Industry, Bitcoin Steps In Where Credit Cards Fear To Tread – NPR, Dec. 15. 2015

<sup>12</sup> Ibid.

<sup>13</sup> Note that this linkage is based on the anecdotal comments cited, essentially treating Backpage as a proxy for broader trafficking activity. While this may not be scientifically rigorous, it is however directionally interesting data.

<sup>14</sup> IWF 2016 Annual Report: [https://annualreport.iwf.org.uk/assets/pdf/iwf\\_report\\_2016.pdf](https://annualreport.iwf.org.uk/assets/pdf/iwf_report_2016.pdf)

This highlights the second point touched on earlier. If cryptocurrencies offer such obvious challenges to investigation, and we are seeing them there in some limited frequency, why is the use of them not far *more* widespread in commercial sexual child exploitation? The answer seems to be three-fold.

The first deterrent seems to be the manifestation of Allen's somewhat prophetic observation during his 2013 testimony. The FBI's successful "bust" of the Silk Road market and various other media articles, studies (including those cited herein) and arrests have made criminals less confident that bitcoin, "is really that secure" says Inspector Gannon. The more such weaknesses and prosecutions are reported, the more criminals have to rethink their payment options.

Of course, wherever there is a need, the market seeks to fill the vacuum. Monero, Darkcoin and other newer alternatives are explicitly seeking to develop architectures that render cryptocurrency as close as possible to totally anonymous, completely obfuscated and utterly untraceable. While adoption of these alternatives remains quite limited at this time, it is possible that one of these ultra-secure newer "coins" will gain traction in the commercial child sexual exploitation marketplace. The user pools and access/exchange points for these relatively tiny "alt coins" do, however, dramatically reduce the available buyer pool, which is a distinct positive.

The second challenge for criminals is that Child Abusive Material (CAM) and child exploitation is considered so far out of any bounds of human decency or acceptability, that even among Internet "freedom fighters," privacy advocates and yes, criminals themselves, it is seen as a worthy cause to combat. From the Bitcoin Foundation that helps shepherd development of the network to the administrators of Alphabay, Silk Road 3.0 and other Dark Web markets (who have *no* problem with sales of guns, fake passports or methamphetamine), even the staunchest defenders of most types of criminal trade have actually banded together to scrub their sites and rid their communities of CAM and those who peddle it. This has helped to further reduce the use of bitcoins as a payment method for commercial exploitation, as well as reduce its presence somewhat, even on the Dark Web<sup>15</sup>.

The third and most important challenge is again economics. "The problem is liquidity," says Gannon. "If you're living in poverty in a rural area in the Philippines, which is where we see a lot of this coming from right now, and doing a live stream, getting paid in bitcoins doesn't really help you. If you can't take it down to the store and buy food with it, it's not really useful currency. We do see bitcoin, we see some ukash, but right now it's still a lot of the traditional methods. Western Union, Moneygram, that sort of thing."

Detective Selby echoes this. Despite its relatively large user base, the utility of bitcoin payments is limited if you can't convert them back into cash. "Everyone knows the exchanges are where we'll get ya," he says, so without a way to make bitcoins into something more useful, even the world's most

---

<sup>15</sup> IWF's 2016 annual report actually noted a decline of almost 50% in Dark Web-hosted sites in that year.

widely accepted crypto-coin has a serious liquidity problem for many of those conducting commercial child sexual exploitation.

## What Can Industry Do?

As detailed in the excellent, in-depth study, “Combating Illicit Trade of Child Abusive Material on the Internet,” authored by Johan Wadenholt in cooperation with the Swedish Financial Coalition, there are three common angles of attack to combat commercial CAM online:

1. Limit Access to CAM
2. Limit the Ability to Pay for CAM
3. Find the perpetrator

Option #1 is often the easiest to accomplish quickly. Major technology firms from Google and Microsoft to large ISPs use common tools including image hashes, URL blacklists and data from organizations like IWF and the National Center for Missing & Exploited Children (NCMEC) to attempt to limit, filter or remove CAM materials. Sadly, numerous studies have documented that, despite application of all three methods outlined above, there is still enormous demand for, and availability of, CAM online, especially on the Dark Web<sup>16</sup>. This is because on the Dark Web, option #1, limiting access (e.g. via voluntary search result filtering by Google, Microsoft or blocking by ISPs) is not applicable. So while the number of sites that have CAM content available has, per some reports, declined, the interest and traffic to those sites remains enormous.

Option #2, a central focus of the FCACP, has proven quite effective in traditional payment systems, and the voluntary cooperation of the Bitcoin Foundation and community have great potential to continue to limit the use of cryptocurrencies to pay for CAM and live exploitation. The evolution of niche cryptocurrencies that are even more complex and anonymous than Bitcoin may make truly anonymous and untraceable payments more achievable, at least among the most sophisticated and technical users. However, as noted previously, the miniscule level of adoption of these alt-coins helps to starve CAM producers of customers, potentially driving them back to Bitcoin or more traditional payment methods and networks.

---

<sup>16</sup> For example, according to a six-month study conducted in 2014 by Dr. Gareth Own at the University of Portsmouth running dozens of Tor nodes to examine traffic patterns, CAM sites made up approximately 2% of the sites cataloged during the study on the Tor network. However, those sites received roughly 80% of the traffic volume. As reported in “Combating Illicit Trade of Child Abusive Material on the Internet,” authored by Johan Wadenholt in cooperation with the Swedish Financial Coalition.



This leads to discussion of option #3. Certainly, identification of the perpetrator is not a new discipline, so the question at hand is how it changes in the specific cases involving cryptocurrencies. Fortunately, at least for the time being, Bitcoin remains the overwhelming favorite cryptocurrency, as well as the most widely known and accepted. As detailed extensively in the Investigation section, at least in those cases involving Bitcoin, Litecoin, Ethereum or other options that use a Bitcoin-like public blockchain, there are some effective tools and avenues for the investigation, discovery and prosecution of both CAM and in-person exploitation cases.

It is also important to note that not all data-gathering efforts need necessarily wait for a case to be reported. For example, many industry players (including LookingGlass) proactively harvest data on web sites, wallets, addresses, and Dark Web hosts. Dark Web sites can actually be checked for what services they are running and whether either the server or the content indicates a specific Bitcoin address. For example, as shown in the screenshot here, each Dark Web site can be summarized in a “report card” detailing what services were found running on the host, including any Bitcoin wallet or addresses found.

**Darknet - Onion Scan Details**

[View results as JSON](#)

Key	Value
bitcoinAddresses	5dadbb8a46ecb7f508338d520521f847eec7b01b
bitcoinDetected	-
certificates	-
exifImages	-
foundApacheModStatus	-
ftpBanner	-
ftpDetected	-
ftpFingerprint	-
hashes	
hiddenService	4a6kztzytb4ksafk.onion
interestingFiles	-
internalPages	-
ipAddresses	-
ircDetected	-
lastAction	none
linkedSites	blockchain.info bto-x100.com
mongodbDetected	-
openDirectories	-
pageReferencedDirectories	img
pageTitle	Bitcoins Multiplier

This means that any address(es) associated with any site offering CAM can be queried in the blockchain and every transaction to or from that address can be identified. Just this one data set can potentially provide a wealth of intelligence for identification of the perpetrator, including but not limited to:

1. The longevity of the site/purveyor (based on timestamps on transactions)
2. Transaction/customer purchase volumes (from Bitcoin transaction data)
3. Financial scale of the business (by multiplying the bitcoins received by the historical price of bitcoins at the moment of transaction)
4. The *approximate* number of purchasers/customers (though single customers can theoretically employ more than one wallet and a small percentage of cautious users will likely do so).

Also, thanks to the nature of the blockchain, every transaction involving the wallet(s) linked to this site has a timestamp down to the second. This may be extremely useful in corroborating other activities logged or discovered during an investigation, e.g. when a PC has been seized during an arrest.

Finally, visualization of linkages and timelines for all transactions of not only the seller, but of every buyer, can potentially lead to the identification of one or more of the purchasers. As discussed in the Investigation section, not all users are equally savvy or infallible. If address ABC123 is among the purchasers of CAM on a criminal site, and ABC123 has *ever* used a legitimate coin exchange or purchased something with a mainstream merchant using Bitcoin, that “crossover” point between the Bitcoin network and the “real world” provides an excellent opportunity to identify the user, either for individual investigation and prosecution or as a potential asset to be used in an attempt to discover the identity of the purveyor.

## Conclusions

This paper has attempted to accomplish three distinct tasks:

1. Provide FCACP members and other appropriate consumers a relatively non-technical primer on Bitcoin, blockchains and cryptocurrencies.
2. Identify the strengths, but also the weaknesses, of Bitcoin and its brethren as an anonymous way to pay for commercial child sexual exploitation, including CAM.
3. Summarize what is known (at least by its authors) about the actual use of cryptocurrencies in commercial child sexual exploitation at this time, and detail some of the investigative tools, options and methods available to both investigators and the payments industry to continue the battle to identify, impede and reduce commercial child sexual exploitation that leverages cryptocurrencies.

In summary, the blockchain is a remarkable, innovative and potentially transformative technology for the financial industry, and many others as well. However, its ostensible anonymity and untraceability, while somewhat true in theory and under perfect conditions, is actually quite fallible in the real world and in the hands of real users. The combined problems of:

- Complexity of use
- Few widely-accepted alternatives
- Aversion to child sexual exploitation even among the Dark Web’s (otherwise) worst criminals
- Illiquidity
- Publicized successes by law enforcement

mean that abusers using these new forms of currency, while posing some new challenges, are by no means impossible to identify or beyond successful prosecution. With industry, technical experts, and leading organizations like ICMEC, the FCACP, NCMEC and IWF working together to share knowledge, advance training and the wealth of new tools and techniques available, we can continue to bring the fight to abusers. Cryptocurrencies may make the job more difficult or require some new methods, but in the end, if we “follow the money,” there is still a path to finding, and punishing, the perpetrators.

## Disclaimer

This report ("Report") was created and written by volunteers on behalf of the Financial Coalition Against Child Pornography (FCACP) and represents the current views of the issues addressed as of the date of publication. The content of the Report is based on the individual input of the contributors, and does not necessarily reflect the opinions or policies of the companies at which the individuals work, the International Centre for Missing & Exploited Children (ICMEC), or of any of the FCACP member companies, other than LookingGlass Cyber Solutions, the creator of the Report.

The Report is for informational purposes only and does not render legal, financial, business or other professional services or advice. This Report may not be correct, complete, and/or up-to-date, so recipients should use this Report only as a starting point for their own independent research. If legal advice or other expert or professional assistance is required, the services of a competent professional should be sought. **THE FCACP AND ICMEC MAKE NO WARRANTIES, EXPRESSED, IMPLIED, OR STATUTORY, AS TO THE INFORMATION CONTAINED IN THIS REPORT.** The listing of an organization or entity herein does not imply any sort of endorsement by such organization or entity.

Complying with all applicable copyright laws is the responsibility of the recipient. The Report may be freely redistributed in its entirety at no charge provided that the Report is not modified in any way and any disclaimers, legal notices, including all copyright notices, are not removed. It may not be sold for profit or used in commercial documents without the written permission of the FCACP, which may be withheld in the FCACP's sole discretion.