BEFORE THE EUROPEAN UNION COMMISSIONER FOR JUSTICE, CONSUMERS, & GENDER EQUALITY

B E T W E E N:

CRYPTOCURRENCY VICTIMS

Claimants

-and-

BITCOIN VOLUNTARY ASSOCIATIONS, SOCIAL MEDIA, DOMAIN PRIVACY PROVIDERS, ET AL

Defendants

To: Commissioner Věra Jourová

From: Dr. Jonathan Levy, Solicitor and Attorney for Cryptocurrency Victims

In Re: Cryptocurrency Victim Claims - A Request for Consultation and Remediation

We represent consumers worldwide, including citizens of the European Union (EU) and European Economic Area (EA), who have been victimized by organized crime firms based or controlled from or doing business in the EU under the guise of "cryptocurrency." My clients have all been robbed and cheated by these criminals, sometimes repeatedly while the EU and its member nations stand aside or even aid and abet the criminals as in the case of the United Kingdom which provides a haven for crypto criminals by permitting unfettered use of the .io top level domain and Companies House. The claimants here are but a tiny representative sample of the tens of thousands who fall victim each year to cryptocurrency organized crime firms utilizing cryptocurrency to achieve their ends.

Cryptocurrency volume is estimated be over 80 billion Euros each and every day with a market capitalization of over 270 billion.[1] This volume figure is less than official EU estimates which pegged capitalization of just the top 100 Cryptocurrencies at well over 300 billion in 2018.[2] As cryptocurrencies are in fact both data and involve financial transactions, the majority of these transactions touch upon the European Union in some fashion and come under the EU regimes of data protection and anti-money laundering. The largest cryptocurrency Bitcoin which makes up more than 50% of volume is controlled from within the EU as are its derivatives.[3]

The World Bank has also defined cryptocurrencies as digital currencies that rely on cryptographic techniques to achieve consensus The EU has also estimated 7 billion Euros of cryptocurrency related fraud and criminal activity occurring annually.[4] This represents an unheard-of transfer of wealth to criminal organizations and constitutes a security threat. Only the transfer of looted funds by Nazi Germany 1933-1945 exceeds this figure on an annual basis. Yet despite being aware of the victimization, transfer of wealth to criminals, and daily transfers in the billions, to date the EU Commission has done nothing for consumers and very little regarding tax evasion and money laundering despite being aware of the magnitude of the crisis.

The criminals are not alone. They could not function without fintech and blockchain companies, exchanges, banks, and especially social media which have accelerated and made possible this illicit transfer of wealth. These silent partners in crime have also been enriched, sometimes egregiously so as in the case of social media by setting up the victims and selling their data to crypto criminals.

Much of this "success" is fueled by publicity and the unregulated access afforded the purveyors of cryptocurrency by social media platforms such as Facebook, Instagram, LinkedIn, YouTube, Twitter Snap Chat, WhatsApp and Telegram. Domain proxy registrants or privacy providers and cooperative domain registrars, resellers, and internet service providers allow and encourage anonymous individuals to conduct billions in transactions each and every day. Even corporate registries like England's Companies House are used extensively as props to establish legitimacy by criminals with no obvious fear of being prosecuted. Offshore corporate jurisdictions such as St. Vincent, the Seychelles, Belize, and Dominica are also popular dodges for crypto criminals eager to throw off any pursuit as to their actual whereabouts.

While it is possible to utilize cryptocurrency for every day transactions or for legitimate reasons of privacy; we know some, if not the vast majority, of those transactions involve unregulated speculation and capital raises, gambling, pump and dump schemes, Ponzi and pyramid funds, unmonitored movement of funds across national borders, unlawful asset protection, tax evasion, and transactions in contraband (narcotics, weapons, and

[1] See CoinMarketCap for daily figures https://coinmarketcap.com/all/views/all/

[2] Legal context and implications for financial crime, money laundering and tax evasion – Study, Directorate-General for Internal Policies of the Union (European Parliament), Published: 2018-09-06, https://publications.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1/language-en/format-PDF/source-76403102

[3] *Ibid.*

[4] *Ibid.*

pornography) and payment for criminal services. Ancillary to that €7 billion figure estimated by the EU are the uses of cryptocurrency as the motive, means, and method for the commission of what to date has been the almost perfect crime of looting the bank, investment, credit card and retirement accounts of unsuspecting, unduly trusting, and unwary citizens of the EU and EA who invest blindly in cryptocurrency related schemes.

To date there have been tens of thousands of victims and few if any means of justice. A single transaction may easily involve 4 or 5 national jurisdictions and the ultimate origins of the criminal and their identity may simply be unknown. National authorities, especially in Europe have been slow to meet the challenge leaving victims with no remedies.

The highly vaunted blockchain, supposedly transparent and inviolate, is a particularly cruel hoax. Cryptocurrency proceeds from unlawful transfers can easily and instantaneously be mixed or blended thus destroying the blockchain. The EU has pointed out that bitcoin mixing which is illegal money laundering *per se*, should be outlawed yet nothing has been done. Anecdotally, it is believed bitcoin mixing or blending originated in the EU. The largest bitcoin mixer, bitblender.io, is maintained on the TLDcc controlled by the UK Foreign and Commonwealth Office and continues operating with the full knowledge of the UK Foreign and Commonwealth Office (FCO).[5]

The General Data Protection Rules (GDPR) extend the EU's jurisdiction over data and information. Cryptocurrency and blockchain are information yet no national authority is equipped to deal with crypto crime. The GPDR on its own therefore is a useless remedy poorly suited to combat crypto crime but nonetheless vests the EU with jurisdiction over these transactions which utilize blockchain and social media.

Claimants[6]

At the heart of this situation are the victims. Let us put a human face on this tragedy as well as expose some of the criminals allegedly involved. Each claimant has retained (paid) this office as counsel and complied with AML (Anti Money Laundering) and KYC (Know Your Client) requirements on file with counsel. Each claim has been verified by counsel. These very sad claims unfortunately are typical of thousands of others, if not tens of thousands.

Jacopo G is a citizen of Italy who resides in Seattle, United States and works in the tech industry. He was approached via LinkedIn Messenger (social media) by a lone criminal using the name "Rolf Sanders" who gained his trust in January 2019. "Sanders" offered to trade FOREX (Foreign Exchange) for Jacopo on a Seychelles based platform, IQ Option, but required payment in Bitcoin. The criminal by utilizing false accounts (online account interfaces showing impressive but completely false trading gains) and WhatsApp messaging was able to eventually induce Jacopo to transfer $15,250 of Bitcoin and "deposit" it with the criminal who then absconded with the cryptocurrency. IQ Option disclaimed any knowledge of the

[5] Letter - Levy to British Indian Ocean Territory Administration, Principal Legal Advisor, May 21, 2018.

[6] Claimants last names have been partially redacted to protect their privacy as retaliation by organized crime groups is always a concern as is revictimization however all names, identification documents, details of transactions, receipts, transactions, emails and other documentary evidence are on file with lawyer including KYC and AML requirements.

account. The whereabout of "Sanders" and the Bitcoin transfers are untraceable according to Blockchain.info (Blockchain Luxembourg S.A.) which transferred the Bitcoin for Jacopo and has no recourse for fraudulent transfers. The combination of Bitcoin and social media applications created a perfect crime with no suspect or transaction to trace or recourse available. In addition, the criminal also obtained a copy of Jacopo's Washington state identification document. Jacopo's losses and consequential damages exceed €35,000.

David H is a citizen and resident of the United Kingdom and a small business owner. In 2017 David began investigating cryptocurrency investments. Eventually he invested up to £50,000 with a so-called cryptocurrency trading platform, Cryptexmarkets.com (Cryptexmarkets). Cryptexmarkets induced Hammond to invest by providing false accounts showing profits of £150,000. David also convinced friends and relatives to invest over £100,000. Cryptexmarkets purports to be operated by a Dominica shell company. However, the true ownership of the website is masked by a US corporation, Domains By Proxy, LLC. When Hammond sought to withdraw his funds in 2018, his account was closed, and his money stolen. David's damages direct and indirect exceed €150,000.

Drew J is a citizen and resident of the United Kingdom who suffers from a long-term mental health condition and when unwell, this affects his ability to function effectively. Drew obtained Bitcoins as early as 2009 when he was given some in exchange for work. In 2017 as the Bitcoin price exploded he became more interested in cryptocurrency but was quickly victimized in rapid succession first by EtherDelta (etherdelata.com), a so called decentralized Ethereum trading platform operated by US resident Zachary Coburn utilizing social media such as Reddit, YouTube, and Twitter to generate millions of transactions.[7] EtherDelta took 6 Ethereum tokens from Drew on deposit which then disappeared without recourse. After seeing ads on Facebook and Google for Etoro, Drew was then relieved of $18,000 by Etoro.com in a series of cryptocurrency trades. Etoro purports to be the world's leading social trading platform. Etoro operates from offices in London and Cyprus and claims to be regulated in Cyprus and the United Kingdom. In 2018, Drew was bombarded with online ads from Instagram and likely Google via Etoro promoting cryptocurrencies. Desperate to reclaim his losses, Drew became involved with a "cloud mining operation" based in Holland called FinTech Mining (fintech-mining.com), recruited Drew via high pressure sales tactics and relieved him of $6000 for a fraudulent cloud mining operation package which falsely promised high returns. In February 2019, Drew began receiving sales calls from a company called Cointeck.io. The .io domain is controlled by the United Kingdom Foreign and Commonwealth office which is aware that .io is haven for fraud and crime. The calls became increasingly high pressure and due to his rapidly declining mental health condition, Drew was groomed into "investing" all his assets, 130 Bitcoins, including £27,000 he borrowed. However, his funds were gone in short order due to false trades by Cointeck. Cointeck personnel mocked him and cruelly taunted him causing Drew to fall into a suicidal condition, that he has found next to impossible to recover from to this day. No funds were returned and Cointeck continues in

[7] US Securities & Exchange Commission, *SEC Charges EtherDelta Founder With Operating an Unregistered Exchange*, Nov. 8, 2018, https://www.sec.gov/news/press-release/2018-258

business with an address in Switzerland and is supposedly associated with CCLR Limited which is registered in Estonia. Drew's aggregate damages exceed €1.2 million or more than 130 Bitcoins.

Nadia D is a citizen of Slovakia. In January 2018 she was "friended" on Facebook by a tout posing as a cryptocurrency investor who put her in touch with "a good Christian lady" who had made him lots of profits. Nadia did not find this unusual as she was open about her interests in Christianity on her Facebook account. Nadia's new friend was eager to share her success as an investor broker in cryptocurrency and asked for a minimum $5000 investment with a promise of 50% monthly interest through a company called Zilton Capital (ziltoncapital.com). Zilton Capital deals in cryptocurrency and claims to have offices in New York and Singapore and is an affiliate of InterCapital SM Limited in Belize. In reality Zilton Capital are simply criminals using the cover of imaginary companies and a website to lure deposits from the unwary. Zilton Capital also used a forged or fanciful certificate allegedly issued by the United States Securities and Exchange Commission to establish credibility. The true ownership of the website is cloaked by a company called Privacy Protect, LLC of Burlington, Massachusetts, United States. By use of a false accounting showing profits, Zilton Capital defrauded approximately €60,000 from Nadia. Zilton Capital also stole funds from Nadia's brother and friends. When her account showed €300,000, she tried to withdraw funds. Zilton capital attempted to extort an $80,000 advance from Nadia. When she refused to pay, her funds on deposit were blocked. She reported Zilton Capital to authorities in the United States and United Kingdom but neither jurisdiction opened a case. Nadia's losses and damages exceed €100,000.

Steve S. is a citizen and resident of Australia and is a small business owner. In 2018 he became interested in cryptocurrency and began investigating it on his computer using Facebook among other sources where many cryptocurrency related sites existed. Facebook harvested this information and pushed an ad to him disguised as an endorsement by two local businessmen of a criminal organization called Cryptoallday (cryptoallday.com). Steve clicked on the ad and watched the video it contained, he then entered his email and phone number. Within 10 minutes a screener called him back and a few minutes later a high-pressure salesman began his pitch. The criminal made many false promises about profits, trading and safety of the account. He induced Steve to invest $4000 of Lite coins, a Bitcoin derived cryptocurrency and using a false accounting showed an immediate profit. When Steve tried to make a withdrawal, he was subjected to high pressure sales tactics. He invested 5 Bitcoins then worth about $75,000. Eventually he invested a goodly portion of his savings and retirement totaling 55 Bitcoins or approximately €600,000. Steve also induced his sister and good friend to invest with Cryptoallday. When it seemed Steve would invest no further funds, Cryptoallday concocted a story that Steve was hacker and closed his account the showing €600,000 without recourse. As a result, Steve not only suffered financial loss but became paranoid, depressed, and anxious. Cryptoallday continues its criminal operations using a Seychelles front company Petrasoul Ltd and claims to have offices in the European Union. Cryptoallday.com masks it domain ownership by using a privacy firm called PrivacyGuardian.org in the United States. In 2018, Steve lost an additional 16 Bitcoins or $200,000 to another company, USI Tech (United Software Intelligence Technology which) is a

company that claimed to develop the world's first automated trading platform for Bitcoin (BTC). The company claimed to be based in the United Arab Emirates but likely was operated from within the European Union. The website usitech-intl.io is no longer in operation and was registered in the .io domain under the control of the United Kingdom Foreign and Commonwealth Office. Twitter, Facebook, YouTube and WhatsApp were all used by the criminals in carrying out these schemes. Steve seeks recompense of €1.2 million.

Jacqueline S. is the sister of Steve S. above and resides in Australia and works as a heavy machine operator. She was introduced to the Cryptoallday criminal organization by her brother Steve in July 2018. She eventually invested all her retirement funds and also borrowed A$48,000. The funds were converted to cryptocurrencies, Bitcoin, Ripple, and Bitcoin Cash and deposited with Cryptoallday. Cryptoallday stole her funds in October 2018 totaling 27 Bitcoins worth over $350,000 by unilaterally closing her account. In 2018, Jacqueline lost an additional 3 Bitcoins or $45,000 to another company, USI Tech (United Software Intelligence Technology which) is a company that claimed to develop the world's first automated trading platform for Bitcoin (BTC). The company claimed to be based in the United Arab Emirates but likely was operated from within the European Union. The website usitech-intl.io is no longer in operation and was registered in the .io domain under the control of the United Kingdom Foreign and Commonwealth Office. Twitter, Facebook, YouTube and WhatsApp were all used by the criminals in carrying out these schemes. Jacqueline has become depressed and indebted and seeks damages of over €500,000.

Errol T. is a citizen and resident of Australia. He is self-employed. Several years ago, Errol was severely injured in a road accident and has had to undergo numerous operations on his leg, knee, and hip due to complications. He received a modest settlement for this injury which he invested. Based on high pressure tactics from Cryptoallday, he was induced to cash out his investments and deposit all his savings which amounted to 35 Bitcoins or A$500,000 with Cryptoallday. Cryptoallday utilized Facebook and WhatsApp in its scheme. As in the case of Steve and Jacqueline above, Cryptoallday froze Errol's account and stole his Bitcoins in late 2018. Errol is now left with no savings or retirement and has become depressed and anxious. He seeks damages of over €500,000.

Andries D. is a citizen and resident of South Africa. In December 2018 he saw a Facebook ad for MGM Markets (mgm-markets.com) which claims to be a "leveraged" cryptocurrency trading platform and which purports to be based in the United Kingdom. The domain registration for mgm-markets.com is incomplete and shows only that the registrant is in Bulgaria. Andries deposited 5 Bitcoins on the direction of MGM Markets which cost him $26,000 at market rates. A false accounting showed the account balance reached 16 Bitcoins at which point MGM Markets attempted to extract an advance fee from Andries which he refused to pay and was blocked from withdrawing his funds. MGM Markets then attempted to extort $26,000 and asked that this be paid to a bank account in Turkey. MGM Markets also obtained copies of Andries' identification. Andries seeks damages of no less than €50,000.

Symon C. is a citizen and resident of the United Kingdom. In March 2018, Symon saw an ad for CCT Market (cctmarket.com) on Facebook. In April 2018, he was contacted by a salesman for CCT Market who induced him to invest approximately €16,000 by rendering a series of

false accountings showing profits made from supposed cryptocurrency speculations. Symon wired funds to Germany and Poland. CCT Market purports to have offices in London and is affiliated with a St. Vincent shell company, PHHLT Marketing Limited. The true ownership of the company website is cloaked by a company called Privacy Protect, LLC of Burlington, Massachusetts, United States. When Symon's account reached more than £100,000 in Bitcoin due to his trading acumen, CCT Market tried to extract an advance fee of £8000 from him which he refused to pay and was blocked from withdrawing his funds and the profits which would have accrued had the account been funded. Symon seeks a minimum of €100,000 in damages and compensation

Cryptocurrency Resolution Trust is a Commonwealth of the Bahamas Trust established under the Bahamas Trustee Act of 1998. The following claims have been assigned to the Trust for collection:

a. **Mr. TC**, the original settlor of the Trust, is a citizen and resident of the United States. He began accumulating Bitcoins and by 2013 had amassed 1000 Bitcoins through peer-to-peer transactions deposited into a Blockchain.info wallet. During May 2013, 996 Bitcoins disappeared from Settlor's wallet. Settlor was alerted by a text message on his cell phone indicating that his Bitcoin wallet had been emptied. TC made inquiries with Blockchain.info and Dr. Jay Best of the Massachusetts Institute of Technology but was unsuccessful in tracing the 996 Bitcoins which had simply disappeared along with any blockchain. Based upon new research and technology available in Bitcoin tracing, TC discovered his Bitcoins had been tumbled by a hacking and money laundering operation known as Bitblender which maintain a website at bitblender.io. It is not known exactly how the Bitblender provides services however it is known that the user must surrender control of Bitcoins to Bitblender with instructions as to where the ' tumbled' coins are to be deposited. Bitblender's operations are described at Bitblender.io and are as follows:

"Bitcoin mixing is the name given to the process of exchanging your Bitcoin balance for an equal (or similar) amount from a different source. In other words, it is the process of obscuring where your coins came from, which in turn makes your digital trail much harder to follow."

"Mixing your coins is a great way to cover your tracks and make your bitcoin transactions impossible to follow. This protects you against criminals, nosey parkers, and if you are indeed using Bitcoin for activities prohibited by the law, it also of course protects you against law enforcement."

The EU terms this process as "mixing" and is aware that it used for criminal purposes. The European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance in its August 2018 white paper has recommended mixing be criminalized: "Furthermore, the EU should think about imposing a specific ban on such aspects surrounding cryptocurrencies that are aimed at making it impossible to verify their users (e.g. mixing) and criminally sanctioning these aspects." (p.13) However the EU has not yet acted and bitcoin blending and mixing continues at the rate of millions of Euros every day.

The domain registrant information for bitblender.io is Privacy Protect, LLC (PrivacyProtect.org) of Burlington, Massachusetts, a domain masking service. Previously, Bitblender used a similar service in Switzerland. The .io Top Level domain is controlled by the United Kingdom Foreign and Commonwealth Office (FCO) as part of the national security zone, British Indian Ocean Territories. A UK company, Internet Computer Bureau Ltd. also known as "ICB", manages the sale of .io domains for commercial use. Batelco/SURE and the UK FCO British Indian Ocean Territories Administrator maintain a relationship with ICB. The UK FCO has been aware of the Bitblender issue for almost two years yet has not acted. Mr. TC seeks return of his 996 Bitcoins.

b. Mr. JH is a citizen of the Republic of South Africa, residing in Pretoria, South Africa. In November 2017 Andrew Kirov, a self-described "senior broker" in cryptocurrency investments purportedly based in Oslo, Norway referred Claimant to AXE Cryptocurrency "AXECC" doing business as AXECC.IO. AXECC through its brokers and/or touts Tomas Miller, Sofia Rojas and Tanya Brown induced Claimant to deposit £123,923 in a series of transactions from November 2017 through June 2018, the majority of which were obtained through the simple expedient of providing a running false accounting showing trading profits. JH's payments were made to AXECC in a series of approximately 20 transactions including various other payments such as "taxes" and "fees." The payments were in mixed transactions of Pound sterling, Euros, and US dollars as well as cryptocurrency. On April 10, 2018, AXECC produced a false assessment from Her Majesty's Revenue & Customs ('HMRC') in the sum of €8722 with which they induced Claimant to pay to them. HMRC later confirmed the tax bill assessment was a complete forgery but Claimant was indeed deceived by it and paid the funds to AXECC who corruptly personated HMRC. On May 21, 2018, AXECC provided a false accounting to Claimant demanding a €6000 service fee before Claimant's funds could be released, which the Claimant paid this fee as well. And on June 11 and June 13, 2018, AXECC demanded that JH pay service fees totaling 3000£ and €1000, which he did. AXECC however did not release the promised €284,607 but instead JH was contacted in June 2018 by two of claimant's agents, the Andrew Kirov and Rainer Swartzmann who intentionally and falsely promised to gain more funds from Claimant that in exchange for an additional payment of €20,767.85, the said €284,607 would be released to Claimant. Pursuant to an agreement with Kirov and Swartzmann, Claimant paid €20,767.85, but no funds were released Claimant. The entire charade being what is termed an "advance fee scam." AXECC purports to be affiliated with the St. Vincent shell company Lemato Partners LTD and also claims to have offices in the United Kingdom and Switzerland. AXECC also obtained copies of JH's identity documents.

The domain registrant information for axecc.io is Whois Privacy Corp., Ocean Centre, Montague Foreshore, East Bay Street, New Providence, Nassau, The Bahamas, a domain masking service. The .io Top Level domain is controlled by the United Kingdom Foreign and Commonwealth Office (FCO) as part of the national security zone, British Indian Ocean Territories. A UK company, Internet Computer Bureau Ltd. also known as "ICB", manages the sale of .io domains for commercial use. Batelco/SURE and the UK FCO British Indian Ocean Territories Administrator maintain a relationship with ICB. Mr. JH seeks damages of no less than €284,607.

c. **Mr. AT** (Doubly Claims) is a citizen and resident of Italy and is the representative/agent for a group of 14 Italian investors who invested substantial amounts of cryptocurrency worth £1,700,000 (360 Bitcoins + 75 Bitcoin Cash) with crypto trading platform DOUBLY.IO from January 2019 through April 2019. DOUBLY.IO OR "DOUBLY" purports to be a cryptocurrency trading or investment platform utilizing its Top-Level Domain .io website: DOUBLY.IO receiving payments in primarily cryptocurrency such as Bitcoin, Litecoin, Ethereum, Bitcoin Cash and Dash. It purports to be based in the United Kingdom and uses the Companies House registry to bolster its claim to legitimate when in fact it is an obvious criminal enterprise. The .io domain registration for DOUBLY.IO is masked and leads to a Panamanian privacy service WhoisGuard, Inc which is listed as the domain registrant. DOUBLY.IO also utilizes a shell company and a sham insurance company to establish legitimacy and to deceive its victims, Doubly Ltd. and Financial Global Insurance. These entities have no physical assets and conduct no actual business outside of being a facet of the deception used by DOUBLY to ensnare investors and as a mail drop for receiving correspondence for DOUBLY. The DOUBLY.IO website states that its purpose is:

"Our focus is on automated systems with artificial intelligence which work 24/7 in stock market trading. You could say it's a money machine that never stops raising funds for you! The AI Trading Bot captures the best investment opportunities in the cryptocurrency market by solving complex algorithms and automatically opens positions. By using different trading tools and analyzing the price history, he usually achieves optimal profits."

DOUBLY claims it has devised a unique trading strategy that can produce an extremely high return of up to 4.5% a day, the generic term for this is a High Yield Investment Program or "HYIP"; a high-yield investment program (HYIP) is a type of Ponzi scheme, an investment scam that promises unsustainably high return on investment by paying previous investors with the money invested by new investors. The Claimant asserts that DOUBLY does not trade cryptocurrency or any other investment as represented but simply induces investors to divest themselves of money and/or cryptocurrency and then posts false invoices showing impressive profits in order to obtain more deposits from victims.

DOUBLY through social media (Telegram, Facebook, and Instagram) and its network of brokers, salesmen and/or touts induced Claimant to deposit at least £1,700,000 in a series of transactions from January 2019 through April 2019, the majority of which were obtained through the simple expedient of providing a running false accounting showing trading profits and false promises of guaranteed profits. Claimant was encouraged to continue to fund the DOUBLY account as their "profits" grew and small withdrawals were permitted as a show of good faith but in reality, to dupe Claimant into investing more and more funds. In April 2019, "Mr. Greene" and others at DOUBLY blocked Claimant's accounts and attempted to extort $102,000 from Claimant with false allegations of account manipulations. Claimant refused to pay and was not permitted to withdraw or access the alleged funds held by DOUBLY.As a result of DOUBLY's many intentional misrepresentations which were relied upon by Claimant their direct losses totaled at least €2 million.

d. **Mr. AT** (Abacus Ltd. Claims) is a citizen and resident of Italy and is the representative/agent for a group of 5 Italian investors. Abacus Ltd. is purportedly an English company operating

the website abacuslimited.org. Abacus Ltd. is an illegal HYIP, High Yield Investment Program, accepting deposits in Bitcoin and utilizing social media (Telegram). It falsely claimed to generate daily returns on investment of 4.2%. The domain registration for abacuslimited.org is masked and leads to a Panamanian privacy service WhoisGuard, Inc. Based on false accountings, Abacus Ltd. deceived AT into depositing 17 Bitcoins before the site shut down without recourse. AT seeks return of 17 Bitcoins and compensation for loss of use.

The Role of Social Media

Without social media; crypto criminals would be deprived of access to many victims.

Facebook operates as an easy conduit and enabler on several levels. First it provides a home base for crypto scammers as part of a trusted community by allowing them to set up pages and groups. Secondly, Facebook allows crypto criminals to purchase ads which are then pushed on unsuspecting Facebook users using targeted intelligence and data harvesting. Facebook has profited directly and thus enabled a portion of the 7 billion in crypto fraud and criminality. Google AdWords also used similar methods to Facebook but seems to have mitigated its policies regarding crypto crime by banning some crypto related offers.

LinkedIn also operates as a trusted community. However crypto criminals take advantage by posting false profiles and messaging other users with no fear of enforcement by LinkedIn.

Telegram and WhatsApp are instant messaging services favored by crypto criminals to carry out their crimes unobserved. Instagram profiles are another source of information for criminals as are Instagram accounts promoting cryptocurrency scams. Finally, Twitter and YouTube are used extensively to market crypto related criminal activity.

According to Michael McKibben[8], an expert on social media retained by counsel, all these social media sites could monitor and interdict crypto criminal activity. Instead they choose to either ignore and tolerate criminal activity or in the case of Facebook, monetize it by selling leads and pushing ads on the unwary victims.

The Role of Domain Privacy Services, ISPs and Corporate Registries

While each criminal platform is somewhat different; many share similar characteristics.

1. They often use offshore companies or the UK Companies House registry to give the appearance of legitimacy.
2. They always use domain registry proxy services to mask the real operators of the criminal websites; as these services are always in difficult or likely impossible for consumers to unmask.
3. Internet Service Providers, Domain Registries and resellers and Hosts (Go Daddy Inc. etc.) provide services to obvious criminal enterprises without fear of liability.

[8] Michael McKibben is credited with inventing the social media software that was the basis for Facebook. See: CNBC, Facebook Stole Our Invention, 5 March, 2012, https://www.cnbc.com/id/46631326

4. The .io domain in particular is marketed to crypto related companies; it is controlled by the UK FCO under the British Indian Ocean Territory Administration.

The Myth of Cryptocurrency Immunity

The European Union seems confused at best how to classify cryptocurrency when in fact the answer is obvious. While the Bitcoin currencies are allegedly decentralized and participation as a node "permissionless," they are still controlled by nodes who are real actual and legal persons who operate the node servers, the majority of whom reside in the EU.[9] Ethereum and Lite Coin, are popular cryptocurrencies, and are also examples of a permissionless blockchain. The cryptocurrencies are simply very large unincorporated or voluntary associations in which each current or former node has liability for the entire operation and which lacks juridical protections for its members or associates. As an unincorporated association devoted to a common voluntary purpose, the cryptocurrencies therefore must comply with AML and GDPR regulations just as would any other unregistered nonprofit association . They obviously have done nothing of the sort and the current chaos is the result. The EU must hold the nodes, the actual operators, responsible. To do anything less would be to grant *de facto* extraterritorial status and immunity to cryptocurrencies. The instructive comparison is to terror cells and criminal organizations which are also unregistered yet collaborate toward a common purpose. If the cryptocurrencies operate or are controlled from within the EU, they must be subject to same rules as any other voluntary association that deals in finance

Fraud

It is overlooked that both blockchain and the ledger which comprise the heart of cryptocurrencies are fraudulent.[10] As noted above, Bitcoin mixing and blending destroys the blockchain and renders stolen cryptocurrency untraceable, yet the EU has failed criminalize an activity which is money laundering. There is no legitimate reason for Bitcoin mixing save to launder the proceeds of criminal activity. Yet the cryptocurrencies and exchanges tolerate it even though it destroys their highly vaunted blockchain. Secondly, the Bitcoin and Bitcoin derived ledgers contain massive fraudulent entries. The EU waffles on the existence of the apocryphal Satoshi Nakamoto who obviously never existed: "Contributory to the mystic nature of Bitcoin is that until now it remains unclear whether Satoshi Nakamoto is a real person, a pseudonym, or perhaps even a group of hackers.[11]" It is inconceivable in the 21st century that a person from an industrialized nation could leave no trace of birth or death yet be one of the richest men or women in the world. This Nakamato is a fraud. Nakamoto's Bitcoin and Bitcoin derived (Bitcoin Gold, Bitcoin Cash, etc.) ledger entries are estimated at between €10-20 billion. Yet they are false, and the true ownership is masked. There are no restrictions on this wealth and it is very likely responsible for manipulations in the prices and trading volume of cryptocurrency as cryptocurrency being divorced from the real-world

[9] Global Bitcoin Node Distribution https://bitnodes.earn.com/

[10] *Ad Ibid*, Blockchain is a particular type or subset of so-called distributed ledger technology ("DLT"). DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes.

[11] *Ad Ibid*, at section 3.2.1

economy nonetheless trades with great volatility and is driven by unseen forces. To believe that the human hand is not involved is laughable. Great fortunes can be made if one knows to go short or long on cryptocurrency. Control of large ledger entries by criminal elements masquerading as a modern myth is an exploit worthy of the greatest criminal mind of the Century.

Remedy Requested

The EU agrees that the founder of the Bitcoin Satoshi Nakamoto is a likely a fiction.[12] In fact, she is a fraud and criminal by any reckoning. She does not exist yet billions of Euros in cryptocurrencies, the true extent of which are unknown, are under her name or her proxies. Therefore, the Bitcoin ledger and the ledgers of its various derivative cryptocurrencies are fraudulent. This would yield an estimated 10-20 billion Euros in compensation if the EU were to assert jurisdiction over the unincorporated entities known as decentralized permissionless cryptocurrencies. These Nakamoto ledger entries should immediately be sequestered for the benefit of the victims and consumers**.**

Social media and domain privacy proxies also should be tapped for a compensation fund; while crypto criminality would still exist with social media and domain privacy providers; it would be confined to the edges or the Internet and Dark web instead of being easily accessible and heavily marketed. These domain proxy or privacy services should pay a heavy price as their services are almost always utilized by crypto criminals without fear of recourse and it is obvious they are used for purposes other than legitimate privacy concerns by their public content. Facebook and other social media giants have been key to the misery caused by crypto criminals; unlike Google AdWords, these social media companies have not acted with alacrity or urgency to mitigate the issue. Facebook, Instagram, Twitter, and YouTube are rife with content controlled by crypto criminals.

All responsible financial systems have a reserve fund for victims of fraud and crime; there is no reason cryptocurrency should be exempt from these requirements. When a dangerous financial system will not impose controls upon itself, it must be done from above. Failure to act under these circumstances equates with nonfeasance towards consumers and a deliberate undermining of the European GDPR and AML regimes.

Dangers

If the issue of harm to consumers is not of concern to the EU, then the massive flow of funds into the hand of organized crime should be. At least €7 billion a year is being generated to fund various organized criminal establishments known to be active in cryptocurrencies including the Ndràngheta[13], various hacking and extortion rings, Eastern European and Israeli gangs, and other unseen and anonymous criminal firms.

[12] *Ad Ibid*, The EU has posited a group of hackers is responsible for Bitcoin; although it is just as likely that the original concept was hijacked by criminals in the mode of the master Russian pyramid scheme artist, Sergei Mavrodi.

[13] The Italian press has suggested the Ndràngheta utilizes crypto currency for money laundering and untraceable payments for extortion and kidnapping rackets.

Therefore, we beseech the Commissioner for Justice, Consumers and Gender Equality to take up this matter as an urgent priority at the European Level. The claimants above have taken many risks to start this process and should be compensated and legal and expert fees paid. We anticipate an influx of secondary claims that will round out this process, especially as to crypto utility and equity tokens and alt coins which are also riddled with unaddressed criminality and fraud. The claimants therefore stand ready to cooperate with any remediation or consultative process the Commission may choose to propose. Ignoring this issue cannot be a solution as the problem will only compound itself. The existing European legal framework is failing to deal with this issue.

Since crypto exchanges and crypto criminals can be anonymous and located in jurisdictions that do not have effective money laundering, law enforcement, consumer protection and terrorist financing controls in place only a supranational response and remedy will suffice.

Respectfully submitted,

Dr. Jonathan Levy[14]
Attorney & Solicitor
Legal Representative for Crypto Currency Victims

[14] Dr. Jonathan Levy is a licensed attorney and European lawyer. He holds a PhD in Political Science as is a faculty member at Norwich University and a member of the Institute for National and International Security (INIS). For English law matters, he is a consulting solicitor at the firm of Berlad Graham LLP.