

A person wearing a black balaclava and gloves is shown from the chest up, looking down at a white keyboard on a wooden desk. The background is slightly blurred, showing a window with blinds.

# Terrorist Use of Cryptocurrencies

A Blockchain Compliance White Paper

---

Simone D. Casadei Bernardi

April 2019



BLOCKCHAIN  
CONSULTUS

**Terrorist Use of Cryptocurrencies**  
is published by  
**Blockchain ConsultUs Ltd.**  
Kemp House, 160 City Road  
London EC1V 2NX, United Kingdom  
Company number 11595594  
[www.blockchainconsultus.io](http://www.blockchainconsultus.io)

© Blockchain ConsultUs Ltd, 2019

This document is protected by law. This representation of Blockchain ConsultUs' intellectual property is provided for non-commercial use only. This document can be freely distributed, provided no changes are introduced hereto. Any amendments or changes hereto, as well as this document's distribution for profit making, are allowed only upon written consent by Blockchain ConsultUs Ltd. For information, please email [contact@blockchainconsultus.io](mailto:contact@blockchainconsultus.io).  
Cover image: © luckybusiness/Adobe Stock. Image on page 8: © chagpg/Adobe Stock.

# Terrorist Use of Cryptocurrencies

*Cryptocurrencies are easy to use, secure, and if used correctly can hide your identity. That would explain why increasing news reports claim that terrorists are using them to fund their actions. Is that claim true, and if so, to what extent? And are there any real-world examples to draw on?*

<b>What Makes Cryptocurrencies Appealing to Terrorists?</b>	<b>4</b>
<b>Terrorism and the Online Age</b>	<b>8</b>
<b>Examples of Cryptocurrency's Use in Terrorism</b>	<b>10</b>
<b>Did ISIS Use Bitcoin and Other Cryptocurrencies?</b>	<b>13</b>
<b>The Limitations of Cryptocurrency</b>	<b>15</b>

Whilst every effort has been made to ensure the accuracy of information presented, the author and the editor disclaim all responsibility for and accept no liability for any errors or losses caused by any inaccuracies in this publication or the consequences of any person acting or refraining from acting or otherwise relying on such information. They do not assume any liability for the information contained herein, its interpretation or for any reliance on it. This white paper should not be construed as a recommendation, endorsement, opinion or approval of any kind. It has been produced for information only and should not be relied on for legal purposes. Professional advice should always be sought before taking action based on the information provided.

# What Makes Cryptocurrencies Appealing to Terrorists?

---

Cryptocurrency is an area of great promise, and not just for those interested in privacy or investing. The fact that it makes online payment not only quick, but secure, means that crypto is of appeal to criminals too. While it's incorrect to claim that cryptocurrency is only or mostly used for fraudulent or illegal purposes, it is by some, nonetheless.

There are several reasons why criminals generally, and terrorists specifically, would want to use cryptocurrency as a payment method.

## The Online Revolution

At the heart of the need for cryptocurrency is the terrorists' need to operate online.

Today's violent political actors still make their statements in the real world, with attacks and kidnappings. This aspect of terror will likely never change.

But like in every other section of society, the internet has revolutionised how we do what we do. Through social media terrorists can reach thousands, millions, through the power of just one post. Through creating online content, they can broaden their reach and sow the seeds of their ideology further than before.

## Ease of Use

For the purpose of online transactions, cryptocurrencies are becoming increasingly easy to use. Years ago, Bitcoin and other coins were the domain of those in the know. Today, Bitcoin's dramatic rise and fall in value have made it a worldwide household name, and the flourishing of a number of exchanges make it easier than ever to use, especially when such platforms are based in off-shore jurisdictions or fail to meet minimum standards when it comes to the contrast of money laundering and terrorist financing.

Praiseworthy efforts are made by national and international banks to impede transfers of fraudulent funds—whether that be from fraud, tax evasion or other crimes. A terror group can't use bank accounts like we can, as records are kept, transactions are easily traceable and access to funds could be revoked at any time.

Cash will always be the easiest form of currency to use. But there are several caveats to be aware of. Cash can be lost, stolen or destroyed; and in the case of local currencies, may be just as volatile as cryptocurrencies.

As such, cryptocurrency is easier for groups like these to use, encouraging uptake.



### Crime and Privacy

Bitcoin and other coins provide high levels of security when used correctly. Moreover, Bitcoin is pseudonymous. While not completely private, your unique address is publicly available—and any transactions from it can be tracked. However, the identities behind these accounts aren't revealed unless the person identifies themselves, for example by asking publicly for donations.

Meanwhile, terror groups rely on privacy. As a terrorist purchasing bomb-making equipment and supplies for an attack, it's vital that your movements and actions aren't traced. While there is no evidence as of yet that cryptocurrencies have been used in this way, it's clear that they could be.

### Cryptocurrencies Can Be Laundered

As it disguises ill-gotten funds, making them appear legitimate, money laundering is of central importance to any criminal operation. To simply put one's fraudulent proceeds into a bank account would be to raise suspicion; and to carry around ever-increasing amounts of cash would be unwise.

Bitcoin and other currencies have

been used for this purpose in the past. The idea is simply to use dirty money to buy Bitcoin, through one exchange or another, and transfer it to a clean wallet.

Depending on the complexity of the scheme—and the amount of money involved—there are then two ways to get the money back.

The first is to simply withdraw it from the new account, relying on the 'privacy' of cryptocurrency. This brute force method is ineffective, as the transaction between the two wallets can be easily discovered, hence why this method isn't used by most criminals.

The more effective method is to keep the money in the clean wallet, gradually 'sipping' it from that account to yet another. This method is better since relatively minor transactions over a longer period of time are less noticeable. This was the method used by the cyberterrorists behind the May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, and similar criminal acts.

Better yet for a criminal is a tumbler service. Accessible through the deep web, these third-party services mix your coins with those of others, before transferring yours on to a third account, in varying small amounts. While these transactions are still recorded in the blockchain, it's impos-

sible to tell whose money is whose—dirty money is made clean.

### International Reach

Terror groups have relied on foreign funding for years. The IRA, for example, was funded by Irish heritage associations in the U.S. from the early 20th century onwards. ISIS and similar groups are funded by donations, too, whether from the Syrian or Iraqi diaspora or from sympathisers in other countries, in the region or far from it.

The issue with sending payments internationally is that they are easily traceable. There is no way to anonymously send a payment through a bank, for example. Even global money transfer companies often involved in scams, like Western Union, require your identity before they send your money onwards.

Shipping physical cash internationally is anonymous. But the risks involved are too great—at any point between the sender and the recipient, the package could go missing, or customs authorities could confiscate it; in other words, there's more than a chance that the cash inside never reaches its destination.

Cryptocurrencies neatly sidestep

these issues. They allow you to send money internationally without making your identity known to anybody. Provided that the person or group uses a pseudonym on an exchange, and the transaction wasn't publicly solicited, then their identity isn't public.

### Shifting Model of Terrorist Funding

Besides these advantages, the way that terrorists raise funds is changing. Groups intent on violent political action have historically been funded by government sources—foreign governments, that is. Hezbollah were trained and funded by Iran's Islamic Revolutionary Guard Corps. Iran have also been accused of funding Shia militias in Iraq.

But state-sponsored terrorism is far from the only kind. Other terror groups rely almost exclusively on donations. Al-Qaeda was formed in 1988, and bankrolled by Osama bin Laden. But with increased exposure on the world stage, they grew to rely on donations to keep afloat. The CIA estimated that prior to the 9/11 attacks, al-Qaeda had an annual budget of \$30 million, and that the majority of this was brought in through donation.

ISIS, too, diversified the way that they

received funds. While they did receive cash from sympathetic regimes nearby, that wasn't the sole source of their income. They used theft, kidnapping, extortion and more to raise money. Soliciting donations, either online or off, is just one piece of the puzzle.

But every little helps, after all. And even more importantly, terrorists are increasingly taking their fight online.

# Terrorism and the Online Age

---

Terrorists seek change in the real world, yet today, need to spread their message online. This dichotomy creates a dual demand: a terrorist needs secure funds for online transactions, and cash for everyday expenses.

First and foremost, a terror organisation needs to fund its physical actions. The logistical needs of a terror group are just as real as those of a business. Funds are required for transport: cars, motorbikes and petrol. Bomb-making equipment, and the ingredients of each bomb, cost money.

Besides that, there are the basic costs of food, shelter and general supplies. As of yet, there is no evidence that terror groups use cryptocurrencies to meet these needs. Cash is still king: in the former territories of ISIS, for example, the group attempted to create their own currency. The only thing that stopped them was that people preferred to do their business in stable U.S. dollars.

But while terror groups do much the same things in the real world as they always have—bombing, extortion and kidnap—spreading the message online has become a core part of modern terrorism.

## Terrorism and Social Propaganda: the Context

Modern terror has evolved. Today's

terror groups rely on propaganda—but unlike the posters, murals and signs that historical terror groups used, today's groups spread their message online.

This change is necessitated because increasingly, terror groups have failed to instigate actual political change. But what they have succeeded in doing is encouraging others to their cause, both in their host countries and abroad.

Al-Qaeda were the first to do so. They gained not just notoriety for their propaganda, but a following too. The idea of proselytising online fits with their mission, as al-Qaeda view themselves as a global movement, one which relies on a global communications network to function. Their goal is not just to spread 'terror', but to spread their message to the world-wide Muslim diaspora.

More recently, ISIS became famous for their violent and horrific propaganda. The idea grew beyond simply 'spreading a message', and became about recruitment. ISIS' videos were responsible for drawing in fighters from across the world, from Indonesia to the United Kingdom.

All of this is to say that terror is as much an online phenomenon as a physical one. And thinking more broadly, some 'terror groups' exist solely online—Russian bot farms and Chinese-government sponsored hacking teams, for example, push the



boundaries of the answer to what is a terrorist?

### Why Cryptocurrency?

To be clear, there's no absolute need to use cryptocurrency in order to do so. Anybody with an account can spread their message on Facebook or Twitter, and receive many followers. However, there are suggestions that terror groups use cryptocurrencies to purchase website domains, for example.

In the same way, one could ask why social media? While it is possible for terror groups to reach like-minded people through real-world means, their use of social media is more broadly dictated by the general trend towards it. More people use social media, more people use cryptocurrency, and more people spread political messages online—on both sides of the spectrum.

***Overall, the use of cryptocurrencies should be seen as part of a general shift towards online terrorism.***

Given that this is happening, one would expect to see a slow but steady uptake of cryptocurrency and money laundering methods among terrorists—and that was exactly what we saw.





# Examples of Cryptocurrency's Use in Terrorism

---

Terrorist funding is an important topic—one which receives a large amount of media and government attention. As such, we can state with reasonable certainty the extent to which terror groups actually use cryptocurrency.

## Risk Factors: Who Might Use Cryptocurrencies?

Modern terror is decentralised. While large groups still exist, most networks are spread thinly—with one or two leaders forming a web of sorts, and their individual followers spread out across the country. Cryptocurrency could be used at any of these levels.

Risk factors with regards to cryptocurrency include:

- **Lone wolf attackers.** At the lowest level, these actors typically only have one or two connections with a terror group, and solely online. These attackers can use cryptocurrency to securely buy terror supplies.
- **Small terror cells located away from the main group.** These cells aim to recruit on a local level, while maintaining links with the larger group in their host country. The group could either receive cryptocurrencies securely from the central group, or assist lone

wolves by financially backing them.

- **Large groups that hold territory,** ISIS being the primary example. These groups manage large amount of land, and large amounts of money. Cryptocurrency could be an easy way to do so.

But how do these risks bear out in reality? Have terrorist groups actually taken up cryptocurrency, or have we yet to see them make full use of it? The truth is a lot more piecemeal and haphazard than you might imagine.

## Origins

Perhaps the first example of cryptocurrency funding terrorists was in the Gaza Strip—and was unrelated to ISIS. The group involved was the Mujahideen Shura Council (MSC), founded in 2012.

The organisation has used both improvised explosive devices (IEDs) and rocket attacks against Israel since then, and had an effective social media presence until their account was closed by Facebook.

The Ibn Taymiyyah Media Center, or ITMC, is their propaganda unit. It seeks first to raise donations, but also to raise awareness of what the MSC does and how. Their Facebook

account was closed, and their Twitter accounts are inactive as of 2019. They released dozens of videos in 2016 and prior.

Many of their videos and posts are instructional. One from May 2016 shows how to make ricin, a deadly poison, and suggested several ways to use it. But more to the point in July 2015, they set up a fundraising social media campaign on Telegram.

The campaign was named 'Jahezona', meaning 'Equip Us', and the aim was to raise \$2500 per jihadist fighter. Their slogan was 'from you money, and from us our blood', making clear that they relied on the donations of people as opposed to government sources.

***Their adverts contained a QR code to make donating Bitcoin easy, along with the message 'Donate to the mujahideen'.***

This was perhaps the first instance of a terrorist group using such means to raise money. In total, they received around \$540-worth of Bitcoin in total. These transactions were publicly visible on the blockchain. However, it was less the success of the individual campaign and more what it heralded that was important.

### Spread

Malhama Tactical, private contractors that trained Syrian fighters, was one of the next groups to raise funds on Twitter. A small group, their emphasis is on training rather than fighting: they run what they call a 'virtual university' for battlefield operations. They published their videos online and shared them directly with followers through social media.

Their channels on Facebook, Twitter, Telegram, VK.com and YouTube are popular—and the group sought to leverage their popularity with a donation drive.

Again, the campaign was ineffective—they raised less than \$100.

But that hasn't put them off. According to Memri Cyber & Jihad Lab, the group are still active online, and are still posting videos asking for donations. One of their more recent videos, from 2019, shows the group training, firing guns, manoeuvring through a forest in tactical gear.

***The video ends with a plea: 'Support Us', and a Bitcoin address.***

It's unclear as of yet how much the group are making with each video; but whatever the case, it appears that the group take an 'every little helps'

approach.

### Flourishing

Most peoples' conception of modern terrorism is based on ISIS, and it is abundantly clear that ISIS utilised social media and propaganda to further their reach. One might, therefore, assume that they, too, sought to raise money online through cryptocurrency.

ISIS are unique. By force, they sought not just to remove a government, but to take land for themselves—and become a state. To do so requires far more than a campaign or two that raises \$100, or \$540. Rather, they had their eyes on larger prizes which could only be gained through capturing and keeping territory. Their funding sources included:

- Proceeds made, or more accurately stolen, from their occupied territory. This includes funds taken from banks, money made from oil reserves, taxation and extortion. This was the main source of ISIS' financial strength.
- Kidnapping and ransom.
- Donations originating from Saudi Arabia and the Gulf states, either from supporters of ISIS or under the guise of supposed humanitarian aid.

- Donations or material support from the fighters that travelled to join them.

Much of ISIS financial strength came from their control of oil wells. According to an FATF Report, ISIS sold crude oil for cash at significantly discounted prices. But even at low prices—\$20-35 per barrel, far under the \$60-100 average for the time—the group were able to fund their activities. The best estimate is that they would sell 50,000 barrels per day at these prices.

As is clear, this is a far more lucrative operation than raising money through social media. Only 5% of ISIS' budget relied on outside donations, both through social media and otherwise. Rather, they operated almost as a government, albeit through fraud: local cells in Iraq and Syria were required to send 20% of their income on to regional leadership groups. These funds were then redistributed wherever they were needed.



# Did ISIS Use Bitcoin and Other Cryptocurrencies?

---

Bitcoin and other cryptocurrencies were used to fund ISIS—to an extent. And interestingly, the money wasn't always sent directly online; Bitcoin and other coins were used in several ways. Here's how.

## Cryptocurrency Money-Laundering

In 2017, a woman was indicted for attempting to send ISIS financial support through Bitcoin and other currencies. She fraudulently obtained credit cards, using them to purchase cryptocurrency online, totalling more than \$50,000. Some of the funds were also generated through a fraudulently obtained loan.

However, she didn't then send the money directly. Converting the cash into cryptocurrency was a money laundering operation, as she then withdrew the money and attempted to send it via four banks—American Express Bank, Chase Bank, Discover Bank and TD Bank. The money was wired successfully to shell companies in Pakistan, China and Turkey.

It was only when the woman attempted to travel to Syria and join ISIS in person that she was stopped, and her scam identified.

## Direct Purchases

Evidence for the use of Bitcoin in

purchasing terror supplies like bomb-making kits is thin. However, there are suggestions. In 2018, a pro-Islamic State tech group published a Q&A on social media on several topics. One of the questions that a follower asked pertained to using Bitcoin for online purchases—ones that they would prefer authorities not to track.

The group answered that while Bitcoin has a 'high level' of secrecy, it doesn't guarantee anonymity. Instead, the group recommended Zcash—a digital currency that uses cryptography to ensure transactions remain private.

This isn't evidence in itself of terrorists using cryptocurrency; but it does suggest that lone wolf attackers are at least encouraged to try it.

## Direct Donations

The evidence of direct donations, too, is thin. In 2018, Europol, the European Union Agency for Law Enforcement Cooperation, released a report indicating that ISIS had received small donations through Zcash and Bitcoin. In their report, they state that they had requested donations in both currencies.

However, the use of these funds was limited. Rather than directly fund terrorist action, the donations were supposedly used to purchase website domains. The report also sought

to clarify that ISIS had not directly funded individual terrorist attacks in Europe using cryptocurrency. Rather than being a cornerstone of their strategy, it seems that cryptocurrency was a useful but limited tool that the group could use on occasion.

### ***Did Cryptocurrency Use Merit Media Attention?***

*The cases summarised in this chapter, in and of themselves, are interesting. But they hardly merited the media attention they received.*

*In part, this was due to the flourishing of crypto as a medium. As Bitcoin's value soared, the mainstream media fell in love—in part because of the incredible returns that some people saw, as well as its novelty. The added dimension of cryptocurrency being used to fund crime and terror only increased its media profile.*

*But in terms of actual documented use in funding terror, cryptocurrency was a very small part of the puzzle. ISIS found only a very small fraction of their funding in cryptocurrencies, both before and after their explosion in value.*

*More than anything, that was due to the very real limitations of cryptocurrency.*

# The Limitations of Cryptocurrency

---

Despite much fanfare over terrorist organisations using novel means of acquiring funding, uptake is still limited. In part, this is a reflection of the generally still limited scope of cryptocurrencies, even after Bitcoin shot to fame. But it's also due to the nature of cryptocurrency, as an online, tech-heavy and volatile way of sending or receiving funds.

So, what are the limitations of cryptocurrencies? And for what reasons do they discourage terrorist groups?

## Lack of Technological Infrastructure in Third-World Countries

On 7<sup>th</sup> September 2018, the U.S. Subcommittee on Terrorism and Illicit Finance met to discuss how modern terror groups find funding. Attack their funding, they claimed, and you attack the terror groups by proxy. As such, identifying their funding sources is of vital importance to security.

The Subcommittee admitted that many reports had emerged on the terrorist use of crypto platforms. However, they sought to clarify that there were still limitations on the adoption of alternative currencies. Chief among these was the technology available to terrorists in certain parts of the world. To quote the Subcommittee, cryptocurrency is a “poor form of money for jihadists because they usually need to purchase goods

with cash often in areas with weak technology infrastructure.”

The Middle East's data network coverage isn't as complete or as fast as that in the West. And even where it may have been—for example in large cities—this infrastructure is itself one of the first targets for terrorists. For groups operating out of rural areas, the situation is even more difficult. Cash and bank transfers offer no such limitations.

## Lack of Security Skills and Knowledge Among Terrorists

Cryptocurrency and blockchain might appear complicated. Blockchain especially is opaque to a newcomer, so despite being a real and concrete idea, the term is increasingly used as jargon—diluting its meaning. For anybody interested in learning about cryptocurrencies, coming to understand the blockchain is therefore without a doubt the most complicated part.

This hinders how a terrorist group can use cryptocurrency. While it might work for small ad campaigns, good for a few hundred dollars, the steep learning curve means that managing more money over a longer time is too difficult.

Even worse, Bitcoin can still be stolen, either through fraud or through copying the key to your wallet. Any group

intent on keeping most of their money in Bitcoin would become aware of this issue, and could therefore decide against it.

There's no such learning curve related to the use of cash or electronic money bank transfers. While these methods of acquiring funding have their drawbacks too, they're at least easy to understand. And while online security is difficult to maintain, keeping cash securely is simple too, provided that you have access to weapons.

### Lack of Access to Required Tech

Without technology, there's no cryptocurrency. Without access to technology, there's no access to your wallet. As noted above, many areas where terrorists operate lack the infrastructure necessary to support an always-online means of funding.

A terrorist group may also lack access to the necessary technology itself. While it is possible to manage cryptocurrency on a smartphone, the lack of consistent network signal makes doing so difficult; but at the same time, consistent access to a desktop or laptop computer isn't a given. And even if a group does have access to actual computers, they may become

damaged, or the group may have to abandon them.

This also prevents terrorists from being able to mine coins. A terror group's hideout is likely to be raided or destroyed, and given that mining operations are exceptionally expensive since Bitcoin's boom, this kind of investment is unappealing to groups like these—even if they can access the required tech.

### Cryptocurrency Volatility

Whatever your opinion on investing, it's true that cryptocurrency has a reputation for volatility. Price fluctuations, both up and down, make it equal parts attractive and dangerous. Whatever organisation you look to fund, be they legal or not, they will need a steady and secure form of income. Cryptocurrency doesn't fit that bill as of yet.

As such, asking for donations in Bitcoin or another cryptocurrency may be a good idea for short-term campaigns. It allows terror groups to reach more people, and leverage their online following. But as a long-term solution to funding, it makes a poor choice.

Consider the needs of a large group

like ISIS. On the one hand, they do need to fund lone wolves working abroad—cryptocurrency allows them to do that. But in terms of money management, ISIS' budget stretched into the millions or perhaps billions, and dollars or gold are preferable because of their stability for such large amounts of money.

### The Blockchain

While deposits to a wallet are anonymous, the technology behind Bitcoin and other cryptocurrencies is nonetheless disruptive. The blockchain is public, and while the founding ideal behind cryptocurrencies is their anonymity, it is possible to figure out who a wallet belongs to.

It's already being done. Private companies like Chainalysis use proprietary blockchain analysis software and public clues to identify the people behind wallets involved in fraud or other criminal behaviours.

The most famous use of their software was related to a court case, in which they helped the FBI discover the identities of two fraudsters. The pair had been stealing Bitcoins from the wallet of a Silk Road drug dealer. Another company, CipherTrace, does much the same work as Chainalysis. This presents an important problem

for a terrorist group. Movements of money can be tracked when donations are solicited through public advertisements. This allows law enforcement officers to identify the wallet belonging to that particular group. They can then track the amount of money they receive, and when they spend it. This information could be used to predict upcoming terror threats.

Furthermore, through tracking the payments made from the terrorists' wallet, investigators could incriminate the wallets they regularly send payments to. If the security services have identified a number of groups' addresses, they could unearth previously unknown links between terrorist groups.

### Difficulties Withdrawing Money

Crypto can be used for various online applications, but ultimately, terrorists are interested in enacting political change in the real world by violence. To do so, they need to work with cash or bank funds.

Cryptocurrency is still useful for online transactions. But to buy weapons, supplies, food and everyday items they still need cash. Withdrawing Bitcoin from an exchange leaves



traces, which terrorist groups naturally seek to avoid. And withdrawing through peer-to-peer leaves them open to fraud.

Whatever the case, turning cryptocurrency into cash is much more difficult than using regular currency.

### The Heat

Besides each of these reasons, one far more simple limits the use of cryptocurrency by terrorists: the weather. While the media were happy to drum up reports that ISIS had taken small donations in Bitcoin, it would have been difficult-to-impossible for them to actually mine cryptocurrencies.

Put simply, the region is too hot. Mining cryptocurrencies to a meaningful extent requires a large volume of high-quality equipment, but that's not all that's needed. To mine effectively requires cooling systems, as the necessary hardware quickly heats up. Keeping that hardware cool is difficult enough in a regular environment; in hotter parts of the world, it's practically impossible.

But none of these are the most important reason why terrorists don't use cryptocurrency. There's one key-reason that terrorists have yet to rely on Bitcoin, or any other form of

cryptocurrency. It's that any terrorist group can make far more money through alternative means. ISIS, as we saw above, sought funds through a variety of manners.

***But whatever donations they may or may not receive, nothing came close to the money they made from commodities.***

Their stranglehold on the region's oil production was the driver behind their success. The Washington Post estimated that ISIS were generating \$20 million per month from oil alone. Aside from oil, ISIS requisitioned cash and gold from banks in occupied regions.

According to the U.K.-based Syrian Observatory for Human Rights (SOHR), ISIS reportedly hoarded 40 tonnes of gold bars in Syria. These had mostly been stolen from the Bank of Mosul, but there were many more banks besides in occupied regions.

Once Mosul was recaptured, 50 tonnes—ten tonnes more than estimated—were found by U.S. forces. In context, the bars were worth at least \$2.1 billion in total. The U.S. supposedly cut a deal with the terror group, such that hundreds of field leaders were allowed safe passage from their stronghold in Deir Ezzor, in exchange

for information on where the gold was hidden.

Political games aside, one thing is clear from this episode. What little donations ISIS could have taken were dwarfed by many orders of magnitude by what the group made from theft alone.

# Providing **Pan-European Legal, Compliance and Strategy Advice** on Blockchain Projects



Your goals + Our expertise + Where you are + Where you want to be + Getting you there



## Legal & Compliance

- > Selection of the jurisdiction of the company
- > Company formation
- > Preparation of compliance measures
- > Drafting of documents for the AML/KYC procedures
- > Elaboration of the optimal legal concept of tokens
- > Privacy and GDPR
- > Preparation of agreements with investors and user agreements
- > Dealing with competent regulatory authority and self-regulatory organisations
- > Opening of accounts with banks and payment institutions
- > Escrow services



## Strategy

- > Investor relations
- > Business planning
- > Road mapping to find the right go-to-market partnerships
- > Marketing and PR in the crypto industry
- > Risk assessment and sustainability analysis
- > Brand creation



## Technology

- > ICO/STO/crowdsale ready-made platforms
- > Recruiting of technical specialists
- > Drafting of technical tasks

## There are Blockchain consulting companies. And there's **Blockchain ConsultUs!**

We are a boutique consulting firm who specialises in helping blockchain and decentralised ledger technology projects/organisations keep compliant and reach their goals in an ever-changing digital landscape.




We assist companies across the European continent, so if you run or have in mind a Blockchain-related project, we can help you. Wherever you are based.

Our team of specialists use their legal, compliance, tax, and strategic knowledge to better assist you in the management of complex projects every step of the way.

Consultus (/kon'sul.tus/).  
Perfect passive participle of cōnsulō:  
"I consult, reflect, take counsel, consider, or deliberate"



**Blockchain ConsultUs Ltd.**  
Kemp House, 160 High Road  
London EC1V 2NX, England  
[contact@blockchainconsultus.io](mailto:contact@blockchainconsultus.io)  
+44 (0)20 8798 0253

 [blockchainconsultus.io](https://blockchainconsultus.io)  
 [linkedin.com/company/blockchain-consultus](https://linkedin.com/company/blockchain-consultus)  
 [t.me/blockchaincompliance](https://t.me/blockchaincompliance)

Business Meetings in Lugano (CH), Frankfurt (DE), Tallinn (EE), Amsterdam (NL), Milan (IT)



**Disclaimers and Copyright Statement.**

No reproduction or translation of this publication may be made without prior written permission. Applications for such permission, for all or part of this publication, should be made to:

**Blockchain ConsultUs Ltd.**  
Kemp House, 160 High Road  
London EC1V 2NX, England.  
[bulletin@blockchainconsultus.io](mailto:bulletin@blockchainconsultus.io)

**For further information,**  
please contact:  
[bulletin@blockchainconsultus.io](mailto:bulletin@blockchainconsultus.io)

