convex

Kidnapping risk in the cryptocurrency world

June 2025

Executive summary

The cryptocurrency sector is fraught with concerns over privacy and security, particularly due to individuals broadcasting their wealth as “crypto billionaires” on social media. This behaviour is primarily seen in individuals seeking to build an influencer profile, but even industry figures with greater awareness of the need for privacy can be at risk.

A surge of kidnappings in France has highlighted these risks, with notable violent incidents involving crypto billionaires. Such high-profile cases might be just the tip of the iceberg, with others going unreported.

Historically, violent cryptocurrency-related incidents tended to take place outside Europe and typically involved robbery rather than kidnapping. These trends have shifted, driven by the increasing value of Bitcoin since 2022.

Organised crime groups are believed to orchestrate many, if not all, of these kidnappings. The dark web plays a crucial role, as it facilitates payments and information exchanges about potential targets. Unlike traditional billionaires, who rely on banks to secure their financial assets, crypto billionaires are in full custody of their holdings, making them vulnerable to physical threats.

Criminals identify targets through dark web data breaches or displays of wealth on social media. Influencers and investors are particularly vulnerable, given that flamboyant lifestyles are an effective way of garnering followers. However, even if an individual is careful, family members of crypto participants are frequent targets. Furthermore, the links between cryptocurrency and organised crime can place unsuspecting individuals in dangerous situations.

Prevention strategies include maintaining strict online privacy, situational awareness, avoiding in-person trades with unknown parties, and standard security precautions. Security experts also recommend spreading holdings across multiple devices and locations to mitigate risks.

Wave of kidnappings in France

A spate of kidnappings and attempted kidnappings in France targeting individuals known or perceived to be crypto billionaires has brought the spotlight onto the sector. As is common with kidnapping cases, in the experience of Convex, these high-profile incidents are likely to be only part of the total, with others going unreported.

Two cases were especially notable owing to the violence employed to extort payment:

- On 21 January 2025, a former crypto start-up founder and his partner were abducted from his home in the French countryside; the perpetrators cut one of his fingers off and sent a video of it with the ransom demand.
- On 1 May 2025, in what was either a copycat crime or one planned by the same criminals, the father of a crypto investor was abducted in Paris into a van, and also had his finger cut off.

In both these cases, the police were able to locate and rescue the victims, arresting the perpetrators. Reportedly, the ransoms were either not paid or the transactions blocked. In a statement concerning the January case, the French police said that most of the suspects had a criminal record; additionally, according to some reports, the suspects did not know each other prior to committing the crime.

Then in April, the police announced that two additional suspects had been indicted: the organiser of the kidnapping, an individual known as “Le Mex”, and his partner. “Le Mex” had already been in prison for another kidnapping in 2023, following broadly the same modus operandi – although the victim was not mutilated that time. In that case, the victim was the father of a popular French streamer known for apparently having made millions playing casino games online.

Escalation in crime as crypto gains value

The fact that the alleged mastermind of the January 2025 abduction had already committed a similar crime in 2023 shows that using the internet to locate and target wealthy individuals is not new. Crypto billionaires, in particular, have been the targets of crime from the start, owing to the close interrelation between the crypto world and the internet. Crimes targeting holders of cryptocurrency, especially Bitcoin, go at least as far back as 2014.

In the 2010s, a fair share of violent cryptocurrency-related incidents took place in areas with a high prevalence of Russians and Ukrainians, including holiday spots favoured by these groups in South-East Asia (Thailand, Vietnam).

In the late 1990s and 2000s, Russia and Ukraine both saw the rapid growth of a technologically sophisticated cohort, out of which grew many IT companies now with global reach, such as Kaspersky or Grammarly. Simultaneously, in these two countries, organised crime also flourished, penetrating a wide range of sectors. In this environment, new IT millionaires, including crypto millionaires, became attractive targets.

Perhaps understandably, incidents involving obscure IT billionaires from former Soviet states did not, for the most part, make headline news in Western media. However, incidents involving cryptocurrency holders in the US also flew under the radar. The reason for this is primarily that, in the 2020s, there has been an escalation in three main dimensions:

- Severity – previously, the incidents involved mainly armed robbery, and the sums extorted from victims were relatively small; now, kidnappings are on the increase, and the ransoms demanded are large
- Geography – cases are now more frequently taking place in western Europe as opposed to the wilds of Ukraine and Thailand
- Targets – high-profile figures in cryptocurrency as opposed to obscure individuals

This escalation in recent years has been driven by a rise since 2022 in the value of Bitcoin, in particular. It is worth noting that many lesser-known cryptocurrencies have crashed in value, so criminals mainly target known or perceived holders of Bitcoin.

Organised crime and the crypto world

The French police believe that, at least in some cases, the kidnappings are ultimately organised by criminal groups based outside of France. Organised crime and cryptocurrency are inevitably linked owing to the fact that cryptocurrencies are the main method of payment on the dark web – which, as a result, has been a key factor in the growth and spread of bitcoin.

The dark web is also said to be the main hub for organising these kidnappings. Criminal structures offer payment in exchange for information on crypto billionaires.

Crypto billionaires – as opposed to normal currency millionaires – are attractive because they are essentially their own vault, whether they have their holdings in a software or a hardware wallet.

Whereas a “normal” billionaire essentially outsources the physical security of his financial assets to the banks, crypto billionaires are the custodians of their own safes. This makes them vulnerable to kidnapping and to the so-called “$5 wrench attack”: a criminal finds out someone has substantial cryptocurrency holdings, and threatens to beat them up with a wrench until they have revealed all their passwords and crypto keys.


-1104
SL
Long
+1104

Modus operandi

Step one: preparation

The first step is to identify the potential targets. As noted above, rewards for information are posted on the dark web; this has created an industry of hackers attempting to break into cryptocurrency exchanges to obtain the names and addresses of clients.

On 15 May 2025, leading digital currency platform Coinbase announced it had suffered a data breach affecting a "small subset" of its customers. Although the intent behind the attack was to extract a ransom from Coinbase, the company's refusal to comply means that the data – containing names, addresses and emails – are likely to be on the dark web now.

However, paying for information is not the only recourse available to criminals looking for targets. Relevant information is also freely available on social media: many people involved in cryptocurrency trading have – or have had until now, at least – a propensity to boast about the value of their holdings.

These individuals tend to be investors and influencers, who rely on attracting followers and therefore need to be seen to be living fabulous lifestyles (of course, this can have unintended consequences: influencers pretending to have more cryptocurrency holdings than they have put themselves at risk).

Given their necessary high level of exposure on social media, influencers/investors are easier targets than CEOs and entrepreneurs in the crypto world, whose lifestyles and security protocols are more in line with those of other wealthy businessmen. Consequently, despite high-profile exceptions, most of the reported crimes involving holders of cryptocurrency have targeted investors, influencers and traders.

There is nonetheless an additional vulnerability shared by all types of crypto participants: family members. Since December 2024, of five kidnapping incidents in France and Belgium reported in the press, four involved relatives of the target; in one of these cases, the target himself lived in Dubai. Such cases are essentially a version of what is sometimes referred to as 'tiger kidnapping'. This is a highly targeted kidnapping involving the abduction or holding of a hostage (or claim to have done so) with the intention of forcing an employee, relative or another to facilitate the immediate theft of any valuables, or to concede some other form of ransom from an organisation or individual. The term 'tiger kidnap' is thought to derive from the fact the perpetrators stalk their prey to study their movements before striking.

All the above shows the importance of not disclosing any kind of personal information online; moreover, it can be equally important not to discuss the extent of one's crypto currency holdings in person, especially at conferences, but more broadly as well.

Case study: Costa del Sol, 2025

A cryptocurrency broker based in London and vacationing in Marbella got chatting to three British men in his hotel bar. They arranged to meet for a meal, and afterwards, the men invited the trader back to their house for drinks. The trader was then bound and asked for a ransom of EUR30,000, to be collected by raiding his clients' crypto wallets.

The victim said he needed to call a client to access his crypto wallet, but instead called a friend in London and, speaking in Hindi, told him he had been kidnapped. As a result of this call, the Spanish police were able to rescue the broker. The police found more than EUR8,000, weapons and 25kg of cocaine in the house.

The Spanish police, who rescued the victim, believe that the gang planned the abduction after the victim told them what he did for a living during the initial chat.

Step two: execution

As cryptocurrency extortions escalated from armed robbery to kidnapping, the initial methods employed tended to involve home or work invasions. However, one feature of the spate of kidnappings in France is that abductions on the street are the preferred approach.

Usually, armed perpetrators unload from a van, into which they drag the victim; in all the publicised street abductions, this has happened in broad daylight. Often, the van has the livery of a known delivery service, such as the national post office or UPS. The victim is then driven far away (often to a different urban centre) and held at a location controlled by the kidnappers.

The method is crude and not always successful. On 13 May, three assailants alighted from a delivery van and tried to grab a woman; she was, however, with her husband, and the two of them resisted the attack until passersby began to gather, and finally, a neighbouring shopkeeper came out and threatened the criminals with a fire extinguisher. The kidnappers drove away, but the incident was caught on several cameras and reignited public alarm over the kidnappings.

Prevention

As well as adhering to general principles of personal security, including being aware of the threat, maintaining situational awareness and maintaining a low profile, the most important focus in terms of prevention is the pre-offence stage where perpetrators engage in lengthy target selection and planning. For this reason maintaining information security and strict standards of online privacy and discretion are key.

Even where an individual has been careful, the infiltration of criminal elements into the world of cryptocurrency and the anonymity that is at the heart of the cryptocurrency model mean that any counterparty could prove to be high risk. In particular, any unknown counterparty that requests an in-person (OTC) trade should be avoided. Other standard security precautions apply, such as being especially cautious on dating apps.

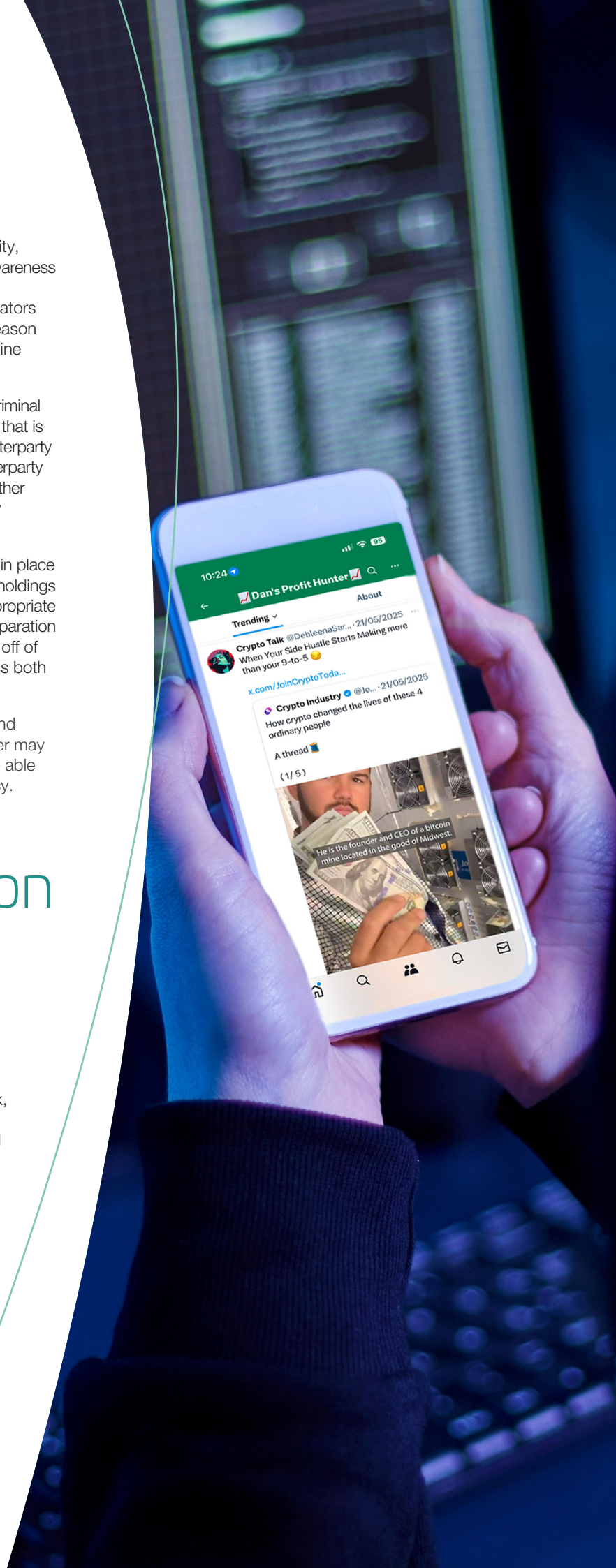
It is also recommended that those who might be at risk put in place precautions for a worst-case scenario, including spreading holdings across multiple devices and locations and ensuring that appropriate risk management controls are established (for example a separation of delegations and approvals to include multi-director sign off of significant transactions). These risk controls should address both corporate and personal wealth and holdings.

Finally, they should also consider how they would report and escalate incidents, including where they or a family member may be acting under duress, and how they can ensure they are able to access specialist crisis response advice in an emergency.

Further information and advice

If you would like to discuss any of the issues raised in this paper, contact **Convex Crisis Response: crisisresponsemanagement@convexin.com**

In the event of a suspected kidnap, threat, extortion, hijack, hostage situation, malicious detention or disappearance, Convex clients should call the 24/7 Operations Centre and ask to speak to the Convex Response Duty Officer.



Convex Insurance UK Limited

52 Lime Street, London EC3M 7AF
+44 (0)20 3886 0560

Convex Re Limited

Point House, 6 Front Street, Hamilton HM 11, Bermuda
+1 441 232 0112

Convex Europe S.A.

37 Boulevard Joseph II, 2ème étage,
L-1840 Luxembourg, Grand-Duchy of Luxembourg
+352 27 86 22 76

Convex Guernsey Limited

Bucktrout House, Glategny Esplanade, St Peter Port, Guernsey, GY1 1WR

convexin.com

06_25/Cryptocurrency Kidnap Document/GC