**Crypto firm** moved $4.2m of **assets** to digital wallet linked to **alleged** **Russian arms dealer**

Analysis shows link between Copper Technologies and Jonatan Zimenkov, who was later **hit with US sanctions** over Ukraine **invasion**

A cryptocurrency firm transferred digital assets worth more than $4.2m to a crypto wallet belonging to a member of an alleged Russian arms-dealing network who was later **hit with US sanctions**, it can be revealed.

Details of the transactions involving Copper Technologies raise questions about whether UK laws governing crypto have adapted quickly enough to keep pace with a rapidly **evolving** sector that has come under increasing **scrutiny** over **the level of anonymity** it can provide.

Analysis of crypto records by the Guardian and the International **Consortium** of Investigative Journalists (ICIJ) highlights a connection between one of the most **prominent** cryptocurrency companies and Jonatan Zimenkov, **an Israeli-born Russian national.**

Zimenkov, 29, **was subjected to**[**US sanctions**](https://ofac.treasury.gov/recent-actions/20230201)in February 2023 for allegedly assisting the Russian military with the invasion of Ukraine, as part of the “Zimenkov network” – **an arms-dealing** and **sanctions evasion network** headed by his father, Igor Zimenkov.

Records show Copper transferred millions of dollars worth of **digital currency** inMay 2021 to a wallet that has since been identified as belonging to JonatanZimenkov. Sanctions **were imposed on** him 19 months later. Copper, which **recruited the former chancellor of the exchequer Philip Hammond**, as an adviser in October 2021, was based in London at the time of the transfer, but has since moved to **Switzerland**.

While Zimenkov was not subjected to sanctions when the transaction took place, the US Treasury department’s Office of Foreign Assets Control (OFAC) has said **it believes the network had been active over several years by the time it imposed restrictions on 22 individuals and entities in multiple countries.**

In its **citation**, it said the Zimenkov network had been involved in multiple deals for Russian cybersecurity and **helicopter sales abroad**, as well as attempts to supply weapons to **an unnamed African country**.

**There is no suggestion that Copper breached any sanctions or any other regulations in place at the time of the transaction.**

However, **the revelation shines a light on the opaque world of cryptocurrency** and the anonymity it can offer, as well as raising questions about how **digital assets** and transactions involving them should be regulated **within the wider financial system**.

“Copper **takes its compliance, legal and regulatory obligations very seriously**, and has acted **in full compliance with** all applicable **regulatory standards**, including all applicable **sanctions prohibitions**, in the UK,” a spokesperson for the company said.

The Guardian and ICIJ understand that Zimenkov was not a Copper client, meaning it did not have a regulatory obligation to check his identity. The company did not answer specific questions about the **nature** of its relationship with Zimenkov.

Financial companies have the option to file a suspicious activity report (SAR) when a transaction **raises any red flags**, even when the rules are not obviously breached. It is not known if Copper filed a SAR, which must be sent to **a law enforcement body** such as the UK’s National Crime Agency.

According to guidance issued in 2020 by the finance industry’s joint money laundering steering group, it was considered “**good practice**” for crypto firms to gather information about the recipients of transfers to assess potential risks.

But it was not until late 2023 that the UK also adopted a travel rule obliging crypto companies to carry out checks on funds transferred to external parties, after concerns from regulators that this risk was being **overlooked.**

Transfers of digital currency such as **bitcoin** and **ethereum are logged on** a **blockchain**, the digital **ledger** that **underpins** the cryptocurrency ecosystem. While transactions are recorded, they can also provide anonymity to people trying to **disguise** financial relationships because funds are held in online wallets that do not have to be matched to the **holder’s identity**.

**Blockchain logs** show that in May 2021 Copper transferred more than 1,700 units of ethereum, worth more than $4.2m at the time, to Jonatan Zimenkov. **They were transferred in**[**two**](https://etherscan.io/tx/0xf68ee46abb732dc1f148142251e83aa730cae3daca0a09fa393eb7e74bce4c27)[**transactions**](https://etherscan.io/tx/0xd8d5cbf151c49db5c756a006cd816df9f7ae38b2489edc53d7a2fef6fe1fb682)**on the same day**, according to the blockchain analytics platform Etherscan.

The purpose of the transactions – and the original source of the digital assets – is unclear. Zimenkov did not **return any requests for comment.**

The owner of the wallet that received the ethereum transactions is not named in blockchain records, which only show their digital currency address – **a string of letters and numbers**.

That same address was included in a [US Treasury announcement in February 2023](https://ofac.treasury.gov/recent-actions/20230201), **detailing** sanctions against the Zimenkov network.

Details of the alleged Zimenkov sanctions **evasion** network revealed by the US highlight the potential benefit of **verifying** the identity of people on the other end of such **asset transfers**.

The address was listed as belonging to Jonatan Zimenkov, who held Russian, Israeli and Italian **citizenship**, according to **US authorities**. He attended **college and university** in London, according to a **brochure** for a private school.

The Treasury claimed the Zimenkovs “engaged in projects connected to Russian defence capabilities, including supplying a Russian company with **high-technology devices** after Russia launched its **full-scale invasion** of Ukraine”.

**In its sanctions announcement**, the US Treasury said the Zimenkov network supported the Russian defence exporters Rosoboronexport and Rostec, both of which were subjected to sanctions.

According to the US Treasury, Igor Zimenkov worked closely with his son and others “to enable **Russian defence sales** to third-country governments.” Jonatan Zimenkov had **maintained power of attorney for companies** in the network on behalf of his father, the department noted.

Russian public corporate records show that Jonatan Zimenkov was registered as an “individual entrepreneur” in the country in 2019, **conducting business activities** including “**wholesale** trade of ships, aircraft and other vehicles”.