# Meet the guy uncovering crypto's biggest thefts

Rich Sanders is the closest thing the cryptoworld has to 911.

*By Amanda Hoover*
*August 4, 2022*

Ian Balina was reviewing initial coin offerings, the crypto industry's equivalent of an initial public offering, live on YouTube in 2018 when a hacker emptied around $2 million worth of cryptocurrency from one of his wallets. It may have been his old college email address that he used as a backup to another account that made him vulnerable. His bravado about his accumulated wealth likely didn't help.

When a viewer noted in the comments that his wallet had emptied, Balina said he thought he was being trolled. But he checked and saw that the funds had vanished, he later said in a YouTube video detailing the hack.

It was a humiliating mistake for a prominent crypto evangelist who wrote the book on crypto investing. But these fumbles aren't unusual, particularly for the uninitiated who might store their wallet keys poorly or send crypto to fake investors who promise them tempting but unrealistic returns. Once the crypto is gone, they have little recourse to recover their investment other than calling people like Richard Sanders.

Sanders is the kind of guy you seek when all your apes are gone. He and his company, CipherBlade, investigate digital thefts of $100,000 or more and

other online crimes by scouring blockchains, or digital public ledgers that record every transaction and change-of-hands cryptocurrencies make.

Sanders specializes in blockchain forensics. He took on the Balina case and followed a group of teen hackers to a Discord channel. He joined it, pretending to be a 19-year-old woman, gained their trust, and ultimately learned how they carried out the scheme. (Balina did not respond to a request for comment about where his case stands now and what role CipherBlade played, but he said on YouTube in 2021 that the hackers had been caught. The FBI did not respond to a question regarding criminal charges related to the case.)

CipherBlade is the closest thing to 911 the cryptoworld has. The schemes Sanders and his investigators uncover can be fraudulent investments run by people posing as crypto traders or wallet hacks and breaches on cryptocurrency exchanges—easy money handed to thieves by lax storage of wallet keys. But there are also romance scams, embezzlements, ransomware attacks, and blackmail, where people get others to willingly shell out crypto and then run off with the loot. There are also soon-to-be ex-spouses hiding money from one another in crypto.

Sometimes, Sanders's work is clearing the names of crypto exchanges that are accused of money laundering. At others, it's following money on the blockchain used for crimes as devastating as human trafficking. In the new world of digital wealth, riffs on classic crimes flourish. The calamitous difference for victims, though, is that government investigators have been largely ill-equipped to dig into these scams, and the decentralized nature of crypto means there's no institutionalized protection for investments.

US consumers lost more than $1 billion in cryptocurrencies to fraudsters between January 2021 and March 2022, according to the Federal Trade Commission, and $14 billion was stolen worldwide in 2021, according to Chainalysis, a leading blockchain data platform. In February, the FBI launched a virtual assets unit, and in May, the SEC said it would nearly double the size of its Crypto Assets and Cyber Unit, reaching a grand total of 50. Officials have

seized more stolen crypto than they can manage, and the federal government in 2021 had to contract a bank capable of storing and liquidating the assets.

But even that very bank, Anchorage Digital, later came under fire for failing to follow anti-money laundering regulations. In the tangled web of blockchains, government investigations move slowly. Federal agents take on crypto scams as just a subset of the broad range of thefts they investigate. Sanders's operation, which includes nine people, is far more nimble.

Even a blockchain sleuth has limitations. As a private enterprise, CipherBlade lacks subpoena power. Sanders can't go rogue and facilitate the return of money. Instead, he's a new kind of go-between, a private investigator for the growing number of people who are losing wealth in crypto.

"We basically hand these cases to law enforcement on a silver platter," he told Morning Brew. "We say, 'We have done everything for this individual shy of doing things that we don't have the legal power to do.'"

Government officials have been slower to catch up, but they are getting better at investigating and prosecuting crypto cases. In February 2022, officials announced the FBI's largest seizure ever: $3.6 billion related to a 2016 hack of the virtual currency exchange Bitfinex. Many associate bitcoin with anonymity; the very online couple behind the money laundering in that scam, Heather Morgan and Ilya Lichtenstein, showed the world how untrue that was.

It's highly traceable, especially for experts like Sanders, and that makes finding criminals even easy in some cases. Wallets seem anonymous, but after a heist, people will often want to convert crypto to cash. This is usually done on major exchanges that require KYC, or know your customer, regulations that mandate people supply identifying info. But even with added attention, law enforcement can't bring all the crypto scammers to justice.

“As [much as] law enforcement is going to increase the amount of resources that it’s going to devote to this issue, it’s never going to catch up,” said Tal Lifshitz, an attorney who focuses on cryptocurrencies and digital assets. “There’s always going to be a space for private investigators, private lawsuits, and litigation to fill in the gaps for the cases that the government is just not going to pursue.”

Cue people like Sanders. He started as an enthusiast and has grown to a full-time investigator. The 32-year-old isn’t some pseudonymous online persona. From his home office in Pittsburgh, he talks fast, detailing complicated crypto scams—and how not to become a victim who needs to hire him. This is where he digs into scams and crimes from around them the globe. (He’s also a devoted Swiftie, and his office doubles as a dance floor when he takes breaks from analyzing blockchains to dance to “Shake It Off”.)

Former military, Sanders said he enlisted in the Army at 17 and served in Iraq and Afghanistan. He went on to work in psychological operations for the Army. That’s where he learned to find “unconventional solutions to unconventional problems,” he said, a skill that translates to hunting down crypto on blockchains. “There was no playbook for these types of investigations. We have made the playbook.”

Sanders won’t say exactly how he got into blockchain forensics and learned to scour the web for these transactions. There’s no direct pipeline to this kind of work. But he did say he started CipherBlade in 2017 after helping some friends in the crypto world who had been hacked or scammed. Word spread, and Sanders had more work than he could manage as a solo blockchain enthusiast, he said.

CipherBlade now boasts connections to Chainalysis and other big investigative players in the blockchain world, and has been contracted by the US government to serve as an expert witness (it’s one of several companies to which the government has cumulatively paid out millions of dollars to

investigators. The case Sanders was hired for is ongoing, and he declined to elaborate on its nature until it closes).

In addition to hackers, Sanders said his firm investigates civil cases, like divorce proceedings where a spouse has hidden cash by investing in cryptocurrency. There are also romance scams that climb into the six-figure range. Sanders said he has received reports from people seeking his investigative skills, but can't help them if they don't want the authorities involved; for instance, if they are concerned about having committed tax evasion.

"Bottom line is this: We are not a rogue agency…we operate within the limits of the law," Sanders said.

But it's not just about chasing wealth for people who forgot to lock up their wallets. Sanders works with the nonprofit Anti-Human Trafficking Intelligence Initiative. He looks at the wallet addresses the initiative has scraped from the dark web and analyzes them, seeking links to crypto exchanges, like Coinbase. Then, law enforcement can use that information to subpoena identifying information to make arrests of buyers and traffickers.

The impeccable nature of the blockchain's record-keeping brings new light to perpetrators of crimes like these. Instead of using bitcoin to buy and sell exploited material anonymously, people are often leaving paper trails.

"When it comes to blockchain analysis, it's not just about going after these pots of gold of hundreds or thousands of bitcoin and getting somebody super wealthy," he said. "I'm personally going to have, as just one example, a hell of a lot more interest in a bitcoin wallet that processes even several hundred dollars for child exploitation material or terror financing than a wallet that processes, let's say, 100 times that amount for scam proceeds."

In the world of scams, though, the magnifying glass has been turned onto Sanders. CipherBlade wrote a report disputing findings of The Wall Street

Journal that claimed a crypto exchange, ShapeShift, had allowed unfettered money laundering on its platform. (The report contended The Wall Street Journal had overestimated ShapeShift's problem.) Some sleuths went looking into CipherBlade's background and questioned the company's claims of recovering millions in stolen crypto and credibility, but had no evidence to contradict it. It's not surprising that someone akin to a crypto bounty hunter might raise eyebrows. Sanders thinks skeptics are right to have questions and poke holes in the industry.

"I actually agree with a lot of them a lot of the time," he said, in relation to the skeptics. "But that's kind of the ironic thing—I've actually taken their side on quite a lot of things against my industry. They are right: This industry needs a whole lot more skepticism."

Sanders himself is a crypto industry skeptic but a blockchain believer. He has spent enough time embedded there to see the tech's power and potential, but has also seen too many people make mistakes. "I'm so frustrated because the technology behind this, the underlying technology, is fascinating, amazing. And I am a true believer in blockchain tech," he said. "If you look at the industry right now, the majority of the volume and the participants are speculative investments. And that's not a good look."

But as long as there are scams and rug pulls and mysteries to uncover on the blockchain, there's work for Sanders.