

Keys, clues and crypto: How ASU researchers are building smarter tech

Professor Gail-Joon Ahn leads team of digital detectives who work the bitcoin beat

By Kelly deVos, ASU News
May 27, 2025

The cybercrooks who haunt the digital shadows can use cryptocurrency to move fortunes under the radar, with no strings to hold them back.

For those looking to dodge detection, crypto isn't a curiosity — it's the perfect getaway car: [fast, silent and anonymous](#).

[Gail-Joon Ahn](#) — a professor of computer science and engineering in the [School of Computing and Augmented Intelligence](#), part of the [Ira A. Fulton Schools of Engineering](#) at Arizona State University — is a cybersecurity thought leader who has spent his career devising innovative ways to protect and enhance computer security systems.

Now, he's turning that expertise to one of the field's most pressing challenges: stopping that cybercrook getaway car in its tracks.

[Cryptocurrency](#) is a type of digital money that operates without a central authority like a bank or government. Instead, it uses a technology called [blockchain](#), a digital, decentralized ledger that records every transaction across a network of computers. When someone sends cryptocurrency, the transaction is verified by network participants, then permanently added to the blockchain. Because these transactions don't require personal information like names or locations, the system allows for easy and often anonymous transfers of value.

“Legitimate users turn to cryptocurrency because it's irreversible, secure and efficient,” Ahn says. “Unfortunately, these same attributes are attractive to those who want to commit financial fraud.”

For the past decade, the team in the [Center for Cybersecurity and Trusted Foundations](#), or CTF, founded by Ahn in 2015 and currently led by Fulton Schools Associate Professor [Adam Doupé](#),

has been doing a deep dive into the world of crypto-funded cybercrime.

Following the money

It was the 2014 [CryptoLocker attack](#) that first got the cybersecurity expert's attention.

CryptoLocker was a notorious form of ransomware that typically spread through malicious email attachments. Once opened, the malware silently encrypted the user's files using strong cryptographic algorithms. Victims were then presented with a ransom demand: Pay a specified amount in bitcoin within a tight deadline, usually 72 hours, or lose access to their files forever. The malware was especially dangerous because the encryption was virtually unbreakable without the private key held by the attackers.

Ahn theorized that cybersecurity professionals could identify and track payments made to the malware's operators. By analyzing information from the blockchain, including time stamps and payment patterns, the researchers found 795 ransom payments totaling 1,128.40 bitcoin — worth about \$310,472 at the time of the transactions.

Their work showed that bitcoin was not truly anonymous and that careful analysis of blockchain data would reveal surprising connections and insights.

Out to prove that blockchain data could empower digital detective work, the team continued on. They found that the CryptoLocker hackers didn't just collect ransoms; they moved the money around to hide their tracks. The researchers mapped the flow of cryptocurrency from victim payments to various central wallets where the money was pooled.

One of the most intriguing findings of the team's early research was a possible link to the [Sheep Marketplace scam](#), where about 96,000 bitcoin, worth more than \$100 million at the time, was stolen. Though there was no direct evidence that the same group was behind both crimes, the interconnected money flow found by the ASU researchers suggested some collaboration.

"To us, the links between various bitcoin-based cybercrimes pointed to the existence of an ecosystem where deviant actors share resources or methods," Ahn says.

Patented protection

It's one thing to chase threats, but preventing cybercrime is Ahn's real goal.

As work progressed, the researchers turned their attention to creating new solutions to protect cryptocurrency transactions. In 2023, Ahn and the team received a patent for their project, "Systems and Methods for Blockchain-Based Automatic Key Generation."

They created a new way to generate secure digital keys using information already stored in the blockchain. Instead of relying on a central server, Ahn's system picks a random piece of data that everyone on the network can see but no one can predict.

This data is used like a seed to create a unique security key. Because the seed comes from shared blockchain records, users can generate matching keys without needing to send secret

information over the internet. The seeds change often, keeping the system secure and avoiding delays or single points of failure.

Moving forward, Ahn and the team are exploring collaborations with state and local law enforcement agencies. The team is also investigating how their patented technology can be further leveraged to monitor and detect any malicious activities within blockchain-based transactions. Such early-warning capabilities would significantly contribute to building more secure and resilient cyber communities.

[Nadya Bliss](#) — the executive director of the [ASU Global Security Initiative](#), where CTF's work is concentrated, and a professor of practice in the School of Computing and Augmented Intelligence — says that it's important to both study threats and create tools to tackle them.

“Cyber defense is a game of catch-up, with bad actors often having an advantage. Researchers like Gail are working to change that, though,” Bliss says. “This kind of research — producing novel, innovative tools with real-world application — is exactly what is needed.”

Ahn hopes that the techniques developed by the researchers can help in future investigations. As cybercrime continues to evolve and grow, so must our tools for understanding and combating it.

“It's a bit of a cat-and-mouse game,” Ahn says. “But it's essential for us to track down the mouse.”

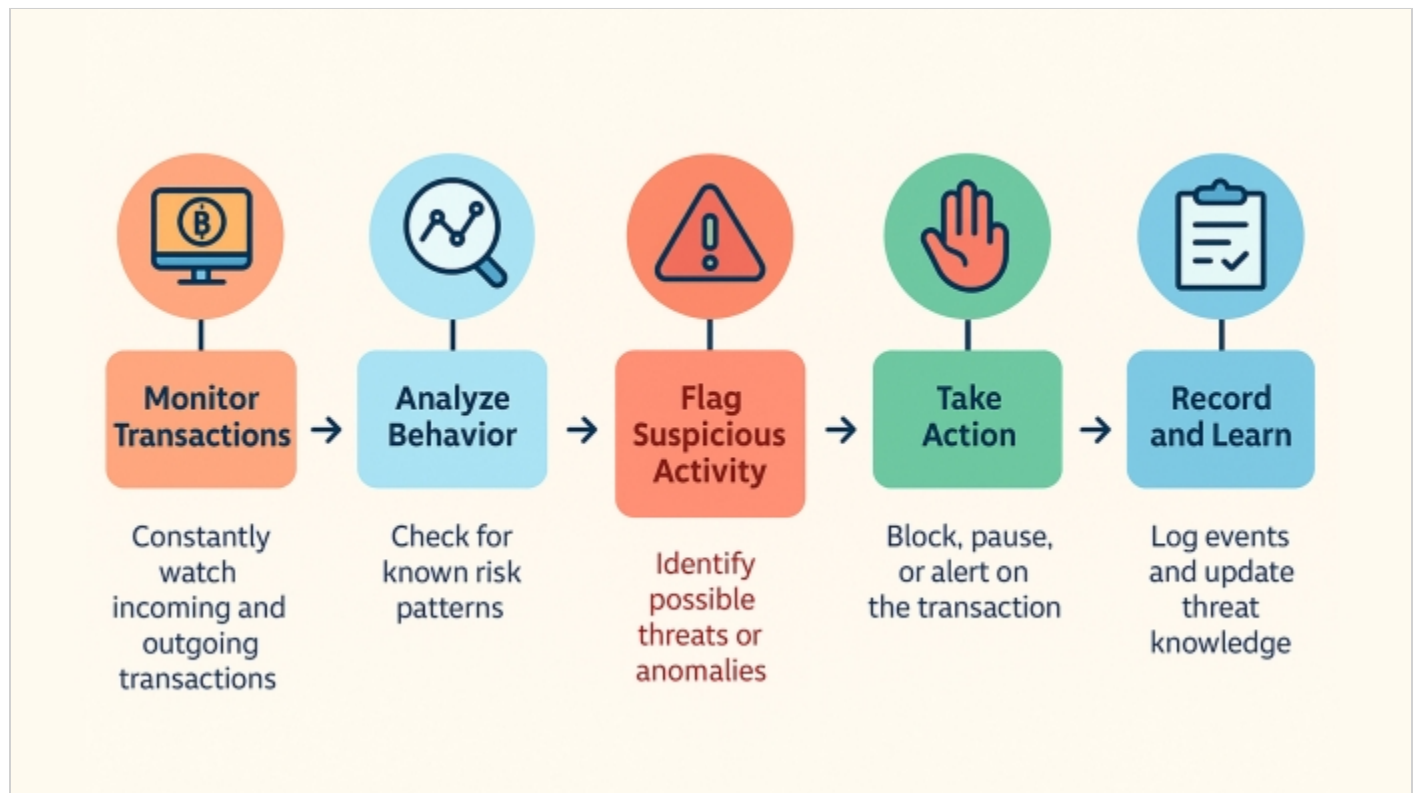
This story originally appeared on [ASU News](#).

Main image



Gail-Joon Ahn, a professor of computer science and engineering in the School of Computing and Augmented Intelligence, is leading a team of researchers who are devising ways to track and protect payments made via cryptocurrency. The team seeks to bolster law enforcement efforts to stop cybercrime. Graphic by Andrea Hesser/ASU

Text image(s)



An illustration shows the research underway by Ahn's team. The researchers are exploring how their solutions can be expanded to further protect blockchain transactions, creating innovative payment processing solutions that watch for suspicious behavior and block exchanges before damage is done. Graphic by Kelly deVos/ASU