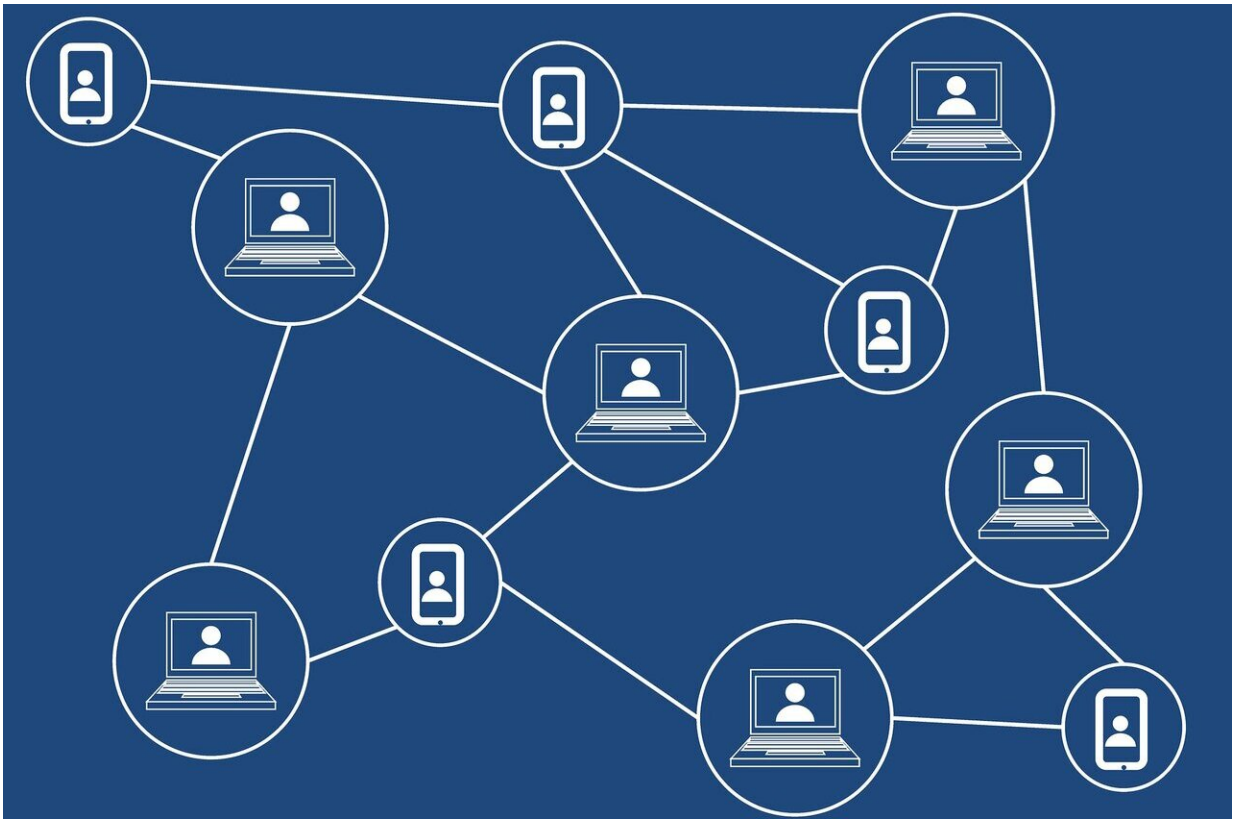
Privacy 'poisoning' poses threat to companies using blockchain

April 10 2019, by Henry Kenyon



Credit: CC0 Public Domain

A new type of cyberattack that can render blockchain technology unusable may become a major headache for organizations that depend on it.

Known as privacy "poisoning," the attack involves loading private data, such as names, addresses and credit card numbers, or illegal material, such as child pornography, into a blockchain, therefore putting the network in conflict with local laws. The result is that the affected chain with all of its contained data cannot be used unless expensive and time-consuming steps are taken.

Blockchain is a digital ledger of transactions run on a network of computers with no centralized governing or regulatory authority. It's run by those who use it. The technology is increasingly being explored by banks and financial services firms, governments and startup businesses for its potential to improve the effectiveness of payment systems while cutting costs.

A factor in the rise of blockchain poisoning is the introduction of strong data privacy laws such as the European Union's General Data Protection Regulation, or GDPR, and California's Consumer Privacy Act, or CCPA. Both allow consumers to request that personal data held by a company be deleted or erased.

This is a problem for blockchain systems because they are designed to prevent changes to past transactions, and there is no central authority charged with correcting problems. So-called public blockchains such as those that underpin cryptocurrencies like bitcoin and ether are most at risk because anyone can participate. Participants in private blockchains must be invited and validated by the network starter.

Bart Willemsen, an analyst with research firm Gartner Inc., said the one-two punch of privacy poisoning and privacy laws will hit public blockchains especially hard.

Willemsen estimated that by 2022, three out of four public blockchains will suffer privacy poisoning—inserted personal data that renders the

blockchain noncompliant with privacy laws. Businesses wanting to implement the technology must determine if any of the data being used falls under privacy laws, he said in an interview.

Under GDPR, individual privacy rights include the "right to be forgotten," which means that any personal data appearing publicly would have to be deleted.

"Organizations that implement blockchain systems without managing privacy issues by design will run the risk of storing personal data that can't be deleted without compromising chain integrity," according to a Gartner report.

Willemsen cited a story, which he admitted may be apocryphal, of a meeting by the European Commission where a participant paid for a pizza in bitcoin and the recipients thought it would be funny to immortalize the moment by putting their names in text fields that can be written into the bitcoin blockchain.

"You would indeed always be remembered, and therein exactly lies the problem," Willemsen said.

These text fields in public blockchains are indelible. Willemsen noted that what constitutes personal information covers many things, from names to unique references that can be traced back to an individual.

Willemsen said Gartner clients have had similar problems, though he declined to discuss the circumstances, citing confidentiality agreements.

Indelible vs. erasableIn addition to the California law, similar legislation, with strong consumer privacy protections, is pending in New York, New Jersey and Washington.

Businesses seeking to use blockchain as a secure solution may want to rethink, said Jenny Leung, a lawyer with Blakemore, Fallon, Garcia, Rosini & Russo in New York.

She noted that on Jan. 1, 2020, the CCPA will give California consumers the "right to erasure" which is similar to the GDPR's right to be forgotten, in that it allows people to request companies to delete any personal data they have stored. But information stored on a blockchain can't be erased, which can get companies into trouble with the law if they've launched or organized the blockchain-based service, she said.

The only way to delete the data may be through an elaborate "reforking" process, which moves the entire network to a new set of data and invalidates the old set.

Private blockchains are slightly more resistant to privacy poisoning, although it can occur. In those cases, any companies that are still connected to the ledger can force all the participants to join in a "hard fork" to erase the offending data. Or private blockchains can force all them to stop operating or destroy all copies of private keys to render the encrypted data permanently inaccessible, Leung said.

This process becomes too expensive and complicated for public blockchains, she said. It might take hundreds of millions of dollars to rent enough crypto-mining equipment to alter the network or orchestrate a hard fork by convincing the majority to move to a new chain that doesn't contain the affected data.

"It's not something you want to do every time you want to delete something," Leung said. "It's costly and time-consuming."

Besides malicious attacks, Willemsen noted that many instances will most likely be caused by human error and bad process design. It doesn't

matter under the GDPR if a blockchain exposed personal data innocently through an error, he said.

Once privacy poisoning becomes more widespread, Willemsen said he expects several things to happen. The first is that people will continue to disregard privacy practices the same way they do for other types of cybersecurity. Automated hacking tools may emerge from certain online communities to target exposed public blockchains or to render competitors' systems useless, he said.

Companies interested in using a public ledger may want to opt for private blockchains, said Randi Eitzman, senior threat pursuit analyst with FireEye iSIGHT Intelligence, a cybersecurity threat research and analysis service.

Blockchains are ultimately "just costly centralized data storage," Eitzman said in an emailed response to questions. "Firms looking for secure data storage might avoid using them depending on their cost-benefit analysis, but a simple solution would be to avoid storing any sensitive customer information on a blockchain."

Regarding attacks on public blockchains, Eitzman noted that easy-to-use tools that allow anyone to write and store data on-chain, such as Bitstagram, a mobile application that lets users upload their smartphone photos to a blockchain, already exist. With such tools, it wouldn't take much for someone to upload illegal content, she said.

"The benefit of a public ledger is that all transactions are easily viewable and can be tracked," she said. "Anyone who stores sensitive or illegal content on-chain is doing so at their own risk."