Silk Road wound through dark side of the Internet

October 3 2013, by Glenn Chapman

Bitcoin's minted to reveal a code are displayed in a shop on April 26, 2013 in Sandy, Utah

There is a dark side to the Internet, and it can be used for evil as well as for good.

A massive online bazaar hawking narcotics, weapons, forgeries, and other illicit items or services operated openly for years by relying on tools designed to safeguard privacy or foster a new world of Internet commerce.

Underground website Silk Road was seized by US authorities this week and its accused mastermind Ross William Ulbricht is to appear in federal court in San Francisco on Friday to determine whether he should remain in custody while the criminal case against him proceeds.

"Every technology has almost immediately been used to do bad things," said Alex Stamos, chief technology officer at Artemis Internet, which specializes in online security.

"People are going to do illegal stuff, but it turns out that it is really tough to run an eBay for drugs and not get caught."

Silk Road thrived on the principle that assurances of anonymity would free sellers and buyers to engage in transactions barred by law or frowned upon by society.

To accomplish this, Silk Road combined a Tor network for being invisible online with Bitcoin digital currency that can be as difficult to trace as cash trading hands in a dark alley.

"Part of the reason for the site's longevity is that it was hosted as a hidden service on the Tor network," Trend Micro security threat researcher Robert McArdle explained in a blog post.

Free Tor software lets people wrap data such as messages, website visits, or online transactions in layers of protection including encryption and then bounce it about machines in a worldwide peer-to-peer network to cover trails.

Each machine along the way only peels back a slight layer; enough to send the data to its next point in a journey

Tor community members volunteer their computers to provide relay points and the resulting network makes it a challenge to trace Internet activities.

"Tor is not only used for criminal and dubious purposes, but is also commonly used by those who wish to have a sense of anonymity online or who live in countries where access to the Internet is restricted," McArdle said.

Encrypting data and obscuring online identities has been highlighted by a scandal about US spy agencies snooping on the Internet in the name of fighting terrorism.

"It is very difficult to be anonymous on the Internet," Stamos said. "You basically have to be perfect. You screw up once and you are doing something illegal, and you are toast."

Along with giving buyers and sellers promises that none would know who they are in the real world, Silk Road required deals to be consummated with Bitcoins, an Internet Age version of cash. The four-year old currency is increasingly used to make payments in online transactions.

Bitcoins are created or exchanged using complex software protocols that have resulted in them being referred to as "cryptocurrency." While cash tends to be paper or metal, Bitcoins are snippets of code given value by scarcity and the faith that they can be traded for goods or services online.

Owners tuck the digital currency away in Bitcoin "wallets," programs

that safeguard the valuable code and allow it to be exchanged with other Bitcoin wallets.

There are a variety of "wallets" ranging from digital pouches tailored for smartphones to "vaults" hosted on secure servers online and backed up to prevent loss.

Bitcoin owners have private software "keys" needed to spend the digital currency, and transactions are publicly logged in what is called a "block chain" to help ensure the integrity of the process.

"It is not actually anonymous; it is pseudo-anonymous," Stamos said of using Bitcoins. "Every transaction is publicly viewable."

Silk Road tadded "Bitcoin Tumbler" software that jumbled data to make it even harder to determine which wallets digital currency came from.

The FBI reportedly confiscated approximately $3.6 million worth of Bitcoins from Silk Road.

While investigators did not release details regarding the seizure, they could do so by getting hold of devices or servers containing the Bitcoins or by breaking into wallets, which are typically password protected.

Ulbricht was arrested while using a laptop at a San Francisco library on Tuesday, and if he was logged into his account FBI agents could have gotten easy access to his stash of Bitcoins.

"People who do Bitcoins now, almost always crypto-geeks, get ripped off all the time and there is no way to undo a transaction," Stamos said. "It's a world where everyone keeps loads of cash and the only way to have Bitcoins is to be very well armed to protect them."

There is an estimated $1.5 billion in bitcoins on the market and the digital currency can be transferred directly between smartphones or any other type of computers, raising concerns by regulators it will be used for criminal or terrorist activities.