‘DARK WALLET’ IS ABOUT TO MAKE BITCOIN MONEY LAUNDERING EASIER THAN EVER

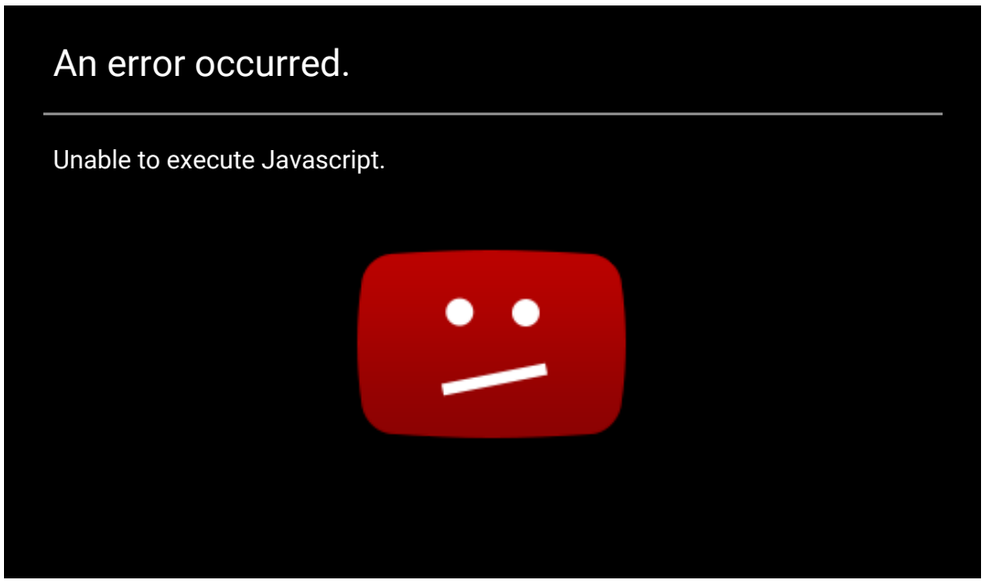
From left, Cody Wilson and Amir Taaki. *Photo: Julia Robinson/WIRED*

GOVERNMENT REGULATORS AROUND the world have spent the last year scrambling to prevent bitcoin from becoming the currency of choice for money launderers and black marketeers. Now their worst fears may be about to materialize in a single piece of software.

On Thursday, a collective of politically radical coders that calls itself unSystem plans to release the first version of Dark Wallet: a bitcoin application designed to protect its users’ identities far more strongly than the partial privacy protections bitcoin offers in its current form. If the program works as promised, it could neuter impending bitcoin regulations that seek to tie individuals’ identities to bitcoin ownership. By encrypting and mixing together its users’ payments, Dark Wallet seeks to enable practically untraceable flows of money online that add new fuel to the Web’s burgeoning black markets.

“This is a way of using bitcoin that mocks every attempt to sprinkle it with regulation,” says Cody Wilson, one of Dark Wallet’s two 26-year-old organizers. “It’s a way to say to the government ‘You’ve set yourself up to regulate bitcoin. Regulate this.'”

Here’s a teaser video the group posted earlier last week ahead of the software’s release:



Dark Wallet was conceived last summer by Wilson and Amir Taaki. Wilson first gained notoriety by creating the world's first entirely 3D-printed gun; Taaki is an Iranian-British free-market anarchist and developer of high-profile bitcoin projects like the decentralized online marketplace prototype DarkMarket. Together they launched a crowdfunding campaign on Indiegogo in October that raised $50,000, along with tens of thousands more in bitcoin. The accompanying video promised what Wilson described as "a line in the sand" in the struggle over bitcoin's political future. At a debate at New York's Museum of Modern Art in March, Wilson described his intentions for Dark Wallet more directly: "It's just money laundering software."

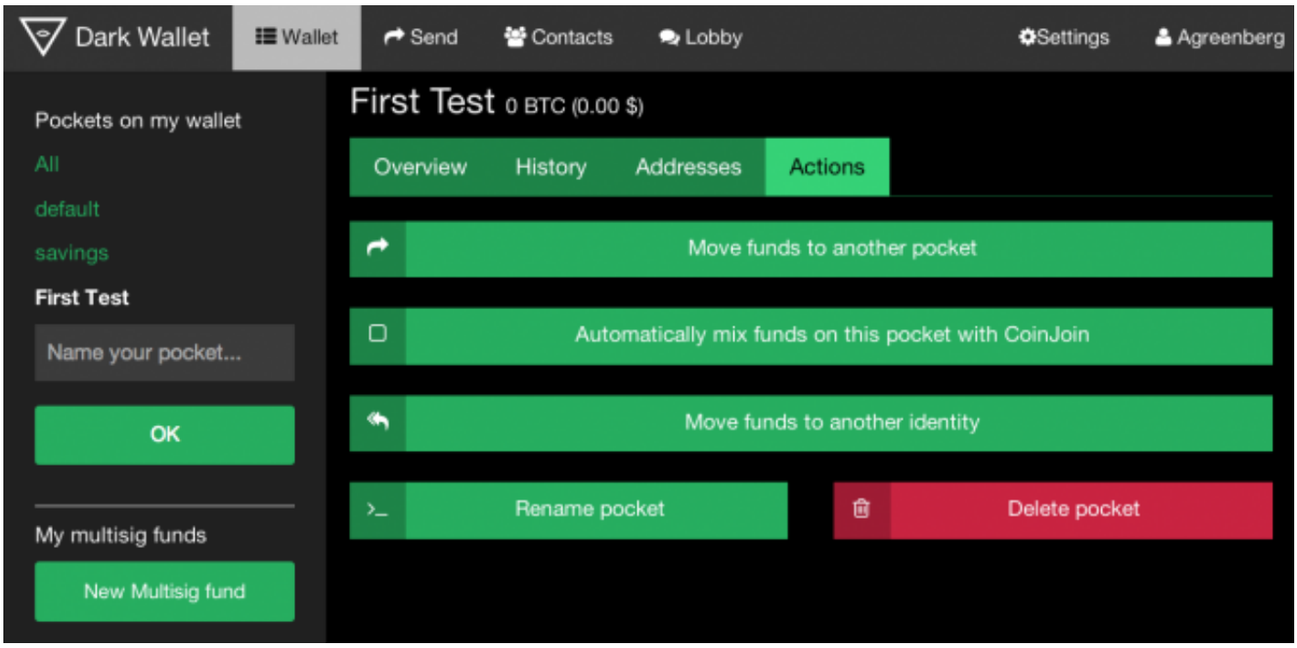
Despite those provocations, financial regulators have kept mum about the project. The New York Department of Financial Services, which held hearings about bitcoin in January and says it plans to create a "bitlicense" for some bitcoin-based businesses, didn't respond to a request for comment. In a statement to WIRED, the Financial Crimes Enforcement Network wrote only that it's "well aware of the many emerging technological efforts designed to subvert financial transparency. It's certainly our business to be interested and vigilant with respect to any activities that may assist money laundering and other financial crimes."

Wilson's and Taaki's money-laundering app is politically incendiary, but it's not necessarily illegal, and they argue that the code is protected by First Amendment safeguards on free speech. But Wilson states plainly that he intends Dark Wallet to be used for anonymous online black markets like the Silk Road, the bitcoin-based drug bazaar seized by the FBI in October. "I want a private means for black market transactions," says Wilson, "whether they're for non-prescribed medical inhalers, MDMA for drug enthusiasts, or weapons."

Nor does he deny that Dark Wallet might enable heinous crimes like child pornography, murder-for-hire, and terrorism. "Well, yes, bad things are going to happen on these marketplaces," Wilson says. "Liberty is a dangerous thing."

But as dangerous as Wilson's vision may be, Dark Wallet also fills a real need for privacy in the bitcoin economy. Despite its reputation as an anonymous currency, bitcoin transactions are in some ways nakedly public–even more so than those made with traditional money.

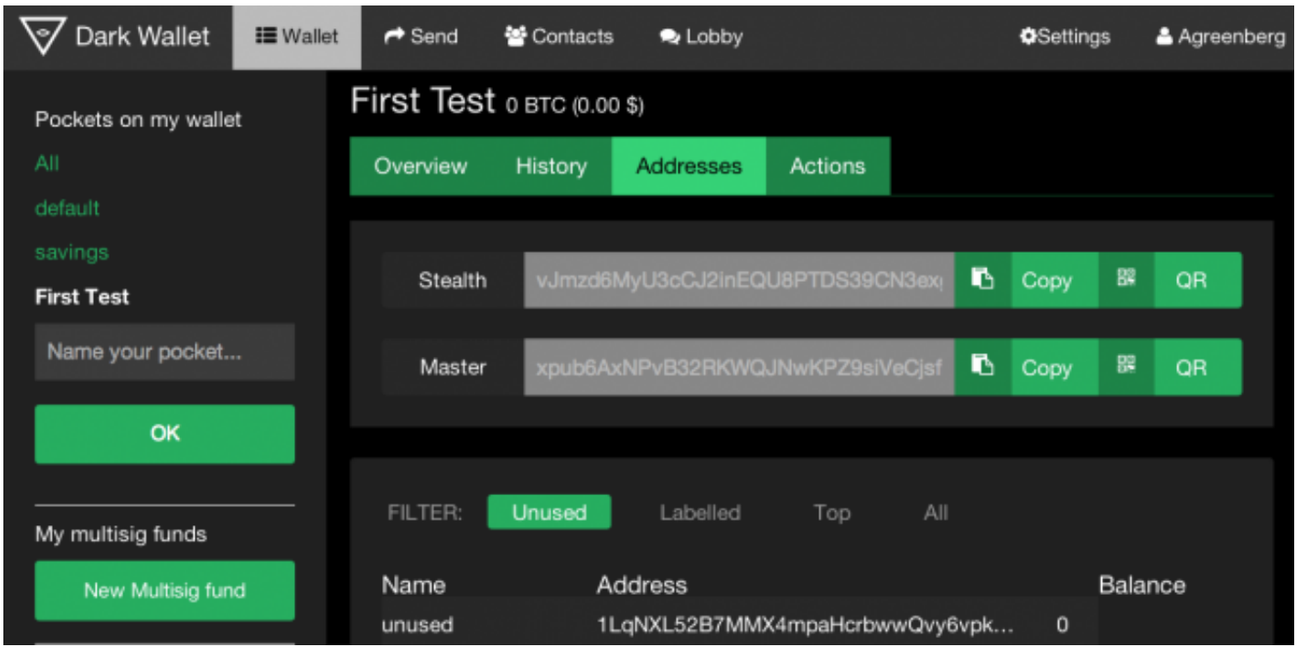
Every bitcoin payment is recorded in the public ledger known as the blockchain, copied to thousands of users' computers and checked to prevent forgery and fraud in the Bitcoin network. If bitcoiners don't take special pains to anonymize their coins, all of their spending can potentially be traced back to their bitcoin addresses by any corporation or government agency that cares to look.



A screenshot from Dark Wallet's interface showing its CoinJoin function. (Click to enlarge.)

Dark Wallet avoids those privacy and trust problems by integrating laundering by default into every payment its users make. Its central tool is a technique called CoinJoin: Every time a user spends bitcoins, his or her transaction is combined with that of another user chosen at random who's making a payment around the same time. If, say, Alice is buying alpaca socks from an online sock seller and Bob is buying LSD on the Silk Road, Dark Wallet will combine their transactions so that the blockchain records only a single movement of funds. The bitcoins simultaneously leave Alice's and Bob's addresses and are paid to the sock seller and the Silk Road. The negotiation of that multi-party transaction is encrypted, so no eavesdropper on the network can easily determine whose coins went where. To mix their coins further, users can also run CoinJoin on their bitcoins when they're not making a real payment, instead sending them to another address they own.

One bitcoin privacy issue CoinJoin solves relates to what are known as "change addresses." When bitcoins from any single address are spent, the unspent fraction of coins are sent back to a change address that the spender controls. Future transactions from that change address can be tied to the same user. But with each successive CoinJoin transaction, the coins are mixed with another new user's payment, and the likelihood of guessing which change address belongs to which user is cut in half again. "When you start to join transactions, it muddles them," says Taaki. "As you start to go down the chain, you can only be 50 percent sure the coins belong to any one person, then 25 percent, then one out of eight and then one out of sixteen. The conditional probability drops very fast."



Dark Wallet's stealth address function. (Click to enlarge.)

To protect the identity of the user receiving coins instead of spending them, Dark Wallet offers a different technique known as a stealth address. Any user can ask Dark Wallet to generate a stealth address along with a secret key and then publish the stealth address online as his or her bitcoin receiving address. When another Dark Wallet user sends payment to that address, Dark Wallet is programmed to instead send the coins to another address that represents a random encryption of the stealth address. The recipient's Dark Wallet client then scans the blockchain for any address it can decrypt with the user's secret key, finds the stealth payment, and claims it for the user. "The important thing is that when someone pastes your stealth address into [blockchain search tool] blockchain.info, absolutely nothing shows up," says Peter Todd, a bitcoin consultant who advised Dark Wallet on the stealth address feature. "The payment is entirely hidden."

Dark Wallet's developers admit it's still at an early stage, and that, like any cryptography project, it will only prove itself and patch its bugs over time. Taaki says, for instance, that the software will eventually combine more than two users' payments in every CoinJoin transaction, and also integrate the anonymity software Tor to better protect users' IP addresses. In its current form, Taaki says Dark Wallet protects IPs only by obscuring them behind the server that negotiates CoinJoin transactions, which may still leave users vulnerable to identification by sophisticated traffic analysis. "It's not foolproof, but it's a strong tool," says Taaki. "And it's going to get better."

In the meantime, the group isn't shying from a confrontation with regulators. Even its name is chosen specifically to reference the FBI's repeated warnings about the Internet "going dark"–that encryption tools could effectively turn off law enforcement's ability to surveil criminal and terrorist suspects online.

"Dark Wallet is a way to reify that nightmare and give it back to them," says Wilson. "There is a 'go dark' problem, and we're going to have it with bitcoin. That's what bitcoin is for. That's what we want to see."