HONOR AMONG THIEVES

Self-regulation of the digital black market

Text by Justin Levinson
Illustrations by Barry Bruner

"I don't want to get killed, robbed, or attacked. All that happens regularly on the street," explains Thurgood Jenkins, the pseudonym used by an up-and-coming marijuana dealer on online black market Silk Road. "Money does things to people. I'd rather just not have to deal with it."

Jenkins's customer base doesn't fit popular conception of drug users. To even find him, potential customers need to jump through several hoops, including setting up complex software. Once there, they exchange in virtual currency, then receive narcotics at their doorstep. Not your typical street clientele.

"I feel like I'm dealing with much more straight-up people. They seem like a tight-knit community that just wants things to go smoothly, not wanting to cheat each other," Jenkins mused. He feels that more complex entry requirements mean people are less likely to rip him off. In the bustling online black markets, trust in one's fellow criminal keeps the bazaar humming.

Many of the same unspoken rules apply as in the physical world. Dealers selling counterfeit, illegal, or otherwise shady goods aren't on the Internet's versions of shopping centers and strip malls; they're tucked away, out of sight. Buyers want to go where nobody knows their names. The anonymizing network Tor, a hotspot for underhand conversations and activity, makes this possible.

Conceived by the US Navy to protect government communications, Tor now houses a vast array of conspirators who prefer to conduct their business away from prying eyes. Activists share secrets and swap documents, citizens in heavily censored countries gain access a free Internet, and whistleblowers leak information to journalists without fear of reprisal. The anonymity is attractive to less savory pursuits too: narcotics and weapons change hands, child pornographers trade pictures, and forums discuss methods for cashing in on stolen credit card numbers. In this netherworld, markets like Silk Road flourish.

Back Channels

When a buyer logs onto Silk Road to make a purchase, their session routes through the computers and Internet connections of volunteer activists, who ferry traffic through a digital Underground Railroad. In a regular Internet browsing session, the path data takes from a user's home computer to the destination site is both predictable and traceable: at any point along the way, an observer can see the data, its origin, and its destination. But inside Tor, like a bank robber trying to drop a tail, the connection takes random twists and turns to hide its tracks. Each node operates on a need-to-know basis, only aware of the previous and next link in the chain.

Through the looking-glass of Tor are underground hangouts and back-alley markets, inaccessible from the Internet outside. These sites, known as "onions", host a variety of content: message boards, blogs, and e-commerce, most of which contains content that posters prefer to keep in the shadows.

Nekro, a community leader and maintainer of Tor directories, sees these hidden forums as essential venues for assembly. "[They're for] people who wish to discuss extremely sensitive topics that they may not be able to get away with on the clearnet: morals of pedophilia and incest, debates on human psychology, drugs, militant groups, Anonymous, human rights, religion, Marxism, etc. I've found that the discussion is usually more intelligent and thought-provoking. People follow by example: if they see intelligent and active discussion, they'll mirror it."

Tor's slow speed makes typical Internet contraband—pirated music, porn, and movies—hard to come by. But marketplaces dealing in illicit merchandise are legion. The currency of this digital realm is virtual and not tied to any geography. The most popular is Bitcoin (see "Flipping the Coin", p. 17), a form of electronic cash far from the reach of law enforcement and tax collectors. Unlike traditional money, these currencies aren't issued or backed by any central authority: they're peer-to-peer and governed by the community's rules.

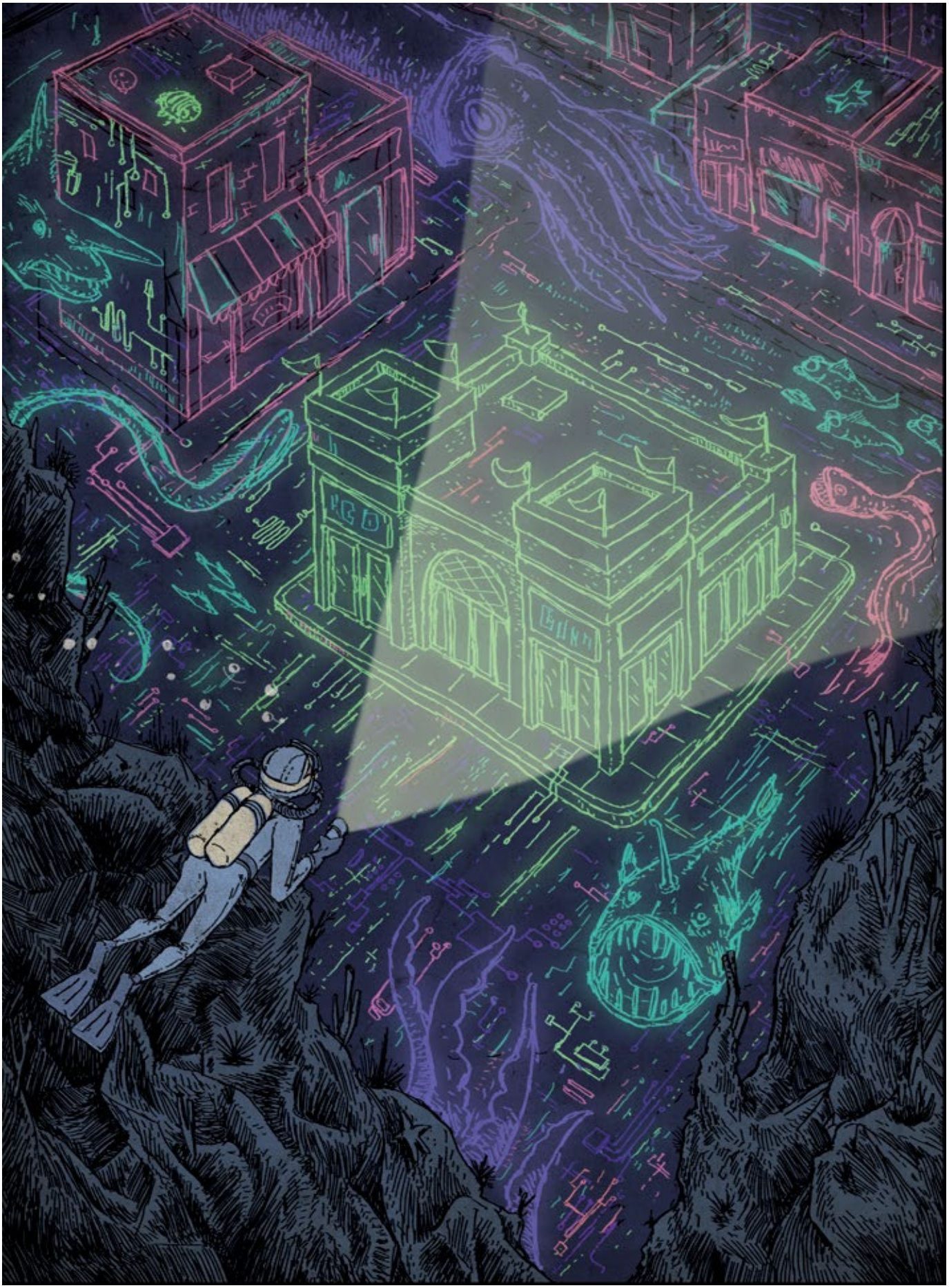
Like the communities themselves, the currencies were designed to make transactions both public and anonymous. Parties are identified only by their wallet IDs, which can be changed before each transaction for additional privacy. With no central authority to keep a ledger, each trade contains a record of every transaction that came before it, drawing on the network to keep everyone honest without revealing real-life identities. Keeping the history up-to-date on the vast network requires significant computational power, provided by users themselves in exchange for more bitcoins.

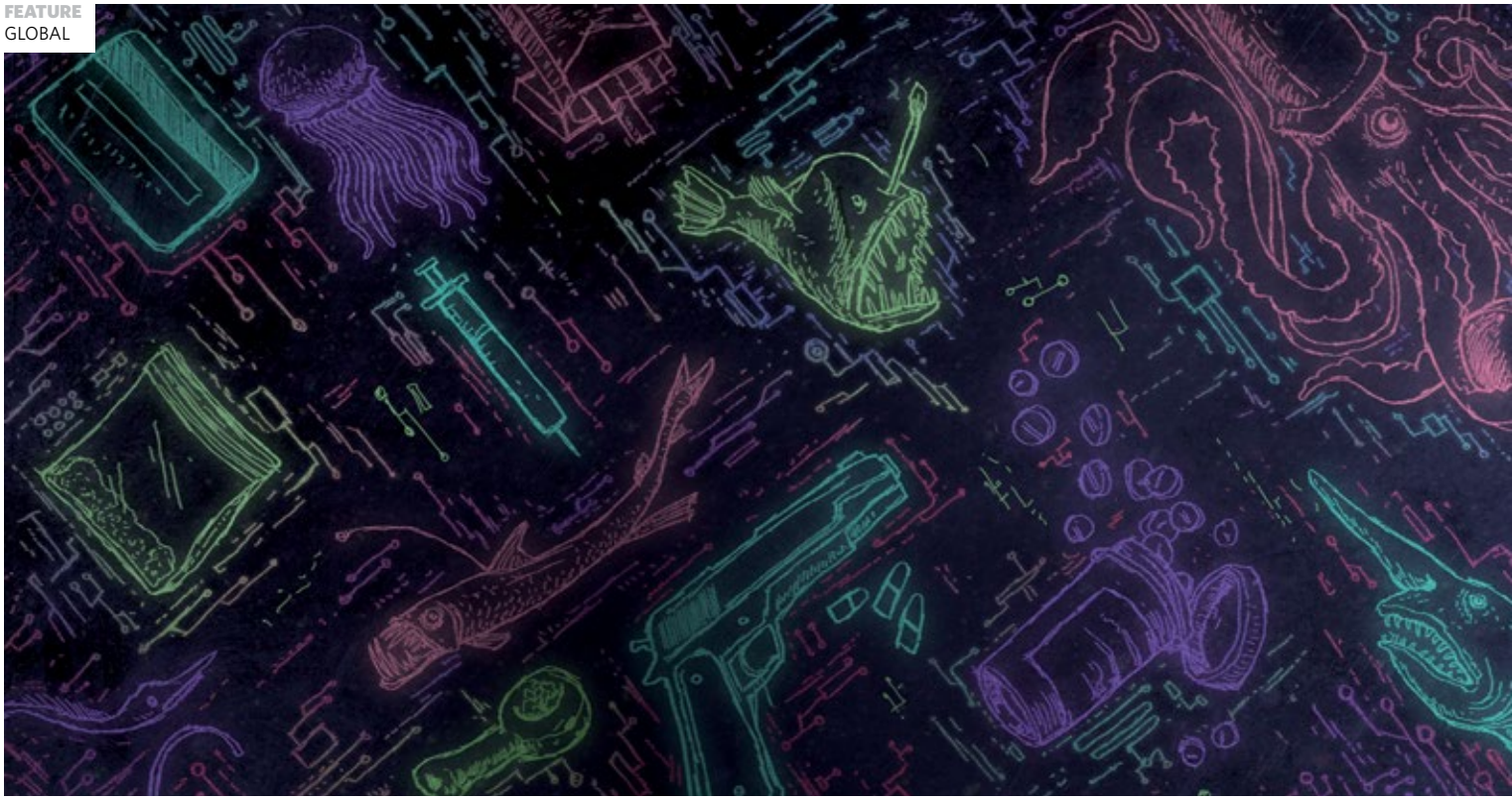
Honor Systems

This transparency scratches the surface of an age-old problem: transacting with potentially untrustworthy players. Popular marketplaces like Silk Road and Atlantis deal with this by requiring the use of escrow systems. Buyers place money on hold for a seller, then release the funds when the product arrives—consumer protection.

Vendors too have recourse against dishonest buyers that sometimes bests traditional e-commerce sites.

Additional reporting by Kyra Phillips of the Misfit Economy.





"I've been scammed on eBay while selling legitimate objects because of Paypal's customer protection," admits Jenkins. "If they just say the item wasn't described or didn't show up, you lose."

On Silk Road, buyers need credibility. Some vendors, like Jenkins, require that customers without feedback or transaction history forfeit the ability to request refunds or reshipments.

The real protection, however, comes from other participants in the market. Customers can leave feedback for sellers, letting other potential buyers know the quality of product, shipping speed, and stealthiness of packaging to avoid detection during transit. Vendors work hard to earn positive reviews and customer loyalty by providing samples, throwing in freebies, shipping quickly, and offering quality product.

"I offered samples for free: free shipping, free weed, free everything, in return for reviews," Jenkins recounts. "The sample-review ratio at the beginning was a little disheartening, but the following influx of orders kind of negated that."

But like a local restaurant, quality can slip for even the most highly rated establishments. On some occasions, sellers ask customers to "finalize early"—releasing money from escrow prior to receiving the product—particularly for new customers with little transaction history. Once the money's out of escrow, buyers lose all protection against fraud.

Eileen Ormsby, a journalist who follows Tor and its marketplaces, has seen some of the most trusted vendors turn rogue. A few days before a massive drug discount sale on Silk Road, a top-rated vendor known as Tony76 told the community he had a problem. Rival sellers were going to place thousands of dollars in fake orders, and he would lose both his product and the money. The community members, always willing to take care of highly rated vendors in times of need, agreed to finalize their transactions early—and gave Tony76 the boost he needed to vanish with more than USD 100,000.

"People begin to think they have a friend-like relationship," explains Ormsby. "When they give some bullshit excuse for needing people to finalize early, buyers' defenses are down because they don't think their 'friend' will betray them. The anonymity of the marketplace then allows them to simply disappear with all the released cash for unfulfilled orders."

Other scams abound as well. Several marketplaces offer dubious hitmen services, requiring a transfer of thousands of dollars' worth of bitcoins and a leap of faith that your target will disappear. In another, an eloquent and lengthy letter sent out to buyers and vendors offers a share of the profits in Silk Road for just a small investment. And some clever hackers have put up fake "Buy It Now" buttons or even ersatz clones of the entire Silk Road site, designed to fool unwitting buyers into revealing their PINs and draining their accounts.

But for every scammer, there's a community member taking pleasure in outing him. "I like comparing Onionland to a tightly-knit town," says Nekro. "Everyone knows everyone else, and everyone knows the stink on certain people. I've just dealt with a scam artist who likely stole a few

thousand dollars before I gave him a public lashing."
Some vendors selectively scam buyers to increase their margins without hurting their feedback ratings, but anyone who feels they've been wronged quickly heads to the marketplace forums to air their grievances and warn other potential buyers. In lieu of a corporate regulatory body, active users double as vigilantes to create and maintain relative law and order in these Internet frontiers.

Short Arm of the Law

Vendors and customers alike are always under the watchful eye of law enforcement. Authorities are well aware of the activities on Silk Road, but the small quantities purchased make it prohibitively expensive to go after low-level dealers who can't turn in bigger fish.

Ormsby attended one dealer's trial. "It was interesting watching the judge wrap his head around the notion that the defendant had cooperated by 'giving up' his supplier (Silk Road), but that cooperation was worthless in that it did not assist police in busting anyone higher up the chain because the defendant himself had no idea who he was buying from. The judge did take the cooperation into account favorably when sentencing."

Not that the investigations are easy, even when the police are lobbed a softball. Jenkins mentions people who use their real email addresses on Silk Road, ones also tied to a Facebook account. "There were multiple examples of how dumb people were being, and none of them had been busted."

He thinks the authorities know what they're up against. "For instance, they find that some vendor used his real email address for his PGP [encrypted email]. They then look into it and launch a full investigation... Well, turns out the vendor just nabbed that email address from a chain email he got three years back, and law enforcement just wasted countless hours and money on a wild goose chase."

The community forums offer tips on how to avoid the courtroom. Internationally mailed packages risk getting caught in customs, so most suggest purchasing locally—reassured, at least in the US, by the postal inspectors' inability to open mail without a search warrant. Vendors take their own precautions: wiping for fingerprints, triple-sealing their product in vacuum foodsaver bags and mylar, then disguising the shipments as regular mail.

At the back of his mind, Jenkins knows, as do all dealers, that even with these precautions, trafficking in illegal goods is dangerous business. "I've lost sleep from it, had nightmares. I have a lot to lose. I have no idea how much risk I'm in. Nobody really does."

The meteoric rise in Bitcoin's popularity, as well as the growth of illegal marketplaces like Silk Road, point to the shifting nature of online commerce—despite clamor for new legislation to maintain the status quo. Traditional legal systems don't apply when the parties are anonymous. The carrot-and-stick arrangements that govern mainstream marketplaces have been replaced by an informal structure of social norms, vigilantes, and belief in the basic honesty of the majority. And it works with surprising efficiency, despite its criminal nature. Money and products may change hands, but here, the real currency is trust. ●