TACTIC
ENCRYPTION

A vital tool for activists and organizers — and everyone else — to communicate securely outside the prying eyes of the state and corporate bad actors.

CONTRIBUTED BY

Dave Oswald Mitchell

Dave is Beautiful Trouble's political corrections officer and the co-editor of *Beautiful Trouble: Toolbox for Revolution* and *Beautiful Rising: Creative Resistance from the Global South.*

"FREE AND PUBLICLY AVAILABLE ENCRYPTION TOOLS THAT ALLOW PEOPLE TO COMMUNICATE SECURELY ACROSS DISTANCE *ARE* STRONG ENOUGH TO FOIL THE CODE-BREAKING EFFORTS OF THE MOST POWERFUL COUNTRY'S MOST POWERFUL COMPUTERS."

"I am a secret so everyone can know me. First you must count every part of me, then translate those parts into signs that do not describe me. Together we are shackled, and with the sign that does not describe me you can open me up and read me as I am. People will give you their promises for me, and if wrongdoers try to take me away from you, you can find me and tell the world where I am hidden. I began as a silent speaking, a key to open every door; now that I have opened all the front doors, I am the key that locks the back doors by which wrongdoers try to escape the scene of the crime. I am the nothing that makes everything happen. You don't know me, you don't understand me; and yet still, if you want justice, I will help you to find it. I am blockchain. I am encryption. I am code. Now put me to use."
—Kim Stanley Robinson, *The Ministry of the Future*

When whistleblower Edward Snowden exposed the extent of US government spying on the communications of millions of people around the globe, he took care to emphasize one key fact: *encryption works.* Free and publicly available encryption tools that allow people to communicate securely across distance *are* strong enough to foil the code-breaking efforts of the most powerful country's most powerful computers, leaving Big Brother unable to decipher your messages, emails and phone calls—if you encrypt them.

Encryption, then, is a vital tool for activists and organizers—and everyone else—to communicate securely outside the prying eyes of the state and corporate bad actors. Its use has proliferated in the

POTENTIAL RISKS

Encrypting your data and communications is digital self-defence 101, but it also isn't foolproof. Striking the right balance between exercising healthy caution and taking simple measures to protect yourself, on the one hand, and remaining open to the risks and uncertainties that any social transformation effort will entail, on the other, is a constant balancing act requiring a common sense approach.

RELATED TOOLS

Stories

- CryptoRally in Mexico City
- Hacking Apartheid

Tactics

- Civil disobedience
- Currency hacking

years since Snowden's leak through messaging apps like Signal and Telegram, email programs like ProtonMail and PreVeil, and web browsers like Tor Browser. And if you believe the hype, its uses may extend well beyond personal privacy, potentially challenging the very foundations of state power and global finance.

Encryption simply means writing in code. While its uses certainly predate the digital age (see: STORY: Hacking Apartheid), cryptographic methods have long been closely guarded by states and corporations. But with the explosion of digital communications in recent decades, publicly minded software engineers like Phil Zimmerman have democratized the technology, making it freely available and accessible to all.

The *public-key encryption* tools now in common use aren't just about security, however. They're also about trust—restoring our trust in our ability to speak freely and openly to one another, but also our trust in our ability to verify the identities of the people we're communicating with to guard against online catfishing, identity theft, and man-in-the-middle attacks.

Public-key encryption is a method of encoding data so that only an intended recipient who has the *private* key to decode it can read it. It also allows both sender and receiver to verify the identity of the other through the use of a *public* key. Equally a tool of security and trust, privacy protection and public verifiability, encryption is the very essence of a riddle wrapped in an enigma.

This public/private information encoding technology has, since 2008, given rise to *blockchain*, a system of assembling or "mining" data into documents, contracts, and exchanges that are unchangeable, transparent, and self-governing. Blockchain in turn has enabled all manner of new and emerging technologies and speculative assets, from cryptocurrency (a decentralized digital currency whose value is rooted in blockchain) to NFTs (digital art that uses blockchain to certify its authenticity and ownership).

So what does this procession of emerging technologies have to do with creative activism and social change? Frankly, we're still figuring that out, but the techno-optimists are bullish.

Ben Case and J. Armstrong argue, for example, that these emerging technologies represent a prefigurative zone in which radicals can build out the institutions of a post-capitalist future in the shadows of the state: "The combination of encryption basics with open-source hardware (and perhaps cryptographic currency, like Bitcoin-based Freicoin) has the potential to grow into a network of direct working-class control of the means of communication, production and exchange on a global scale."

Whether this emerging internet 3.0 will turn out to be empty hype, cyberpunk capitalist hell, or harbinger of a coming technocommunist utopia is TBD. Yes, use, promote, and experiment with the widely available tools for encrypted communication, even

Principles

- Practice digital self-defence
- Seize the means of communication
- Take risks, but take care

Theories

- Prefigurative politics
- Temporary autonomous zone

TAGS

Communications, Digital organizing, Digital security

as you treat with skepticism the most hyperbolic claims of crypto-enthusiasts.

LEARN MORE

"Encrypted resistance: from digital security to dual power"
Roar Magazine, 2015
https://roarmag.org/essays/encrypted-resistance-from-digital-security-to-dual-power/

A feminist manifesta of the blockchain
Claudia Hart, 2021
https://hyperallergic.com/639180/a-feminist-manifesta-of-the-blockchain/