

Thursday 7 August 2014
For immediate release

Introducing XChat: more private than BitTorrent Bleep and more secure than Protonmail

XC's new instant messaging feature, XChat, is purely peer-to-peer, encrypted from end to end, and leaves no trace on the computer you use it on.



Today **XC** has unveiled **XChat**, a next-gen instant messaging app with industry-leading privacy and security features. Furthermore XChat is available inside the XC TOR Stick, which hides your IP address and leaves no trace on the computer it is used on.

XChat complements **XCurrency**, XC's existing app for flexibly private payments, and is founded upon on the Xnode communication protocol, a Bitcoin 2.0 technology at the core of XC's network. It is completely decentralised, involves trusting no third parties, and is end-to-end encrypted. As such it represents the highest level of privacy currently available.

HOW DOES IT WORK?

In its current form, XChat is effectively a next-gen **BBM**. People can send instant messages to each other, but with no central servers at all. To use it you enter the recipient's address (which is analogous to a phone number), and their public key (which is related to a secret "private key" in their app that enables it to decode your message). XChat will soon come to mobile devices, and future releases will include group chat, voice calling and video calling.

TRUE PEER-TO-PEER MESSAGING

Unlike traditional messaging apps, XChat uses no central servers, and so only the people conversing have control over the information exchanged. As such, no corporation or government has the ability to use or seize your information. This makes XChat more secure than "secure" messaging services like **Protonmail** which rely on servers and thus present a central point of failure or attack.

In fact, XChat is more decentralised than even BitTorrent, whose protocol **relies on servers to look up and locate users**. Would you want to give third parties the power to store your address and relay your information? With XChat, apps find each other, unlike BitTorrent's recently-announced messaging app, Bleep.

END-TO-END ENCRYPTION

XChat communication is encrypted from end to end with AES256 so that no third party can decipher your message. In fact, you'd need more processing power than the entire internet to break XChat's encryption! This makes it impossible (i.e. computationally infeasible) for anyone to snoop on your messages, so your privacy is assured.



IP ADDRESSES KEPT SECRET

For anyone who does not want to reveal their location, XChat can be run from the **XC TOR Stick**, which incorporates a TOR node that obfuscates your IP address. In addition, the TOR Stick runs inside the TOR network so that it does not use exit nodes. This means that packet sniffers are useless against XChat as there are no incoming and outgoing packets to be matched. Even if a message is sent to a recipient outside TOR, the message originates inside the network and so there is only an outgoing packet, again flouting packet sniffers. In this way, XChat avoids common vulnerabilities of TOR.

NO DATA STORED ON COMPUTER

The TOR Stick is, effectively, its own operating system. Based on Debian and similar to **Tails**, it comes either on a flash drive or as an ISO which you'd run in a virtualised environment, and it only uses your computer's RAM. When you're finished using it, no trace of your activity is left on the computer. This also makes it malware-free.



XChat will soon come to mobile devices

RECEIVING ADDRESSES OBFUSCATED

If this is not enough, soon XC will add yet another layer of privacy. XChat addresses are soon to be implemented as "stealth addresses". Someone can send a payment to your XC address, but you will receive it on a different address that not even the sender knows. As such, you can publicly display your XChat address as a kind of cryptographic "business card" for both payments and messages, without any link to it existing on the blockchain.

Finally, combining this with **XCurrency's Privacy Mode** will conceal the amounts sent to this address and the address itself. The result is that neither the sender, receiver, nor the amount paid is revealed, resulting in 100% privacy for XC users.

GET XCHAT

XChat is available now, for free, [here](#).

The TOR Stick can either be ordered today at the [XC Merch Store](#) or downloaded for free as an ISO file [from XC's website](#).

Physical TOR Sticks will be shipped in the near future, at Rev 3 as per XC's [roadmap](#).

ABOUT XC

XCurrency is a three-month-old Bitcoin 2.0 platform for flexible digital transactions that has undergone a meteoric rise in popularity. Due to its newness there is currently a lack of technical documentation of its design, although in the coming weeks a white paper will complement the existing information on XC's website, and XC will offer a substantial bounty to anyone who can provably break XC's anonymity. Note also that XC is committed to the open source model. Open source code is vital for the

health and advancement of cryptographic technologies, and so XC will **make code available** on a delayed timeline. This way, the community will derive the benefit of XC's ground-breaking technologies, while reducing the incentive for developers to flood the marketplace with clones that lack a long term future. As such, XC stands to enrich the digital currency ecosystem and to spearhead advancements in security, functionality, and flexibility.

xc-official.com

Read the Chinese version of this release.