Wednesday 17 September

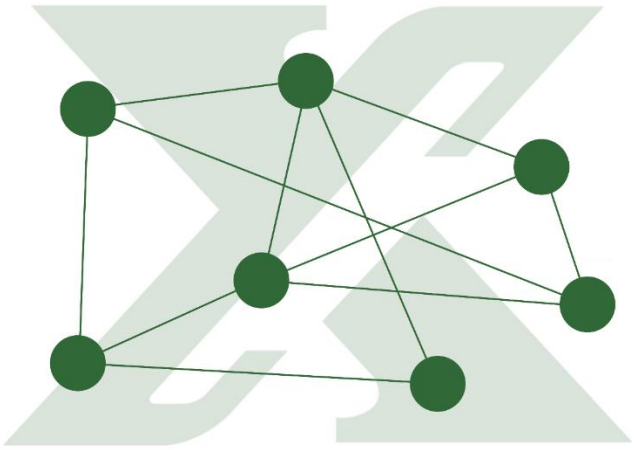
For immediate release

XCurrency's revolutionary privacy advancement: trustless *ad hoc* mesh networking

XC's final instalment to its privacy technology is a breakthrough on three fronts: privacy, scalability, and mobility.

XCurrency has released the central and final component of its privacy-centric payments solution, and much like the multifaceted ingenuity in Satoshi Nakamoto's invention of the Bitcoin blockchain, it is a single protocol with far-reaching implications. Its immediate function is to allow any app on the XC network to communicate on behalf of other apps without the others having to trust them; however its implementation has game-changing aspects.

Put briefly, when someone makes a private payment using the XC app, the transaction is split into fragments, which are sent to several other nodes also making payments. These nodes form *ad hoc* mesh networks with each other that exist only for the duration of each transaction, in which no node functions as a hub or "server." The nodes mix transactions in a manner analogous to coinshuffle, where no node knows which other node's coins they're forwarding, and no link exists on the blockchain between sender and receiver. The effect of this is true privacy: due to forwarding, the senders' and receivers' identities are concealed, and due to transaction-fragmentation, the amounts sent are concealed. In fact, since all nodes can forward transactions, nodes cannot even tell whether a given fragment originates from the node it receives it from or whether that node forwarded it from somewhere else.



While "trustless multipath mixing," as the above is called, has the direct purpose of making transactions truly private, what is of greater value is that it sets new paradigms for distributed content servers, mobile blockchains, and private web browsing. It is the true foundation of XC's web 3.0 plans. How this is possible is as follows:

A "CoinJoin killer"

It has often been assumed that the next major advance in cryptocurrency would be a cryptographic one. It turns out, however, that XCurrency's major breakthrough is as much an extension of advanced networking technology as it is a cryptographic innovation. One of the most popular techniques for anonymising transactions is CoinJoin, however in comparison to XC's trustless multipath mesh, it is at a decisive disadvantage:

- CoinJoin is vulnerable to a denial-of-service attack: if a single node fails (or refuses) to sign a transaction, then every participating node has to re-sign. In contrast, by design XC's mesh is continually and dynamically altering its topology, and has no trouble of this sort.

- CoinJoin has no intrinsic way of disciplining bad nodes, whereas XC's mesh is capable of discovering bad nodes and excluding them from the mesh.

- Nodes participating in a CoinJoin transaction generally know the sender, receiver, and amount sent. Thus, even though the blockchain does not record a link between sender and receiver, the information can be extracted from a node. XC's trustless mixing conceals links between sender and receiver even from forwarding nodes, and its multipath fragmentation conceals the amount. Thus even if nodes are hacked, they cannot reveal sensitive information.

- CoinJoin generally requires a mixing server or some form of semi-centralised supernode (cf. DarkCoin "masternodes"). XC's mesh networks are entirely distributed, even with the recent addition of Xmixers.

A TOR REPLACEMENT

The Onion Router, an aging US-government initiative with several vulnerabilities, is the *de facto,* though imperfect, means for the privacy-conscious to conceal their IP addresses. However a trustless mesh network is ideally suited to conceal IP addresses, since nodes mix content and are not able to discover the nature of the content, and because its distributed topology renders it highly resilient to attacks against any one node or collection of nodes. As such, XC nodes make an excellent foundation for next-generation IP-concealment. This feature can be expected in future XC developments. Added to the privacy features above, it results in 100% privacy for XC users.

IDEAL FOR MOBILE

In order for a cryptographic platform to go mainstream, it is absolutely essential that it be truly mobile-friendly. This is directly where XCurrency is headed. Trustless multipath mesh networks are ideally suited to this purpose, as can be seen from analogous technologies like mobile ad hoc networks (MANETs), which are continuously self-configuring, infrastructure-less networks adept at handling the fluctuating signal strength and changing locations of mobile devices.

XC founder and lead developer Dan Metcalf is a leader in distributed wireless network design, as his LinkedIn profile suggests. When founding XCurrency, he perceived that his core contribution to the advancement of cryptocurrency would be to use this expertise to improve the privacy and mobility of blockchain-based technologies. XC's trustless multipath mesh networking will excel on mobile devices, and the blockchain will be as much at home on mobile as it is on PCs and servers. Mobile apps will form *ad hoc* networks upon demand, require no servers, secure XC's network, and trustlessly mix transactions just as PC- and server-based apps do.

Mobile apps will form *ad hoc* networks upon demand, require no servers, secure XC's network, and trustlessly mix transactions.

WEB 3.0

XCurrency recently announced its plans for a distributed content delivery service, and a trustless multipath mesh is the ideal delivery vehicle for such a service. Any device, mobile or not, will have the capacity to store and serve content even though its signal strength fluctuates and its connections to its peers change continuously. And for clients, service delivery will remain robust regardless of any one node's quality of service, and the system's distributed nature makes it effectively invulnerable to attack.

XC's plans for web 3.0 will be further enhanced by being able to recruit mobile devices as content servers. Furthermore, XC users will gain another source of revenue from running XC on their mobile devices. By simply installing XChat (instant messaging with true privacy), users will thereby gain a source of remuneration.

XCurrency is preparing to launch publicly, and trustless multipath meshes are an integral part of its approach. With the final piece of its privacy puzzle in place, XC is optimally positioned to deliver a platform for next-generation distributed apps and services.

xc-official.com