anonymous secure decentralized SMS

stealthtext transactions

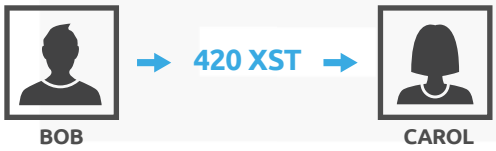
stealthtext

WHITEPAPER

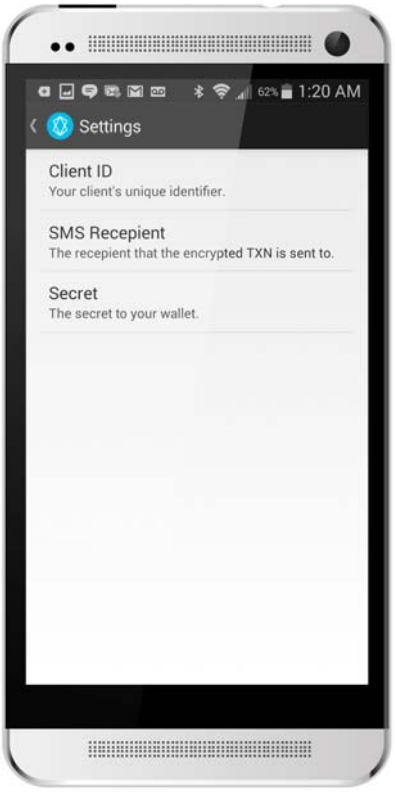
WHAT IS STEALTHTEXT ?

stealthtext is a way to send ***stealthcoin*** privately and securely using SMS texting. ***stealthtext*** is invaluable in situations where you can not access a data plan. With ***stealthtext***, you can send others ***stealthcoin*** directly from your wallet and receive confirmation by SMS. Unlike other services, it uses banking-grade encryption to protect your transactions from the prying eyes of onlookers. Additionally, your transactions are tamper resistant, so you can be completely confident that the transaction you enter into your phone is faithfully executed by the ***stealthcoin*** network.

LET'S IMAGINE ...



Bob wants to send 420 **XST** to Carol although Bob operates under serious constraints today. He has his phone and can send texts (SMS), but for reasons beyond his control has no access to his data services. Bob absolutely needs his transaction to get to Carol securely and privately (anonymously). He can't afford for anyone to tamper with his transaction, like blindly "flipping a bit" to change the amount, nor can he afford for an adversary, such as a competing business, to know the nature of his transaction with Carol.

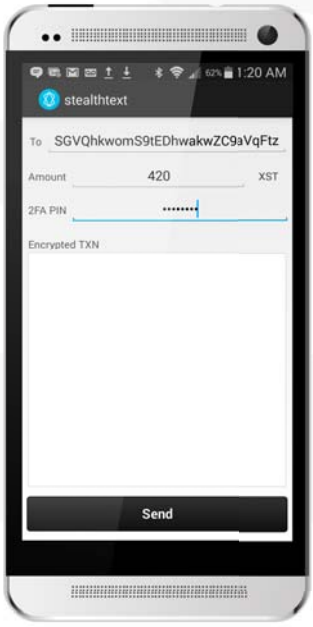


Bob is in luck though, because he has installed ***stealthtext*** on his phone. In his settings dialog, he has entered his client ID, the phone number of his SMS forwarding service (like google voice), and a secret Passphrase. The client ID, useful for routing or selecting accounts, may be any sequence of seven or fewer characters.

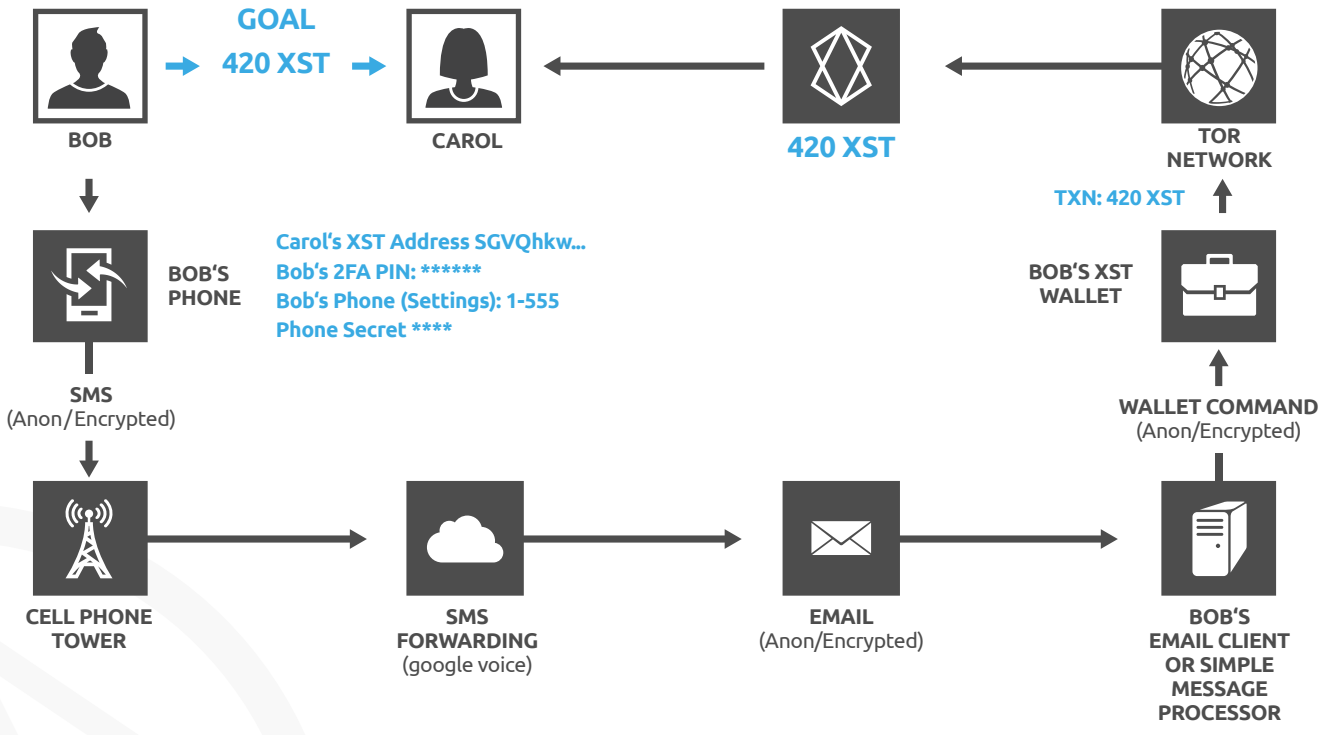
Because his phone sends text messages using the SMS protocol but ***stealthcoin*** is a TCP/IP protocol, Bob needs a route (or "pipeline")

between his phone and his wallet. Bob may have previously established his own pipeline using tools provided for ***stealthtext***. Or Bob might be the customer of an online wallet service that provides a pipeline. Either case is possible because anyone can set up his or her own pipeline. Bob's wallet (whether in the cloud or his computer at home) knows his secret passphrase and his PIN, which together make both parts of ***stealthtext***'s two-factor authentication.

To make his transaction, he enters Carol's **XST** address (SGVQhkwom..), the amount (420 **XST**) and his PIN, which he shares with no one and has memorized. He then hits "Send" and confirms the transaction. ***stealthtext*** then sends the anonymous, encrypted transaction through SMS where it enters the pipeline.



In this example, the SMS message with the anonymous transaction is routed to Bob's SMS forwarding service (like google voice) which then turns it into an email that is sent to Bob's email account. If using google voice, this email account would be a gmail account. The email is then handled by Bob's mail client, which is enabled to send it to a simple message relay running on his computer. This message relay extracts the encrypted transaction from the email and sends it, still encrypted, to the wallet as part of a command.



The ***stealthcoin*** wallet recognizes this command and decrypts the anonymous transaction. Because the transaction is encrypted on Bob's phone but never decrypted until it gets to his wallet, the transaction remains secure and anonymous while traversing the entire pipeline. As with all transactions, the wallet broadcasts Carol's 420 **XST** to the TOR network, which ensures that Carol gets her funds safely and privately.

STEALTHTEXT IS:

1 ANONYMOUS

stealthtext is anonymous because no one except Bob can know the contents of the encrypted transaction while on transit to his wallet. Once there, it remains anonymous because ***stealthcoin*** uses the Tor network. It is true that an adversary may be able to note meta-information about the communication, like the phone number. However, since the transaction is fully encrypted, it is impossible for anyone but Bob to know whether Bob is sending ***stealthcoin*** to Carol, a thank-you note to his grandmother, or a recipe to his wife.

2 SECURE

stealthtext uses AES encryption combined with GCM authentication. This combination of cryptographic technology ensures that a multitude of attacks that try to blindly manipulate the encrypted transaction to change its value, recipient, or otherwise corrupt it, will be detected by the wallet. In fact, the transaction will be rejected by the wallet if just one bit of one byte of the encrypted transaction is modified.

Moreover the wallet has safeguards against delayed transactions and "replay attacks". That is, once the wallet broadcasts the transaction, it will not accept the same transaction again. So, if an adversary intercepts the message and sends it numerous times to Bob's wallet, the wallet will not re-send the funds no matter how many replays the adversary attempts to create.

3 DECENTRALIZED AND TRUSTLESS

Any person or servcie can establish a pipeline. They only need the ***stealthtext*** Android application and a ***stealthcoin*** wallet of a version greater than or equal to 1.2.0.1. Any SMS forwarding service can send the message to any medium of delivery. Email is probably the the most convenient for a majority of users because google voice can send SMS messages to gmail, taking care of most of the pipeline. Of course the medium could also be http or some other protocol, depending on one's SMS service. If using google voice and gmail, the only glue in the entire pipeline is a program that can change an email with the encrypted message into a wallet command. We call this program "***stealthrelay***" because it relays the message from email to the wallet. ***stealthrelay*** will be available as an open source project with downloads available for Linux, Mac, and Windows.

4 SMS

stealthtext does not rely on Bob's phone having data capabilities. This allows Bob to send funds anonymously and securely from any part of the world where SMS is available, or when his data services experience outage due to adversarial attack or natural causes.

stealthtext

CRYPTOGRAPHY

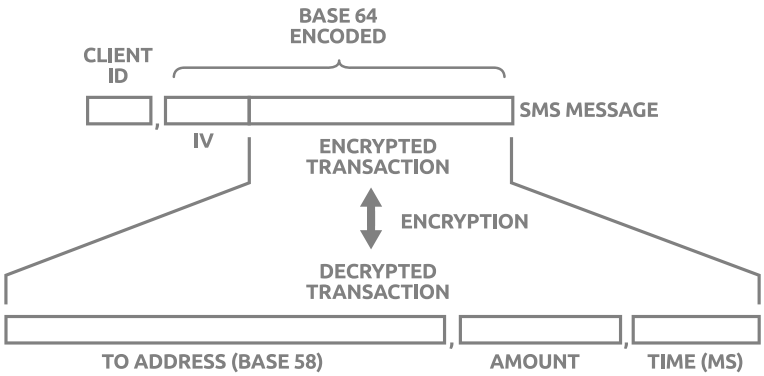
stealthtext uses the American Encryption Standard (AES) block cipher combined with Galois/Counter Mode (GCM) authentication. AES has a 16 byte block size and is the National Institute of Standards and Technology (NIST) standard FIPS 197. GCM is recommended by NIST in its NIST Special Publication 800-38D.

SMS MESSAGE DATA STRUCUTRE

The SMS message is packed as printable text. It may have any text encoding, but UTF-8 or ASCII are most common. The message consists of two parts, separated by a comma. The first part is the client ID, which can be any printable string of seven or fewer characters. The second part is a base 64 encoded block that itself consists of the 16 byte, cryptographically random AES/GCM initialization vector (IV) followed by the encrypted transaction. Decrypted, the transaction consists of the base 58 ***stealthcoin*** recipient address, the transaction amount, followed by the system time in milliseconds.

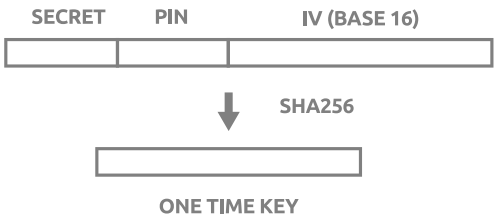
This system time, established by the phone, is used by the wallet as the transaction time (nTime). To protect against replay attacks, all new ***stealthtext*** transactions are checked against all previous transactions for nTime. Any new ***stealthtext*** transaction with an nTime of an existing transaction will be rejected by the wallet. Although this safeguard is in place, it is highly recommended to have the final relay filter transactions by comparing their cipher texts, and rejecting duplicates.

Additionally, the wallet will reject ***stealthtext*** transactions differing in system time from the wallet by more than five minutes.



KEY DERIVATION

The AES/GCM encryption key is the SHA256 hash of the ***stealthtext*** secret, the PIN, and the cryptographically random IV represented as a base 16 string. Including the IV in the key derivation ensures that the encryption key for each transaction is unique, in accord with cryptographic best practices.



stealth-coin.com