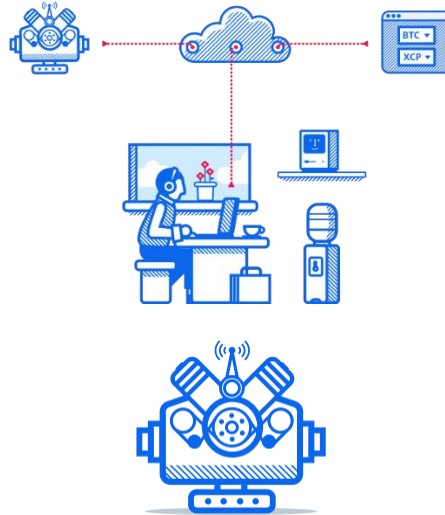Counterparty

Pioneering Peer to Peer Finance

BITCOIN SMART CONTRACT COMMUNITY

The Protocol

The technology that allows Counterparty nodes to communicate with each other via the Bitcoin blockchain.

Assets

Create your own digital tokens in a matter of seconds, which can represent anything and are easily exchanged peer-to-peer.

XCP

The native currency of Counterparty, used for advanced features and representing stake in the protocol.
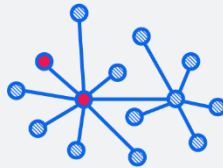
Counterparty Features

Counterparty Wallets

Secure, fast, and user-friendly web, browser and mobile wallets that provide all the power of Counterparty.

Bitcoin-Aware

Counterparty smart contracts are Bitcoin aware and can also interact directly with Counterparty tokens.
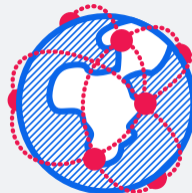
Lightning Network

Currently under development, payment channels support will allow rapid exchange of assets and are compatible with the Lightning Network.
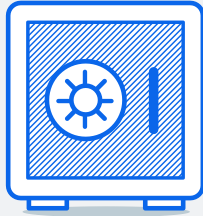
Asset Creation

Custom named assets can be created for a small anti-spam fee and numerical assets are free to create.

Decentralized Exchange

Exchange assets trustlessly using the Counterparty's DEx (Decentralized Exchange).

Secure & Open Source

All Counterparty software is open source and has been formally reviewed by several well-known Bitcoin security experts since it's release in January 2014.

Tokens

Custom Counterparty tokens can be used for a wide range of purposes and act as their own cryptocurrency, while still running on the Bitcoin blockchain. Unlike ordinary bitcoin, custom tokens can be used to represent any kind of value.

Tokens are being used today to:

- conduct successful crowdfunding and voting,
- monetize access to decentralized application ("DApp") software features,
- represent a product or personal brand,
- act as a sort of "blockchain domain name",
- as an authentication token,
- to represent digital goods, such as in-game cards,
- as a proxy for a real-world good or service (i.e. tokens exchangeable for paper, biofuel, etc),
- act as a reward for providing valuable time or resources,
- as an educational service to explore the functioning of a blockchain,
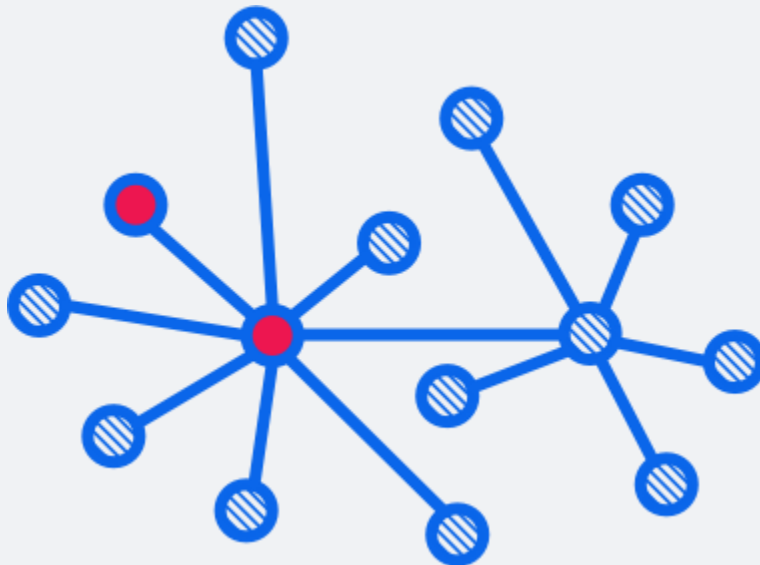- and purely for fun.

Asset Exchange ("DEX")

In the physical word, exchanging assets is fraught by risks and problems, such as potential theft and reliance on an escrow agent or central counterparty. On Counterparty, the roles of escrow agent and clearing house are filled by the Counterparty protocol itself, eliminating unnecessary costs, time, and third-party trust. In any transaction the required funds are debited from each party's address immediately, and are not released until the conditions of the contract have been met.

Payment Channels

Work on the upcoming Lightning Network promises to enable nearly instant, cheap and safe exchange of bitcoin between untrusted counterparties.

Features in Counterparty are under development that will allow for use of uni- or bi-directional payment channels with Counterparty tokens. Future work will allow the use of the Lightning Network with Counterparty, enabling rapid, decentralized and off-chain exchange of tokens that settles onto the Bitcoin blockchain.

Voting

Blockchain-based voting avoids many of the issues inherent with voting in "real world". Digital signatures allow for identity and voting rights to be easily established and verified, and the blockchain itself provides an unalterable, append-only record of who voted, and when.

Counterparty provides multiple methods to perform fully decentralized voting on the blockchain:

- Counterparty tokens may be created and distributed and then sent to specific addresses to signify a vote for a specified option (e.g. DevParty),
- Counterparty broadcast messages may be used (e.g. the recent Counterparty board elections), or
XCP stake voting is under development, to allow for powerful, decentralized governance of the Counterparty protocol.
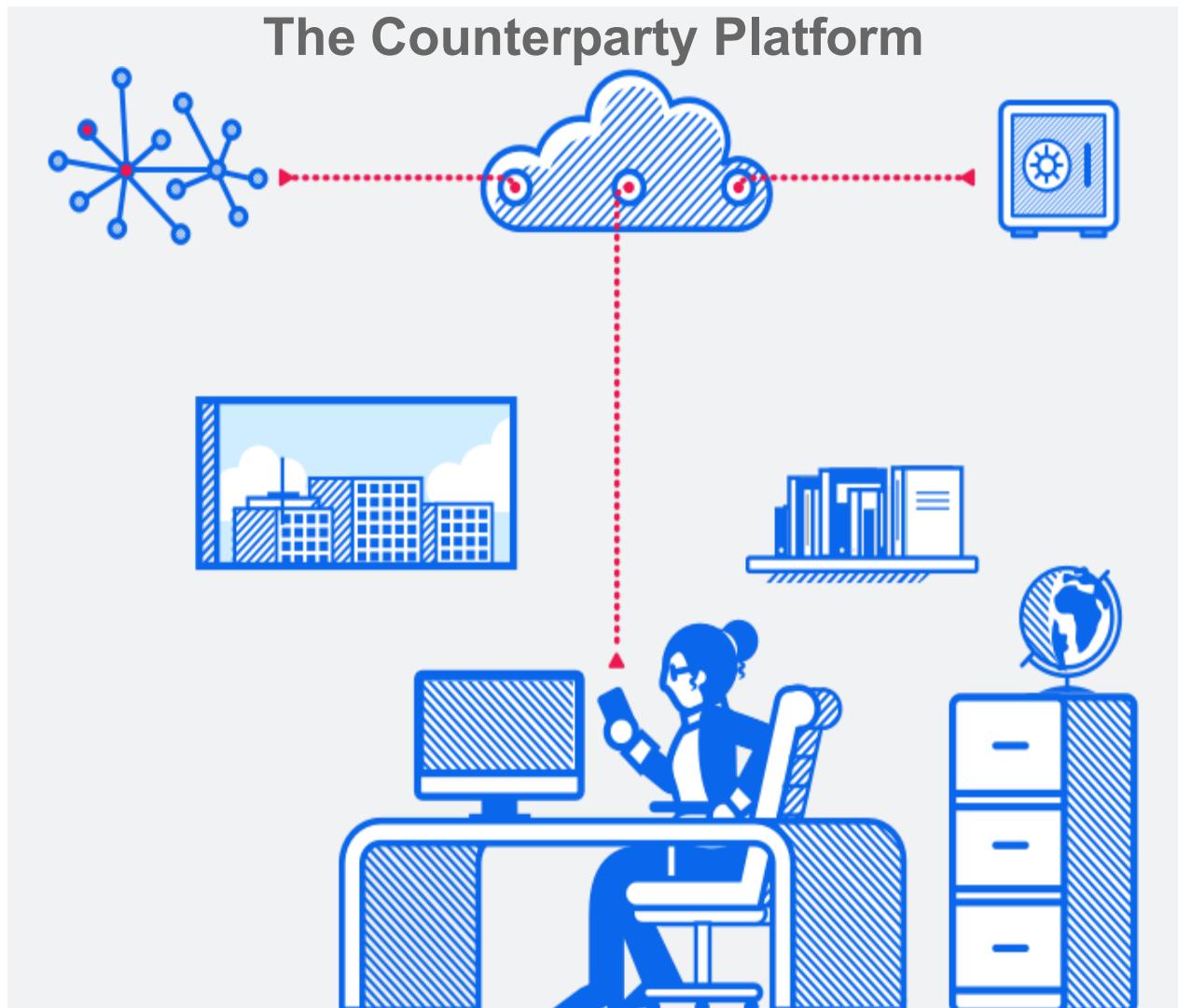
Multisignature Addresses

Multisignature transactions require signatures from more than one Bitcoin private key to spend their funds. Counterparty supports various multisignature schemes, such as 1-of-3, 2-of-3, 3-of-5, and more. Using our technology, a Bitcoin "multisignature address" may be created, and some quantity of a Counterparty token sent to it. Some quorum of signers will then be required to digitally verify and sign any transaction that sends these tokens somewhere else.

In practice, this allows for enhanced security measures around Counterparty token access and distribution. Scenarios where this could be useful include:

- Allowing team members and third-party firms to initiate transactions that can be approved later by management,
- allowing issuers of tokens to safely store these tokens, as well as to control their distribution, and
- allowing third-party auditing services to ensure the delivery of goods and services once contractual obligations have been satisfied, and only release funds once verified.
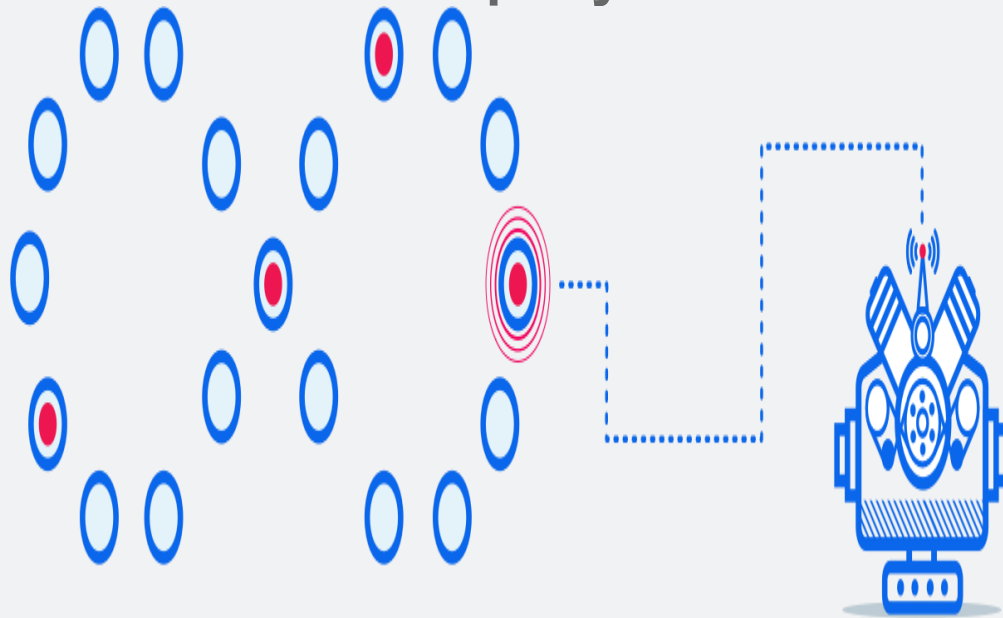
The Counterparty Platform

Counterparty extends Bitcoin's functionality by "writing in the margins" of regular Bitcoin transactions, opening the door for innovation and advanced features not possible with ordinary Bitcoin software.

The Counterparty Protocol

The Counterparty protocol is open source and extensively tested. Besides allowing users to create and trade any kind of digital token, Counterparty enables anyone to write specific digital agreements, or programs known as Smart Contracts, and execute them on the Bitcoin blockchain. Smart Contracts are a revolutionary technology which opens the door to endless possibilities. By using the Bitcoin's decentralized ledger network and Counterparty's built-in scripting language, real-world scenarios can now be transformed into code and executed automatically with no need for an intermediary.

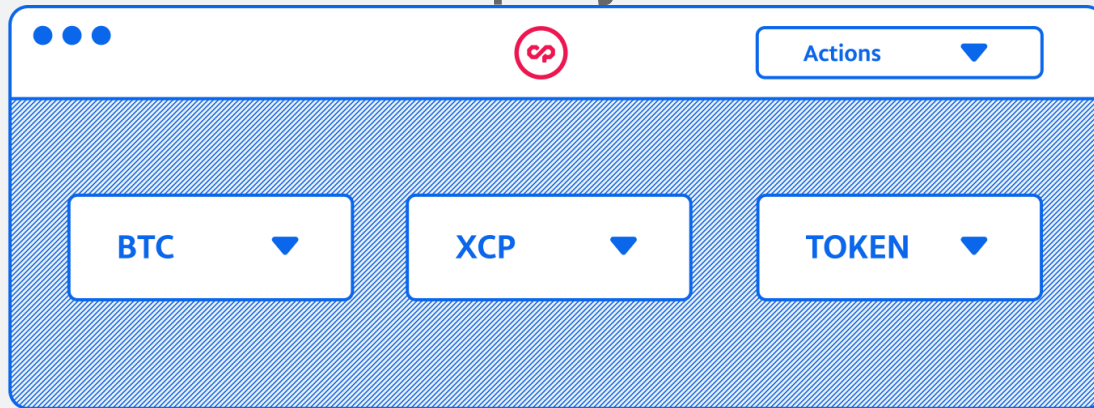[Read the technical details of the Counterparty Protocol >](#)

XCP

XCP is used to provide functionality where it isn't technically possible to use BTC. For instance, XCP is the currency used to pay for the execution of all smart contract code. More generally, XCP represents stake in the Counterparty protocol, and is the voting currency for changes to be decided on by the community.

XCP was created by "burning" bitcoins, which involved sending coins to an unspendable address in exchange for XCP, ensuring an even and fair distribution of the currency. In January 2014, over 2,100 bitcoins were burned, creating about 2.6 million XCP. You can purchase XCP through several exchanges.

Counterparty Wallets

Counterparty currently has four different types of wallets: a desktop wallet, a web wallet, a mobile wallet, and a Chrome extension wallet. These wallets provide all of the functionality of the Counterparty's reference client, while preserving the security of your funds.

When you use one of the Counterparty wallets, all transactions are signed on your device and your private keys are never stored on the servers. All information sent to the servers is first encrypted by the wallet client for maximum security, and every trace of your session is erased when you log out. All you need is your unique passphrase for easy and secure access.

Common Wallet Features

Create and manage new tokens on the Bitcoin blockchain

Distribute profits in BTC, XCP, or any other Counterparty currency

Trade BTC for XCP or any Counterparty token fully peer to peer

Create and manage multisignature addresses

Store tokens offline using Armory

Broadcast data feeds to the Bitcoin network

Counterwallet

is a free web-wallet for Bitcoin and Counterparty, the world's first protocol for decentralized financial tools.

Secure

All encryption is handled client-side. Neither your passphrase nor any of your private information ever leaves your browser.

Counterwallet passphrases are highly secure, and protect your wallet from any brute force attacks. They are also rather easy to learn and hard to mistype.

Simple

With Counterwallet, your passphrase is literally your wallet, and all of your addresses and keys are generated on-the-fly when you log in.

There are no wallet files to backup or secure, and using your passphrase you can access your wallet from any trusted machine with a web browser.

Open-Source

Counterwallet is entirely open-source, so you know that it works exactly the way that it is supposed to.

If you like, you even run your own Counterwallet server.

The **Counterparty Foundation** is a non-profit organization dedicated to advancing the Counterparty protocol and its products, educating the community on the Counterparty technology, driving global Counterparty awareness, and ensuring Counterparty remains a successful and growing financial platform. The Foundation is governed by five directors, one Founding Director, and **four Community Directors**.