Bitcoin version 0.4.0 is now available for download at: http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoi
0.4.0/

The main feature in this release is wallet private key encryption; you can set a passphrase that must be entered before sending coins. See below for more information; if you decide to encrypt your wallet, WRITE DOWN YOUR PASSPHRASE AND PUT IT IN A SECURE LOCATION. If you forget or lose your wallet passphrase, you lose your bitcoins. Previous versions of bitcoin are unable to read encrypted wallets, and will crash on startup if the wallet is encrypted.

Also note: bitcoin version 0.4 uses a newer version of Berkeley DB (bdb version 4.8) than previous versions (bdb 4.7). If you upgrade to version 0.4 and then revert back to an earlier version of bitcoin the it may be unable to start because bdb 4.7 cannot read bdb 4.8 "log" files.

Notable bug fixes from version 0.3.24:

Fix several bitcoin-becomes-unresponsive bugs due to multithreading deadlocks.

Optimize database writes for large (lots of inputs) transactions (fixes a potential denial-of-service attack)

Wallet Encryption

Bitcoin supports native wallet encryption so that people who steal your wallet file don't automatically get access to all of your Bitcoins. In order to enable this feature, choose "Encrypt Wallet" from the Options menu. You will be prompted to enter a passphrase, which will be used as the key to encrypt your wallet and will be needed every time you wish to send Bitcoins. If you lose this passphrase, you will lose access to spend all of the bitcoins in your wallet, no one, not even the Bitcoin developers can recover your Bitcoins. This means you are responsible for your own security, store your passphrase in a secure location and do not forget it.

Remember that the encryption built into bitcoin only encrypts the actual keys which are required to send your bitcoins, not the full wallet. This means that someone who steals your wallet file will be able to see all the addresses which belong to you, as well as the relevant transactions, you are only protected from someone spending your coins.

It is recommended that you backup your wallet file before you encrypt your wallet. To do this, close the Bitcoin client and copy the wallet.dat file from ~/.bitcoin/ on Linux, /Users/(user name)/Application Support/Bitcoin/ on Mac OSX, and %APPDATA%/Bitcoin/ on Windows (that is /Users/(user name)/AppData/Roaming/Bitcoin on Windows Vista and 7 and /Documents and Settings/(user name)/Application Data/Bitcoin on Windows XP). Once you have copied that file to a safe location, reopen the Bitcoin client and Encrypt your wallet. If everything goes fine, delete the backup and enjoy your encrypted

wallet. Note that once you encrypt your wallet, you will never be able to go back to a version of the Bitcoin client older than 0.4.

Keep in mind that you are always responsible for your own security. All it takes is a slightly more advanced wallet-stealing trojan which installs a keylogger to steal your wallet passphrase as you enter it in addition to your wallet file and you have lost all your Bitcoins. Wallet encryption cannot keep you safe if you do not practice good security, such as running up-to-date antivirus software, only entering your wallet passphrase in the Bitcoin client and using the same passphrase only as your wallet passphrase.

See the doc/README file in the bitcoin source for technical details of wallet encryption.