A cryptographic hash function is a verification of a message integrity, so that a modification of the message change the hash function in a complex way, that it is not possible to evaluate without a force brute algorithm; so that the hash function permit the distribution of signed files.

I think that it is possible an alternative method of distribution of signed files.

A server A can distribute the file to the client C with pretty good privacy program, making public the private and public keys of a server B, so that the client C can download and decrypt the files using the PGP program, or the client C can use a server B that make the download and decryption work on behalf the client C, so that the client must have no knowledge, and must not have, the PGP program.

The PGP Global Directory could contain a public/private keys for cleartext and signed distributions, so that if the PGP program strengthens the cryptography, then an update of the cleartext distributions list could be updated.

Only the server A can change the contents of the file, so that the file is signed.