PGP Verification

This document is an **overview of the PGP verification process**. The following guides provide detailed, step-by-step instructions with exact commands for:

- **macOS**
- **Linux**
- **Windows**

When you download Bitcoin Knots, it's important to verify that the file was produced and signed by the developer, and that it has not been altered.

PGP verification checks two things:

1. **Integrity** – the checksum list proves your downloaded release file matches exactly what the developer published.
2. **Authenticity** – the signed checksum list proves the checksum file really came from the developer.

At a high level, here's what happens:

Download three files:

- The release file for your operating system (the zipped binary you'll install)
- The checksum list (`SHA256SUMS`) – lists the hashes of all release files and is used to verify the integrity of your download
- The signed checksum list (`SHA256SUMS.asc`) – the cryptographic signature of the checksum list, proving it came from the right developers

Understand the key process:
PGP works with private/public key pairs. After a release is built, developers use their **private key** to sign the checksum list. With their **public key**, we can use GPG to verify that the signature was created with the corresponding private key,

proving the authenticity of the release.

Confirm the developer's key:
GitHub is a common place to find a developer's public key, but you should never rely on it alone. It's best to confirm the key's **fingerprint**, a unique 40-character hexadecimal string, against another source the developer controls. This might be their personal website, a verified social media account, or a post they've signed with the same key.

Verify and compare:
After importing and verifying the developer's signature, you then compare the hash in the checksum file against your downloaded release file to confirm its integrity.