Hyphanet einfach erklärt

Antwort auf die Frage: Kann mir jemand Free-/Hyphanet erklären, als wäre ich fünf?

Du führst ein Programm auf deinem Computer aus, das sich mit anderen Programmen auf anderen Computern verbindet. Du kannst darin auf Links klicken, aber Links enthalten nicht nur eine Datei und eine Domain. Sie enthalten auch einen Entschlüsselungsschlüssel. Wenn du auf einen Link klickst, lädt er zuerst eine Datei von einem anderen Computer herunter, die weitere Links zu sehr kleinen Teilen enthält, aus denen die eigentliche Datei besteht. Dann verwendet er den Entschlüsselungsschlüssel, um die Datei zu entschlüsseln. Anschließend lädt er all diese Teile herunter, entschlüsselt sie und setzt sie zusammen, um die gesamte Datei zu bilden.

Aber woher kommen die Dateien? Sie werden auf anderen Computern im Netzwerk wie auf einem Proxy zwischengespeichert. Wie findet man den Computer für deine Datei? Jedes Programm gibt sich selbst eine Zahl zwischen 0 und 1. Jeder Schlüssel kann auch in eine solche Zahl zwischen 0 und 1 umgewandelt werden (ausgenommen der Entschlüsselungsschlüssel). Um den Schlüssel zu erhalten, schaust du dir die Programme an, mit denen du verbunden bist, und fragst das mit der ähnlichsten Zahl, ob es nach dem Schlüssel weiterfragen kann.

Warum sind sie da? Weil das Einfügen genauso funktioniert wie das Anfordern.

Warum ein Cache? Weil Daten, auf die nicht zugegriffen wird, innerhalb von 2 Wochen (reguläre Dateien) bis zu 1 Jahr (winzige Chat-Nachrichten) verschwinden.

Wie kann man damit einen Chat oder ein Forum oder eine Website erstellen? Schlüssel haben ein Präfix und einen Dateinamen-Teil. Du kannst viele Dateinamen auf das Präfix hochladen, z. B. Nachricht-1, Nachricht-2, ... Wenn du also das Präfix eines Benutzers kennst, kannst du alle Nachrichten abrufen, indem du einfach Namen mit einem bekannten Muster auswählst. Und es gibt Optimierungen, die es ermöglichen, in weniger als 30 Sekunden benachrichtigt zu werden, wenn die nächste Nachricht eingefügt wird.

Oder in Nicht-als-ob-ich-fünf-wäre-Sprache: Es ist eine vollständig dezentrale, die Privatsphäre respektierende Datenbank mit Namespaces, mit der du Schlüssel abonnieren kannst.