CashWeb

v1.0

Shammah Chancellor
shammah.chancellor@cashweb.io

Harry Barber
harry.barber@cashweb.io

David Schlesinger
david@cashweb.io

July 26, 2020

Abstract

CashWeb is a suite of protocols providing an open messaging standard with a reference implementation called "Stamp". It uses a federated network topology, similar to XMPP and SMTP, to provide the necessary scaling characteristics to replace those technologies. There is an estimated 300 billion emails sent each day as of 2020.[1] It is unique in that it provides end-to-end encryption and abuse mitigation without the need for central moderation.

1 Introduction

1.1 History

Early adopters of the internet saw it as a platform for inexpensive and fast sharing of new ideas, and receiving feedback. Systems like Usenet[2],[3] Email[4][5][6],[7] and XMPP[8][9][10][11] were built as decentralized platforms for this purpose.

However, due to the inherent design limitations of these systems, it is significantly more costly to receive messages than to send them. The expense of message processing is placed on the recipient with respect to processing power, long-term storage, and mental attention. This incentivizes sending large volumes of low-value messages. This cost has lead to a reliance on centralized systems to identify and filter messages while users delegated authority over their online identities and communications to third parties in exchange for convenience. As a result, a loss of user privacy and control over online identities occured.

As of June 2017, Facebook reported 2 billion users. By October 2018, Gmail reported 1.5 billion active users[12] and Cloudflare routed 10% of all internet traffic.[13] By June 2020, Google, Apple, and Microsoft held a total of 85% of total market share of email clients.[14] We now rely on very few companies to reliably and honestly manage critical internet services. Critical services which are not the source of revenue for these companies.

The centralization of the internet into a few large platforms, while providing the benefit of a seamless experience across the web, resulted from the inability to construct decentralized alternatives with similar convenience. However, since the development of Bitcoin,[15] it is possible to construct decentralized systems which do provide the conveniences users expect out of today's internet. The CashWeb protocols are centered around leveraging cryptocurrency to provide seamless online experiences – thus restoring user authority over their digital identities and privacy.

1.2 Forces of Centralization

1.2.1 Identity Management

In the past, internet service providers (ISPs) offered email services to their customers. This meant that when a user moved residences or wanted to switch service providers, their email address would change (e.g. john.doe@sonic.net). Using email accounts provided by global companies, like Google and Microsoft, enabled users to avoid the effort associated with updating their contacts and potentially missing valuable communications.

Due to delegating the management of email accounts to third party businesses, digital identities have become more stable. As a result, businesses and users have begun to rely on them for more and more important communication and as a digital identity. It is now the root of our online identity and provides the authentication mechanism we use for logging into most websites. Today, loss of access to our email has become a life-altering event with significant consequences. Maintaining access to our email may be out of our control, as a loss may result due to a compromised password or a judgement by the provider.

Should we now want to migrate email providers for personal reasons, it has become an insurmountable task. Users may find themselves effectively powerless to hold their service providers accountable. Having our online identity under our sole control is of the utmost importance.

1.2.2 Spam

While email was envisioned as a person-to-person and machine-to-machine messaging system, the vast majority of emails are now machine-to-human. These messages largely consist of useless advertisements, but require processing power and human attention to evaluate and identify for deletion. Large-scale centralized email providers (e.g. Gmail[1] and Hotmail[2]) benefit from their message volume by being able to identify similar messages sent to a large number of different customers and filter them out.

Ironically, companies we actively do business with are sending more "opt-in" marketing messages. These are largely served unfiltered by centralized platforms despite the original promise of these platforms to provide users with only high-value communications.

At the same time, much of our high-value communications with personal acquaintances have moved to digital platforms like SMS, Telegram, Messenger, WhatsApp, Twitter, and Signal. In order to dissuade spam on these platforms, they require providing a telephone number, or email, or both, in order to have an account.

If an account starts producing too much unwanted content on these systems, the account is restricted or deleted. The identifying phone number or email address is permanently banned.

1.2.3 Consequences

While large services have provided us with much-needed convenience, centralized providers must also generate revenue to maintain their infrastructure and generate a profit. Many of these services provide access to email and websites for "free."

> "If you are not paying for it; you're the product being sold."
>
> - Robert Danielson

Some providers still provide paid email access while essentially offering privacy as a product. However, these providers still have access to the same data about their users as free services. There becomes a financial incentive to sell this data while maintaining a guise of privacy. Regardless of the ethics of paid providers, emails exchanged with free email providers (e.g. Gmail) are still indexed and categorized for advertising.

In non-email systems, our identity is increasingly tied to our email or phone numbers. This association means that there is a clear association between all other accounts and digital interactions. Being able to collate all this data about a user, and form a more complete profile, is extremely valuable to advertisers.

Indeed, various companies (e.g. LiveRamp) purchase data across multiple services and collate it based on emails and phone numbers. Device fingerprinting is also employed to combine this data with ones web

[1] `https://mail.google.com`
[2] `https://outlook.live.com`

browsing history while also providing a way to associate email addresses and phone numbers should users log in to two different accounts during the same session.

The stated purpose of this is to provide highly-specific advertising. This may be desirable to users in finding products they want. However, there are many other purposes this data is used for which are of concern. These other uses are outside the scope of this paper.

2 The CashWeb Protocol

2.1 Philosophy

In order to provide an alternative to the existing system, Cashweb adheres to the following principles:

2.1.1 Simplicity

In order to attract a wide-range of users, CashWeb must be a solution which requires minimal technical expertise. It must be possible to use third parties to provide hosting and operation of services for those uninterested in provisioning their own hardware.

Similarly, the base protocol must be as simple as possible to attract a wide-range of developers.

2.1.2 Migratability

Users must have control over access to their own identities, and the ability to migrate from one service provider to another. The ability to easily migrate between service providers enables users to hold service providers accountable for their actions and fosters healthy competition.

2.1.3 Recoverability

In the case of a loss of identity, it must be possible to recover gracefully. In order to make authentication transferable from one service provider to another, asymmetric cryptography must be employed so that identification is not a responsibility of CashWeb service providers. Should a user lose their phone or computer, and another person obtains their private key, their identity must be able to be recovered.

2.1.4 Security & Privacy

In order to protect the privacy of users, the contents of messages must not be readable by third parties including CashWeb service providers. All communications between two parties should be encrypted by default using well established standards such as the Advanced Encryption Standard (AES) and elliptic curve cryptography (ECC).

In addition to the strong default security, users must be able to upgrade their security using existing overlay networks (e.g. Tor).

2.1.5 Permissionlessness

The protocol must be open-source and well-maintained reference implementations/documentation should be provided. This model provides easy access to potential developers and will allow growth in the ecosystem surrounding CashWeb.

While the base protocol is open and publicly maintained, individual software implementations may be privately maintained.

2.1.6 Scalable Privacy

The protocol should allow for users to determine their level of desired privacy. The base layer should provide protocol mechanisms for users to determine what they keep private, while providing defaults which are reasonable for most users.

2.1.7 Simplicity & Extensibility

In order to allow for the ubiquitous use, the most basic feature set must be extremely simple. It should also be extensible enough to provide for businesses to provide more complicated functionality without disrupting existing user and software clients.

2.1.8 Integrability

The protocol should be built on standard web technologies which most users and software developers are already familiar with such as HTTP.

2.2 Central Concepts

In order to meet the requirements described above, CashWeb protocol revolves around the following core concepts:

2.2.1 Web Standards

The CashWeb system adheres to the established web standards to allow quick and easy integration into existing protocols and infrastructure. "Bearer"-style tokens are used extensively in combination with existing cryptocurrency payment standards to allow authenticated access to resources to be purchased with cryptocurrency. Messages are sent and received using HTTP/2[16] and WebSockets[17] to enable the use of existing internet infrastructure and services.

2.2.2 Cryptocurrency

In order to maintain secure communication and the permissionless nature of the CashWeb system, it must be impractical for a single party to send large volumes of unsolicited messages. All messages sent should impose a cost on the sender that is paid to the recipient. In order to support this requirement, payments need to be at the center of the design.

Traditional systems require trusted third parties and complex integrations with the traditional banking system. Visionaries, like Hal Finney, conceived of this problem being solved through "reusable proof-of-work" (RPoW). Unfortunately, Finney's original design was impractical due to the need for centralized management of the RPoW tokens. However, this idea can now be realized through the use of peer-to-peer digital cash systems like Bitcoin (BTC).

Using a cryptocurrency, instead of traditional banking integrations, synergizes well with secure, open, permissionless communication. The same keys may be used to send and receive funds that are used to provide encryption for messages.

Unfortunately, the Bitcoin (BTC) network does not support the transaction volume which would be necessary for a widely used messaging platform. Most other cryptocurrency systems also do not intend to support volumes on the order of email, ignoring spam. The ones that do support these volumes have centrally managed economic policies. Such management would give them authority over the ability to send and receive messages.

Thus, Bitcoin Cash (BCH) was selected due to its roadmap being highly compatible with the requirements of the CashWeb project. The Bitcoin Cash roadmap stresses the importance of instant transactions accomplished on a global scale while building on the tokenized proof-of-work conceptualized by Satoshi Nakamoto.

2.2.3 Identity

Each user identity is pseudonymous, and associated with a public key. These public identities can be easily and inexpensively generated from a single master key. Each identity key is acknowledged by the network via various small payments to the miners of the Bitcoin Cash network. These small payments include a cryptographically verifiable commitment to the identity which can provide proof that the payment was made to any third party.

Additionally, these pseudonyms can be made such that they can be proven to have been derived from another hidden key at a later date. Such proofs enable the specific key associated with a pseudonym to be revoked, and rotated, in a trustless way. This enables the contacts of the pseudonym to be informed without the need

for re-establishing trust. The specific details of these identity schemes are left to further detailed protocol specifications, and the protocol is extensible to future schemes should a need arise.

2.2.4 Message Format

All messages within the CashWeb system use the Protocol Buffer[18] message format. "Protobufs" are now in wide use, easy to implement in a variety of languages, and serializable to binary.

2.3 Infrastructure

2.3.1 Keyservers

The CashWeb protocol includes a network of keyservers which provide a public & distributed metadata registry. The registry is intended to track small amounts of metadata associated with cryptographic keys. Each entry in the keyservers is replicated across the network to provide censorship resistance. A peer-to-peer protocol is included which provides eventual consistency.

This metadata is indexed by the hash of users public key and includes said public key, a body of information, and a signature covering the body providing integrity, authentication, and non-repudiation. Metadata updates are permissioned by providing valid signatures.

Uploading data to the keyserver is protected by a "Proof-of-Payment protocol" (POP protocol). This provides a way to anchor on-chain value to specific updates and therefore allowing DoS resistant replication across the keyserver network.

The specialised CashWeb keyserver has the following benefits over existing GPG infrastructure:

- Anti-DDoS mechanisms are considered from inception and hence we can arrive at a more simple and robust overall design.
- HTTP2 makes it significantly simpler to interact with. It is immediately compatible with off-the-shelf load balancers.
- The payload format is more concise than what existing keyservers provide. However, X.509 certificates can also be provided inside an entry associated with a given address.

The CashWeb keyserver can be used for a wide-range of applications (which are eluded to below), however our primary use-case is to record a pointer to the specific relay server managing that user's messages. In this way any user with access to the keyserver network and a hosted address, may lookup the address on the keyserver network and then redirect to their specific relay server in order to bootstrap communication.

Another function of keyservers is to provide revocations of keys in the event that a user loses their on-line private key. The keyservers enable the publication of new keys to existing contacts in a trustless manner. This allows for key-rotation on Bitcoin, which has been a significant deficiency in all cryptocurrencies since the Bitcoin whitepaper was written.

2.3.2 Relay Servers

«««< HEAD Relay servers provide the combined purpose of both POP and SMTP servers. They accept messages on behalf of the clients, and verify basic integrity of these messages. They also host profile information including avatars and other information. While the relay servers currently only provides messaging, profile names, and icons, the software can easily be extended to provide status messages, microblogs, and other potentially useful functions. ======= Relay servers provide the combined purpose of both POP and SMTP servers. They accept messages on behalf of the clients, and verify basic integrity of these messages. They also host profile information including avatars and other information. While the relay servers currently only provide messaging, profile names, and icons, the software can easily be extended to provide status messages, microblogs, and other potentially useful functions. »»»> More fixes from Robert Danielson

The distinction here between keyservers and relay servers is made due to separation of concerns:

- Keyservers provide global replication and therefore censorship-resistance for small amounts of unencrypted data.
- Relay servers serve only specific users and therefore can cheaply host large amounts of encrypted personal data.

Uploading to, and pulling messages from, the relay server should be protected by the Proof-of-Payment protocol. This allows for paid, but pseudonymous registration to the service; protecting user privacy. Users can easily migrate between relay service providers should they choose due to using a standardized authentication and authorization mechanism, along with the global keyserver network.

2.3.3 Messaging Client

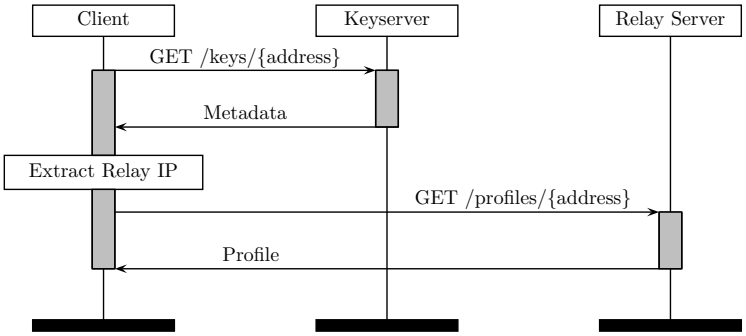
An end-user client is necessary for interacting with this system in a easy-to-use way. The client serves to manage funds associated with sending and receiving messages, update keyservers as to which relay server the user accepts messages, and connect to and process messages received from the relay servers.

The messaging clients are the most complex portion of the CashWeb system. It must also handle management of digital funds used to generate stamps and other micropayments. As such it must also take on the responsibility of being a cryptocurrency wallet. Additionally, the majority of the protocol is handled via encrypted structured payloads that the messaging client needs to parse and process. Both the keyserver and the relay server are for the most part agnostic to the protocols that wallets may use to talk to each other.

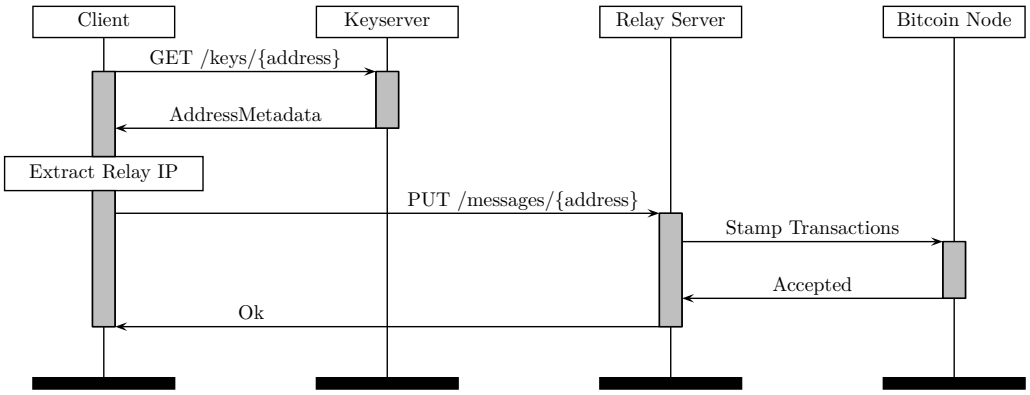
This allows the functionality to evolve gracefully over time without needing major changes to the underlying communications infrastructure. Wallet developers may add and evolve functionality over time. Wallets need only ignore payload types they don't understand, while enabling protocol changes without needing wide-scale consensus on additions.

2.3.4 Protocol Flow

msc Profile Retrieval



msc Message Send



3 Applications

3.1 Standardized Authorization & Authentication

The Proof-Of-Payment (POP) protocol enables the standardized and seamless use of existing HTTP technology, but without the use of complicated billing infrastructure and account management. It allows the pseudonymous purchase of a JWT[19] API token, without requiring an account management system, billing frontends, or other complicated infrastructure.

3.2 Distributed Identity Management

Having a standard keyserver infrastructure benefits a range of applications. Such as cryptographically secure, but updatable, contact exchange via QR codes or other mediums. The ability to rotate this information allows for important key revocation and rotation events. It provides a comprehensive mechanism for managing online identities in a decentralized and trustless manner. Having neutral identity infrastructure provides a strong incentive for participation from all online users; unlike centralized identity providers (e.g. Google, Facebook, etc.)

3.3 Open Messaging

The combination of the POP protocol, keyservers, and relay servers, allows for advanced privacy features and SPAM-free communication. The ability to send structured messages with attached value, allows for all kinds of fee-based human-to-human, human-to-machine, machine-to-human, and machine-to-machine message processing. The most obvious application of this is peer to peer payments and messaging. However, there is potential for other services such as online "bots", marketplaces, Web3.0 applications, and decentralized financial protocols.

4 Conclusion

The CashWeb protocol's aim to provide censorship-resistant solutions to common technological problems which continually are reinvented in proprietary ways. CashWeb, like the underlying cryptocurrency technology, allows for the disintermediation of authentication, identity management, and messaging. It enables the seamless use of payments across all internet infrastructure without the introduction of permissioned financial intermediaries.

Attaching payments to peer-to-peer communications enables the disruption of existing internet power structures. Centralized moderation is obviated, and thus CashWeb provides digital "neutral ground" for the collaboration of all willing parties. It removes the incentive for continued "walled-garden" communications networks.

Digital currency combined with messaging, as originally imagined by Hal Finney,[20] provides equal footing for all participants in the global dialog. This is a critical step, and critical infrastructure, in maintaining human rights and economic freedom as technology continues to evolve. It also has the potential to change the way humans communicate and think by enabling us to focus our attention on information which is objectively valuable.

Because CashWeb operates on integrated micropayments, users are no longer a product.

References

[1] Statista. Daily number of e-mails sent worldwide per day. Web document, 2020.

[2] Dan Kohn, Ken Murchison, and Charles Lindsey. Netnews Article Format. RFC 5536, November 2009.

[3] Charles Lindsey and Russ Allbery. Netnews Architecture and Protocols. RFC 5537, November 2009.

[4] Pete Resnick. Internet Message Format. RFC 5322, October 2008.

[5] Dr. Marshall T. Rose and John G. Myers. Post Office Protocol - Version 3. RFC 1939, May 1996.

[6] Dr. John C. Klensin. Simple Mail Transfer Protocol. RFC 5321, October 2008.

[7] Steve Hole and Alexey Melnikov. IMAP Extension for Conditional STORE Operation or Quick Flag Changes Resynchronization. RFC 4551, June 2006.

[8] Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Core. RFC 3920, October 2004.

[9] Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence. RFC 3921, October 2004.

[10] Peter Saint-Andre. Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM). RFC 3922, October 2004.

[11] Peter Saint-Andre. End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP). RFC 3923, October 2004.

[12] Gmail, October 2018.

[13] Cloudflare. African traffic growth and predictions for the future. Web document, 2018.

[14] Litmus Labs. Email client market share. Web document, 2020.

[15] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Web document, 2008.

[16] IETF. Rfc7540 - hypertext transfer protocol version 2 (http/2). Web document, 2015.

[17] IETF. Rfc6455 - the websocket protocl. Web document, 2011.

[18] Google. Protocol buffers version 3 language specification. Web document, 2015.

[19] IETF. Rfc7519 - json web token (jwt). Web document, 2015.

[20] Hal Finney. Reusable proofs of work. Web document, 2004.