Webcash

Simple Electronic Cash for Simple Electronic Payments

https://webcash.org/

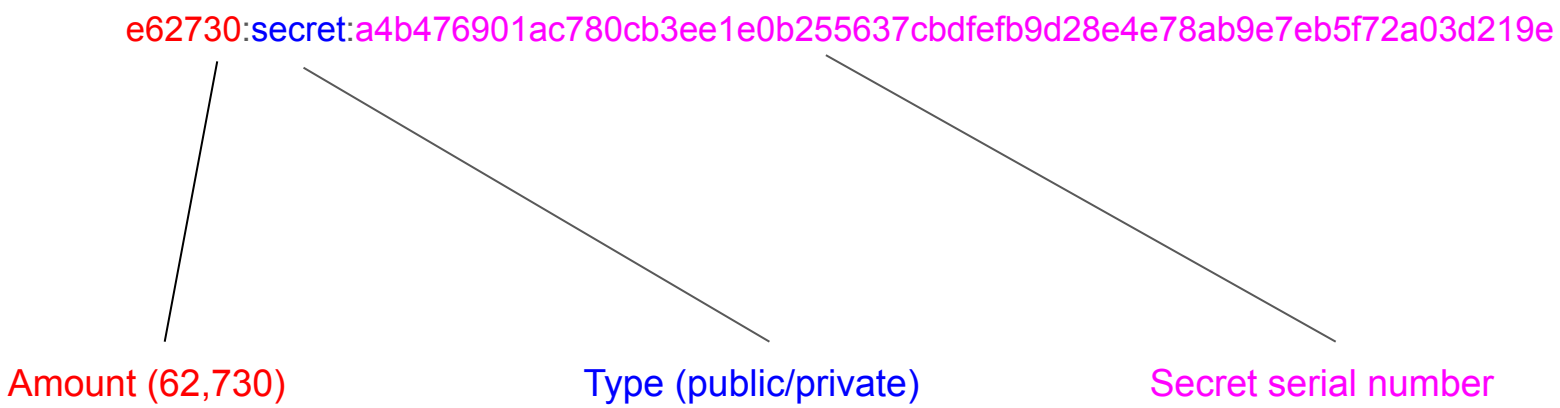
March 2022

Bryan Bishop <kanzure@gmail.com>

Properties of simple Internet payments

- Easy to use and understand
- Simple to integrate
- Fast
- Low or zero fees
- Private
- Fair mining
- Monetary policy focused on scarcity
- Decentralized peer-to-peer (p2p) payments

This is webcash



(It's kind of like a Bitcoin private key)

Roles

Central Server: The central server maintains a database with a list of already-spent webcash and outstanding webcash not yet spent. Provides the server side for the webcash protocol.

Users: keep and transmit webcash between themselves. They talk to the central server to (1) confirm that webcash has not been already used, and (2) use new secrets to protect their webcash from double spending.

Wallet: Stores webcash for a user. Software designed to talk to the Central Server on behalf of a user. Implements the client side of the webcash protocol.

Miners: create new webcash by Proof-of-Work, talking to the server. Implements the client/miner side of the webcash protocol.

Payments step-by-step (1)

Alice wants to pay Bob the amount of $10 webcash.

1. Alice knows she has $10 webcash and where she wrote it down.
2. Alice finds her webcash in a Word document on her computer.
3. Alice copies (Ctrl-C) the $10 webcash into her clipboard.
4. Alice pastes (Ctrl-V) the $10 webcash in an email sending to Bob.
5. Bob receives the $10 webcash, and opens his webcash wallet software.
6. Bob asks his wallet to insert/save the webcash into his wallet.
7. Bob's wallet contacts the webcash server and asks (1) has this webcash been double spent, and (2) please use Bob's new webcash secret so that Alice cannot double spend that same webcash going forward?

Payments step-by-step (2)

Alice has $100 webcash and wants to send $10 webcash to Bob.

1. Alice opens her webcash wallet and asks it for $10 webcash.
2. The wallet either (a) finds a denomination of $10 already in its ledger, or (b) finds $100 webcash and has to split it up.
3. To split up $100 webcash, the wallet talks to the central webcash server and asks for $10 and $90 webcash.
4. Alice copies (Ctrl-C) the $10 webcash and emails the webcash to Bob.
5. Bob asks his wallet to insert/save the webcash once he reads the email.

Alternatively, similar to physical cash, Alice could give $100 to Bob with the expectation that he will return change.

The central webcash server

- Kept very simple
- Functions:
  - (1) Status check: does this webcash exist? Has it already been spent before? What is the denomination on the webcash?
  - (2) Replacement: given some valid outstanding webcash, replace the webcash with a new secret so that its security can be reset.
  - (3) Database of unspent webcash and spent webcash
  - (4) Web form interface for users that want to try without an webcash wallet (it's harder to use though...)

While the server is centralized, webcash payments are themselves decentralized. The server only talks to a single user when they present webcash, and it does not transfer webcash from one person to another.

Centralization is not for everyone, and that's OK: some users prefer completely decentralized cryptocurrencies, and others don't want to run blockchain nodes.

Mining with Proof-of-Work

webcash is created by decentralized miners that submit new webcash created by Proof-of-Work to the central webcash server.

The protocol requires a fee of 5% of all mined webcash.

Monetary policy

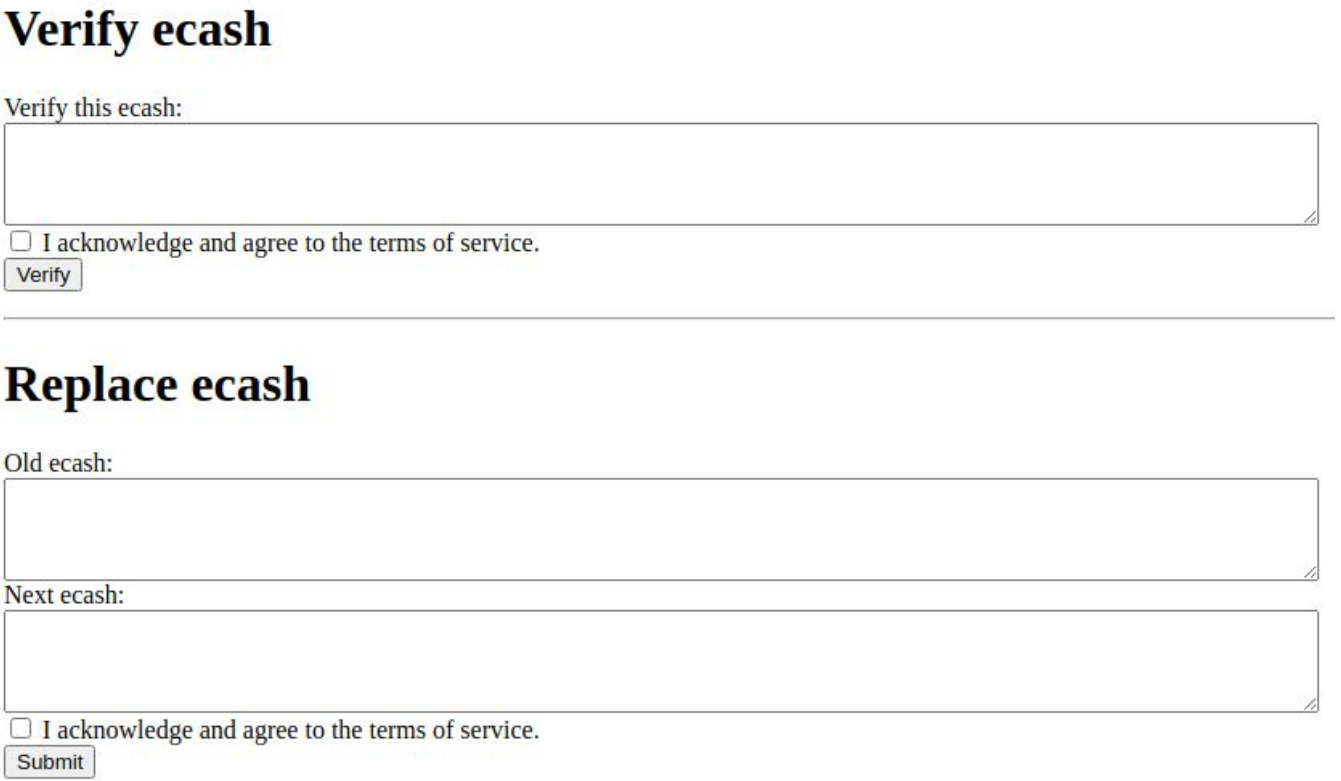
The webcash monetary policy is based on scarcity.

The supply schedule calls for 200,000 webcash every 10 seconds halvening every 2 months for 3 years for a total supply of 210,000,000,000 webcash.

Wallets

- Terminal client (python) -- done
- Terminal miner (python) -- done
- Web form interface -- done
  - Not as user friendly, but available for users who want to try it out.
- Web wallet (react/typescript) -- WIP (needs styling)

Web form (wallet "alternative") on webcash.org



Comparing to Bitcoin

- No addresses
- No accounts
- Faster confirmations
- Cheaper - lower/zero transaction fees
- Easier to understand and integrate into new platforms
- Easier to build wallets
- Mining is decoupled from payments
- Payments are made directly from one user to another user using any protocol they wish.

Have you heard of NoSQL? Well, webcash is NoBlockchain technology.

Food for Thought

No addresses: While there are no addresses in the webcash system (as the webcash server doesn't work that way), it's still possible to use asymmetric encryption like PGP. Merchants can post a public key to their website, and users could encrypt webcash to that public key so that only the merchant can decrypt their payments. All of this is possible "on top" of webcash and does not need to be a part of the webcash system itself.

Other properties

- Nothing backs webcash. There are no dollars in reserve. It's not a stablecoin.
- webcash is not a deposit and no depositor relationship is created by the use of webcash, and as such, Users are not "registered" as no depositor relationship exists;
- Similarly, there are no withdrawals as there is nothing to withdraw
- It's not a loan.
- webcash is not registered in your or anyone else's name, and is your sole responsibility to protect and manage its exposure or loss;
- Users of webcash are not customers of the webcash server.

See the Terms of Service for more information.

Disclosures, acknowledgements and agreements

API requests to the central webcash server must have an agreement to the webcash Terms of Service. This way, the rights of users and the server are outlined and agreed to before commencing use of the services.

API requests that do not include this acknowledgement will not be honored.

The protocol could be upgraded for any number of disclosures, acknowledgements, or agreements.

The Terms of Service can be found on the website:

https://webcash.org/terms

Compliance

Nothing in the design of webcash prohibits regulated entities from fulfilling their regulatory obligations, including customer due diligence, transaction monitoring, recordkeeping, reporting suspicious transactions, and complying with the FATF Travel Rule.

Users must comply with all applicable laws and regulations regarding their use of webcash, per the webcash Terms of Service. See the Terms for more information.

Transaction history data obtained by the webcash server could be utilized by blockchain analytics companies to assist regulated entities with fulfilling their regulatory obligations. There are currently no specific plans for publishing this data.

Why webcash?

- Fast, decentralized payments at the speed of Internet commerce
- Everyone loves mining
- Monetary policy that encourages early adoption
- Internet commerce - simpler integration
- No blockchain nodes
- Represents a missing piece of e-cash history -- focused on adoption and simplicity, rather than mixing banking with privacy maximalism (a noble cause itself, of course)
- Why not?

Next steps

Setup a webcash wallet today.

Start mining.

Join our discord group.