

Comparison of Payment Methods (and Cryptocurrencies)

INTRODUCTION GOES HERE - TO DO

Comparison of Payment Methods

Source: eylenburg.github.io

Last updated: 3 May 2024

Utility

Scalability / number of transactions

Payment speed

Transaction fees
(assuming no currency conversion)

Decentralization

Can transactions or accounts be blocked?












Can funds be frozen or confiscated?

Fungibility

Privacy

Anonymous accounts/wallets

Transaction privacy

| Fiat money | | | | | Cryptocurrencies | | | |
|--|--|--|---|--|--|---|--|---|
| Physical cash | Bank transfer | Bank-issued card (debit/credit) | PayPal | Central Bank Digital Currency (CBDC) | Bitcoin (BTC) | Bitcoin Cash (BCH) | Litecoin (LTC) | Monero (XMR) |
|  |   |   |  |  |  |  |  |  |
| Theoretically unlimited number of transactions as payments are decentralized (peer-to-peer). | Theoretically unlimited number of transactions as payments are decentralized (bank-to-bank). | Technical limits are unknown. Reportedly, VISA processes ~24,000 TPS and Mastercard ~5,000 TPS on average. | Technical limits are unknown. Reportedly, PayPal processes 192 TPS on average. | TBC | No, the blockchain can process only 7 TPS and is chronically congested. The "Layer 2" <i>Lightning Network</i> allows "millions to billions" of TPS. | Theoretically unlimited TPS due to variable blocksize (since May 2024). | No, the blockchain can process only 56 TPS, although this is currently sufficient. <i>MWEB (Mimble-Wimble Extension Blocks)</i> improve scalability by aggregating multiple transactions. The "Layer 2" <i>Lightning Network</i> allows "millions to billions" of TPS. | Theoretically unlimited TPS due to variable blocksize. |
| Instant | Depends on the bank or country, can be instant or take several days. | Instant | Instant | TBC | 10 minutes for one block confirmation. Instant with the "Layer 2" <i>Lightning Network</i> . | 10 minutes for one block confirmation. Instant with 0-conf which is relatively safe for BCH due to double spend proofs. | 2.5 minutes for one block confirmation. Instant with the "Layer 2" <i>Lightning Network</i> . | 20 minutes to fully confirm payment and be able to spend received money (10 block confirmations, 2 minutes per block). |
| None. | Depends on the bank or country. Usually no fees, with some exceptions (e.g. for large transfers or certain international payments). | Depends on the card issuer and country. Various fees, both variable and fixed, are charged and add up to on average around 2-3% of the transaction value. The fees paid by the merchant/recipient. | Various fees are charged, usually paid by the merchant/recipient. A typical fee for a domestic online purchase would be 2.9% + \$0.30. Payments to "friends and family" are free. | TBC | Depends on the desired transfer speed and the network congestion. From 03/2017 to 03/2024 the average fee was about \$3.50 but of course this is highly dependent on the BTC/USD exchange rate. Cheap transactions using the <i>Lightning Network</i> are also possible. | Very low fees. Normally, a transaction costs a few USD cents. | Very low fees at current network usage. Normally, a transaction costs a few USD cents. Cheap transactions using the <i>Lightning Network</i> are also possible. | Very low fees. Normally, a transaction costs a few USD cents. |
| | | | | | | | | |
| Not possible | Yes (by bank) | Yes (by bank or card issuer) | Yes (by PayPal) | Yes (by government/central bank) | Not possible if using a non-custodial wallet. | Not possible if using a non-custodial wallet. | Not possible if using a non-custodial wallet. | Not possible if using a non-custodial wallet. |
| Yes, if physically confiscated. | Yes (by bank, police or government) | Yes (by bank, police or government) | Yes (by PayPal, police or government) | Yes (by central bank, police or government) | Not possible if using a non-custodial wallet. | Not possible if using a non-custodial wallet. | Not possible if using a non-custodial wallet. | Not possible if using a non-custodial wallet. |
| Generally yes, but it is possible to identify specific banknotes by their serial number. | No | No | No | No. Each unit of money is uniquely identifiable and all transactions are centrally recorded. | No. Due to the public blockchain, coins can become "tainted" and wallets can be blacklisted. Source of funds can be obscured by mixing (<i>CoinJoin</i>), with various downsides. | No. Due to the public blockchain, coins can become "tainted" and wallets can be blacklisted. Source of funds can be obscured by mixing (<i>CashFusion</i>), with various downsides. | No. Due to the public blockchain, coins can become "tainted" and wallets can be blacklisted. Coins used in <i>MWEB</i> transactions are fungible. | Yes |
| | | | | | | | | |
| (no accounts) | No, KYC required by law | No, KYC required by law. Except for certain prepaid cards paid with cash or crypto. | No, PayPal requires customer identification. | No (TBC) | Yes, but most CEX require KYC. | Yes, but most CEX require KYC. | Yes, but most CEX require KYC. | Yes, but most CEX require KYC. |
| Private by default. Even sender and receiver can remain anonymous from each other. | The involved banks and the government (on request) can view transactions. Sender and recipient know each other. | The involved banks, the card issuer, and the government (on request) can view transactions. Sender and recipient know each other. | PayPal and the government (on request) can view transactions. Sender and recipient know each other. | The government has direct visibility of financial transactions and the spending of everyone. Sender and recipient know each other. | Everyone can view transactions on the blockchain. Using the <i>Lightning Network</i> slightly improves privacy. | Everyone can view transactions on the blockchain. | Everyone can view transactions on the blockchain, except for <i>MWEB</i> transactions. Using the <i>Lightning Network</i> slightly improves privacy. | Private by default. Even sender and receiver can remain anonymous from each other. View keys exist for opt-in transparency. |

| | Fiat money | | | | | Cryptocurrencies | | | |
|--|--|--|--|--|---|--|--|--|---|
| | Physical cash | Bank transfer | Bank-issued card (debit/credit) | PayPal | Central Bank Digital Currency (CBDC) | Bitcoin (BTC) | Bitcoin Cash (BCH) | Litecoin (LTC) | Monero (XMR) |
| Wealth privacy | Only the owner knows his/her total wealth. | The bank and the government (on request) can see the funds on the account. | The bank and the government (on request) can see the funds on the account. | PayPal and the government (on request) can see the funds on the account. | The government can see the funds on the account. | Everyone can see the funds of a wallet on the blockchain. | Everyone can see the funds of a wallet on the blockchain. | Everyone can see the funds of a wallet on the blockchain, <u>except those relating to MWEB transactions.</u> | Only the owner knows his/her total wealth. |
| | | | | | | | | | |
| Acceptance Useable for in-person payments (e.g. shop)? | Yes | No | Yes | No | TBC | Yes, but negligible point-of-sale adoption. | Yes, but negligible point-of-sale adoption. | Yes, but negligible point-of-sale adoption. | Yes, but negligible point-of-sale adoption. |
| Useable for online payments? | No (except for cash in mail) | Yes | Yes | Yes | TBC | Yes | Yes | Yes | Yes |
| Useable for transfers between individuals? | Yes | Yes | No | Yes | TBC | Yes | Yes | Yes | Yes |
| | | | | | | | | | |
| Other considerations Automatic recurring payments? | No | Yes (direct debit, standing order) | Yes | Yes | TBC | No (unless supported by wallet app) | No (unless supported by wallet app) | No (unless supported by wallet app) | No (unless supported by wallet app) |
| Chargebacks to protect buyers from fraud? | No, not possible with physical money | No, transactions are final | Yes, under certain circumstances | Yes, under certain circumstances | TBC | No, transactions are final | No, transactions are final | No, transactions are final | No, transactions are final |
| Useable without electricity or Internet? | Yes | No | No | No | No | No | No | No | No |
| "Store of Value" narrative | No, fiat money has an unlimited supply as the central bank can create new money, thereby devaluing existing money. | | | | No. It is inflationary like all fiat money and additionally <u>can be programmed to expire after a certain time</u> | Yes, deflationary. Fixed maximum supply which is further reduced by lost wallet seeds. | Yes, deflationary. Fixed maximum supply which is further reduced by lost wallet seeds. | Yes, deflationary. Fixed maximum supply which is further reduced by lost wallet seeds. | Probably yes. There is a perpetual coin issuance (tail emissions) with inflation asymptotically approaching zero. Supply is further reduced by lost wallet seeds. |

So, what's the conclusion?

- **Use Monero if you can.** ← Monero comes close to being the digital equivalent of cash - decentralized, uncontrollable, private. We need to make sure it can be used everywhere, not just in darknet markets or for buying VPNs and donating to piracy websites. We also need to establish decentralized, trustless, KYC-free ways to exchange fiat to Monero and back.
- **Pay in cash in physical shops.** ← The more cash is used, the harder it will be for governments and companies to kill it.
- Resist your government if they try to phase out cash, introduce CBDCs, or attempt to suffocate cryptocurrency use with punitive KYC regulations. **CBDCs = financial totalitarianism.**
- Bitcoin - the first cryptocurrency - has ultimately failed to become a viable payment method. *Lightning* won't be the solution for Bitcoin's scalability and privacy problems either: [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) [\[5\]](#).

Do you have any comments or corrections? [Please drop me an e-mail](#) or [create an issue on Github](#)

► Donations welcome! (click here for details)

