# Bitcoin Cheque: A second-layer payment system

Arild Hegvik

www.bitcoincheque.org

2021-02-28

**Abstract.** A payment system that supports unlimited number of instant Bitcoin payments is described. The system is based on trusted third parties, which record transactions outside of the blockchain and thus overcomes the Bitcoin scalability problem. Payments are standardized and sent as Bitcoin Cheques, and all users can send cheques to each other using a Money Address, which conceptually is like an e-mail address. The banks later clear out aggregated outstanding receivables and payables amounts in bitcoin directly with each other and will not depend on a central clearinghouse. Necessary standards and protocols are described: The Bitcoin Cheque itself, Money Address, Money Account API, Payment Request, and Payment URI. These are flexible building blocks, which can be used to implement a wide range of payment solutions. The system has incentives to enable mass adoption by having a network effect.

## 1. Introduction

Bitcoin [1], as a secure electronic cash system, has been running stable for over a decade with practically no downtime. In the era of central banking and inflating fiat currencies, Bitcoin appears to be one of the very few monies capable of storing wealth. Forcing a government to use a sound monetary system is a prerequisite for maintaining a healthy economy and preserving the sovereignty of the individuals [2]. This is what Bitcoin should aim for.

However, the blockchain technology is imposing a limit on the Bitcoin transaction capacity and thus preventing it from scaling up for mass usage. The time required to confirm the transactions is another barrier holding Bitcoin back from being used for instant payments in daily life.

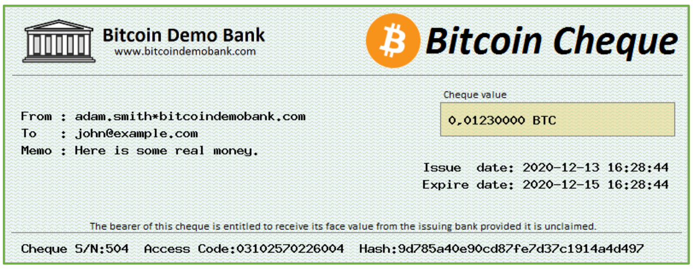
What is needed is a second-layer payment system that can record payment transactions outside of the blockchain. For such a system to succeed, it not only must overcome the technical limitations of Bitcoin, but should also offer attractive features for the public, incentivize people to start using it, be easy to implement, and adaptable to future needs.

This whitepaper describes such a payment system based on trusted third parties offering banking and payment services for its users. It promotes an open standard for cryptocurrency payments, which will enable independent parties to participate in forming payment networks. The system supports features like user-friendly bitcoin transfers, instant payments, clickable payment links, micropayments, and currency exchange. These features can be embedded into any web page.

## 2. Bitcoin Cheque

Bitcoin Cheque [3] is a file promising that its issuer will pay a certain amount of bitcoin to a recipient. The cheque can be used to transfer bitcoins between two persons or as payment for a purchase. Assuming the recipient trusts the cheque and its issuer, this can facilitate instant payment.

The cheque's file format is standardized so that it can be read and processed by different parties. The Bitcoin Cheque shares many characteristics with the long-existing bank payment cheque, which is usually printed on paper. An image of the cheque can be generated to visualize it, as the example in Figure 1 shows. The image can be embedded into the cheque file, or linked externally.



Bitcoin Demo Bank
www.bitcoindemobank.com

Bitcoin Cheque

Cheque value
0.01230000 BTC

From : adam.smith*bitcoindemobank.com
To : john@example.com
Memo : Here is some real money.

Issue date: 2020-12-13 16:28:44
Expire date: 2020-12-15 16:28:44

The bearer of this cheque is entitled to receive its face value from the issuing bank provided it is unclaimed.

Cheque S/N:504 Access Code:03102570226004 Hash:9d785a40e90cd87fe7d37c1914a4d497

**Figure 1: Image generated from a Bitcoin Cheque.**

Conditions can be added to the cheque to set constraints for who can claim and receive its face value. The intended recipient is written on the cheque and can be set as a Bitcoin wallet address, an e-mail address, or a Money Address [3]. A Bitcoin Cheque includes an expiration time. If it has not been claimed within that time, the cheque expires, and the bitcoins will be returned to the user who wrote it. The cheque can be signed digitally so its authenticity can be verified by anybody having the issuer's public key.

## 3. Bitcoin Bank

Bitcoin Cheques can typically be issued by banks, custodian providers, and cryptocurrency exchanges; all of these are referred to as Bitcoin Banks, or just banks.

A Bitcoin Bank can store bitcoins for its users in bank accounts. For a user to write a cheque, it may be necessary to first deposit enough bitcoins to his account. Figure 2 shows a bitcoin transfer between two users by sending a Bitcoin Cheque.

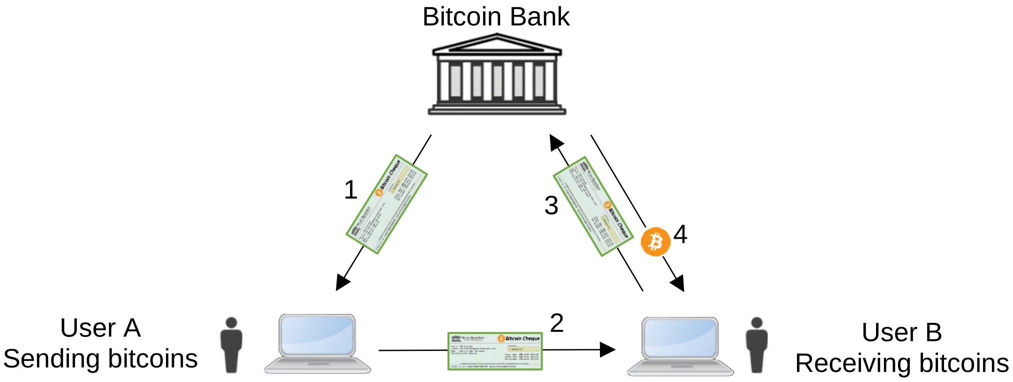


**Figure 2: Sending bitcoins by using a Bitcoin Cheque.**

1) User A wants to send some bitcoins to user B and writes a Bitcoin Cheque at the Bitcoin Bank. The cheque file is downloaded to his computer.

2) The cheque file is sent to user B. The file can be sent by e-mail, or any other medium.
3) User B receives the cheque, verifies it by uploading it to the bank, and claims it.
4) User B withdraws the bitcoins as promised from the cheque by requesting a Bitcoin transaction to his private Bitcoin wallet.

A cheque must be claimed at the bank that issued it in order to gets its face value. After a cheque has been claimed, it cannot be claimed by others. Only the recipient that has been written on the cheque can claim and cash it. If the cheque’s recipient is set to an e-mail address, the bank should verify the person claiming it by sending an e-mail verification link. If no recipient is written on the check, the person claiming it first can cash it.

Bitcoin Banks can charge a fee for issuing Bitcoin Cheques, which can make cheque issuance a profitable business.

## 4. Money Account API

Money Account API [3] is an application programming interface acting as a standardized protocol between different parties in the Bitcoin Cheque payment network. The API should be implemented on any servers participating in the Bitcoin Cheque payments, including Bitcoin Banks and webshops.

Money Account API at a bank can offer support to external client applications, like Payment Apps, to write Bitcoin Cheques, and for the receivers of these cheques to verify, claim, and cash them. The API includes support for the users to withdraw bitcoins from their bank account by requesting a Bitcoin transaction. Webshops and other sites can implement the API to accept cheques as payments.

The API is based on a REST architecture and accessed by using the HTTP protocol, which makes it easy to implement it on web servers and client applications. A web site implementing the API must add an HTTP External Resources Link element to the header section of the web page. The element will typically look like this:

```
<link rel="MoneyAccountAPI" href="https://bitcoindemobank.com/api">
```

The resource link informs the external users where the API is located. Before accessing the API, the web page header section should be read. This gives flexibility to the implementation of the API, which can even be located at another server.

## 5. Money Address

Money Address is conceptually like an e-mail address. And, its closely related Payment App can be considered as the e-mail client’s equivalent, a money client. The difference is these are used for sending money, like bitcoins.

The Money Address has mostly the same format as an e-mail address. The first exception is that the @ (at) character is replaced by a * (asterisk) character, as in this example:

```
adam.smith*bitcoindemobank.com
```

The second exception is the right side for the asterisk character. This part points to a web page where the HTTP External Resources Link can be read, which points to the receiver’s Money Account API. This part can also be a subdomain or a child page. The left side is a user at that site.

When sending a Bitcoin Cheque to another person, that person can be addressed by using his Money Address. The cheque is then sent into the Money Account API as pointed to by that address.

The Money Address can be considered a universal bank account number system. The human-readable address will make it easy to send bitcoins to any person at any Bitcoin Bank.

## 6. Payment Request

Payment Request [3] is a file sent to requests a payment. The file contains details like the amount to pay, the receiver of it, and any conditions for the payment. A Payment Request can be paid for with a Bitcoin Cheque. The cheque should then reflect the amount, the receiver, and any conditions given in the request.

In the same way as the Bitcoin Cheque, the Payment Request can be addressed to a payer by using the Money Address, and then be sent into the Money Account API. If the payer does not have a Money Address, the Payment Request file can be emailed and linked to a preferred Bitcoin Bank where the payment can be made.

Payment Requests can be created in several ways; by using a Payment App, by webshops to request payments for sale of items, or it can be generated automatically by servers as part of subscription services.

When a Money Account API receives a Payment Request, it can act immediately by writing a cheque and pay it, or put the request on hold for user approval, or reject it.

## 7. Payment links and Payment URI

Payment URI [3] is a Uniform Resources Identifier, which connects to the user’s installed Payment App. The URI scheme is “payment”.

The resource identifier can be put in anchor elements on web pages, which will create clickable payment links. When clicking the link, the Payment App will open, and the user can then make the payment from it. The link can be coded like this:

```
<a href="payment:RequestURL=https://example.com/pay?i=3">Pay 0.1 BTC</a>
```

The URL address given by the resource identifier’s RequestURL argument points to a Payment Request file. This file is read using a HTTP Get request. The Payment App can use the details in this file to write a cheque according to the payment requested. The payment is then completed by sending the cheque into the site’s Money Account API.

## 8. Online purchase with instant payment

Payment links can be put on webshops and other sites to collect payment for sale of items, contents, and other services. Combined with using a Payment App, this can facilitate easy and instant payment processing in one or a few clicks. Figure 3 shows an example:

1) A user visits a webshop and wants to purchase an item. The user clicks the payment link. This opens the user’s Payment App, which starts processing the payment by reading the Payment Request file.
2) Based on the information in this file, the app writes a Bitcoin Cheque at the Bitcoin Bank. The cheque is requested via the bank’s Money Account API.
3) The app sends the cheque into the webshop’s Money Account API.
4) The webshop verifies the cheque and claims it via the bank’s API.

5) The webshop hands over the item to the user. The hand over process is site-specific and can be implemented by JavaScript.
6) Later, the webshop cashes the cheque by requesting a Bitcoin transaction via the bank's API. This transaction can contain bitcoins from other sales too.

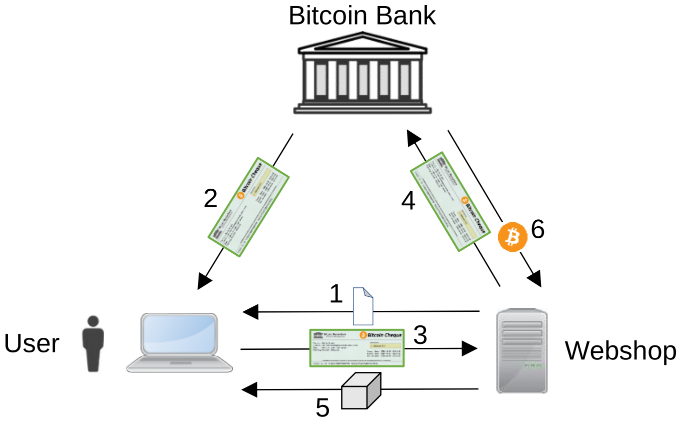


**Figure 3: Making a purchase with instant bitcoin payment.**

If the webshop trusts that the bank later will make the Bitcoin transaction, this process will enable instant payment, and the sold item can safely and immediately be handed over to the user. If the bank cannot be trusted, the webshop should wait for the Bitcoin transaction to be confirmed before handing over the item.

The Bitcoin Cheque and the Money Account API are flexible and can form a wide range of payment solutions. For example, the Bitcoin Cheque can be sent directly from the bank to the webshop. And the cheque recipient can be a Bitcoin wallet address or a Money Address.

A Payment App is not closely tied to a bank. The standardized Money Account API allows any conforming Payment App to be used against any conforming bank.

## 9. Payment network, Balance Accounts and trust

Bitcoin Cheque, Money Address, and Money Account API will enable Bitcoin Banks to participate in payment networks by using the same standards. This way, users at different banks can send bitcoins with cheques to each other, and webshops can accept payments from users at other banks.

When two users at different Bitcoin Banks are sending a Bitcoin Cheque to one another, the cheque can be sent instantly, while the actual Bitcoin transaction will take some time to get confirmed. During this period, the two banks will create Balance Accounts in their balance sheets to keep track of the bitcoin transfer. A balance sheet shows the amounts of assets and debts anybody has at any one time. For the bank issuing and sending the cheque, the balance will show the outstanding payable in bitcoins, and for the bank receiving the cheque, it will show the outstanding receivables. After the Bitcoin transaction has been confirmed, the outstanding payable and receivable amounts in the balance sheets will be cleared.

Figure 4 shows an example of such bitcoin transfer. Here user A has a bank account at Bitcoin Bank A and user B has a bank account at Bitcoin Bank B. User A wants to send some bitcoins to user B.

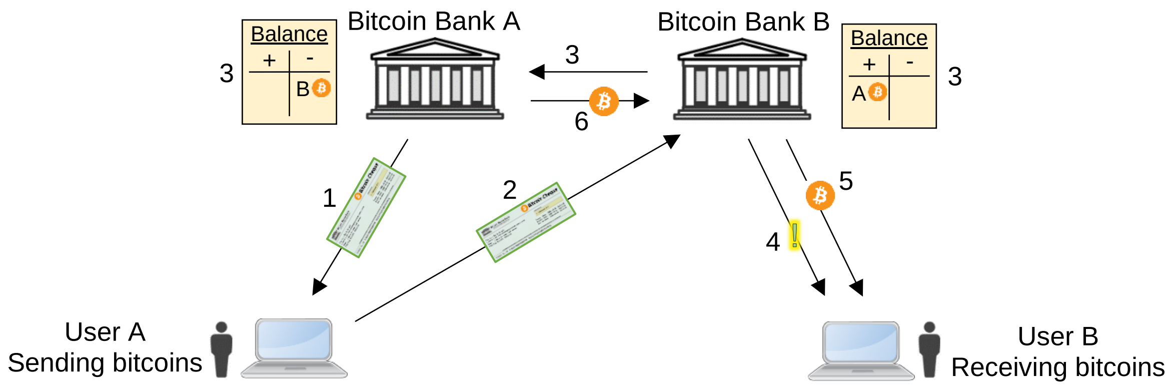


**Figure 4: Sending bitcoins to a user at another bank.**

1) User A opens his Payment App to send a cheque to user B. The amount to send and user B’s Money Address is written on the cheque. The app then requests the cheque via the Bitcoin Bank A’s Money Account API.
2) The app sends the cheque into Bitcoin Bank B’s Money Account API. Bank B verifies the cheque’s digital signature and accepts it.
3) Bank B claims the cheque via the API at bank A and thus creates Balance Accounts in the balance sheets at both banks. Bank A now has outstanding payables in bitcoins to bank B, and bank B has outstanding receivables in bitcoins against bank A.
4) Assuming bank B trusts the other bank will make the Bitcoin transaction, the bank can immediately debit user B’s bank account with the amount. If user B has a Payment App installed, a notification may be given.
5) The received bitcoins put in the bank account are now available for user B for withdrawal to his private Bitcoin wallet. Or he can let the bitcoins stay in the account as saving and immediately start spending in on purchases by paying with cheques.
6) When the Bitcoin transaction between the banks has been confirmed, the banks clear out their outstanding payables and receivables amount from their balance sheets.

A bank receiving a cheque needs to trust the issuer of that cheque in order to immediately transfer the amount to the recipient’s bank account. If the issuer cannot be trusted, the bank should wait for the Bitcoin transaction to be confirmed before handing over the amount. Otherwise, the bank could be scammed and would be left with a loss.

It will be in a bank’s interest that other banks trust it. If it cannot be trusted, it cannot offer its users instant bitcoin transfer to other banks. Trust between banks can be established in several ways. By creating a well-known brand, by a country’s legislation, by doing repeated businesses, or by knowing the persons running the bank.

A bank can also build trust by depositing bitcoins into the Balance Account at the other bank. That bank, when receiving a cheque from this bank, can safely and immediately hand over the bitcoins to the addressed recipient. The bitcoins for the cheque will be taken from the Balance Account, and no need to wait for the delaying Bitcoin transaction to get confirmed.

A Balance Account works mostly in the same way as a bank account for a user, in that bitcoins can be added and withdrawn from it. The differences are that the amounts sent by Bitcoin Cheque transfers are debited and credited to it, and the Balance Account can be accessed by using the owner's Money Account API as login credentials. Banks may pay or charge interests for the amounts held on the Balance Accounts.

After a bank has received a cheque, it does not have to request the outstanding receivable bitcoins to be transferred immediately. If the cheques have small face values, it may be too expensive to clear them individually. In that case it can wait for more cheques from the same bank and aggregate it into one big clearing transaction.

In a network of many Bitcoin Banks, Bitcoin Cheques can be sent between all banks in any direction. Each bank will need separate Balance Accounts against each of the other banks. Depending on where the cheque amounts go, different imbalances will build up between different banks. One bank may end up with outstanding receivables from some of the banks, and outstanding payables to other banks. There are mainly two ways to clear out these imbalances; the bank can request a Bitcoin transaction against each of the other banks, which can be costly if the number of banks is large. A less expensive option is for the bank to write cheques from the Balance Accounts at those other banks it has outstanding receivable and send these cheques to the banks at where it has outstanding payables. Figure 5 shows an example.

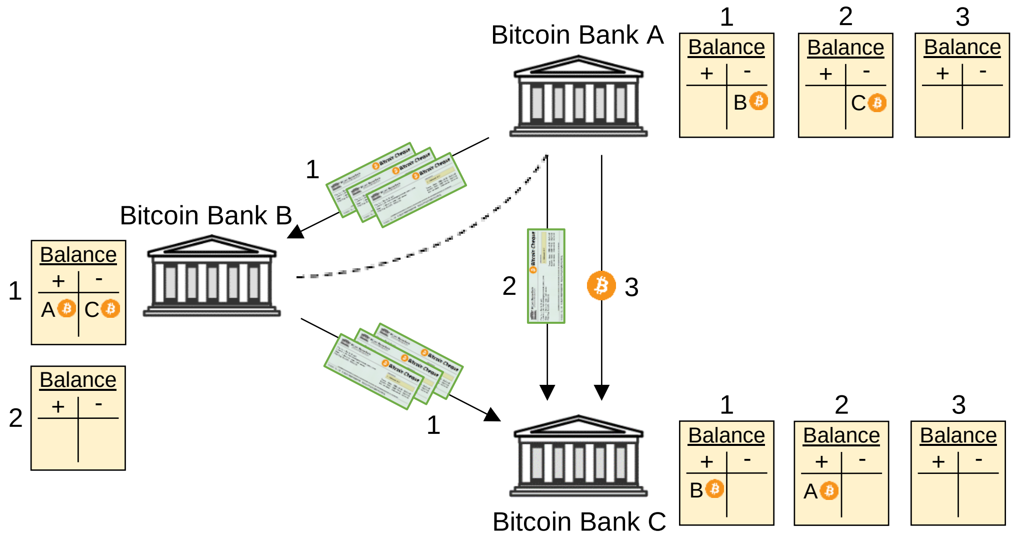


**Figure 5: Bank network clearing out account imbalances.**

1) Users write several Bitcoin Cheques at Bitcoin Bank A and send them to users at Bitcoin Bank B, and users at bank B do the same and send their cheques to other users at bank C. Bank B now has outstanding receivables in bitcoins from bank A and outstanding payables to bank C in its balance sheet. The sum of the sent amounts and the sum of the received amounts happen to be equal in this example.
2) To clear out these imbalances, Bank B writes a cheque from its Balance Account in bank A and sends it to its Balance Account in bank C. This clears out the imbalances between bank A and B, and between B and C. But the cheque sent from bank A to bank C will itself create Balance Accounts between these two banks. Now, bank A has outstanding payables to bank C, and bank C has outstanding receivables from bank A.
3) Bank C clears out the outstanding receivables from bank A by requesting a Bitcoin transaction. After the transaction has been confirmed, the Balances Accounts between all these banks are cleared.

It may appear as bank B and C are exploiting bank A by letting that bank take the cost of doing the Bitcoin transaction to clear out their imbalances. But keep in mind that banks may charge a fee for issuing cheques, and parts of that should cover the cost of the clearing Bitcoin transactions.

Bitcoin Cheques sent in both directions between two banks will cancel out each other in the balance sheet. If a bank is receiving cheques amounting equal to what itself is sending to several other banks, the total balance at this bank will remain unchanged. Computer simulations of random cheque transfers in a network of banks show that when a bank's total balance remains approximately unchanged over time, there will practically be no need for clearing Bitcoin transactions [4].

On the other side, if the bank's total balance in sum has either payables or receivables amounts against several other banks, clearing Bitcoin transactions will be needed. However, costly Bitcoin transactions may not be needed against all the other banks. Computer simulations show that it will be enough for a bank to make one clearing transaction with the total outstanding amount against one of the other banks, and cheques sent between Balance Accounts will distribute the values to clear out imbalances at the remaining banks [4]. There will be no need for central coordination for this to happen. It can be expected that each bank will, in its self-interest, optimize the clearing strategy to reduce its own cost.

## 10. Cheque exchanging

As it will be unthinkable to assume all Bitcoin Banks will trust all the other banks, and a merchant may only trust a few of them, this would otherwise create barriers for accepting instant payments from untrusted banks. To overcome this, a user can exchange his cheque at another bank to get a new cheque that the recipient will trust.

This exchange can be described as buying a cheque by paying for it with another cheque. The banks may charge a fee for providing the exchange service, which is taken from the differences in face value between the two swapped cheques. The Money Account API provides supports for the cheque exchanging. Figure 6 shows an example of purchasing an item by paying with an exchanged cheque.

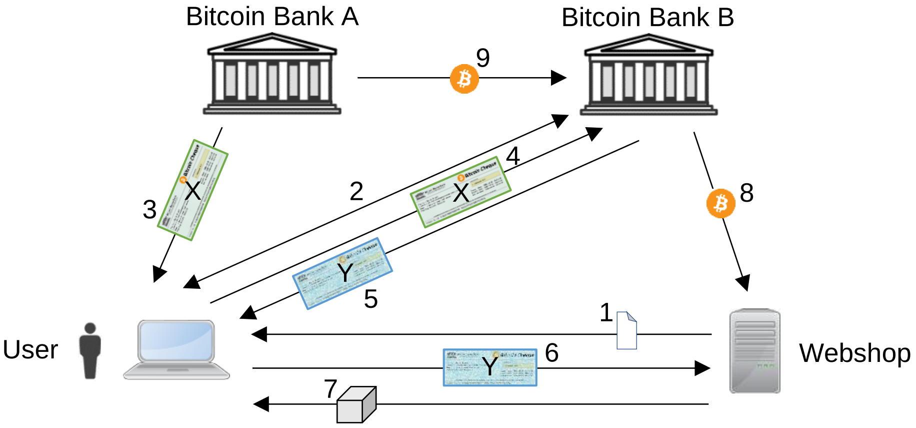


**Figure 6: Purchase with instant payments by using an exchanged Bitcoin Cheque.**

1) A user visits a webshop and wants to purchase an item. The user clicks the payment link, and the Payment App starts reading the Payment Request file from the webshop. The app learns from the file that the webshop trusts Bitcoin Bank B, but does not trust the user's preferred Bitcoin Bank A.
2) The app asks bank B what other banks it trusts, and learns that it trusts bank A. The app retrieves this information by accessing the bank's Money Account API.
3) The Payment App writes a cheque X at bank A. The cheque's face value is set to cover the price of the item plus the exchange fee.
4) The app sends cheque X to bank B and asks for a cheque exchange.

5) Bank B verifies cheque X's digital signature and issues a new cheque Y of the same amount, minus the fee. Balance Accounts between the banks are created.
6) The app uses the new cheque Y to pay for the item.
7) The webshop, which accepts cheques from bank B, verifies the cheque's digital signature and immediately hands over the item to the user.
8) Later, the webshop withdraws the bitcoins as received from cheque Y by requesting a Bitcoin transaction.
9) Bank B clears out the outstanding receivables from cheque X by requesting a Bitcoin transaction. The two last steps can happen in the opposite order as well.

Although this picture may appear complex, it is still simple in that each cheque is processed independently and lives its own life. The processes of exchanging a cheque at the bank and purchasing an item at the webshop are principally the same. They both need to trust the received cheque and its issuer. What matters is the chain of trust, which starts from the webshop trusting bank B, and continues by bank B trusting bank A, one independent link at a time.

In case there is no direct link of trust from one of the webshop's trusted banks to the user's preferred bank, a third bank, or even more, will be needed to close the chain. In this situation, the user's Payment App must exchange the cheque several times, until it reaches one of the banks trusted by the webshop.

In order to find a route, the Payment App must ask each bank which other banks they trust, and thus create a map of trust, as the example in Figure 7 illustrates. The arrows indicate trust. The webshop trusts bank C and F. Bank F trusts bank C, H and I. Bank H trusts only bank B, and so on. The route of red, thick arrows is one possible chain of trust, presumably the shortest and least expensive. The app can then write a cheque at the user's preferred bank A, swap it at bank D, take the new cheque and swap it at bank B, all the way until it reaches the webshop.

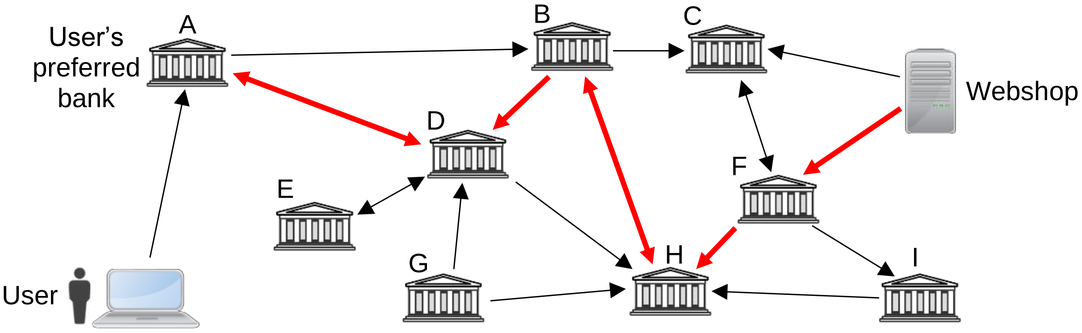


**Figure 7: A map of trust used to create a route for instant payment to a webshop.**

This route can grow to any length as needed. However, as each exchange may require a fee, the total payment cost will increase. At some point, it may become too expensive for the user. Nevertheless, it is still fully possible to pay with a cheque directly from the user's preferred bank to the webshop, even the webshop does not trust that bank. In that case, the webshop should wait for the Bitcoin transaction to get confirmed before handing over the items.

A cheque can be denoted in any currency, and banks can offer to exchange cheques into other currencies. This way buyers and sellers are not required to use the same currency. If a cheque is not denoted in Bitcoin, it should not be called Bitcoin Cheque, but the same principles apply.

## 11. Mass adoption

The described building blocks are flexible and can be used to create a wide range of different services. A complete payment infrastructure is not needed in advance before the world can start using them. One possible way of adoption may be as following:

At the start, the Bitcoin Cheque may be implemented by individual custodian providers and cryptocurrency exchanges to offer simplified bitcoin transfer among its users. Cheques can be sent by e-mail to anybody, including those without a Bitcoin wallet and no Money Address. The e-mail can show an image of the cheque and linked to the site for easy access, which may be appealing to those who have never used Bitcoin. This can attract new customers.

As more entities start supporting the standardized Bitcoin Cheque format, this opens for the possibility of sending cheques between users at the different sites. This will also require a standardized interface like the Money Account API and the Money Address. After the first sites start using it together, a network effect will increase the value of the payment system and pull more sites into using the same system.

Later, as an increasingly number of entities are supporting the Bitcoin Cheque payment system, a user base capable of doing online shopping with cheques will arise. This will enable new ways of monetizing content by using clickable payment links and micro-payment. One possible business case may be clickable links to read single news articles, instead of having to sign up for expensive subscriptions. The sites can redirect visitors without an installed Payment App to a recommended Bitcoin Bank, where the payment can be made, or an app can be downloaded.

After these Payment Apps becomes common on mobile devices, it will be convenient and easy to send bitcoins anywhere to anybody. This will enable merchants to start accepting Bitcoin Cheques at physical stores.

## 12. Conclusion

The Bitcoin Cheque payment system will overcome the Bitcoin scalability problem by recording Bitcoin transactions outside of the blockchain. This second-layer payment system is based on trusted third parties, which can provide banking, cryptocurrency custody and payment services for its users. Payments can be made between any user, and the clearing transactions between the parties can be aggregated and sent directly to each other on the Bitcoin network. No single company, central gateway or clearing houses is needed for the system to work.

The payment system offers features like instant payments, clickable payment links, micro-payments, and direct currency exchange to convert any cryptocurrency, even fiat currencies. Users can send bitcoins as Bitcoin Cheques to everybody else, regardless of what bank they are using. A recipient can be addressed by using that person’s Money Address, which conceptually is like sending an e-mail. The system is design for easy Bitcoin usages in mind.

The payment system is based on open standards and can be easily implemented by using today’s well-known web technology, which will enable a broad base of developers to contribute to it. The flexible building blocks will allow future innovations to create new types of services.

By overcoming Bitcoin’s technical limitations, being easy to implement, and providing user-friendly features to the public, the Bitcoin Cheque payment system thus will have the potential to become a de facto standard for Bitcoin payments. And with more use cases for Bitcoin, its dominance as an accepted and sound money will grow.

## Additional arguments

Lightning Network [5] is another second-layer payment system built on top of Bitcoin. Lightning Network and Bitcoin Cheque are two very different solution to the Bitcoin scalability problem. It is not an argument to say there is only room for one solution. The two systems have different properties and may fit different needs.

Bitcoin Cheque do not require a Bitcoin wallet, and thus do not require the user to take care of the private key. If the private key is lost or stolen, the bitcoins in that wallet may be lost forever. It is unthinkable to assume this would be a good solution for everybody. Many users may be more comfortable by storing their bitcoins in a trusted bank.

Bitcoins stored in private wallets will be locked up and this capital cannot be used for other purposes. Capital is needed for a society to develop and prosper. Bitcoins saved in banks can be lent out where it is most needed. Bitcoins locked up in private wallets are not invested and will not give interest. This may not feel like a problem as long as Bitcoin is increasing in value, but today's situation cannot be expected forever.

It is a common belief among many Bitcoin evangelists that banks, custodian providers and cryptocurrency exchanges cannot be trusted, and therefore users should keep their bitcoins in their own private wallets. And there certainly are many examples of such institutions having been subject to hacking, bankruptcies and economic crises, which have caused users to lose their funds. However, banks are still required to operate according to a country's legislation and therefore are obligated to protect the clients' funds. People losing their funds in regulated banks is not an everyday problem.

Another common belief is that banks are evil and should be avoided at all. But the commercial banks are only playing the game set up by laws voted for by politicians and other rules given by the government. And the current deal is to bailout banks during economic crisis at the taxpayers' expense. In a society with free banking and hard money, there will be no room for a central bank, which can print money for the bailouts and other election promises. This will change the rules of politics, and force banks to play it more conservative and adhere to a better moral [6].

## References

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[2] Saifedean Ammous, The Bitcoin Standard, 2018.

[3] Standards and protocols for Bitcoin Cheque, Money Account API, Money Address, Payment Request, and Payment URI, https://bitcoincheque.org/standards .

[4] Simulations of payment networks, https://bitcoincheque.org/projects/simulations .

[5] Lightning Network, https://lightning.network .

[6] Murray N. Rothbard, What Has Government Done to Our Money?, 1963.