PREPRINT – DRAFT 1.1 July 9, 2026

The Payment Verification Model for Digital Cash Point of Sale Systems

Lukas Saul[1,2], Robert Gludo[2], Jonathan Gludo[2]

1) Vericeive LLC, New Hampshire USA
2) 合肥工业大学, Hefei China [saul@hfut.edu.cn]

Abstract:

With public ledger digital cash payments comes a new type of point of sale (POS) system which has been implemented by several devices and apps. The “payment verification model” for POS minimizes security risk and associated fees while enabling merchants to adopt their point of sale system to different numéraires and different payment currencies. In this paper we outline this system and its advantages and operation. We provide the first systematic security taxonomy, privacy mitigation strategies, and accounting integration guidance specifically for payment verification POS systems.

Introduction:

The point of sale (POS) device has become somewhat ubiquitous around the world, as different forms of electronic and digital payments have proliferated. Mostly these devices have been of the architecture of a “merchant account service”. The devices are provided and to some extent operated by a company which acts as a middle man on behalf of the merchant, collecting customer credit and then making subsequent payments to the merchant. This architecture is necessary for most credit card payments and other privately issued and operated digital token systems such as applepay, wechatpay, alipay, gpay, and many others.

However when it comes to public digital cash payments, for which we mean that a public record of the transaction ledger is available, this architecture is by no means required. The difference is that for public payment networks *a*ny party with network access can independently verify whether a payment has been sent to a given address and how many confirmations it has. It is thus possible for a third party to determine the status of a transaction, and to verify a payment, without being one of the parties involved in that transaction. This enables the payment verification model to be used to enable a point of sale transaction.

The Payment Verification Model

With the advent of public ledgers, another method for POS devices has become available. In this architecture, the point of sale device does not collect customer credit or funds, but acts as a tool in full control of the merchant which enables currency price conversion, payment verification, and additional information services such as receipt printing and record keeping, while never taking any custody or associated liability of any funds.

Public ledger systems are also referred to as triple entry accounting systems (Grigg, 2024). The customer keeps a record, the merchant keeps a record, and a third record of the transaction now exists: the public ledger. While triple entry accounting does not require the payment verification model to be used, the benefits are immediately apparent: there is no inherent counter-party risk, and the merchant has immediate control of the funds paid by the customer.

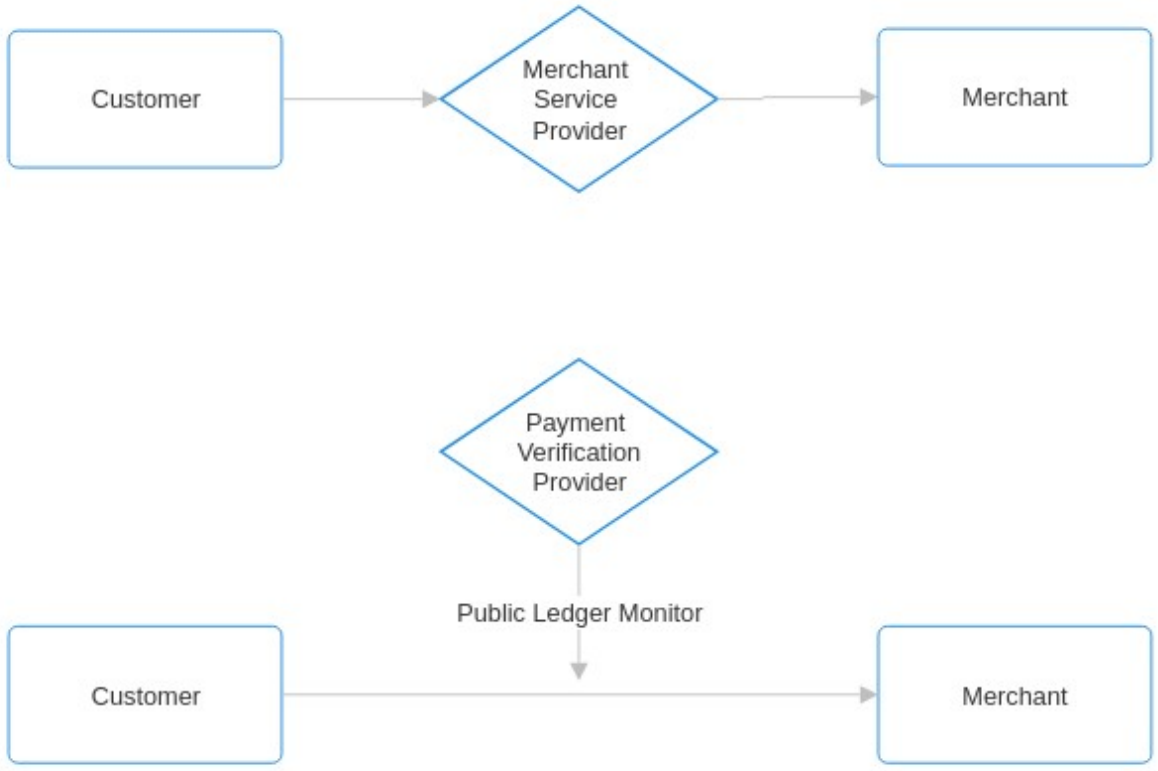

Figure 1 – Comparison of the payment architectures of merchant service model (top) and payment verification model (bottom). Note that no funds pass through the POS device in the bottom model.

History

The first public coin system may have been the Rai stones used by the Yap Island natives (Gilliland, 1975). A digital version was suggested by Wei Dai (1998). However a full digital implementation would wait for the creation of Bitcoin (Nakamoto, 2008). Today many such public digital ledgers exist using a variety of consensus mechanisms.

In the early 2010s, merchants used a technique called the “watch-only wallet” to perform what is effectively payment verification as described here. A coin wallet was given an additional feature of being able to watch an address, so a merchant could determine that a payment was en-route without having the keys to the receiving address physically present. During the 2010s, many merchants would do this “by hand”, by simply printing out a QR code of a coin address, allowing customers to scan and pay the required amount to that address, while they watched a block explorer in a browser to see that payment was indeed on its way.

Perhaps the most notable effort in promoting the idea of the payment verification model was the "Bitrequest" project (https://bitrequest.io) which was first published in 2019 and provides the services of payment verification for free to merchants by using web and app interfaces.

The "Vericeive" company began selling handheld devices with the "Lucky Cat Terminal" software in 2025, which also implements the payment verification model.

Security Concerns

While the payment verification model removes the primary security concerns of a merchant service, by enabling direct peer-to-peer payment without a counter-party, there remain some attack vectors which merchants should be aware of.

1) Compromised Verification Devices

The payment verification device does not hold any funds, and so has a minimal attack surface, but it does display the merchants receiving address for the customer. If a device were compromised, it could be made to display a different address so that customer funds were effectively rerouted to the control of an attacker. For example, a disgruntled employee or even a remote hacker could potentially take control of the POS device and make such changes. To make sure this is not happening, the POS device should display a short, human-memorable identifier or checksum of the receiving address that the merchant can verify against a trusted offline record. Alternatively, a second independent device (e.g., a phone) can scan the same QR code to cross-check. The merchant regularly checks that the addresses are indeed being displayed correctly, and that funds are arriving to the expected wallets. It is also important that configuration screens for these devices be password protected by the manager or owner of the business, so that nobody can change the destination addresses.

2) Payment Reversal Attacks

Merchants who deal regularly with large priced items and questionable clientele are familiar with payment reversal attacks, and so often don't accept credit cards which can allow users to reverse transactions. Public ledger digital cash transactions are as such not reversible, so much of this concern disappears with the payment verification model. Public digital cash transactions are not reversible by customers, but unconfirmed transactions (0 confirmations) can in theory be double-spent. Merchants will sometimes wish to wait for confirmations. For this reason, merchants may want to wait until a suitable number of confirmations are received before providing goods or services to customers. For bitcoin for example, 1–6 confirmations are standard depending on value.

A good payment verification machine will not only show that a transaction has been published, but also show in real time the number of confirmations of the transaction, so that a merchant who is suspicious of a customer can watch the device and wait until they are satisfied a payment cannot be reversed. So-called block reorganization attacks and 51% attacks are possible (though extremely costly), and so merchants making extremely high value sales need to be aware of the right amount of time to wait for the digital asset used as payment before releasing any goods to anonymous or suspicious customers.

Merchant Accounting Integration

Merchants accepting digital cash with a payment verification device (or directly) have an obvious way to integrate with most accounting: treat digital cash payments as cash payments. Most merchants already accept some local currency as cash payment, and so they have in their accounting a means of keeping track of such payments for their own accounting purposes and for whichever reason their local environment requires it. The accounting situation is further eased by the fact that every transaction is stored in its associated network ledger automatically, so records can be reconstructed if any conflict or disagreement arises.

Privacy Concerns

While public payment systems have many advantages due to their fairness, transparency, and ease of accounting, these same features can lead to problems when it comes to privacy. If a static address is used on a payment network, then any customer who sees that address can look up its history. It appears that a merchant would not want to use such a system if they don't want information about these sales to be public. However, some solutions exist which still allow for the payment verifciation model to work in more demanding privacy environments.

1) XPUB and HD wallet seeds

The Hierarchical Deterministic wallet systems (HD) (Maxwell, 2011) enable multiple addresses to be effectively created and controlled from a single seed. In these wallets, a public seed or "xpub" (other formats are also used) can be stored in a payment verification device, so that every address generated for a customer will be unique. In this way the previous sales records of the device are no longer public to any customer. The device still has no information about any private keys; it remains solely a payment verification device.

2) Privacy Coins

Due to the issues around the public nature of these payment networks as outlined, some networks have been created which allow for payment privacy on the protocol level. For these payment networks, the usability of a payment verification POS device is unclear. In order for the device to work, it requires either a "viewer key" in addition to the static coin address, so transactions can be monitored, or for the asset in question to be somehow "unshielded" so the transaction can be verified by the POS device. For example, devices and apps using the payment verification model for point of sale have been made to work with Monero and Zcash transactions.

Numéraires

While multiple currencies and units of value have always been in use everywhere, the advent of global communications and payments has only increased the amount of different currencies and pricing schemes in regular use. The choice of a merchant to declare prices in one unit or another is called the choice of a numéraire. Company coins, precious metals, amusement park tokens, frequent flier miles, and national central bank notes are all examples of numéraires which merchants might use to price goods and services. Legal tender laws do not constrain what merchants can accept as payment currencies or as numéraires, as legal tender laws apply not for sales but for resolution of existing debts.

The payment verification model allows for merchants to use different numéraires if it can convert the amount from the numéraire to the payment currency, thus allowing payment for goods and

service priced in hundreds of different numéraires to be paid in a variety of different payment currencies. It should be noted that no conversion of any assets is taking place here, only a conversion of the amount required to make the payment.

For example, a merchant might have goods priced in Euros [EUR] as their numéraire. A payment verification POS device converts the amount in EUR to a currency that the customer would like to pay (for which the merchant has provided a receiving address), for example USDT on Tron. The device displays a QR code with the amount required and destination, and the customer uses any wallet to make sure that amount gets sent to that wallet. The device then verifies that the payment has taken place.

Error Handling

There are some problems which can arise during payment with a payment verification device, such as power outages, network outages, and user errors. Service outages will mean that the payment cannot proceed. These are outages which could be present with any POS device, and the mitigation path is the same – backup systems are to be ready when possible.

Another potential error can arise in the case of user error such as overpayment or when a refund is requested. In these cases, the availability of a refund is at the discretion of the merchant, as transactions cannot be reversed. Sometimes an address will be used which is not immediately available at the check out counter, and a customer will then need to wait until a refund can be processed by the merchant. As such, these cases are outside the scope of the payment verification device.

Technical Requirements

The hardware and technical requirements of running a payment verifcation POS device are very similar to those for running merchant service providing POS devices: internet connectivity, and required electrical power. If either of these fail, neither of these POS devices will be able to facilitate a transaction. Payment verification POS devices might require an API key so that the merchant has access to the required information sources to convert units and verify payments.

The requirements for setting up a payment verification device are however much lower than for merchant service accounts. No kind of identification, bank accounts, or credit rating is required to run a payment verification POS device, while all of these might be required for setting up a merchant service account.

Conclusions

The payment verification model for POS transactions has the potential to revolutionize the POS space, and reduce the cost of transactions substantially for merchants while increasing the security and the immediate availability of funds. This model is yet another reason that public ledger currencies are of benefit to society, even before considering the implications that fair issuance and sound money can provide.

The payment verification model for POS devices shows remarkable promise as a tool for merchants who wish to be as cost-effective, secure, and as open to different customer-preferred payment systems as possible. In its unobtrusiveness and flexibility it seems in some sense too good to be true. However this model only applies to public digital cash networks; it cannot support privately

issued currencies or private credit instruments. For this reason, we expect that merchants will begin slowly by using payment verifying POS devices, to accept the newer currencies and bring in those customers with digital cash, while still maintaining merchant service accounts for those customers without digital cash wallets.

References:

1) “Triple Entry Accounting”. Ian Grigg, Journal of Risk and Financial Management, 17(2):76, Feb. 2024

2) “The Stone Money of Yap”, Cora Lee C. Gilliland, (Smithsonian Studies in History and Technology 23). Washington, DC: Smithsonian Institution Press. p. 75.

3) “B-money”, Wei Dai, Nov. 1998

4) “Bitcoin: A Peer-to-Peer Electronic Cash System”, Satoshi Nakamoto, Oct. 31., 2008

5) Maxwell, G.reg: Deterministic wallets, June 2011. *https://bitcointalk.org/index.php?topic=19137*