Accepting cryptocurrency at the point-of-sale

Neil Haran @kappturelabs, 29th June 2019

Version 1

Abstract

Our migration towards a cashless society is almost complete. Since the 1990s when electronic banking became common, digital payments have become increasingly widespread.

Consumers today have a lot of choice when making electronic payments online. However, payments made in-person have struggled to keep up. The principle reason for this lack of innovation has been complexities in confirming payments quickly enough; bank-issued payment cards currently dominate the market, resulting in the banks controlling both consumer status and merchant fees.

Early cryptocurrencies, the dominant one being bitcoin, do not possess the qualities required for in-person payments. Their fee structure is uncompetitive compared to the incumbent technology and confirmation of the transaction – the point at which it cannot be reversed – has been too slow.

We propose a new method. Cryptocurrencies being developed today do, for the first time, provide the means to offer a compelling user experience while offering merchants an opportunity to reduce cost and appeal to a passionate new consumer.

Introduction

The value of banknotes and coins in circulation as a percentage of narrow money in the Euro area is 15.4%, a figure that has been in steady decline. Sweden is leading the way in cashless adoption, with only 2.2% of their narrow money being banknotes and coins during the same period[i].

Many of these cashless payments are made with bank-issued payment cards. Since the 1950s when payment cards were first introduced, little has changed to the user experience. Developments have been Chip & PIN, contactless cards, and very recently, IT giants Apple and Google stepping into the marketplace – offering consumers convenience by digitizing their existing payment cards.

A merchant wishing to accept payment cards must enter into an arrangement with an acquiring bank, who typically leases equipment for use at the point-of-sale. Issuing banks, payment processors, payment gateways, payment networks (such as Visa and Mastercard) and the merchant's bank all impose interchange fees on the collected payments – which are paid by the merchant.

Additional revenue is generated for the banks when the issued card is held in a different currency to that of the transaction. This cost, often referred to as Dynamic Currency Conversion (DCC), is paid by the consumer.

Despite these costs, the merchant advantage is compelling. Businesses benefit from reduced risk in the form of employee theft, counterfeit money, and robbery. Cashless payments can also be settled more quickly than with cash[ii], and studies indicate that consumers spend more when offered cashless payment options[iii].

Problem

a. Fees

Payment transaction fees as a percentage of turnover within the hospitality industry are approximately 4.1% for cash, and 1.8% for payment cards[iv].

In addition to transaction fees, merchants may also be charged PCI compliance fees, card scheme fees, authorization fees, and monthly service charges.

Merchants are currently absorbing these fees, and the absence of alternatives has failed to produce a competitive market.

b. Equipment cost

Merchants must use specialized pin entry devices (PEDs) to accept contactless and Chip & PIN payments. The acquiring bank or payment gateway usually supply these and in the UK typically attract setup fees in the region of £300-£400 and monthly rental fees between £6-£15, per device.

At Kappture, many of our customers have 500+ devices per location, so these equipment costs represent a significant expense to the business.

Cryptocurrency payments would require no additional hardware on the latest Kappture terminals.

c. Speed

Contactless payments are fast. 68% of contactless transactions take under 5 seconds[v], with the average Chip & PIN transaction taking 7 seconds longer. In the UK more than half of eligible (under £30) payments are made with a contactless payment card[vi].

Many payments exceed this limit and require PIN entry, slowing the transaction. Additionally, depending on the bank, consumers are required to enter their PIN after 3 to 5 contactless payments irrespective of the amount. Payments conducted via Apple Pay or Google Pay may exceed the £30 limit at the discretion of the bank.

In the high transaction volume sectors that Kappture operates in, up to 12 seconds to complete a payment is still something we're keen to improve on.

Cryptocurrency payments have the potential to be confirmed in well under a second and with limits controlled by merchants rather than banks.

d. PCI compliance

90% of large UK businesses reported that they had suffered a security breach in 2015[vii]. Protecting consumer data against an increasingly sophisticated adversary has never been more critical.

The Payment Card Industry Data Security Standard (PCI DSS) seeks to secure systems so consumers can trust their payment data with merchants[viii]. With the best intentions, the mandatory security standard is criticized for being expensive to implement, confusing to comply with, and ultimately subjective, both in its interpretation and enforcement[ix].

As it stands today, the payment card process suffers a simple flaw – consumers must reveal their private information to merchants when making a payment. PCI DSS is therefore concerned with the ensuing battle of protecting that data.

Cryptocurrency works differently. Consumers never reveal any private information – their electronic wallet 'signs' a request to send funds to the recipient. PCI-like standards are obsolete with this design.

e. Innovation

Banks are not well known for their innovation. A consequence of their fiduciary duty – they are looking after other people's money – it means they cannot move quickly. Mark Zuckerberg's famous quote, "Move fast and break things" applied to central banking would not be appreciated by most consumers.

Cryptocurrency is different. Consumers look after their own money; it is held directly, not with a bank or a service. Innovation can occur organically and with less friction than with traditional banking.

f. Centralization

Banks are regulated by the jurisdictions in which they operate. Pressure can be placed on them to freeze accounts, withdraw currency from circulation, reverse transactions and cap or prevent the withdrawal of funds entirely. Ask the citizens of Greece, Cyprus, Spain, Ukraine, Turkey, Venezuela, Argentina, India, and Brazil, to list some recent examples.

30% of the global population live in a country that has experienced significant depreciation between 2013 and 2018[x]. In August 2018 the Maduro government in Venezuela announced a 95% devaluation in its currency as a result of the country's hyperinflation. In that country, an uncooked chicken costs 14,600,000 bolivars[xi] – a consumer in Venezuela would require a wheelbarrow to move that figure as banknotes.

This problem is not limited to the developing world. Cyprus is a financial hub with a mature economy, used by businesses from all over the world to invest in Europe. In March 2013 depositors in Laiki Bank lost all

funds over 100,000 EUR and other banks imposed 'one-off levies' of around 40% on funds over 100,000 EUR[xii]. Banks were closed for 12 days to avoid a run, and when they did reopen, withdrawals were limited to 300 EUR per day[xiii]. The result of this today is that a third of Cypriots now report that they hold no bank deposits whatsoever[xiv].

Cryptocurrencies move the balance of power from centralized institutions into the direct control of citizens.

g. Inclusion

Globally billions of adults remain unbanked or underbanked[xv]. Of these, 1 billion are crossing the 'poverty' line and have access to smartphones and the internet.

Nigeria is Africa's largest economy, but 60% of citizens do not have a bank account. In Kenya, 21 million users make more than 17 million transactions per day using centralized payment service M-Pesa.

Cryptocurrency adoption in countries like Nigeria and Kenya would give citizens access to an open, public, neutral, censorship-resistant, and borderless[xvi] payment system.

Solution

These problems can't be solved overnight, but we must run alternatives in parallel with the traditional banking system.

Closed-loop

Universities and businesses providing hospitality services on campus may be referred to as 'closed-loop.' Consumers in these environments offer repeat business, are often a 'captive' audience, and the operator tends to have control over the outlets and merchants in the offer.

When Kappture was formed in 2012, one of our principle features was a top-up account. Pre-registered members could pay within a closed-loop campus by tapping an RFID card or scanning a QR.

Our system, like that of our competitors, was implemented as a centralized ledger that we hosted. Members within the organizations we served trusted us to credit their accounts with funds they loaded and to make those funds available when they wanted to spend them.

Top-up accounts were a successful product for Kappture and enabled us to enter markets where payment cards have previously struggled – vending machines being one example. The innovation also meant that bank payment equipment was not required at the point-of-sale, removing many of the problems we've discussed.

However, closed-loop systems have – by their very definition – limited adoption. They do not work well with franchise operations, and members can only spend their funds on campus.

Distributed ledger

All cryptocurrencies operate on a distributed ledger. Most are also decentralized, meaning that no single entity can manipulate the ledger. These features are sometimes referred to as 'trustless'; distributed protocols and software control transactions, not people and legislation.

For the first time, there is the potential to replace the bank-controlled payment ecosystem with something that benefits consumers and merchants.

Cryptocurrency market overview

Cryptocurrencies provide a means for a transaction to occur between two parties who don't trust each other, without the need for a trusted third party. Previously it was always necessary for a third party, usually a bank, to oversee the transaction.

The first cryptocurrency, bitcoin, was described in a 2008 white paper by an individual with the pseudonym Satoshi Nakamoto[xvii]. Satoshi's identity remains a secret, but in the eleven years since his invention, the idea has been developed by enthusiasts worldwide resulting in thousands[xviii] of cryptocurrencies being created with a combined market cap exceeding $336B[xix] at the time of writing.

Some of these cryptocurrency projects are copies of bitcoin and offer little new, some innovate in new areas – like privacy or the provision of smart contracts, and some focus on payments.

As the market is so broad, with so many competing projects, it is not immediately apparent which project

to use. Additionally, the market participants cannot be relied upon to provide impartial advice as many have vested interests. Kappture have made an informed, commercial decision in this regard. The justification for that decision follows.

Working with centralized ledgers in production environments for many years gives us some guidance when considering features.

	Minimum	Target
Fees	<bank cards	zero
Confirmation speed[1]	<bank cards	zero
Decentralization[2]	yes	
Scalability	100tps[3]	linear[4]

Table 1.

a. Mature wallet offering

Many projects have good quality, well-liked smartphone wallets for common platforms. We did not want to go into the business of building more wallet apps and driving adoption there too – the projects we're looking at all have popular wallets.

b. Provenance

We had concerns when looking at projects where early funding was raised via the sale of pre-mined assets. Raising funds in this way is a concept borrowed from the world of stocks and is often referred to as an Initial Coin Offering (ICO).

Public companies are subject to state governance and oversight; how and if, this translates to cryptocurrency projects which most governments classify as assets rather than currency, is not yet understood – and will undoubtedly vary by region. Exposure is not something we want to impose on our customers, especially when considering an international market.

c. Money transmission

Businesses responsible for the transmission of money are required to be legally registered in most jurisdictions.

We would only consider projects where it was possible to build a robust fault-tolerant payment mechanism while merely *observing* transactions. The test for this is simple; is it necessary to hold any private keys to prove payment has been confirmed? If we do, then the project must be excluded.

It is not possible to be a money transmitter without possessing the means (holding the private keys) to transmit money.

d. Code review & maintainability

Our developers had to be comfortable with the project code following a thorough review, and be comfortable maintaining it, if necessary.

<u>Projects</u>

Follows is a list of cryptocurrency projects we looked at when researching this proposal. This limited set was selected based on developer experience; we expected to find several candidate projects.

These results do not do the projects justice and should not be considered endorsements or critique by the authors. Each project has a passionate and enthusiastic community and presumably serves its own goals well.

We have a discrete use-case; fast, feeless, confirmed payments in-person at the point-of-sale. Naturally, this favors some designs. Systems exist today that accept unconfirmed transactions as final payment; a policy that we believe relies on niche use and could become unworkable as adoption increases.

	Results
Bitcoin (BTC)	☒ fees ☒ speed ☑ decentralization ☒ scalability

[1] Confirmed transaction speed.
[2] As defined by the Adjusted Nakamoto Coefficient (ANC). ANC>1.
[3] Arbitrary figure derived from current demand on our centralized ledger.
[4] Many cryptocurrency projects face an exponential scaling problem. They must increase the size of blocks to accommodate more transactions, but in doing so increase the latency of confirming those blocks on the network. We are looking at projects that can scale linearly with adoption. Adoption is a vague concept and metrics vary between projects – we're primarily looking at nodes and users. Increasing participants will drive an increase in bandwidth.

Bitcoin + lightning network	☒ fees ☑ speed ☑ decentralization ☑ scalability
Ethereum (ETH)	☒ fees ☒ speed ☑ decentralization ☒ scalability[5]
EOS (EOS)	☑ fees[6] ☒ speed[7] ☑ decentralization ☑ scalability
Ripple (XRP)	☒ fees ☒ speed[8] ☒ decentralization ☑ scalability
Dash (DASH)	☒ fees ☒ speed ☑ decentralization ☑ scalability
Stellar (XLM)	☒ fees ☑ speed ☒ decentralization ☑ scalability
Nano (NANO)	☑ fees ☑ speed ☑ decentralization ☑ scalability
IOTA (IOTA)	☑ fees ☑ speed ☒ decentralization ☑ scalability

Table 2.

Supporting bitcoin would be attractive. Brand awareness is high, and we can imagine the friction to adoption being reduced for this reason. The native blockchain is not suitable, however, and the 'layer 2' solution built on top of it is neither ready at the time of writing[xx], nor feeless (although it is expected to have very modest fees).

Nano and IOTA are the two most promising projects we researched. Both are based on Directed Acyclic Graph (DAG) data structures, hence their feeless nature and fast confirmation times, and they scale horizontally – where conventional blockchains must scale vertically.

During controlled tests, we found that Nano was faster at confirming transactions than IOTA. Nano can also be aggressively pruned as blocks store account balances rather than transaction amounts – which would require aggregation to determine the balance. IOTA relies on snapshots to enable pruning. At the time of writing, IOTA is centralized although the developers recently announced 'coordicide'[xxi] which aims to solve this.

Our developers found the Nano code to be well maintained and easy to work with, that the proof-of-work (PoW) on block-generation concept is novel and energy saving – an essential consideration for Kappture, and that the project distributed the currency in a fair and free manner – protecting it from possible classification as a security in the future.

In summary, we selected Nano for the following reasons:

a. Fast. Sub-second confirmation is quicker than bank payment cards.
b. Feeless. Zero fees irrespective of the amount. Nano can be used with no minimum payment.
c. Decentralized. At the time of writing it would require the collusion of three unrelated parties (whom all have a verifiable interest in the currency's value), to attack the network. Game theory asserts that these actors will not behave in a way contrary to their interests.
d. Scalable. Every account has a separate blockchain which can be updated independently of other accounts – this removes contention issues associated with early cryptocurrencies[xxii].
e. Green. Our terminals lead the way in energy consumption and supporting a project that relies heavily on PoW would be contrary to this goal.

We retain an open mind regarding the cryptocurrency landscape, but in our opinion, the only project that satisfies our requirements today is Nano.

Implementation

Our systems have been in commercial use since 2012 and serve tens of millions of orders annually. These systems support our customers in managing their inventory, legal and tax obligations, payments, vending, staff, stock, and cash management. We provide industry-leading management and analytical

[5] Several off-chain scaling solutions are being developed, in a similar vein to lightning network. These, too, are not yet ready and were not researched.
[6] No transaction fees, but there is an account opening fee & the protocol implements a form of inflation.
[7] ~1.5 second transaction time, but 2-3 minutes to be irreversible.
[8] 4-5 second confirmation time does not improve significantly on bank payment cards.

tools and innovate in areas like table service and consumer information – allergens and nutritional information, for example. We also offer a range of self-service products.

We support many payment options already, including cash, third-party account interfaces, and over 15 bank payment card interfaces.

The introduction of cryptocurrency to this system is a natural next step, and we believe our customers will have an appetite for it.

a. Overview

Our proposal is native. That is, the consumer pays in Nano, and the merchant receives the same amount of Nano – it's feeless.

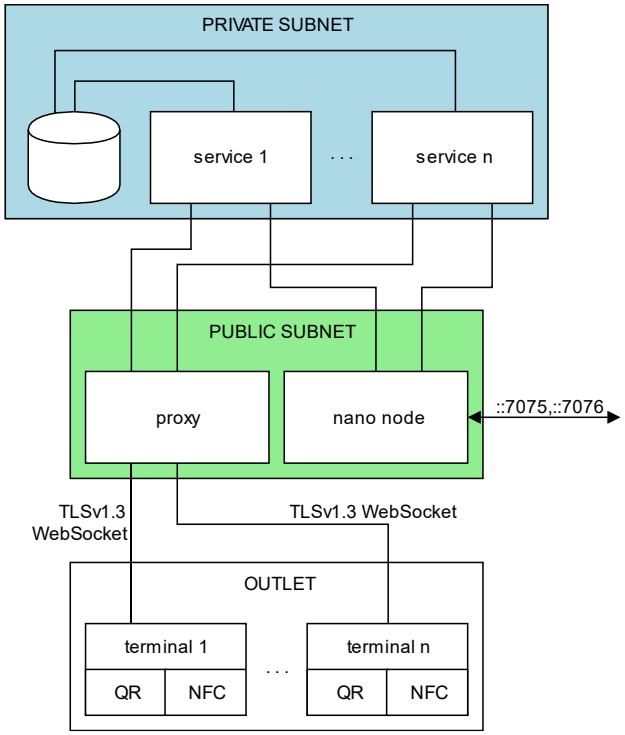
This native approach will surprise some, but to do otherwise misses the point. With few exceptions, consumers in the developed world have access to bank payment cards. Consumers using these cards report that the user experience is satisfactory, and merchants find the fees tolerable.

Introducing cryptocurrency in this competitive market requires that we exceed the status quo; for both consumers and merchants. We can do that in the following ways:

i. Being faster than payment cards.
ii. Offering autonomy over UX influencers like payment limits, security, receipts, and expenses.
iii. Zero fees even when accepting payments from foreign consumers.
iv. Reducing the hardware footprint at the point-of-sale.
v. Appealing to Generation Y + Z. Potential for a cult following and could attract new customers.
vi. Being socially responsible. Adopting this technology in the developed world paves the way for adoption elsewhere – where payment cards are unavailable to many.

Including a payment gateway in this proposal would deliver fiat (local currency) to the merchant but leaves us competing with banks on a level playing field; fees, and we can't win that. Additionally, the payment gateways we tried could not get close to our native implementation in terms of confirmation speed – vital in the hospitality industry.

b. Topology



c. Settlement

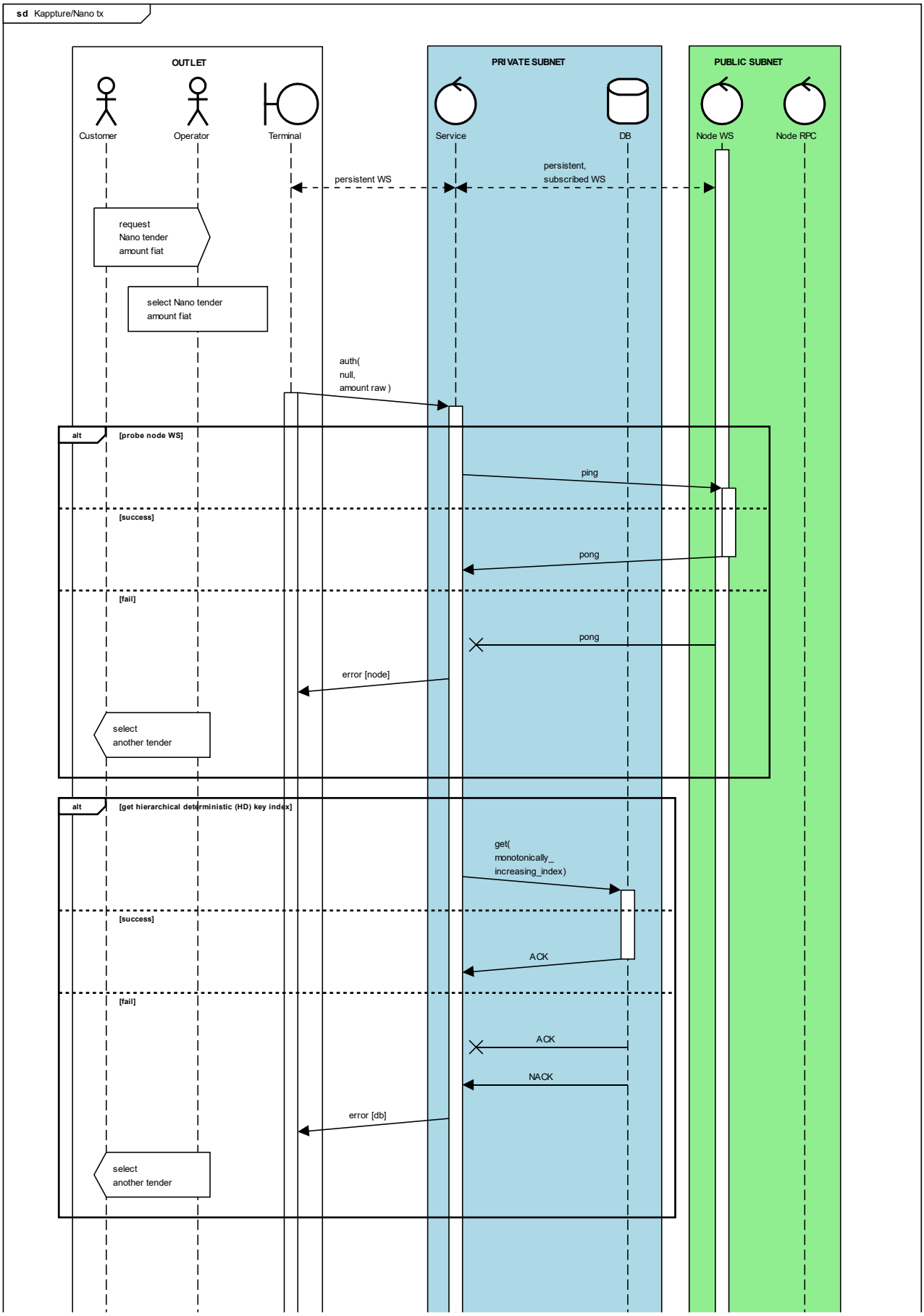
Nano has some unusual concepts. For every transaction that takes place a send block and a receive block must be created, with the receive block referencing the send blocks hash. In this proposal, the send block is created by the consumer with their smartphone wallet, and the merchant's wallet software creates the receive block.

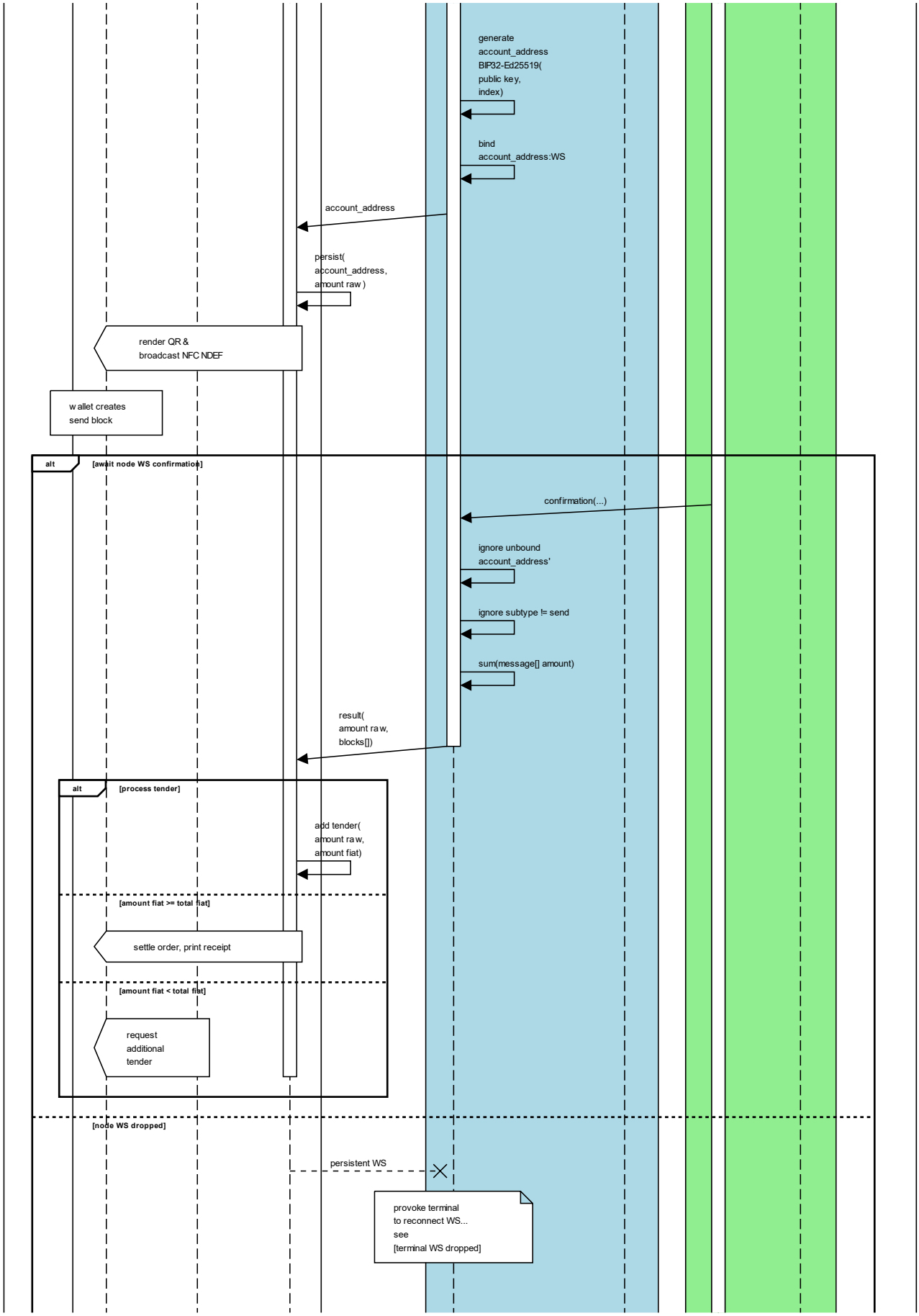
We cannot rely on the merchant's wallet – which might not be running or might be hosted by a third party – to create the receive block promptly. Further, as this proposal does not store private keys, we cannot create the receive block on behalf of the merchant.

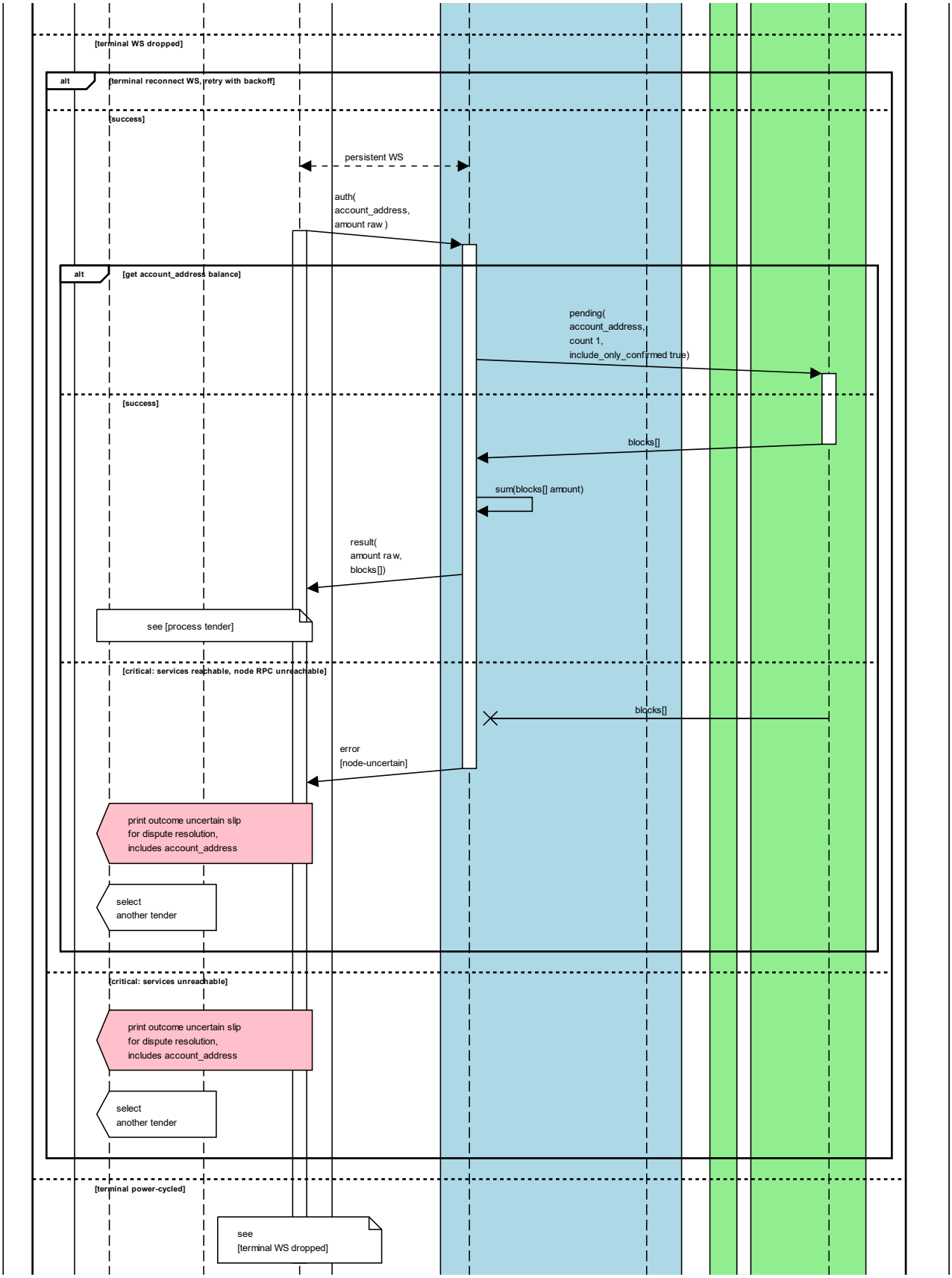
Nano innovates again here with the concept of 'pending blocks.' A pending block is a block that has been sent, but the corresponding receive block has not yet been created. Transactions in these blocks are sometimes called 'unpocketed transactions.' We can prove that a specific pending block has been confirmed by the consensus protocol and is, therefore, immutable – which is all that is required to accept the payment. The receive block can be created later.

These features make Nano transactions extremely fast – often irreversible confirmation can be achieved in a few hundred milliseconds.

d. Sequence diagrams TBC




generate
account_address
BIP32-Ed25519(
public key,
index)
bind
account_address:WS
account_address
persist(
account_address,
amount raw)
render QR &
broadcast NFC NDEF
wallet creates
send block
alt
[await node WS confirmation]
confirmation(...)
ignore unbound
account_address'
ignore subtype != send
sum(message[] amount)
result(
amount raw,
blocks[])
alt
[process tender]
add tender(
amount raw,
amount fiat)
[amount fiat >= total fiat]
settle order, print receipt
[amount fiat < total fiat]
request
additional
tender
[node WS dropped]
persistent WS
provoke terminal
to reconnect WS...
see
[terminal WS dropped]


[terminal WS dropped]
alt
[terminal reconnect WS, retry with backoff]
[success]
persistent WS
auth(
account_address,
amount raw)
alt
[get account_address balance]
pending(
account_address,
count 1,
include_only_confirmed true)
[success]
blocks[]
sum(blocks[] amount)
result(
amount raw,
blocks[])
see [process tender]
[critical: services reachable, node RPC unreachable]
blocks[]
error
[node-uncertain]
print outcome uncertain slip
for dispute resolution,
includes account_address
select
another tender
[critical: services unreachable]
print outcome uncertain slip
for dispute resolution,
includes account_address
select
another tender
[terminal power-cycled]
see
[terminal WS dropped]

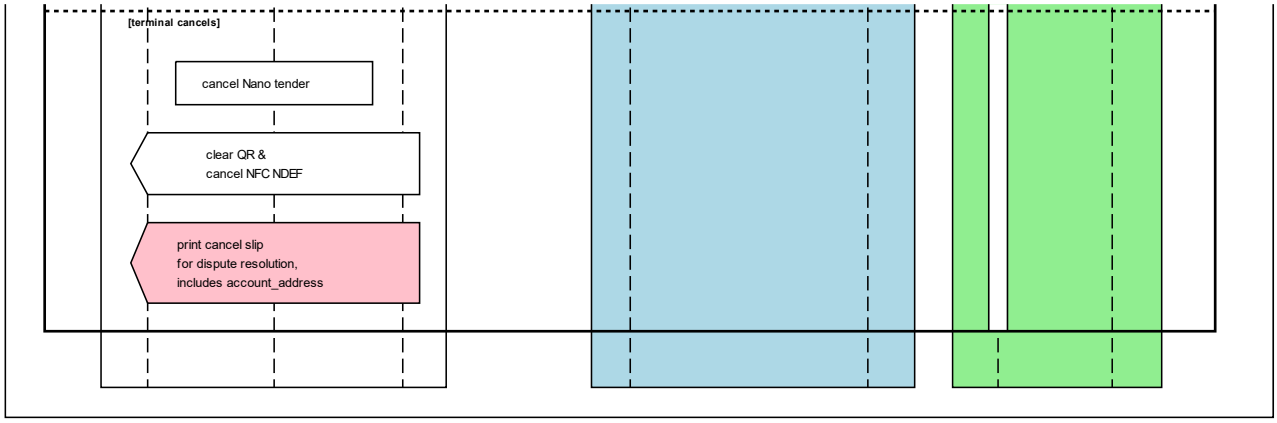


Fig. 1. A payment made at the point-of-sale showing all possible error scenarios, and their recovery.

The 'outcome uncertain' items are error scenarios that cannot be resolved entirely by the protocol. After the QR/NFC has been presented to the consumer, we enter a critical stage where we rely on network connectivity to determine the outcome. If connectivity fails, and it will occasionally, it is necessary to provide dispute resolution; here we print a slip for the consumer – a standard solution in bank payment card implementations.

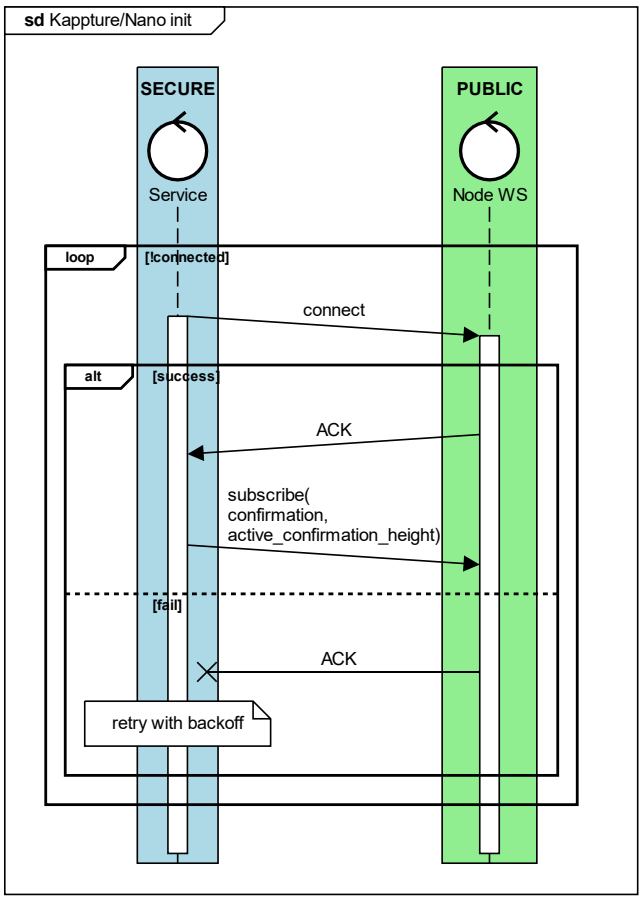


Fig. 2. Services initialization sequence. We use the WebSocket interface available in V19+ of the node implementation.

User experience

Fig. 3. The operator selects the Nano tender key to initiate payment.

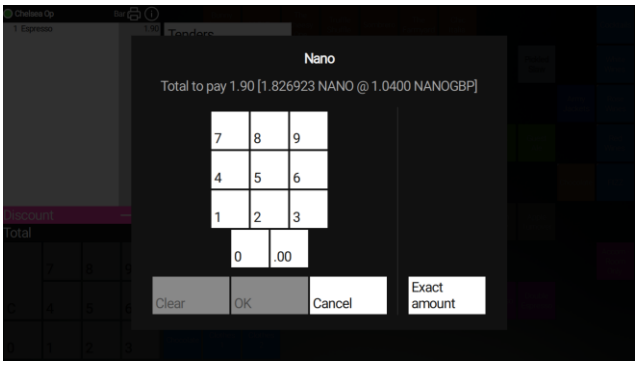


Fig. 4. The operator confirms the tender value. We permit overriding the value – perhaps the consumer wishes to pay part cash, part Nano. Values displayed represent total in fiat, total in NANO, and the rate used expressed as a trading pair. This method of handling currencies is standard, and a feature we already offer to merchants accepting dual currencies – GBPEUR, for example.

Fig. 5. Rendered on the rear of the terminal, facing the consumer. This view displays marketing content and video when not in use.

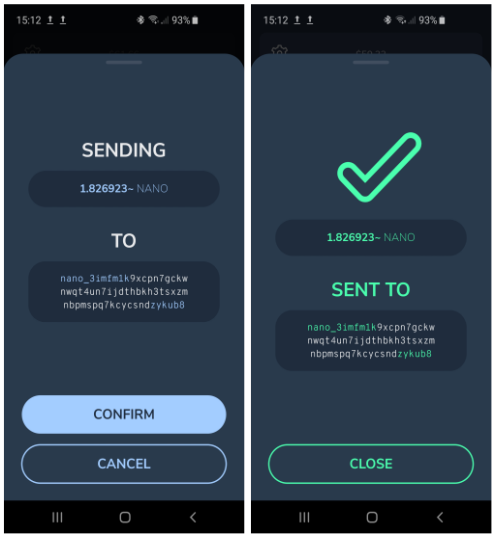


Fig. 6. Example consumer wallet view after scanning QR code, before and after confirming. natrium.io

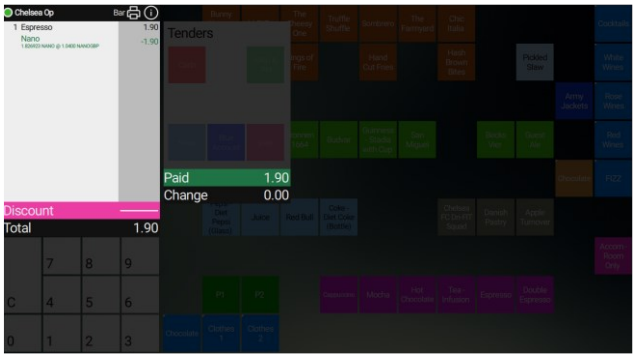


Fig. 7. Operator screen confirms payment practically instantly. The tender type (Nano), amount in NANO, and the NANOGBP rate is also displayed.


Kappture

@kappturelabs
Sterling House, Outrams Wharf
Little Eaton, Derby
DE21 5EL
ENGLAND

SALE

2019-06-28 15:12:45 ORDER 11-27
NJH 1 (27) STAFF EAT IN
OP CHELSEA OP (35)

1 ESPRESSO 1.90
TOTAL 1.90

TOTAL TO PAY 1.90
NANO 1.90
1.826923 NANO @ 1.0400 NANOGBP
CHANGE DUE 0.00

VAT SUMMARY

RATE	NET	VAT	TOTAL
20.00%	1.58	0.32	1.90

Fig. 8. Legal VAT receipt.

Merchant risk

a. Chargebacks

Merchants accepting bank payment cards are exposed to the risk of chargebacks – a type of liability. A chargeback occurs when a consumer disputes the transaction; because they did not receive the goods, the goods were not as described, or they did not authorize the transaction. The bank requires the merchant to reimburse the consumer and, in the UK, typically face fees anywhere from £7 to £150[xxiii].

Confirmed cryptocurrency payments cannot be reversed, by anyone. The writ of a judge cannot undo a transaction that has been confirmed on the network.

In practical terms, merchants would be expected to make good in other ways, with a second transaction, for example.

b. Currency volatility

Our proposal overseas the transfer of an amount of Nano asset from a consumer to a merchant in a safe, feeless, and practically instant way. The merchants operating costs, however, are likely to be in fiat – and their tax liability must also be paid in fiat.

Consequently, the merchant must exchange Nano periodically for their local currency.

Cryptocurrencies often go through periods of intense short-term volatility. When looking at extended periods though the picture is very different. In the 12 months leading up to the date of this proposal, the 30-day bitcoin/USD volatility has ranged between 1% and 6%[xxiv]. During the last month, EURUSD was 4.86%, GBPUSD was 5.95%, and NOKUSD was 8.93%[xxv] – these are major fiat currencies of the developed world.

Kappture can offer introductions to 'off ramps' who can assist with liquidating Nano. If a merchant decides to go down this route, they should budget for commission fees from 0.1% to 0.16%.

Taxation and reporting

Authorities in different jurisdictions have responded to cryptocurrencies in different ways. Within the EU, cryptocurrency is considered currency from a VAT perspective[xxvi], exempting consumers from additional taxes. Within the UK and Ireland, incorporated businesses do not pay capital gains tax (CGT).

HMRC in the UK has provided recent guidance for individuals only. In 2014 they provided guidance to businesses accepting payment in bitcoin, "there is no change to when revenue is recognized or how taxable profits are calculated[xxvii]." The Irish authorities have provided an explicit document[xxviii] that broadly reflects HMRC's position; stating corporation tax (CT) on profits or losses are paid in the normal way, with no special tax rules for cryptocurrency transactions being required.

On considering this guidance, we have made changes to the way we record transactions and the tools we provide. When a sale takes place, our systems record revenue in fiat and cost basis of the transaction. The VAT on goods and services, and CT on profits are still payable, and our system already facilitates that.

As merchants would inevitably hold Nano for some period, and the value of the currency will almost certainly vary to some extent, there is likely to be additional profit or loss that the company needs to report.

Our analytics tools have been extended to cover profit and loss (P&L) of the asset by considering cost basis at the time of the transaction and enabling operators to specify liquidation price at the time of disposal. With these figures, we can provide the reports required when preparing the company's annual accounts.

Please bear in mind that Kappture is primarily a software company, we are not accountants, and we are certainly not your accountants. Please seek expert advice with regards to the points in this section.

Attack vectors

The Nano whitepaper[xxix] describes possible attack scenarios for the protocol itself, including consequences of the attacks and the preventative measures taken.

Here we discuss two additional scenarios concerning our implementation.

a. Adversary controls Kappture server infrastructure

For reasons discussed, we do not hold private keys. Not only is this prudent from a legal perspective, but it also makes any attacks on our infrastructure unrewarding and means we do not require secure element hardware.

We do hold parent public keys, however. From these, we create account addresses through a process called deterministic hierarchical key derivation. Our services handle this process and send the account addresses to the terminal for rendering.

If an adversary were able to replace the parent public key with one relating to their account, then funds received at the point-of-sale would be credited to the adversaries derived account address.

Only one public key is stored per merchant. This key is isolated from the rest of the system and is encrypted at rest. Few employees within Kappture have access to the credentials required to change this key.

An analog to this attack with bank-issued payment machines is adversarial manipulation of the merchant number.

b. Adversary controls terminal hardware

Kappture terminals open two TLSv1.3 WebSockets to our services. One is concerned with the operation of the terminal, including configuration and transaction data, the other is a separate channel to a different endpoint handling cryptocurrency payment only.

Payloads sent and received are digitally signed. This tamper proofing is in addition to the protection offered by TLS. For this reason, we believe that man-in-the-middle attacks (MITM) would be challenging.

If an adversary had control over the terminal hardware itself, it might be possible to spoof the account address rendered for the consumer. Implementing this attack would indicate the adversary had compromised the OS – which accepts only binaries signed by us or had compromised our over-the-air (OTA) update process.

One solution to this, recently proposed by Appia[xxx], is for the services to sign the URI presented to the consumer. The consumer wallet then verifies the signature against a list of built-in trusted certificates and advises the consumer accordingly – much like HTTPS. This solution requires changes to consumer wallet implementations and will be addressed at a later stage.

Next steps

We believe the adoption of cryptocurrencies will happen on many different fronts, with different regions likely having different use cases.

Within the developed world, we see higher education institutions as early adopters for several reasons. Their consumers are a mostly captive audience, their demographic seems particularly interested in the technology, but most significantly they have a use case greater than merely saving fees; many run blockchain courses already – embracing cryptocurrency is practicing what they preach and furthers understanding of any hurdles we may face.

Many universities are already showing interest in adoption by accepting cryptocurrency against tuition fees – and some college endowment funds are investing in cryptocurrency funds[xxxi]. We would consider a joint project between multiple institutions and their contract caterers particularly rewarding and would invite any interested parties to get in touch.

Kappture supplies systems to many British universities already so naturally this is an approach we shall explore further.

Conclusion

We have demonstrated that a commercially viable pure-cryptocurrency solution can be implemented in a secure and scalable way while offering merchants the hallowed ground of payments; fast and feeless.

The proposal does not rely upon any third parties during the transaction process and can be implemented with complete autonomy; there are no application forms, merchants don't provide guarantors or security deposits, merchants can decide on payment limits, and their appetite to risk can determine when they liquidate Nano assets.

We have a working implementation of the solution described in this proposal and will be demonstrating it to the market in due course.

---

[i] https://stats.bis.org/statx/srs/table/CT2?m=4
[ii] https://www.finextra.com/pressarticle/70526/uk-hits-10-year-contactless-payments-milestone
[iii] https://link.springer.com/article/10.1023/A:1008196717017
[iv] https://www.visa.ie/dam/VCOM/regional/ve/ireland/in-page-images/future-of-payments/297x210_visa_irish_pay_report_p16952_dh11-55-45770.pdf
[v] https://www.conveniencestore.co.uk/news/contactless-saves-uk-consumers-34-years-each-month/541731.article
[vi] https://www.finextra.com/pressarticle/70526/uk-hits-10-year-contactless-payments-milestone
[vii] https://www.worldpay.com/sites/default/files/Worldpay-Point-2-Point-Encryption-The-Myths-and-Truths.pdf
[viii] https://www.pcisecuritystandards.org
[ix] https://www.hsdl.org/?abstract&did=27800
[x] https://hackernoon.com/6-reasons-why-crypto-is-here-to-stay-ec9bd62c096
[xi] https://www.bbc.com/news/world-latin-america-45246409
[xii] https://www.theguardian.com/world/2013/mar/26/cyprus-banks-closed-prevent-run-deposits
[xiii] https://www.theguardian.com/world/2013/mar/27/cyprus-emergency-restrictions-cash-withdrawals-banks
[xiv] https://ftalphaville.ft.com/2018/03/20/2199306/how-did-cypriots-respond-to-the-2013-banking-crisis
[xv] https://www.forbes.com/sites/laurashin/2016/08/23/blockchain-101-with-andreas-antonopoulos-how-bitcoin-makes-each-of-us-as-powerful-as-a-bank/#26175caf66d3
[xvi] https://www.ccn.com/crypto/bitcoin-evangelist-andreas-antonopoulos-says-facebooks-libra-isnt-real-blockchain/2019/06/18
[xvii] https://bitcoin.org/bitcoin.pdf
[xviii] https://coinmarketcap.com/all/views/all
[xix] https://coinmarketcap.com/charts
[xx] https://www.bitdegree.org/tutorials/lightning-network
[xxi] https://blog.iota.org/coordicide-e039fd43a871
[xxii] https://medium.com/@bnp117/stress-testing-the-raiblocks-network-part-ii-def83653b21f
[xxiii] https://centus.com/uk/a-complete-merchants-guide-to-chargebacks
[xxiv] https://bitvol.info/
[xxv] https://www.ratesfx.com/predictions/pred-usd.html
[xxvi] https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf
[xxvii] https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies
[xxviii] https://www.revenue.ie/en/tax-professionals/tdm/income-tax-capital-gains-tax-corporation-tax/part-02/02-01-03.pdf
[xxix] https://nano.org/en/whitepaper
[xxx] https://www.reddit.com/r/nanocurrency/comments/c2f9gi/appia_presentation_slideshow_summary_from_london/
[xxxi] https://www.forbes.com/sites/darrynpollock/2018/10/24/universities-show-a-surprising-leading-light-in-cryptocurrency-adoption/#79e554f31bd5