Analysing the Bitcoin Whitepaper

S. Tominaga AKA CSW
Sep 10, 2024
https://x.com/CsTominaga/status/1833385951394927069?t=Hs3f9218cupf8o61_D55bg&s=19

https://t.me/S_Tominaga/330

The Introduction

Commerce on the Internet still relies heavily on the use of trusted third parties. These are otherwise known as Internet intermediaries. For example, it is not possible to investigate and create a system that provides fast, low-cost micropayments and tokenisation services across the Internet without understanding the existing laws that apply to the systems. Internet intermediaries and those systems used by financial gatekeepers to control malfeasance over the Internet are essential for any system that will run without falling to criminal predation. The Internet is fundamentally a means of communication. Issues with law that have arisen because of the Internet are thus a result of the differences between communication in the physical world and communication using systems to provide remote communications of a digital communications platform where people may never meet face to face. Contractual negotiations result from a series of communications that create a legally binding agreement [1], and although the Internet has allowed the development of new methods to facilitate exchange, many of these are analogous to time tested methods.

For example, contracting over postal exchange and by telegram or fax has been addressed for many decades and even across centuries. Yet, past the ability for electronic systems to send to a far wider audience or for the delivery of a message to occur on a faster basis, there is little legal difference between many forms of electronic exchange and contracting and postal contracting.

Although the Internet has changed the backdrop of the economy and society, it has not radically changed the nature of either civil or criminal transgressions. Rather, it has added a layer of complexity through the speed and volumes of its enabled transactions. The issue for the law and society is not an introduction of new crimes or new transgressions but an enhanced capability both to engage in these activities and the increased capacity to find them. Here again, another issue develops with the juxtaposition of security and privacy. The increased ability of the intermediaries to monitor and control our actions is directed by the need to protect personal liberty. The incorrect balance of these forces leads to either too little security and a possible finding of negligence (or worse) or the breach of controls designed to protect society and the possible criminal effects of these actions.

Further, the added layer of complexity that has been created through the existing intermediary solutions has limited the possibilities for new forms of commerce that were promised at the birth of the Internet. The inability to offer micropayments has stifled the growth and development of new and novel technologies leading to the sale of privacy and personal information. Anonymity and leaky international boundaries impede the prosecution of the primary malfeasors, increasing the cost of providing secure technical solutions that do not offer a path to criminal activity. The malfeasors require payment intermediaries to process their transactions. The requirements imposed on intermediaries to track and trace this form of risk have led to the collapse of the eCash payment system and the inability of pre-existing systems to provide micropayments services.

What is a Payment Intermediary?

The Bitcoin White Paper mentions the term trusted third-party. Another name for this that is used within legal writings is a payment intermediary. Financial intermediaries are trusted third parties in Internet communications and Internet value exchanges. The transaction goes through a middleman function rather than a peer-to-peer or person-to-person exchange. In bitcoin, the system was designed such that party A can communicate directly with party B without having to go through an intermediary. Many individuals have misunderstood the nature of bitcoin and believe that party A needs to send a transaction to the mining nodes, who then forward it to party B. The node becomes an intermediary rather than a pure ledger function in this scenario. The design of bitcoin was such that individuals would be able to transfer value directly using peer-to-peer exchanges. The receiving party can validate the process and ensure it is cleared and settled by sending it to the (miners) nodes. This distinction is important.

Without the ability to send directly between systems without an intermediary, including bitcoin mining nodes, it becomes impossible to create a peer-to-peer system analogous to cash while simultaneously allowing electronic transfers. Bitcoin solves this problem by allowing a peer-to-peer transfer of cash-like transactions.

The difficulties in transferring cash payments over large distances and between people who may have never met and may never meet created the need for payment intermediaries in Internet transactions. Payment intermediaries provide both trust and some realistic means for a purchaser to reliably transfer consideration to the seller. For instance, if a buyer on an online auction site comes up with the highest bid incurring debt, a payment intermediary would be involved to arrange a transfer of funds either from the purchases banking account or via some payment card system making the transaction.
For example, if party A located in Singapore was to sign up for an account with a licensed online casino such as Lasseter's online in Australia, party A would require transferring funds from their banking account to a trust account managed and maintained by Lasseter's. In addition, when party A has subsequently been successful at their gambling pursuit by playing online poker, the party would require some means of ensuring the return of their winnings. If, on the other hand, party A had accumulated gambling debts, Lasseter's would require some means of ensuring that funds in the trust account we used to pay those debts.

In the case of less significant amounts, this may be as simple as holding party A's credit card details in a database. However, when the transactions are large, an online casino may wish

to use party A's bank to transfer money in advance or otherwise to secure some assurance that A's potential gambling losses will be covered. In practice, the payment card company or bank is an essential actor in the conduct that "party A" desires to enact.

It was originally believed [2]that digital cash or electronic money would be created or minted, allowing for universal credit and facilitating Internet transactions. Although several schemes did emerge, the vast majority of transactions across the Internet are made utilising traditional means such as credit cards [3]. Rather than digital cash being minted, a new type of payment intermediary developed. Peer to peer (P2P) payment systems, [4] such as PayPal, emerged, allowing individuals to receive transactions directly [5], bypassing merchants and acting as a means of consolidating payment methods by providing a mechanism to interact with various banks and payment card institutions directly.

Peer-to-peer processing networks have aided the growth of auction intermediaries such as eBay [6]. Payment card providers, P2P systems, and other entities that act as a mechanism to facilitate commercial transactions [7] also have the capability to stop illicit transactions and act as revelatory enforcement points. For example, a commercial site distributing child pornography from Nigeria cannot be run profitably without an economical method of receiving consideration. If the site operators cannot reliably receive payment, they will quickly shut down. As the financial gatekeepers, payment intermediaries can be used to prevent illicit activity over the Internet. Either through proactive actions or upon the receipt of court orders, an Internet payment intermediary could be used as an aid to curtail undesirable activities occurring across the Internet.
Auction intermediaries

The auction intermediary has become the predominant means of matching buyers and sellers. These range from the classic option structure defined by the industry leader, eBay, to a more dynamic market structure reminiscent of a stock exchange futures exchange trading floor. At the simplest, these parties provide client-to-client matching services allowing individuals and small corporations across the globe to deal (seemingly) directly.

These organisations are the target of most complaints concerning breaches of contract, illicit or illegal goods and even failure to act. One of the difficulties is the direct result of legislative differences between jurisdictions. In many cases, goods or services that may be legal in one jurisdiction could be controlled or proscribed in another. Liability for internet auction intermediaries mirrors those principles that have been created and applied in disputes concerning traditional or real-world auction intermediaries, as may be seen in Fonavisa [8].

Bitcoin has implemented a complex scripting language that allows for the development of escrow solutions. The script system allows for complex contracts, including the creation of bidding systems and even transactions that can be used to track the progress of delivery or act as a bill of lading and exchange. The nature of bitcoin is such that an overlay peer network could be created on top of bitcoin. Using payment channels and time-locked transactions, an option could be created that is provably fair and auditable without requiring the use of intermediaries. This would still enable mediation or arbitration to occur if the buyer did not receive the goods that they were promised and could escrow funds in a way that ensures the seller is paid for honest delivery.

Intermediaries would still operate even with bitcoin as a pavement mechanism. Although individuals would be able to interact directly and have a trusted channel in which to exchange funds, bitcoin does not operate in a manner that allows individuals to discover each other. The ability to integrate micropayments would allow other complimentary services to develop. An auction search facility that list buyers and sellers in times of options or other sales could be created that does not require any information about the negotiating parties, did not sell information to advertising companies and which could be trusted not to take funds as it would not interact directly in the auction process. At the same time, the ability to pay multiple outputs in bitcoin allows intermediaries to be paid for their services. This capability increases trust is none of the interacting participants need worry about fraud.

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments.

Practically no scalable peer-to-peer payment systems existed prior to the introduction of bitcoin. A few local small-scale systems and attempts at making localised money systems and tokens have started and generally ended without much impact. Consequently, most commerce conducted across the Internet has been based on systems using financial institutions. Even payment platforms such as PayPal have in effect become Internet intermediaries or trusted third parties sitting between the buyer and seller to process electronic communications. In scenarios where large Internet merchants such as Amazon have attempted to introduce tokens, these have been exchanged through an interaction with external financial institutions.

Internet intermediaries have evolved to facilitate interactions between different individuals and organisations across the Internet. These organisations involved due to the inability of individuals to directly exchange value. In the physical world, individuals can use cash-based systems and physical cash to directly pay another individual or organisation for goods and services. These cash interactions allow for low risk exchanges of value where individuals can remain private and you do not need to provide high levels of personal information that will be stored by the merchant. In fact, an individual can walk into a store, hand over a £20 note for the purchase of goods and receive change without providing any information about their identity. Outside of the risk of receiving a counterfeit note, the merchant receiving a cash payment can be assured that the transaction is final. No further processing is required on either side of the equation.

Without the ability to make small purchases [9], many promised uses of the Internet and digital technology have failed to evolve. Rather, we have ended with a model that sells information to fund small micro services. For services where the value in any limited period of (say a week) time, in place of monetary micropayments, companies sell services based on the farming of user identity and the provision of advertising.

Where commerce is conducted through intermediaries, additional risk and the requirements of gathering information about the individual apply. In order to minimise the risk faced by intermediaries, it becomes necessary to collect large amounts of personal information concerning the parties to a trade. Intermediaries then need to implement expensive information security systems in order to protect this data. Even then, data breaches and the loss of PII remains a frequent occurrence. Intermediaries that need to remain vigilant and

take action to reduce fraud and system compromise. This greatly increases the cost of providing services and removes all possibilities of providing micropayments and allowing for the growth of individualised resource access.

Inaction from Internet intermediaries has been shown to be risky at best. We have seen that the most effective enforcement framework involves enforcement from the least cost provider as proposed by Mann & Belzley [10]. There are various kinds of services connected with the Internet, and the liability of the service provider may depend on what is being provided. At one extreme there are the long-distance telecommunications providers, at the other there are Internet publishers and other providers of material. In between there are a range of providers such as operators of node computers, Internet access providers, providers of bulletin boards, Usenet group organisers and providers of host computers for web pages. Liability and risk for an Internet intermediary will depend on how court faced with a case of first impression analogises the specific service and classes at against more conventional categories of contracting and information exchange.

For example, should the service provider be viewed as the equivalent of the telephone company, purely a conduit for information? This might be the right analogy for the telecommunications link provider, but clearly does not fit the publisher. On the other hand, if the provider is viewed as analogous to a publisher of a printed publication, there is a much greater exposure to liability [11]. The provider of a host computer for third party web pages could be compared to a printer or perhaps a distributor of printed publications. It could also be argued that a Usenet group or bulletin board is analogous to a library, so that the provider should be treated as the librarian.

The foremost dilemma with the study of electronic law is the complexity and difficulty in confining its study within simple parameters. Internet and e-commerce do not define a distinct area of law as with contract [12] and tort law. Electronic law crosses many legal disciplines, each of which can be studied individually. Examples of a range of areas of law that electronic, e-commerce, and Internet law touch upon can be seen in the following pages.

In fact, existing laws already address many situations that may impact an online payment Internet intermediary. In most cases (for instance), cybercrimes are just age-old crimes committed using a new technology. Identity theft, for instance, has existed for hundreds of years, only now the speed and volume, and hence the consequence of the offence is increased. What is important to the intermediary is the increased scope of responsibility that many of them now face.

New challenges do arise through the nature of widely distributed networks such as the Internet. Some legal jurisdictions have addressed this issue through the enhancement of existing laws. Most, however, have adopted an approach where they define solutions to a uniquely perceived legal difficulty through the creation of separate digital laws. In particular, these are manifest in the numerous additions to computer crime statutes that have recently populated the various criminal codes.
Of distinctive confusion to the internet intermediary is the distinction between what is illegal and what is criminal. This, however, is not a distinction solely confined to electronic law. It is important to note that although many actions are illegal, they may not be criminal in nature.

This is important as the evidentiary requirements in criminal cases are far stricter than in civil litigation. This is also reflected in the actions that the intermediary will be required to take, both to stop another party [13] who is involved in a criminal activity, and the actions needed to minimise the tortuous actions that they may be exposed to.

The study of intermediary and payment provider liability is a topic that was fundamental to bitcoin. Bitcoin is not just technological in scope, incorporates many aspects of law, including:

· Law of International Trade
· Commercial Law
· Competition Law
· E-Commerce Law
· International Trade Finance Law
· Monetary law
· Criminal law

The primary dilemma with the study of electronic law is the complexity and difficulty in confining its study within simple parameters. Internet and e-commerce do not define a distinct area of law as with contract [14] and tort law. Electronic law crosses many legal disciplines, each of which can be studied individually. The range of areas of law that electronic, e-commerce, and Internet law touch upon is vast leading to uncertainty within Internet law and the extent to which this covers intermediaries.

The difficulties in transferring cash payments over vast distances and between people who may have never met and may never meet have created a need for payment intermediaries in Internet transactions. Payment intermediaries provide both trust and some realistic means for a purchaser to transfer consideration to the seller reliably. For instance, if a buyer on an online auction site comes up with the highest bid incurring debt, a payment intermediary would be involved in order to arrange a transfer of funds either from the purchases banking account or via some payment card system for finalising the transaction.

All of this adds to the risk of fraud requiring the intermediary to hold large quantities of personal information, allowing them to identify and track the purchaser. Sellers are thus unable to engage in small transactions or micropayments due to the cost associated with managing losses from malfeasance, and the system is required to protect personally identifiable information.
For the first time, bitcoin allows individuals and merchants to engage in micropayments services where the provision of resource access can be provided for fractions of a US cent. Internet intermediaries have thus developed without the ability to deliver on the commercial promise of the Internet. Bitcoin solves this problem for the first time.

Internet Intermediaries

It was initially argued that widespread disintermediation [15] would occur over the Internet. It was initially believed that the Internet would provide a means to allow transacting parties to deal directly with each other. The opposite has occurred with additional layers being formed rather than removed. There are two primary reasons for this growth of intermediaries, the first is related to the need to connect to the Internet and the second derives from both trust

and the availability of payment. In either case any transaction conducted over the Internet will not be in person. The consequence being that cash exchanges cannot occur, and the third-party will need to provide the trusted source of funds. The simple need to connect also derives from the distance that may be involved. When communicating across vast distances in small amounts of time and intermediary is always needed. In the past telecommunications carriers provided fax and phone services to satisfy this transaction. In effect what the Internet has done is to supplant fax, telephony, telex and electronic data interchange (EDI) with new and more universally accepted protocols. It would be rare to find any two parties with enough resources to construct and connect a global internetwork themselves.

The issue of trust surrounds payments creating opportunities for both payment and auction intermediaries. In a contemporary transaction for the sale of a product any one individual would not be able to assemble the essential resources necessary to reach a global market. The growth of auction intermediaries such as eBay [16] has created the ability to offer products and services internationally creating global markets. The consequence is that intermediaries have created market segments that were not thought possible and did not previously exist curtailing the expected disintermediation of the Internet.

All of this has come with a cost. Many of the expected benefits of frictionless sales and the ability to relay information quickly and been lost as small payments are not available. Intermediaries have needed to implement systems to control security risks, account for fraud and credit card reversals and to maintain excessive levels of private information. This model only achieves privacy through the ability to restrict access to information between the parties involved and the payment intermediary.

In this privacy model, payment providers and intermediaries hold full information on the identity of individuals and other parties making transactions. Although the public is firewalls from viewing information associated with any transactions, both the intermediary and other counterparty such as the intermediaries providing risk services must all hold detailed information about the client or customer.

While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

Most transactions on the Internet have been relatively large impaired to the possibilities and promised solutions. Solutions have been formed for many of the issues with electronic payments, though all these solutions have increased the cost of providing services and require the provider or intermediary to maintain excessive amounts of information about their customers.

An Internet intermediary can in effect provide either of two services to either a single party or multiple parties. These services include the provision of access to communication channels or the provision of an additional service over these channels. In the first instance we are looking at a traditional Internet service provider or ISP. An ISP can provide general backbone routing services and connectivity. This is the most fundamental of the services as without a connection to the Internet no other Internet-based services may be accessed. Additionally, an ISP can also provide access to systems and storage space.

The second instance involves an Internet content provider or ICP. An ICP can cover a far wider range of activities than an ISP. In its most basic form this is the provision of transaction services between parties, identification and authorisation of parties, the provision of search capabilities or a combination of any of the above. In effect, the addition of web portals to traditional banking systems has turned the banking industry into an Internet content provider. The bank provides authorisation, identification and transaction processing capabilities. These capabilities extend beyond simple transaction processing and the accessing of one's own account. Services such as PayPal [17] have emerged to offer intermediary payment facilities over the Internet allowing users to transact without developing these capabilities themselves and offering a service in such a manner that the end client may not even be aware of the existence of the payment intermediary.

The system, or how people process payments over the Internet at present works very well for most transactions. Vendor's can take actions that minimise risk and unable fraud to be recorded. Overall, the cost of these actions has been built into the majority of transactions as they occur at present. Stable electronic markets have been formed over the Internet replacing a variety of retail operations. Internet intermediaries cover risk through the introduction of costs and other controls allowing individuals and merchants to operate profitably. They may do this only above certain minimum levels in the present system. Additionally, this system relies heavily on trust and brand leading to the aggregation and conglomeration into retail operations into a few large players. To be viable, the path towards the promised disintermediation of services over the Internet would need to be built on a low-cost, low transaction fee system. The nature of such a system is one that supports micropayments and that is it scales becomes less expensive.

Mayer et al, declare that trust is "the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party".

A model based on trust leads towards an aggregation of smaller entities. Over time, large platters such as Amazon and eBay develop a brand-based reputation. The reliance on trust limits the willingness of transacting individuals to risk operating on smaller sites. Over time, more and more people start trusting brand based decisions and the trust model leads to a large aggregation rather than a disintermediation effect. Where the Internet could provide many small sites, large conglomerates form that slowly consume the smaller competitors. A part of this problem comes from the economics of removing risk. Where potential users of the site are unable to determine the amount of risk and hence trust needed, they will generally move towards a more well-known site.

The trust-based model and its propensity to aggregate services based on brand and shared knowledge becomes a determining factor into market formation. Individual buyer and seller need a slowly translated into specific ones that match the environment being provided. The trust-based model influences the willingness and ability of individuals involved with the system to seek additional resources and for merchants to seek to help their clients overcome pressures associated with risk and vulnerability.

The trust-based model of the Internet completely precludes casual transactions for small value outside of well-known marketed brands. The inability to engage in micropayments limits the potential range of offerings and the inability to transfer value without the transacting parties experiencing significant levels of risk and vulnerability herds people towards known services. Where websites and other services offer a potential alternative, but the system or service is not known, the lack of trust leads people to limit the potential amount of commerce they would be willing to do. If individuals knew that they would not be placing their money at risk, but any potential sale either conducted at a low enough financial level that a loss was irrelevant or that they could protect the exchange with out needing to fall back to a third-party, many potential offerings could evolve.

At present, payment intermediaries provide a means of limiting loss is associated with the potential for fraud. In being able to rely on payment intermediaries including those such as Visa, individuals minimise the need for trust dealing with third parties such as websites and merchants by placing trust in a payment provider and intermediary who can act to recover lost funds. This process is inefficient and expensive. It leads to many potential services that are legal but that act on the fringe becoming unavailable. More importantly, it adds cost increases the transactional frictions between trades.
Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes.
There are numerous forms of services that involve one party taking a loss including gambling, lotteries and even in auctions where people feel that they have overpaid or overbid. In any of these scenarios, the trust-based model allows individuals to interact with the trusted intermediary in order to in validly seek to stop or reverse transactions. In this scenario, a completely legal transaction involving one party's loss of value can result in a miner fraud being committed against the merchant. In licensed casinos, individuals commonly seek to reverse transactions following losses. It is not uncommon for individuals losing money to argue that their credit card was compromised or that they have had a computer compromised and their funds stolen.

Many people have come to the false belief that a non-reversible transaction means that their money cannot be seized even in criminal prosecutions. Cash involves non-reversible transactions. When you hand someone a £20 note and they leave the store, there is no legal requirement for the shop owner to return your £20 if they come back an hour later and say they didn't like their coffee. In theory, if there was something wrong with the coffee the individual would be able to start an action to recover their money. This involves a court case and because cash is fungible, it doesn't matter which coins are given back.
In modern accounting systems, most transactions are set to be non-reversible. If an error occurs, the error can be corrected. This is achieved by adding a new record. The bitcoin blockchain does not preclude changing ownership and this would be within the rules. To do so, a court order would be recorded stating the change and the reason and this could be saved on chain. Under the rule of law, courts act as a public function. They can be audited and viewed by all individuals. In a system based on the blockchain, if a seizure of criminal assets or recovery of funds has occurred, this will be public. It is not that it is not possible, it is that any alterations are publicly auditable.

With credit cards, the security risk and ease of which a criminal fraud being can lead to an expenditure, it becomes simple for parties to deny making a transaction if they change their

mind afterwards. The losses associated with credit cards are built into their fees increasing the cost of transactions and setting a minimum effective value of transactions in the five dollar and above range. This instantly invalidates many uses of monetary exchange of the Internet. This also does not invalidate an individual's right to take action in court. Financial institutions and intermediaries do not remove court functions, rather they add a separate layer.

In the current model, the individuals exchanging value, the financial intermediary and the court all end up involved in mediating and resolving disputes. This increases the cost of providing these services. In the model created by bitcoin, dispute resolution becomes distributed, the legal system is truly distributed. Each party has their own lawyers and they act as peers exchanging information between each other. There is no need to involve third parties in the dispute.

Bitcoin removes the necessity to have financial intermediaries interjected between peers. This does not remove the right or ability for individuals to take an action against another person with whom they have traded with. Bitcoin does simplify some of the process. The template structure of bitcoin allows individuals to securely and privately incorporate identity information and marker information such as invoices. The individuals may also pay tax and other amounts instantly such as VAT. With this, an individual seeking to take action for a small value in small claims court would be able to use the information available as evidence. If they have received a template from the trading party, this negotiation can be done in a way that is able to be provably linked to the other individual. This can be done in such a way that both individuals remain private. The value exchange is also done using digital signatures which retain evidentiary value and can be admitted for use in court.
Where the values are too small, many industries have ombudsman and mediation services that can act as a mediator. At present, many of these ombudsman services are funded by government and do not cost the individuals engaging the service anything. The nature of the system is analogous to cash with receipts. The parties engaged in trade can remain private but simultaneously and engage in final transactions without needing to involve a financial intermediary. The statement, completely non-reversible refers to the finality of the transaction on chain. This does not mean that individuals lose their rights to dispute transactions.

The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services.

With the possibility of reversal, the need for trust spreads.

The ability to delete an entry in a log is analogous to the reversal of the bitcoin transaction. Bitcoin's main selling point is the capability of delivering micropayments across the Internet. No system has been able to do this before bitcoin. Where small casual transactions are involved, the cost of a third-party trust provider exponentially increases the cost of delivering a micropayments solution. Users can seek comfort in the merchants reputation and the consumer protection requirements that is associated with selling on the Internet.

The merchant on the other hand needs to protect themselves from fraud. Internet sellers have had to go to third-party intermediaries is no system existed that acted like cash on the

Internet. Where a purchaser in a physical shop has paid a merchant using cash and received a receipt, it is possible to dispute a sale using existing methods. None of these methods existed for online sales before bitcoin. Purchases would be able to easily defraud sellers and often would be able to get away with a theft. With bitcoin, a purchaser has an invoice that they can use if they wish to dispute a sale and the seller has a transaction that is analogous in nature to cash.

Merchants must be wary of their customers, hassling them for more information than they would otherwise need.
A certain percentage of fraud is accepted as unavoidable.
No system is perfect, and definitely not bitcoin. Unfortunately, bitcoin cannot implement all possible controls that would stop fraud and, where frauds are small, the cost of finding the perpetrator and recovery money would exceed the benefit. Double spend attacks are unlikely to ever occur, but this does not stop people from deceiving purchases and making sales without delivering the product or even is posing as other individuals. With bitcoin, many of the existing frauds that occur within modern transaction system such as credit cards and older system such as checks have been mitigated. But as with any existing system, an individual or group who steals access to someone else's bitcoin wallet can make transactions posing as the victim.

Further, where websites and marketing material are compromised and altered, a fraudster could trick a user into paying into the wrong template address. As an example, if a hacker is able to compromise the exchange mechanisms between a user and a merchant, the user could be tricked into sending bitcoin to another address and not that which the merchant has issued as a payment address. A deceptive merchant could also issue a payment request for an amount that exceeds the bill possibly leading to a careless user paying more than they should.

Whilst all these frauds and thefts are possible, bitcoin maintains a ledger of all the activity on the system allowing the users and merchants to report any illicit or criminal activity. Over time, any large-scale fraud would be able to be tracked and a possibility of recovery of at least some of the bitcoin would exist.

These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.

In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.

The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

The postal acceptance rule and payments on the Internet

The postal acceptance rule states that where acceptance is to be sent by post, the contract associated with that acceptance is considered as concluded at the moment of posting the letter, not when the letter is received (or in fact if the letter is received). If the offeror does not wish to conclude, the contract through acceptance via the post, s/he may stipulate the form of acceptance. (The “postal acceptance rule” was introduced to present assurance to the “new” British penny post. It dates back to Adams v. Lindsell, 1 Barnewall and Alderson 681, In the King’s Bench (1818); See also Household Fire Insurance Co v Grant [1879] 4 Ex D 216).

Although telex, faxes and e-mail are separate technologies, they share many features. In both Entores v. Miles Far East Corp ([1955] 2 QB 327) and Brinkibon Ltd v Stahag Stahl (1983), the courts declined to extend the application of the postal acceptance rules.

The postal acceptance rule as a general consideration does not apply to Web-based communications. This follows as most Web-based systems employee mechanisms such as check-sums to maintain constant communication between the client and server systems. The constant verification this communication channel provides for the implication that communications take place though an immediate send process. Thus, both parties receive communications instantaneously.

In a similar manner to the web, a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a payment intermediary. This form of contractual negotiations is distinct from e-mail and deserves separate consideration. “Click-wrap” Internet contracts (Reed, 2004) have their own issues, but they still mirror many of the technologies that have preceded them. Thus far, payment intermediaries have been required a system such as DigiCash and EGold use intermediaries as a solution to the double spending problem.

Extrinsic evidence necessary in the case of electronic signatures, then would need to include:
(a) That the signature key or its equivalent was in the possession of the alleged signatory or his authorised agent;
(b) That the use of that signature key produces the electronic signature affixed to the document in question; and
(c) That the mathematical probability that some alternative key in the possession of a third party could have created the same signature is sufficiently low to convince the court that the signature was in fact affixed by the signatory. (van de Graaf, 1987).

In the case of the public key encryption systems, proof that the signature verifies successfully with the signatory’s public key should be sufficient if that public key can reliably be attributed to the signatory. In a limited value system such as micropayments, digital signatures would be able to provide much of the solution but the cost of ensuring that

intermediaries are covered against fraud and loss makes the use of micropayments infeasible in today's Internet.

The result of this is that commerce on the Internet has come to rely nearly exclusively on payment intermediaries with the associated costs and processing electronic payments. For the majority of day-to-day transactions, the system works well enough. The inherent weaknesses of the trust-based model come through the need to mitigate fraud and the associated economic costs that this creates. Micropayments would require the introduction of micropayments that are economically infeasible to mediate. To be of use, such a system would rely on either the buyer or the seller being willing to place trust in the other party to a level where they would prefer to walk away from a transaction than to dispute it. Mediation, arbitration and disputes that lead to court processes increase the friction of trade and increment transactional costs.

Micropayments and even small casual transactions are thus precluded from being used and as with cases theory of the firm, intermediaries grow into the size that is economically viable. Many economic solutions fail to be implemented or developed due to the transactional frictions that exist. At present, no mechanism exists to make payments over communication channel without a trusted payment intermediary.

Electronic payment systems including digital currency systems of the past have always required third-party interactions. Systems including Digicash and EGold have looked to incorporate system such as traitor tracing and methodologies to expose parties who engage in fraudulent transactions or double spending. Some early electronic systems would use a timestamp server created by announcing the hash of a contract or transaction using a USENET system or even publication in newspapers. This would prove the existence of data at a point in time but due to a lack of automation did little to limit the costs associated with micropayments.

Both Digicash and EGold required a central party that can check for the existence of double-spends. This trusted central authority. or mint, would validate transactions ensuring that double spends did not occur or, if they were to occur would engage in activities such as traitor tracing for the publishing of the malfeasance private key. Mint based models such as Digicash relied on banking systems that acted as payment intermediaries. These intermediaries would act to decide on the ordering of payments and implement fraud measures similar to that involved in credit card companies. This need for a trusted intermediary removes the capability of these systems to engage in very small transactions.

It was originally believed [18] that digital cash or electronic money would be created or minted allowing for some type of universal credit and would facilitate Internet transactions. Although a few systems did emerge, numerous transactions that occur across the Internet are made by means of traditional means such as credit cards [19]. Rather than digital cash being minted, a new type of payment intermediary developed. Peer to peer (P2P) payment systems, [20] such as PayPal, emerged allowing individuals to receive transactions directly [21], bypassing merchants and act as a means of consolidating payment methods by providing a mechanism to interact with various banks and payment card institutions directly.

Peer-to-peer processing networks have aided the growth of auction intermediaries such as eBay [22]. Payment card providers, P2P systems, and other entities that act as a mechanism to facilitate commercial transactions [23] also have the capability to stop illicit transactions and act as revelatory enforcement points. A commercial site distributing child pornography from Nigeria cannot be run profitably without an economical method of receiving consideration. If the site operators cannot reliably receive payment, they will quickly shut down. As the financial gatekeepers, payment intermediaries can be used to prevent illicit activity over the Internet. Either through proactive actions or upon the receipt of court orders and Internet payment intermediary could be used as an aid to curtail undesirable activities occurring across the Internet. Unfortunately, we demonstrate that these new P2P systems suffer from the same costs and limitations of their predecessors and that these limitations add a minimum cost of any Internet transaction and stop the ability for payment processes to engage in small or micro transactions effectively.

[1] An electronic contract has a twofold structure. Thought of electronically, the contract is a sequence of numbers and code saved to some electronic or magnetic medium. Alternatively, the contract becomes perceptible through a transformation of the numeric code when broadcast to a computer output device such as a printer or screen . Prior to the passing of the ECA, this dichotomy exasperated the uncertainty contiguous with whether an electronic contract can be regarded as being a contract in writing.

[2] Anderson et al. in their Dec 1997 presentation “Exploring Digital Cash” argued that digital cash would “likely continue to evolve remarkably quickly”.

[3] In 2002, roughly ninety percent of internet transactions used credit cards. Ronald J. Mann, Regulating Internet Payment Intermediaries, 82 Texas L. Rev. 681, 681 (2004).

[4] In this context, P2P stands for “person-to-person.” The term is to be distinguished from the more common use of the same acronym to describe the peer-to-peer file sharing discussed in the context of piracy.

[5] See Mann, at 683.

[6] Id.

[7] Because of the fluidity of payment mechanisms on the internet, there are a wide variety of service providers of various kinds (such as organisations like Checkfree, Cybernet & Authorize.net
) that might or might not be regarded as intermediaries, depending on the circumstances. For purposes of this book, however, we focus on the dominant intermediaries like Visa, MasterCard, and PayPal.

[8].Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

[9] Large-scale purchases of under two US dollars remain infeasible even now. The fees on such an exchange can come to $0.30 or 15% of the transaction. Individual transactions in the order of USD $0.001 to $0.05 are not even considered. Using bitcoin, it should be possible for providers of services to take initial deposits of under a single cent and to provide

updates to pages or other resources for as little as one thousand of a cent or less. The individual accessing the page or service would at best be risking only a single cent and would not need to accept or provide any personal information. Where necessary, keys and identity could be linked in a limited manner allowing the provider of the service to send goods to an address without needing to know all the habits of the user.

[10] Mann, R. & Belzley, S (2005) “The Promise of the Internet Intermediary Liability” 47 William and Mary Law Review 1 <
http://ssrn.com/abstract=696601
> at 27 July 2007]

[11] The distributed nature of the Internet means that a publisher can reach far more people. A company with a web site in the UK for instance has direct access to the US, Canada, Australia and many other countries with the primary limitations being language.

[12] It has been argued that the digital contract may appear on the computer screen to consist of words in a written form but merely consist of a virtual representation . The Electronic Communications Act 2000 [ECA] has removed the uncertainty and doubt surrounding the question as to the nature of electronic form used in the construction of a contract. In this, the ECA specifies that the electronic form of a contract is to be accepted as equivalent to a contract in writing

[13] Such as with regards to taking action on notice of hosting child pornography.

[14] It has been argued that the digital contract may appear on the computer screen to consist of words in a written form but merely consist of a virtual representation. The Electronic Communications Act 2000 [ECA] has removed the uncertainty and doubt surrounding the question as to the nature of electronic form used in the construction of a contract. In this, the ECA specifies that the electronic form of a contract is to be accepted as equivalent to a contract in writing.

[15].See, Shapiro, Andrew L., Digital Middlemen and the Architecture of Electronic Commerce, 24 Ohio N.U. L. Rev. 795 (1998).

[16]Ebay.com states its purpose to be “the world's online marketplace; a place for buyers and sellers to come together and trade almost anything!” (for a detailed description, see http://pages.ebay.com/help/newtoebay/questions/about-ebay.html).

[17] PayPal is an online financial transaction broker; PayPal lets people send money to each other's e-mail addresses. At no time will either party see the other's credit card or bank information. Currently, 95% of eBay's purchases go through PayPal. Like an escrow service, PayPal acts as the middleman holder of money. Through its policies, practices, and business integrity, PayPal has earned the trust of both parties. See
https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/bizui/WhatIsPayPal-outside

[18] Anderson et al. in their Dec 1997 presentation “Exploring Digital Cash” argued that digital cash would “likely continue to evolve remarkably quickly”.

[19] In 2002, roughly ninety percent of internet transactions used credit cards. Ronald J. Mann, Regulating Internet Payment Intermediaries, 82 Texas L. Rev. 681, 681 (2004).

[20] In this context, P2P stands for “person-to-person.” The term is to be distinguished from the more common use of the same acronym to describe the peer-to-peer file sharing discussed in the context of piracy.

[21] See Mann, at 683.

[22] Id.

[23] Because of the fluidity of payment mechanisms on the internet, there are a wide variety of service providers of various kinds (such as organisations like Checkfree, Cybernet & Authorize.net) that might or might not be regarded as intermediaries, depending on the circumstances. For purposes of this Essay, however, we focus on the dominant intermediaries like Visa, MasterCard, and PayPal.