Designing Money [Extended Abstract]

Leonard Adleman
University of Southern California
adleman@usc.edu

Rolfe R. Schmidt
rolfe@alumni.princeton.edu

1 Abstract

Money has existed in various forms for thousands of years. The ancient Lydians used coins of gold-alloy; the ancient Chinese, notes of paper. Today, the most important form of money is bank money (BM) issued by governments and stored in databases.

It is the transfer of BM, through the use of payment cards (e.g. debit cards, credit cards, gift cards), that underlies the bulk of Internet commerce. Recently, cryptographically based forms of money, such as Bitcoin, have arisen as an alternative to BM. Bitcoin, has made it clear that digital money can be designed to meet specific needs, and that the tools of computer science can endow money with remarkable properties.

We will argue that existing payment card systems are slow, costly, and a threat to privacy, and that Bitcoin does not meet the needs of governments. We will present a new form of money, Aurum, designed from first principles to be issued by governments and other trusted institutions.

Aurum is based on a simple but novel technological primitive we call "automatic replacement". With automatic replacement, each transaction results in the permanent destruction of the buyer's note, and the virtually instantaneous creation and delivery of a new note for the seller. We will argue that the use of automatic replacement can yield greater privacy that either Bitcoin or payment card systems.

We have implemented Aurum in prototype and simulated transactions at a rate of over 7000 per second (approximately the average transaction rate for the entire US economy). As reported below, each transaction was completed in milliseconds at a cost of less than one-thousandth of a cent.

We will describe how such a low cost high-speed form of digital money can lead to a new wave of innovation and be the basis for future economic growth.

2 The Origin of Government Money

In the West, the first government money appears to have been a Lydian coin issued in about 650 BC that bore the stamped likeness of a lion with sunburst, the symbol of the king [25]. The imprimatur of the state allowed Lydian coins, and the government money that followed, to supplant earlier forms. The success of government money in general, and the Lydian coin in particular, was based on trust; trust born from power. People could trust Lydian coins because the state had the power to guarantee their weight and metal content, to ensure that they were accepted throughout the realm, and to execute counterfeiters.

No sooner did government issued coins exist than states, such as Athens, began to manipulate them for social purposes [14]. Monetary policy had arrived. Governments have never relinquished their prerogative to use their money for what they deem to be good purposes, and it seems likely that they will resist innovations that might deprive them of that prerogative.

3 United States Physical Currency

In 1789, Article 1, Section 8 of the United States Constitution granted Congress the power to "coin money", thereby giving birth to the United States Dollar (USD). At that time, USD took the form of metal coins, but today it includes paper notes and BM. All forms of USD are governmentally regulated and issued by the Federal Reserve.

We still have notes and coins, which together we will refer to as United States Physical Currency (USPC). USPC has persisted because it has many desirable properties. It also has at least one undesirable property - mass; it cannot travel at the speed of light and cannot be used for digital commerce. This leads us to consider the problem of designing a form of government money that retains the desirable properties of USPC, but is digital. Let's review some of these properties:

- Privacy: Most often, when we spend USPC, we do not give our names or other private information. However, this privacy is not absolute. For example, the Government requires that businesses report the identity of individuals spending USD in any form in amounts of ten-thousand dollars or more.

  In general, the privacy conferred by a form of money is intimately related to the nature of the information, what we call the footprint, left by transactions. Often, when small amounts of USPC are used for common purchases, virtually no footprint is left. However, under other circumstances the footprint may be substantial. For example, when USPC is used in banks, the footprint may include hard-copy, digital and even video records that persist for a great deal of time. These records may contain information such as times, amounts, names, addresses, account numbers and even social security numbers.

- Security: Security has many aspects, but some of the most important are:
  - Resistant to counterfeiting. The Government combats counterfeiting by integrating physical features, such as water marks and 3D ribbons, into its notes, so that widely available methods of duplication and printing will produce copies of insufficient quality to be passed. The current approach is good, but not perfect. For example, it has been widely rumored that North Korea possesses presses on which it produces counterfeit one-hundred-dollar bills that defy detection [20].
  - Resistant to double spending. For USPC, controlling counterfeiting is sufficient to control double spending. We trust that once an individual spends a note, they no longer possess a passable copy, and cannot spend it again.
  - USPC is not secure against misplacement or theft. Once an individual loses possession of a note, no one, not even the Government, will replace it. This lack of security arises from our use of coins and notes as negotiable bearer instruments. If you possess it, you may spend it.

- Universality: USPC has many properties that facilitate its wide spread use. Among them:
  - Using USPC does not require special status: For example, the unbanked and underbanked, who may lack sufficient status to have a relationship with a financial institution, can use USPC.
  - Using USPC does not require special skills: The vast majority of individuals, including the illiterate, innumerate, and atechnical can use USPC.
  - Using USPC does not require special technology: notes and coins may be used in environments with minimal infrastructure; there is no need for computers or even pens.
  - Using USPC does not require significant time: For example, settlement is instantaneous. When a dollar bill is spent, the recipient immediately receives a dollar bill and may immediately spend it.
  - Using USPC does not require substantial expense: Neither buyer nor seller pays a processing fee when using a dollar bill. However, in considering expense, one should include the cost of maintaining the system. When existing notes become unfit, they are collected, destroyed, and replaced by new ones. In 2016 the Federal Reserve spent $660 Million to print new bills worth $216.5 Billion [18]. These notes are reused. From this, it seems reasonable to estimate the mean cost per transaction as less than 0.1% of transaction value.
  - Widely accepted: Because the US Government demands it, USPC may be used at many places to buy many types of goods and services, to satisfy debt, and to pay taxes.
  - Small denominations: A penny can be used to transfer what is viewed by many as a trivial amount of wealth. As a result, goods and services of small value can be bought and sold, and those of larger value may be priced with high precision.

- Governability: The Government regulates the USD to enact monetary policy. Government action, such as quantitative easing, changes the value of our USD. The Government also regulates USD in an effort to prevent financial crimes. For example, the Bank Secrecy Act requires that financial institutions report all USD transactions of ten-thousand dollars or more, and all "suspicious activity".

The Government has determined that it is worthwhile to sacrifice some privacy for the law enforcement and national security benefits of deterring money laundering in the service of crime or terrorism.

The hard learned lessons of the past have led to the laws and regulations that today govern the economic affairs of financial institutions, companies, and individuals. Whether you approve or not, we have left important decisions about our money and our economy to the political process.

4 Payment Cards

Banks store BM using database management technology. Transferring BM between account holders typically requires a distributed transaction involving the databases of multiple banks and third parties. Ultimately, the payer's account balance is reduced, the payee's account balance is increased, and the balances of the banks' accounts at central banks or clearing houses are adjusted to offset the change in liabilities. Institutions use various electronic funds transfer systems to transfer BM, but individuals typically use payment cards.

Today, the transfer of BM via payment cards is the primary means by which individuals make purchases over the Internet. Payment card systems have the following properties:

- Privacy: Card payments leave a large footprint. The card itself has your full name, physical signature, card number, expiration date, and card security code. The magstripe has similar information. When you use a card, the information is commonly stored together with a date and time of use, location of use, and a list of items purchased. All or part of this information is typically retained in the databases of merchants, banks and various third parties involved in the BM transfer. This footprint can lead to dramatic privacy breaches such as the one that occurred at Ashley Madison in 2015 [6]. There can be little doubt that concerns about privacy breaches diminish the customer base of sensitive sites, but they can also have a chilling effect on basic freedoms, for example, by inhibiting the purchase of books on controversial political topics.

- Security: The information on the card or the magstripe is sufficient for a criminal to use your card for purchases. The few technical barriers to criminal use seem meager. For example, when a signature is required, it can be forged, and the realities of the marketplace seldom allow for close scrutiny and detection. At some locations, such as gas stations and Internet sites, no signature is required. In 2013, the cost of fraudulent payment card use in the United States was 7.1 billion dollars[29].

  The payment industry has done an effective job of concealing this cost from purchasers by indemnifying them. This indemnification protects purchasers, but is paid for by merchants in the form of transaction fees, and ultimately manifests itself in the form of higher prices for consumers.

  The payment card industry has made significant efforts to improve both privacy and security, as is seen in the EMV standards [15]. These changes, however, are no panacea and significant challenges remain [5].

  Payment card footprints put merchants in the unenviable position of having to protect personal information that in many cases they don't need and would prefer not to have. Predictably, attempts by merchants to protect this information often fail. The direct costs and damage to merchant reputations can be substantial as the recent incidents at Target and Home Depot demonstrate [31].

  Because today's banking systems have grown organically, the resulting architecture is complex. This has created vulnerabilities even at the highest levels, as demonstrated by the recent theft of $81 million of Bangladesh Bank funds directly from their account at the Federal Reserve Bank of New York [8].

- Universality: Payment cards enjoy some of the universal properties of USPC. They require little in the way of special skills, are widely accepted, and can transfer small amounts. However:

  - Using payment cards does require special status: acquisition of bank accounts and payment cards requires economic status. This status barrier prevents the unbanked and underbanked from participating fully in today's economy and leads to significant social problems.

  - Using payment cards does require special technology: Online purchasers only require basic computing, but merchants may require special devices and communications technology.

  - Using payment cards does require significant time: Though this is not apparent to the purchaser, it is to the merchant. When you use your card, the merchant's account will be augmented, but the process can take days. During this settlement time the merchant cannot use the money that has been promised.
  - Using payment cards does require significant expense: In the case of credit cards, merchants pay interchange fees of close to 2% of the transaction [13]. Analogous fees for debit cards are approximately 0.79%[1]. Additional markups, sometimes significantly higher, are charged by acquiring banks. Merchants may need to purchase or lease special equipment.

    Consumers also pay. With credit cards, they can spend money they do not possess. If the debt they acquire is not paid promptly, it can lead to fees, penalties, and interest charges. Frequently, credit card debt is not paid promptly, and, in many cases, the burden becomes sufficiently great that bankruptcy results. The total credit card debt in the United States is over 700 billion dollars [26].

- Governability: Payment card transfer BM which is highly governable. For example, the Federal Reserve System was set up in 1913, in large part to facilitate United States monetary policy. Central banks have developed numerous tools for controlling the supply and flow of BM. BM is also governable for law enforcement purposes. For example, the Bank Secrecy Act rule [31 CFR 103.33(g)] – the "travel rule" – requires that US financial institutions pass identifying information with certain fund transmittals of three-thousand dollars or more. Because of the complex architecture of today's banking systems, such governance sometimes creates significant burdens for financial institutions, and the fragmented information that results can be difficult for law enforcement to obtain and analyze.

5 Bitcoin

The use of cryptography in the design of money began in 1985 with a prescient paper by Chaum[11]. Chaum described the tension between organizational and individual security and proposes systems to deal with the resulting problems. Among the proposals is a system for electronic cash which maintains a list of spent notes to prevent double spending. A similar approach is used in Aurum. See also [12, 10, 24].

Bitcoin was introduced in 2008 [23]. Among its most important properties are:

- Privacy: Paradoxically, though it appears that the designer(s) of Bitcoin placed a high value on privacy, it was not achieved. Bitcoin is not inherently private. On the contrary, it is quite transparent. The footprints of Bitcoin transactions are stored in the blockchain, which is large, permanent, and open for all to read. This has been used to glean significant information about Bitcoin users, as seen in [21, 22, 27, 9].

- Security: The system is designed to prevent double spending using a proof-of-work scheme. It was initially claimed that to compromise the system an attacker would need to hold 50% of the computing power of the bitcoin network [23]. It has since been shown that as little as 25% will suffice [17], and there is no proof that an even smaller percentage might not be sufficient. An examination of the miners at the instance of this writing shows that two colluding miners can execute a 25% attack and three colluding miners can execute a 50% attack. Perhaps this should be a concern. In any event, the security of Bitcoin is an open question.

- Universality: Bitcoin enjoys some of the universal properties of USPC. For the common user, it does not require special technology beyond basic computing, and it can be used to transfer small amounts. It does not require special status; it can be used by people without a relationship with a financial institution. In addition, Bitcoin can cross international borders easily and be used by virtually all people.

  - Few special skills are required: Bitcoin software is improving and lightweight applications make it easy for people to transact on the Bitcoin network. Those users operating full nodes need greater technical skills. Those acting as miners must be expert.
  - Using Bitcoin does require significant time: In practice many users accept "zero confirmation" bitcoin transactions which give an impression of real-time settlement. This practice leaves payees vulnerable to loss through double spending. Certainty of

  payment comes with inclusion in the blockchain. This takes about 10 minutes to get a one-block confirmation, and one hour for the recommended six-block confirmation.

  - Using Bitcoin does require substantial expense: Bitcoin users pay direct transaction fees and they pay for mining rewards through inflation. The site [2] monitors this cost in real time. Recently this cost has ranged between one and two percent of total transaction value. This is more expensive than debit cards and comparable to credit cards. In the future, when mining rewards are removed, the expenses incurred by miners will not disappear, and will have to be covered by transaction fees alone.
  - Bitcoin is not widely accepted: While bitcoin's acceptance has grown through time, it is currently accepted by few retailers. If Bitcoin obtains the imprimatur of a state this could change.

- Governability: Bitcoin was designed to prevent governability. It might be governable by the so called "core developers", but such governance would neither be democratic, nor wielded by an agent with a history of trustworthiness. In addition, any governance, whether by a state or not, appears to be antithetical to the underlying principles of many Bitcoin users. This lack of governance is likely to make governments reluctant to adopt Bitcoin and, in fact, resistant to it.

  Lack of governability not only makes it difficult for authorities to regulate the system, it also causes problems for Bitcoin itself, as seen in the recent block size debate[3]. Other blockchain based crypto-currencies such as Ethereum have been forced to improvise governance to overcome unanticipated crises [16].

6 Aurum

Our goal in designing Aurum was to produce a digital form of money that preserved the desirable properties of USPC. The resulting system had to be fast, inexpensive, and secure, while preserving privacy and enabling governability. We wanted the system to be composed from simple easily understood primitives so that its properties could be clearly seen and considered.

All forms of money must have a means of curtailing counterfeiting, but for digital forms of money, this problem is exacerbated because digital documents can be easily and perfectly copied.

To meet the counterfeiting challenge, Aurum uses *automatic replacement. Automatic replacement* is similar to the Federal Reserve process of removing physically unfit notes and replacing them with fresh ones from the Bureau of Engraving and Printing; however, *automatic replacement* takes advantage of modern technology and replaces Aurum notes on each transaction. When an Aurum note passes from a sender to a recipient, the sender's note is destroyed, and a new note is created for the recipient, who may immediately spend it.

In a typical implementation of the Aurum system we have:

- The Issuer: The agent responsible for governing the Aurum system. In particular, the Issuer may order the creation and distribution of notes. The issuer may be a government, but can be any institution. For example, private companies or commercial banks, can act as Issuers to create their own versions of Aurum. The acceptability of issued notes will depend on the power and trustworthiness of the Issuer.

  In what follows it will be convenient to use the US Government as an example. In that case, the natural choice for Issuer would be the Federal Reserve, and Aurum would be intended to be a new form of USD.

- The Authority: An Internet agent responsible for creating notes, destroying notes and overseeing the passage of notes between users. While the Authority must be controlled by the Issuer, it may be hosted by a third party. The Authority maintains:

  - A *destroyed list.* The destroyed list is used to prevent double spending.
  - A public-key, P_A, and a corresponding secret key, S_A, of the RSA public-key cryptosystem, or some other suitable system. P_A and S_A are used to prevent the illegal creation of passable notes (what we call *de novo* counterfeiting).

  In the prototype implementation described here, the Authority will also maintain:

  - A one-way hash function, H.
  - A note database, D.

All but S_A are, at all times, publicly accessible via the Internet.

- Note-content: A plain text digital document with a well defined syntax that contains a value in USD and a unique identifier such as a serial number. The note-content may contain other information, such as the date of issuance, but we will not explore this further here. Roughly speaking, a note-content is similar to a traditional check that has been filled out but not signed. A note-content has no value.
- Note: The result of applying S_A to a note-content; that is, a note is a note-content signed with the digital signature of the Authority. A note has the value in USD contained in its note-content.

A typical transaction would occur as follows:

1. An online shopper informs a web-based merchant that he would like to pay with Aurum.
2. The merchant generates a public key, P_M, and corresponding secret key, S_M (possibly chosen at random by the merchant for this transaction). The merchant sends the shopper an invoice which contains the amount owed in USD and P_M.
3. The shopper, using a digital wallet application, accepts or declines the invoice. In the case of acceptance, the shopper generates a public key, P_S, and corresponding secret key, S_S (possibly chosen at random by the shopper for this transaction). The shopper selects a set of notes of sufficient value. The shopper combines the selected notes, P_M, P_S, and the amount in USD owed the merchant into a single *automatic replacement* request and sends it to the Authority via a secure Internet channel.
4. The Authority executes an *automatic replacement*:
    - Authenticates the notes and their values by applying P_A and reading the resulting note-contents.
    - Confirms that the notes are not on the *destroyed list*.
    - Places the notes on the *destroyed list* (ensuring that they can never be respent).
    - Creates new notes, N_M for the merchant, and N_S for the shopper's change.
    - Encrypts N_M using P_M producing E_M, applies H to P_M producing A_M, places E_M at address A_M in D.
    - Encrypts N_S using P_S producing E_S, applies H to P_S producing A_S, places E_S at address A_S in D.
5. The merchant applies H to P_M producing A_M, and retrieves E_M from address A_M in D. The merchant decrypts E_M using S_M to obtain N_M.
6. The shopper applies H to P_S producing A_S, and retrieves E_S from address A_S in D. The merchant decrypts E_S using S_S to obtain N_S.

There are numerous variations on how to implement *automatic replacement*, but its effectiveness in stopping double spending requires that all parties share a consistent view of the *destroyed list*. This is accomplished by using well-known database techniques to assure that all *automatic replacements* are ACID (Atomic, Consistent, Isolated, Durable) [19]. In addition, our use of public keys, P_M and P_S, hash function H, and the database D is merely one possible way of providing a secure message delivery service.

6.1 Prototype

The performance demands of the Aurum system will be substantial. Combining data from [32, 7], the number of global payment transactions (cash transactions plus non-cash transactions) does not exceed 2.17 trillion per year or 68.8 thousand per second. In the United States the number of payment transactions does not exceed 247 billion per year, or 7,830 per second. To test the Aurum system's ability to meet these demands, we have built a prototype and deployed it on Amazon Web Services (AWS).

The prototype consists of three core programs: an *automatic replacement coordinator*, a *note destroyer*, and a *note creator*. These programs are written in C++ and rely on the CryptoPP library for all cryptographic operations. They implement an Aurum system using the 2048-bit RSA public-key cryptosystem. The prototype also includes a non-core program: a test client used to measure performance.

The *automatic replacement coordinator* is a stateless server that accepts *automatic replacement* requests from external clients over the Internet. When a request is received, it validates that the input notes are authentic and sufficient to cover the requested output notes. If this validation is successful, the *automatic replacement coordinator* orchestrates a distributed transaction over a private network using a modified two phase commit protocol (2PC) to ensure that *automatic replacements* are ACID. This transaction involves one or more *note destroyers* and one or more *note creators*.

The *note destroyer* maintains the *destroyed list* as a set of memory mapped files. There is one bit for each serial number, and all bits are initially set to zero. When a note is destroyed, the bit corresponding to its serial number is set to one. The *automatic replacement coordinator* cannot modify the *destroyed list* by direct action, and may only modify it though issuing *destroy* requests to the *note destroyer*. The *note destroyer* will cause an *automatic replacement* to fail if it attempts to destroy a note that has already been destroyed by either a pending or committed transaction.

The *note creator* creates new Aurum notes. It is the only program with access to the Authority's secret key, S_A. When called by the *automatic replacement coordinator* with a *create* request containing a list of note-contents, the *note creator* will create the corresponding notes. The *note creator* will cause an *automatic replacement* to fail if notes cannot be created for any reason.

We have also implemented a note database using a shared file system. This is not a core part of the Aurum system, it simply acts as a secure message delivery service. In practice we expect other messaging systems to be used as well.

When eight AWS `c4-4xlarge` instances and one AWS `t2-small` instance were used for one hour, the prototype processed 7,768 transactions per second, approximately the transaction rate of the United States. Amazon charged $6.82.

- The cost per transaction was approximately one forty-thousandth of a cent.
- The mean latency from a client's issuance of an *automatic replacement* request to its completion by the Authority was 16 ms. This should have a negligible impact on user experience.
- The energy use was negligible.

Further tests revealed that Aurum is readily scalable. The charge for running the prototype grew linearly with the transaction rate, while the cost per transaction and latency did not change.

In separate experiments we have successfully implemented a transaction signature scheme similar to those associated with EMV and standard Bitcoin transactions. It would be straight forward to implement a smart contract language scheme which would provide smart contracts without the need for blockchains. We have also built and tested a prototype user app for Android smart phones.

For those who wish to explore the Aurum system for research purposes, we plan to make prototype software available. For further details see `adleman.usc.edu`.

In a production system, special purpose hardware should bring down costs and improve speeds. On the other hand, there will be costs associated with maintaining an important organization. To estimate these costs, we used Verisign, a publicly traded company with transaction processing needs similar to those that would be faced by Aurum, as a model. During the third quarter of 2015, Verisign's average daily Domain Name System query load was approximately 120 billion queries per day. During the same quarter, Verisign's total costs and expenses were $111,318,000[30]. Using this model, we estimate that the cost per transaction of a production Aurum system would be approximately one one-thousandth of a cent; orders of magnitude less than Bitcoin and payment cards.

A production Aurum system must survive in the Internet ecosystem. It will be the target of many attacks. It must use the tools that have been developed in academe and industry over the last several decades to resist them. A production system should be geographically distributed and Byzantine fault tolerant. Centralized governance does not mean centralized processing. The destroyed list should be widely distributed and public. Important private keys should be stored in secure locations and secret sharing techniques should be used to distribute them geographically and protect them from compromise [28].

6.2 Aurum Properties

- Privacy: No private information, such as names or account numbers, ever needs to be passed between sender and recipient, sender and Authority, or recipient and Authority. When the Aurum system is implemented as above, the footprint of a transaction consists of one bit in the *destroyed list*. The Aurum system can make failures like those that occurred at Ashley Madison, Target, and Home Depot a thing of the past.
- Security:
    - Resistant to counterfeiting: Under standard cryptographic assumptions, Aurum is secure against *de novo* counterfeiting. The presumed North Korean *de novo* counterfeiting of USPC should have no analogue for Aurum notes.

  - Resistant to double spending: Automatic replacement protects Aurum from double spending and counterfeiting by the duplication of existing notes (what we call duplication counterfeiting).
  - Like USPC, Aurum notes are negotiable bearer instruments and are not secure against misplacement or theft. No one will replace them. However, Aurum notes appear to have an advantage over USPC. At the option of the user, Aurum notes may be securely backed up, and if an original is misplaced, the back-up may be spent. Hence loss due to misplacement may be mitigated. Commercial banks might offer "online safe deposit boxes" that provide such backup as a service to Aurum users. Similarly, at the user's discretion, loss due to theft may be mitigated with the use of a transaction signature scheme.

- Universality:
  - Using Aurum notes does not require special status: Aurum notes will be usable by the unbanked and underbanked. No accounts or memberships are needed.
  - Few special skills are required: Simple apps make Aurum notes easy for both buyers and sellers to use. Those operating an Authority must be expert.
  - Using Aurum notes does not require special technology: A standard mobile device or personal computer is sufficient for both buyers and sellers.
  - Using Aurum notes does not require significant time: Settlement is immediate. Latency is measured in milliseconds.
  - Using Aurum notes does not require substantial expense: As indicated above, the cost of a transaction should not exceed one one-thousandth of a cent. Financial institutions that offer services such as indemnification or secure storage may charge additional fees. Private institutions that issue Aurum notes might also charge for their use.
  - The acceptance of Aurum notes will depend greatly on the trustworthiness and power of the Issuer.
  - Aurum notes can be denominated in arbitrarily small fractions of a cent.

- Governability: The Aurum system is designed to be governable. With regard to monetary policy, in the United States, the current system of executing policy through the Federal Reserve System is not inhibited by the Aurum system. In addition, the Government can modify monetary policy directly through the Authority. For example, by creating Aurum notes at its discretion.

  With regard to financial crimes, the Aurum system may offer some advantages. For example, the Bank Secrecy Act rule requiring that financial institutions report all USD transactions of ten-thousand dollars or more, can be implemented by requiring such institutions to send personal information consistent with their customer identification program (CIP) to the Authority with each such *automatic replacement* request. The Government requirement that trades and businesses file IRS Form 8300 for certain transactions can be implemented in a similar fashion. Thus the "on boarding" and "off boarding" of Aurum notes into and out of conventional institutions can be controlled as it is today. Because all associated information can be retained in the Authority, when due process provides access for law enforcement, the information may be readily obtained in a standard digital form suitable for analysis.

  So while the basic Aurum system is inherently private and produces extremely small footprints, it is flexible enough to increase those footprints and retain additional information when the political process dictates that it is in the best interest of a country to do so.

7 A World with Aurum

The Aurum system would lead to a more efficient economy and engender important economic innovations.

For example, the insignificant cost of Aurum transactions makes micropayments a reality. Even a transaction for one cent is practical. Anyone who produces digital content can now directly monetize it. There is no need to sell advertising, to force potential consumers to register, to fill out forms, remember passwords, pay subscription bills, endure advertising popups, or provide personal information.

It is reported [4] that the digital New York Times has "60 million unique visitors (U.S.) a month. One million of them pay [via digital subscription]; 59 million don't.". The digital subscribers provide about two-hundred million dollars in annual revenue (approximately one-eighth of the total revenues of the Times). But, if we assume that, on average, each of the 59 million non-subscribing visitors reads one article per day, and that each is willing to pay one cent per article via a non-intrusive one-click, then these visitors would add an additional two-hundred-fifteen million dollars to the annual revenue.

Inexpensive Aurum micro-payments will provide creative individuals the opportunity to enrich the world with their ideas. Budding novelists, musicians, graphic artists, bloggers, videographers, and a host of others may directly enter the market and sell their work for whatever the market will bear.

Banks and other financial institutions will have a new basis on which to create novel instruments or improve existing ones. For example, users may go to their bank website and download Aurum notes; eliminating the need for a trip to an ATM.

With Aurum notes, these innovations can be brought to fruition while retaining security, privacy, and governability.

8 Conclusion

We have proposed a simple new form of digital money, Aurum, that provides fast, inexpensive transactions, while preserving privacy and governability. Bitcoin has made it clear that the public is ready to consider new cryptography based forms of money. It seems likely that money in such forms issued by a trusted agent could gain wide acceptance. It may be the case that existing methods of digital payment, such as payment card systems, which have grown organically and been slow to take advantage of emerging technology, will find it difficult to compete.

The money considered in this paper can be thought of as objects in what we call an ownership system. At its most basic, an ownership system consists of a set of objects and a set of owners. At each moment, the ownership system records which owners own which objects. When the ownership of an object changes, the system must be updated accordingly.

USPC are objects which individuals may own. The USPC ownership system is highly distributed with each object owned by the individual who possesses it. There are ownership systems where money is no object. For example, automobiles are objects which individuals own and for which the ownership system is implemented by state governments in a highly centralized fashion. Stocks, bonds, and medical records provide other examples. Many existing ownership systems have arisen in an unsystematic manner and have acquired undesirable features. It does not have to be that way; as with money, the tools of computer science allow us to design ownership systems that meet prespecified requirements.

8.1 Acknowledgements

We thank Professor Bill Maurer, Professor Donald J. Patterson, Taylor Nelms, and Caitie Lustig of UC Irvine, and Jim Bidzos and Burt Kaliski of Verisign for their careful review of an earlier version of this paper and their suggestions which led to substantial improvements.

8.2 Disclosure

Leonard Adleman is a principle in the company Aurum. Patent pending.

References

[1] URL: https://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm.

[2] URL: https://blockchain.info/charts/cost-per-transaction-percent.

[3] URL: https://en.bitcoin.it/wiki/Block_size_limit_controversy.

[4] URL: http://www.niemanlab.org/2015/08/newsonomics-10-numbers-on-the-new-york-times-1-million-digital-subscriber-milestone/.

[5] Ross Anderson and Steven J. Murdoch. "EMV: Why Payment Systems Fail". In: *Commun. ACM* 57.6 (June 2014), pp. 24–28. ISSN: 0001-0782. DOI: 10.1145/2602321. URL: http://doi.acm.org/10.1145/2602321.

[6] *Ashley Madison hack is not only real, it is worse than we thought.* 2015. URL: http://arstechnica.com/security/2015/08/ashley-madison-hack-is-not-only-real-its-worse-than-we-thought/.

[7] John Bagnall et al. *Consumer cash usage: A cross-country comparison with payment diary survey data.* Discussion Papers 13/2014. Deutsche Bundesbank, Research Centre, 2014. URL: http://www.bostonfed.org/economic/wp/wp2014/wp1404.pdf.

[8] *Bangladesh Bank hackers compromised SWIFT software, warning issued.* URL: http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR.

[9] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. "Deanonymisation of Clients in Bitcoin P2P Network". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.* CCS '14. Scottsdale, Arizona, USA: ACM, 2014, pp. 15–29. ISBN: 978-1-4503-2957-6. DOI: 10.1145/2660267.2660379. URL: http://doi.acm.org/10.1145/2660267.2660379.

[10] David Chaum. "Online Cash Checks". In: *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology.* EUROCRYPT '89. Houthalen, Belgium: Springer-Verlag New York, Inc., 1990, pp. 288–293. ISBN: 3-540-53433-4. URL: http://dl.acm.org/citation.cfm?id=111563.111592.

[11] David Chaum. "Security Without Identification: Transaction Systems to Make Big Brother Obsolete". In: *Commun. ACM* 28.10 (Oct. 1985), pp. 1030–1044. ISSN: 0001-0782. DOI: 10.1145/4372.4373. URL: http://doi.acm.org/10.1145/4372.4373.

[12] David Chaum, Amos Fiat, and Moni Naor. "Untraceable Electronic Cash". In: *Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology.* CRYPTO '88. London, UK, UK: Springer-Verlag, 1990, pp. 319–327. ISBN: 3-540-97196-3. URL: http://dl.acm.org/citation.cfm?id=646753.704915.

[13] Payments System Research Department. *Credit and Debit Card Interchange Fees Assessed to Merchants in the United States August 2015 Update.* Tech. rep. Federal Reserve Bank of Kansas City, 2015. URL: https://www.kansascityfed.org/~/media/files/publicat/psr/dataset/us_if_august2015.pdf.

[14] John Dryden. *Plutarch's Lives of Illustrious Men.* Ed. by Hugh Clough. The John C. Winston Co., 1908, p. 167.

[15] *EMVCo Specifications.* URL: https://www.emvco.com/specifications.aspx.

[16] *Ethereum Hard Fork No. 4 Has Arrived as DOS Attacks Intensify.* URL: https://cointelegraph.com/news/ethereum-hard-fork-no-4-has-arrived-as-dos-attacks-intensify.

[17] Ittay Eyal and Emin Gün Sirer. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable". In: *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers.* Ed. by Nicolas Christin and Reihaneh Safavi-Naini. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 436–454. ISBN: 978-3-662-45472-5. DOI: 10.1007/978-3-662-45472-5_28. URL: http://dx.doi.org/10.1007/978-3-662-45472-5_28.

[18] *Federal Reserve System coin and Currency Data.* URL: https://www.federalreserve.gov/paymentsystems/coin_data.htm.

[19] Jim Gray. "The Transaction Concept: Virtues and Limitations (Invited Paper)". In: *Proceedings of the Seventh International Conference on Very Large Data Bases - Volume 7.* VLDB '81. Cannes, France: VLDB Endowment, 1981, pp. 144–154. URL: http://dl.acm.org/citation.cfm?id=1286831.1286846.

[20] *How the U.S. Could Pressure North Korea Tomorrow: Quit the $100 Bill.* URL: http://business.time.com/2012/02/24/how-the-u-s-could-pressure-north-korea-tomorrow-quit-the-100-bill/.

[21] Sarah Meiklejohn et al. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names". In: *Commun. ACM* 59.4 (Mar. 2016), pp. 86–93. ISSN: 0001-0782. DOI: 10.1145/2896384. URL: http://doi.acm.org/10.1145/2896384.

[22] M. Möser, R. Böhme, and D. Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem". In: *eCrime Researchers Summit (eCRS), 2013.* 2013, pp. 1–14. DOI: 10.1109/eCRS.2013.6805780.

[23] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". In: *Consulted* 1 (2008), p. 2012.

[24] Tatsuaki Okamoto and Kazuo Ohta. "Universal Electronic Cash". In: *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology.* CRYPTO '91. London, UK, UK: Springer-Verlag, 1992, pp. 324–337. ISBN: 3-540-55188-3. URL: http://dl.acm.org/citation.cfm?id=646756.705374.

[25] Andrew Ramage and P. T. Craddock. Archaeological Exploration of Sardis, Harvard University Art Museums, in association with the British Museum Press, 2000, pp. 17–18.

[26] Research and Statistics Group Microeconomic Studies. *Quarterly Report on Household Debt and Credit*. Tech. rep. Federal Reserve Bank of New York, 2016. URL: https://www.newyorkfed.org/medialibrary/interactives/householdcredit/data/pdf/HHDC_2016Q1.pdf.

[27] Dorit Ron and Adi Shamir. "How Did Dread Pirate Roberts Acquire and Protect his Bitcoin Wealth?" In: *Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers*. Ed. by Rainer Böhme et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 3–15. ISBN: 978-3-662-44774-1. DOI: 10.1007/978-3-662-44774-1_1. URL: http://dx.doi.org/10.1007/978-3-662-44774-1_1.

[28] Adi Shamir. "How to share a secret". In: *Communications of the ACM* 22.11 (1979), pp. 612–613.

[29] *The US Sees More Money Lost To Credit Card Fraud Than The Rest Of The World Combined*. 2014. URL: http://www.businessinsider.com/the-us-accounts-for-over-half-of-global-payment-card-fraud-sai-2014-3.

[30] *Verisign, Inc Quarterly Report Q3 2015*. 2015. URL: http://files.shareholder.com/downloads/VRSN/1869027888x0xS1014473-15-73/1014473/filing.pdf.

[31] N Eric Weiss and Rena S Miller. "The Target and Other Financial Data Breaches: Frequently Asked Questions". In: *Congressional Research Service, Prepared for Members and Committees of Congress February*. Vol. 4. 2015, p. 2015.

[32] *World Payments Report 2015*. 2016. URL: https://www.worldpaymentsreport.com/reports/noncash.