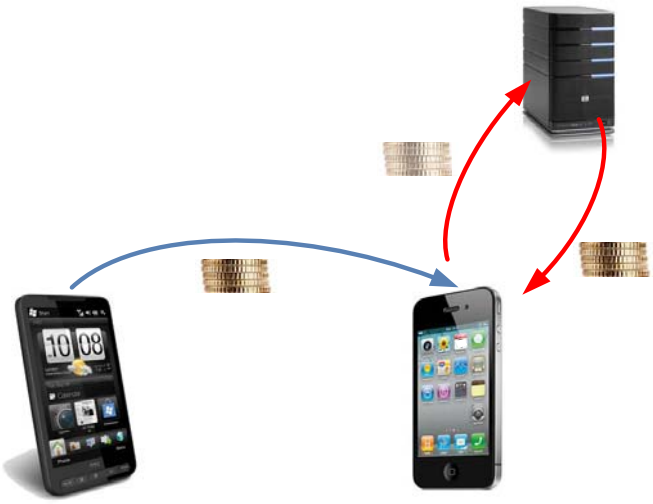
Finding the ultimate digital money



Comments & questions
Helmut Scherzer

Giesecke & Devrient
Prinzregentenstr. 159
D-81677 Munich

Fon.: +49 89 4119 2084
Mob: +49 174 313 9891
Fax: +49 89 4119 1905
helmut.scherzer@gi-de.com
www.gi-de.com

Chip-to-Cloud Security Forum
Smart Trusted Technologies & Services for the Networked Society
September 25-27, 2013 – Nice, French Riviera

Table of contents

1 The definition of digital money

Money from the first day it was invented around 2500 years ago – had always been a ’touchable thing’ which represented a value. The early natives, when they discovered the idea of money as an abstraction of a value, had no idea of such a thing as a "bank account" – yet the idea of money and "coins" is about as old as money is.

From the early trade of goods exchange (e.g. a chicken for a cluster of wood) humanity discovered the brilliance of a ’represented value’ through shells, gem stones, pearls, silver, gold and whatever could represent a value.

One of the major qualities of money has always been the idea of a scarce resource or something difficult to obtain or produce. This quality – called ’proof of work’ – is important to avoid the duplication of money and which maintains it representation of value because it is a handy token with a value on its own."Payment" remains to be an exchange of values – a fundamental concept of money which never changed since its first appearance thousands of years ago.

There are a couple of definitions possible to define "money" (and later "digital money") – for this paper it is enough to use one choice the suits the purpose of the messages given here.

Money is the acknowledged representation of a recognizable value through a transferable carrier.

Digital money is the acknowledged and transferable off-line representation of a recognizable value through information.

The intrinsic value of money has more and more changed from an actual value (e.g. gold) to a value related to the complexity of reproduction. The actual value of a banknote is typically very low compared to its face value, however, the effort to create this low value ’printed paper’ token is very high and would cost an attacker unaffordable work.

Digital money is the extreme of such a representation since a piece of information like a number does not have any intrinsic value at all, however, faking or generating such number might earn the value as ’proof of work’.

On top of the basic definition the usable form of digital money must have some other qualities.

2 The ultimate digital money

On our quest for high end solutions we scrutinized the question of the ultimate digital money and our results will not answer this question forever, neither do we claim its universal acceptance. Yet the results have been found very helpful to distinguish between the existing solutions.

- No Account
- Anonymous
- Stability
- Currency bound
- Central bank option
- Free offline Peer-2-Peer transfer
- Infinite hops
- Offline-Exchange
- Online and offline operations possible

- No forgery possible
- No double spending possible
- No risk to the issuer bank
- Not using cryptography
- Additional services
- Backing up money
- Instant invalidation
- Limited bad press

No Account

The ultimate digital money shall not be account based. While the association of an account is already contradiction our definition of digital money, this does not require further consideration. It shall, however, be understood that any system providing account based transactions will not qualify as 'digital money' at all. This does not critizise account base systems which are very practical for other purposes than digital money and they are suitable for uni-directional payments (e.g. customer to merchant).

Anonymous

Quality No 1 of (digital) money is still the fact that the user can spend/earn it anonymously. People do not like to be tracked by their business operations – while this is an aspect that associates to criminal activities it is actually the very normal user who doesn't want to be read by any institution or individual. Business behavior is considered as a rather intimate property regardless from the content of the transaction.

Stability

The great inflation (Germany 1923) exchanged about 4.2 x 10^9 (4.2 Bio.) "Reichsmark" for one dollar. People did no more use any money since its value could change by a factor of 2 to 10 within a few days.

For digital money this has a consequence.

Currency bound

Digital money **shall represent an existing currency**. No matter what the currency is, the **stability** of digital money will consequently follow the stability of a currency that is managed by banks and finally the world bank. Trust in digital money will only establish if it is backed by an official currency – trying to invent a new currency (→ BitCoin) triggers consequences of changing value (BitCoin: from 20$ - 200$ within several months) that will hardly be honestly taken by any business except for those who are speculating on the stock exchange anyway.

Hence digital money should represent an existing currency. ($, Yen, Euro,....)

Central bank option

A central bank, reserve bank, or monetary authority is an institution that manages a state's currency, money supply, and interest rates [http://en.wikipedia.org/wiki/Central_bank]. Part of this mission is to control the traded money flow.

If digital money is simply bought as another representation of an actual currency (see above) then the central bank does not need to be worried about the actual money volume in a country. Nevertheless **digital money should have the option to be controlled by the central bank**. As with bank notes, this option does not mandate to trade in the quality of anonymity.

Free offline Peer-2-Peer transfer

Offline peer-2-peer transfer shall easily be possible between holders of digital money. As with bank notes, users want to be able to exchange money without having to consult an account, a network or any third party. This quality also is an important aspect to prove anonymous transactions. Of course users do not want to pay for such transfer - like with bank notes. As a consequence such offline-transfer shall be free of cost.

Infinite hops

The basic definition of the ultimate digital money shall allow an infinite (practically a large) number of hops between peers. The size of the ultimate digital money token shall not change, neither shall it add signatures or traceable information when changing its holder. This does not exclude the option of a controllable number of hops.

Offline-Exchange

A major quality of the ultimate digital money would be its ability to be offline-split. This is a difficult claim that most available solutions do not satisfy. Offline split associates the idea that a digital coin/bill can be split into the "exact change" and the remainder. The "exact change" can be spent whereas the remainder will stay with the payee. The typical problem on most digital money implementations is, that the split amounts need to be re-sigend whereas the signing key is of course not allowed to stay on the user's side.

The ultimate digital money shall allow unrestricted offl-line splits up to the granularity of the smallest represented value (for the $ or Euro this would be 1 cent).

Online and offline operations possible

Despite the fact that the ultimate digital money shall be off-line capable, it shall also be online-compatible. Money draft through a Smart Phone shall be possible and also any other banking operations (money transfer). In particular the ultimate digital money shall allow the exchange of digital money with paper based money (ATM draft) and vice versa.

No forgery possible

The ultimate digital money shall not be forgeable. This is a basic claim yet it is important to be named since the ultimate digital money shall also be allowed to be copied!

No double spending possible

A copy, however, shall not be able to used to pay twice with the same bill – this would turn a copy into forgery. The ultimate digital money shall solve this paradox.

No risk to the issuer bank

The ultimate digital money will be risk-free for the issuing bank. This idea comprises that any duplication, forgery or theft will not lead to any financial damage of the issuer of the digital money. Although this claim may appear to be irritating, this is already partly fulfilled by the present paper based money (=bank notes/coins).

Of course managing fake bank notes will not be entirely cost-free for the central bank, however, faking a banknote does not paralyze or kill an entire currency. In particular a fake bank note does not harm the issuing (central) bank nor any private or bank association.

The ultimate digital money would even improve the situation such that any duplication or (attempt of) generation will intrinsically give neither trouble nor cost to the issuing bank or instance and also cannot harm the digital money system itself.

Not using cryptography

One of the hardest claims to the ultimate digital money is, that its **representation** is not depending on cryptology. While cryptology will be vital to many aspects of handling digital money (storage, transfer, exchange, online etc). the actual representation of a digital money value shall be free from cryptography and hence not being attackable by cryptology.

The background of this claim is the idea that even if galactical numbers of security are used (e.g. 78400 bit RSA) it will be hard to convince an issuing instance or central bank that there is no risk to the bank. This is given through the long-term existence of money (can be traded after 30 years) and the unpredictability of possible attacks through unforeseeable technology (e.g. Quantum Cryptography).

A central bank will still have a hard time to issue 100 Bio. units of digital money if they risk a security breach which today is still out of imagination. As the possible catastrophe is too large, even the security level of nuclear plants will not be convincing to central banks. So the ultimate solution to the ultimate digital money is not to use cryptography at all for the representation of digital money.

- As secure cryptography is... there will be enough press out that puts it in question nevertheless. For instance a recent revelation regarding the NSA claims that the old work horses, AES, RSA, etc. have been compromised. (http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1&_r=0). Such article does not prove the claim of broken cryptography, however, it can be sufficiently scaring to a decision maker with a potential victim as heavy as a digital money.

Additional services

If money gets digital, the ultimate digital money shall allow to attach information to allow additional services. This can be qualities for privileges, spending limits, closed group application or purpose of spending - the range shall not be restricted, yet the representation of the ultimate digital money shall allow to attach attributes and these attributes shall be as secure as the digital money itself.

Backing up money

One of the qualities of digital money shall be that it can be copied by its legitimate owner, in particular for the purpose of backup. It shall even be possible that the legitimate owner of digital amount shall keep the same "bill" in different devices (backup or duplication) and s(he) would still be able to spent even parts of the "bill", from any device without having to communicate from one to the other.

The backup idea will be attractive to many users because for the first time in the history of money you would be able to backup money and if the "purse" (=Smart Phone /PC) gets broken, then the money does still exist and can be spent without any administrative interventions. Account based system provide this idea of course, but the challenge to the ultimate digital money is to solve this problem without any association to an account.

Instant invalidation

Directly associated to the backup idea is the instant invalidation. A user would want to invalidate money that s(he) has stored on a device that gets stolen. By returning the backup copy of the stolen money to a financial institution, the user would expect to receive the same amount of fresh money whereas the money in the stolen device is invalidated without having access to the device. At best, this shall be possible even without having to call an emergency number of the intervention of authorities.

Limited bad press

A killer of a digital money system can be a bad reputation which comes from bad press which comes from flaws in the system. The ultimate digital money shall survive successful attacks without raising attraction to bad press.

This can be achieved by limiting the maximum possible damage. If for instance a person is robbed today and his/her purse is stolen, there will not be bad press about the systems of bank notes because such a thing cannot be avoided and is not something expected to be solved by the money system.

The same shall be possible if the ultimate digital money as being attacked by hacking or typical system attacks. Bad press will not develop if the damage compares to the small damage that is common with hacking. Finally the "loss of confidence" will not occur if the attack cannot lead to disastrous results.

3 The evolution of digital money

A view on the history of digital money is necessary to understand the basic principles of today's money systems. Digital money became public around 1990 and about 23 years later it has seen a high public attention through the availability of systems that could be implemented on the growing number of Smart Phones.

3.1 DigiCash

One cannot think of the history of digital money without mentioning DigiCash in the first row. DigiCash Inc. was an electronic money corporation founded by David Chaum in 1990. DigiCash transactions were unique in that they were anonymous due to a number of cryptographic protocols developed by its founder. The company failed, but not because of technical reasons.

Digicash is a payment scheme relying entirely on software, i.e. no hardware token is necessary. In addition, one of its most important goals is anonymity.

Blind signature The so-called "blind-signature" scheme guarantees the anonymity. The bank signs coins without knowing their serial number and assigns them to an owner.

Payments A payment between a spender and a receiver involves the bank as a third party: The coins the spender is willing to pay are transferred to the bank. The bank maintains a database of already spent coins. In this way, double-spending is prevented: The bank will refuse the payment if it realizes that any of the coins in the current transaction is already stored in the database. In spite of that, anonymity is granted, because the bank does not know to whom the coin has been issued at the beginning. In fact, the anonymity is complete, which also means that a thief can steal a coin and spend it without problems.

Refresh problem This implies that each coin can be spent only once. The receiver cannot use it anymore; it must be reimbursed to him by the bank (usually, in the form of conventional money).

This shows the characteristics of the payment scheme: It is anonymous, only software is needed - no secure token, but it involves the bank as a third party for each transaction (which has to maintain a database for digital coins). Therefore the absence of an online connection, cannot be fulfilled: Either the receiver of the payment must have the payment verified immediately (which definitely requires an online connection to the bank), or he must do it offline after the transaction, in which case he would possibly realize a fraud too late. Thus, "peer-to-peer" payments are not possible or insecure.

3.2 Mondex

Mondex was founded in 1990 as an electronic purse with money directly stored in a smart card (and not a background system), with the possibility of a direct transfer of money between purses.

MONDEX purse The security model for the MONDEX system was confidential. MONDEX didn't succeed in the long run because of concerns of the banks against purse-to-purse transactions. In particular MONDEX required a separate "purse" device which had much security inside and was the only allowed carrier of digital money.

Market The attraction of MONDEX was made by its ability of off-line transactions, its major acceptance flaw in the user acceptance came from the fact that people did not want to carry separate electronic devices. Today the Smart Phone is such a device, but its versatility is way beyond that of the MONDEX purse.

Hence the transport in electronic devices is back and now possible, however, the security level of MONDEX cannot be expected a priori from today's Smart Phones. The current technology discussed the Trusted Execution Environment which is a step further into the direction of secure Smart Phones.

3.3 FairCASH

FairCash is a payment scheme based on digital coins and hardware-based electronic wallets (so-called "CASTORs", Cask for Storage and Transport of access restricted secrets).

P2P-Payment By using "P2P-Teleportation", electronic value is transferred from the spender to the receiver (i.e. the spender's wallet to the receiver's wallet).

CASTOR purse

fairCASH fulfills the principles of anonymity, peer-to-peer and transferability, but it has principally the same drawback as "Token money": It relies on the security of the "CASTOR", a secure element where the coins are stored. If an attacker manages to create copies of the coins inside his wallet, there is no way to stop or detect him.

The design presented in [FairCashDiss] may be sophisticated, but it doesn't estimate the consequences on the payment scheme as a whole if an attack would nevertheless succeed. If these consequences are unknown, it is also impossible to estimate the ratio of benefit to effort for breaking the system, which is the crucial factor for determining the risk of a successful attack.

3.4 Google Wallet and others

Although no digital cash in the strict sense of the definition, payment schemes offered by strong market players like Google, PayPal and others deserve some attention.

Google Wallet is a means for contactless payment, which is currently tied to certain technologies (NFC-capable mobile phones and Google's operating system Android).

Privacy threat

In addition, the user needs a Master card issued by the Citibank or a prepaid card from Google. Therefore, the focus of the concept is rather on the convenient contactless payment procedure than on the advantages of digital cash. Besides, privacy concerns arise because Google could (and will) relatively **easily collect data about the consumer's behavior**. Data about the purchased goods are not readily available, but the person and the place and date of payment are.

Facebook Credits are a similar example for a scheme which does not put privacy at the top of the priority list.

Big players

It can be expected that other big players like Apple. facebook etc. will enter the market soon, however the concepts they offer despite a huge advertisement power and the availability of a lot of potential customers cannot compensate the fact that the offered systems are way apart from the idea of ultimate digital money.

> The characteristics of "pure" digital cash, for example the possibility to pass cash from one end user to another one, are not in the focus of these schemes.

3.5 BitCoin

www.bitcoin.org, de.wikipedia.org/wiki/Bitcoin

Satoshi Nakamoto proposed a payment scheme called Bitcoin (see [Bitcoin]) which is "peer-to-peer", thus fulfilling the requirement of "transferability". BitCoin is completely independent of an issuing authority like a bank, which makes it attractive to numerous users, but also raises legal and even political issues. In this sense, it is also a reaction to recent financial crashes, inflations and other considerations how to be independent from official banking and state economy.

b-money

The basis for the Bitcoin concept is the so-called "b-money". A digital coin is designed as a **chain of digital signatures**. The owner of a coin can be recognized by the owner's public key contained in the coin. The transfer of a coin from A to B is achieved by adding B's public key to the coin and signing it with A's private key.

Transaction log mandatory

Double-spending is prevented by storing all previous transactions in the network of peers. Before each transaction the coin's validity will be checked [BitcoinWiki].

Some disadvantages of this payment scheme are documented in [BitcoinWeaknesses]. The major drawback, however, for the serious user who is not considering money as an object of speculation is the idea that Bitcoin does not represent a currency but pretends to be a currency on its own.

Figure 1- Bitcoin Exchange Rate 2013 - September

Stability of Bicoin

Figure 1 shows the Bitcoin exchange rate from January 2013 (Black graph). Although the value was growing from below $20 to a peak of $220 in April, only users who like to gamble on the stock anyway would be enthusiastic about such a rapid change. But what about those who bought in April 2013. They already lost $60 on average until today which is more than 30% of the selling price.

Some people pray Bitcoin for being revolutionary, however, they could pray for any other object of speculation except for the fact that Bitcoins are much easier to transfer than papers from the stock exchange.

> As common digital money, Bitcoin has never had a chance to exist – it does not get even any close to the idea of ultimate digital money yet it might still have a standing as an electronic token that can be use for speculative actions.

Bitcoin, however, deserves the honor to have stimulated the discussion around digital money during the last two years. The ultimate digital money has not yet been found... except perhaps until Sept. 26th 2013 as presented on a Chip-To-Cloud conference in Nice.

4 Finding the ultimate digital money

During our research we scanned many digital money schemes, first we dropped all the account based systems since by definition they would not qualify for a versatile global use. In Africa it is known that many people do not have bank accounts (a native friend of mine confirmed this and told me that this is due to lack of trust to banks while in households there are the most sophisticated hidden corners where (older) people hide their valuables).

The next powerful filter was the offline-option claim. Many suggested schemes did not pass and when we added the third and very hard claim of offline-exchange capability we had already reduced the candidates down to less than five candidates.

It was quite easy to apply the next hurdle which was the demand for a copyable implementation which should still prevent double-spending. As we had already planned to weaken our claims for the ultimate digital money we were prepared that final stroke of demanding the representation of the ultimate digital money without cryptography filtered out everything.

Everything... but one.

As a matter of fact the last system was not created in a small gallic village in the North West of France but a candidate who started to become more and more fascinating and finally showed up as the only idea that actually qualified for any of our claims on the way to the ultimate digital money.

It did even have features which exceeded our claims and at the same time it was so simple that at a first glance we were even a bit disappointed that a.) it had not been our idea and b.) that our hard claims could be answered with a system that was simpler that we could have imagined. But maybe that is the idea of geniality.

The name of the system was **BitMint**.

5 How BitMint works

BitMint was invented by Professor Gideon Samid, PhD (Gideon@BitMint.com) leading academic research on digital currency in the department of Electrical Engineering and Computer Science at Case Western Reserve University. Prof. Samid also advises graduate students performing research on the topic of digital money – currently acquiring PhD candidates (gideon.samid@Case.edu).

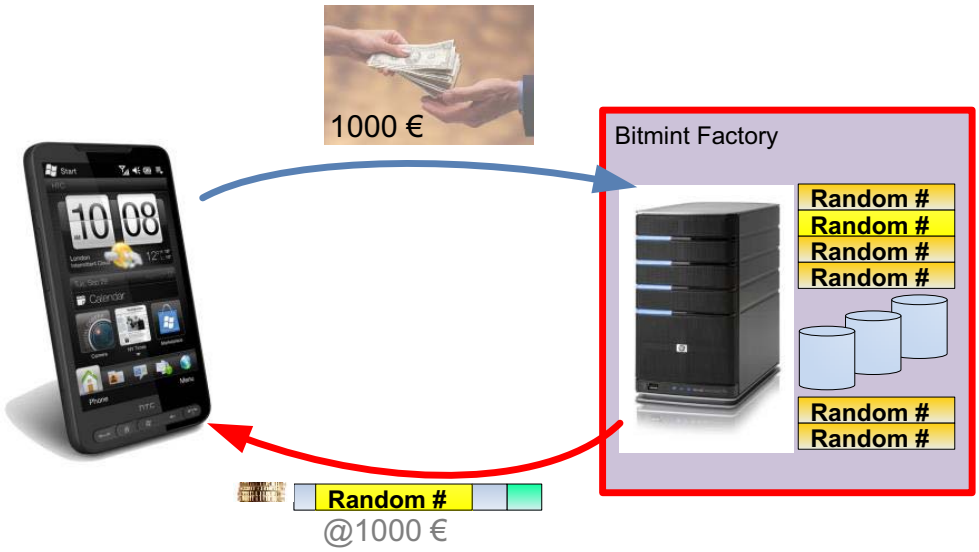


Figure 2 - Example of buying Bitmint-Bill

Value representation

The BitMint novelty is based on the idea that any bit string that represents contents is a bit string that reflects a pattern of some sort. That pattern may be deeply hidden (well encrypted), and may be masked with random bits, but it cannot be eliminated.

Deterministic patterns

Suppose a bit string may represent the numbers: 0 to 99. While such string may look random to the naked eye, it does allow a reader to discern what number it represents. In other words, such string cannot be purely random.

Now, any pattern that is built-in, into the string, however well hidden, may be one day unearthed by a smarter cryptanalyst – which is the death trap of all the digital currency solutions proposed so far (except BitMint). These solutions are based on ciphers that give confidence to their users today, but that are vulnerable to future mathematical insight.

Crypto for communication

It is one thing to use AES, or RSA, the mainstay ciphers banks and governments have come to trust – for the purpose of secret **communication**. Why? Because once these ciphers are considered compromised they can readily be replaced.

Crypto for money?

It is quite another thing to move the **financial** worth of society to depend on such or other ciphers. If BitCoin cryptography, for example, is compromised – all the money carried by it melts away – instantly. People who rush to buy crypto-based digital currency hardly realize the risk they subject their money to. While the typical user doesn't need to understand that idea, the decision makers to launch digital money do very much.

Worst case attack

There is no recourse once the foundational algorithm is breached. And this vulnerability extends to every digital currency that relies on a cryptographic intractability represents by an algorithm however clever, however impressive today.

Pattern-free representation

That is where BitMint is different: the Bitmint-Bill bill is totally pattern-less, purely randomized. Since it carries no pattern, there is no pattern to discover, no credible way to fake or steal the money.

We mentioned earlier that a bit string that carries any information does have pattern in it, so how does the BitMint string convey information and remain pattern-less? In general the BitMint money string conveys its monetary value through a selected function of its cardinal number, or, say its size.

One possible representation is the direct representation of a value by the number of bits that a random number has, this solution is described in 6.1 "How the Bitmint-Bill is built".

Indeed, the only attributes of a string that are not expressed by the identity of its bits are functions of the string size. It is this very principle that allows the BitMint money string to be immunized against future mathematical insight, or future technology.

No risk to the bank

Unlike any other of our scrutinized digital money systems BitMint withstands the coming onslaught of quantum computing. And that principle underlies the claim that the issuing bank of the BitMint currency does not take cryptographic risks, and is not subjecting its users to the horrific catastrophe of a total financial meltdown.

Crypto for save and move

We will see later that cryptography is not shunned, but heavily used, albeit by traders and users who wish to **store** and **move** the money securely. Much as cash can be lost or stolen without undermining the mint, so it is with digital currency, it can withstand cryptographic risk to safeguard against retail fraud, while avoiding any cryptographic risk for the issuing bank, the mint, the total wealth, digitally expressed.

If you buy a Bitmint-Bill of value 100 $, than you buy a **freshly generated random number** which from the moment of your purchase is created in the **BitMint factory**. The random number does not have any cryptological signature nor encryption, it exists in plain text and (!) **it is registered in the BitMint factory.**

The perfect randomization of the Bitmint-Bill, undermines the efficacy of brute force crypto analysis, that requires a deterministic target. Of course the idea of a random number is well known as a one-time password.

For the transmission, of course, cryptology is in place, yet it is not part of the representation of the currency but only required for its secure transport.

The random number may be digitally used to pay and purchase trade until finally the digital coin it is returned to the BitMint factory. On return the BitMint factory will pay the cash back - with the exact face value as returned by a Bitmint-Bill. As the idea is to keep the face value with no deductions (transaction fee) the question of the associated business model rises. The business model options are described in 9 “Business models”.

Hand-in a Bitmint-Bill

After pay-out of the cash the BitMint factory will delete the coin (or relevant parts of it) from its server. Hence any other return will not be successful. At this point the BitMint factory does not care whether the first return was coming from a fraudulent source or a legitimate one. **The risk is not on the bank’s side but on the user**.

This is a major advantage over any other digital cash system and very relevant for the acceptance of banks. It also solves the claim of "Limited bad press" as the maximum fraud (except for hacking the BitMint factory) hits one purse which compares to all the unlucky events happening in the criminal scene every day.

Saving money

The BitMint factory keeps exactly the amount of cash that a client has bought. If a client buys $100, then the BitMint factory saves his $100. Since the client can only reclaim these $100, the BitMint factory is not exposed to any market risk. If the value of the $ falls drastically, the BitMint factory is untouched since they keep exactly those $100 of the customer. No risk, no speculation.

5.1 Online verification

As the risk is on the user’s side, the user might want to have a method to minimize this risk. So any user receiving a BitMint payment may online-verify the received Bitmint-Bill by a simple verification exchange with the BitMint server. The server will not credit cash, but it will return a new, fresh Bitmint-Bill random number in exchange. The returned Bitmint-Bill will be deleted and made unusable for any other imposter.

If the random number is not found valid, the verifying user will be informed and can object the trade s(he) is planning to do.

If the exchange was successful, the receiver may be 100% sure that s(he) has a fresh valid Bitmint-Bill that is free from any risk of fraud. This will promise a high confidence to the user.

5.2 BitMint online world

The refresh example only works in the BitMint online world, i.e. an online connection shall be available on demand. There is also a BitMint offline world which will be discussed later.

In the BitMint online world a transaction requires an Online verification if the receiver of a payment does not trust the payee.

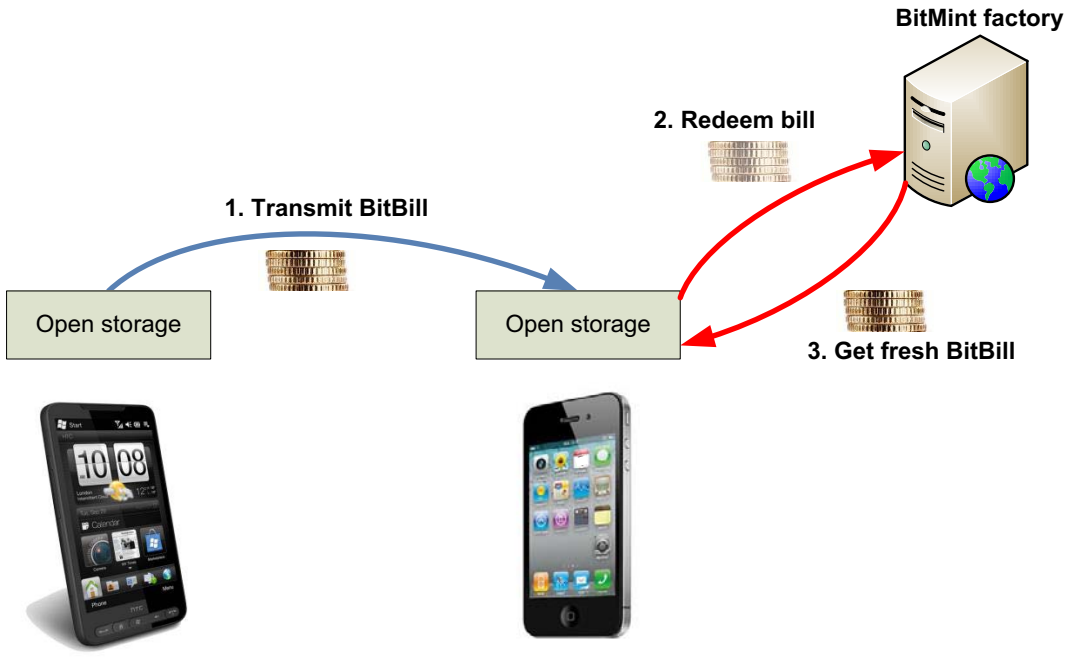


Figure 3 - Online verification on payment example

Pro's

The advantage of online based transactions is, that they do not need any secure element or other security on the side of the user. Of course a user will be able to make clones of Bitmint-Bills. But since we are in online-world, he can spent such a Bitmint-Bill only once. The receiver of a clone will always verify the Bitmint-Bill and deny the trade, if the Bitmint-Bill did not qualify.

Clones become unusable with online verification. Online-Bitmint-Bills can be carried in unsecured devices, e.g. in mobile devices/phones that do not provide a secure element for the offline variant.

Another interesting aspect is discussed in Deposit Bitmint-Bills in the cloud where it is possible to disable Bitmint-Bills on stolen device.

Con's

Reasons to use the BitMint offline world are the limited availability of networks or the associated roaming cost which can exceed the actual amount to pay.

5.3 BitMint offline world

Using Bitmint-Bills offline makes BitMint more flexible. Offline use, however shall avoid cloning of Bitmint-Bills although there is no risk to the bank, user's would not want to be rejected after they received a cloned Bitmint-Bill.

Secure hardware required

As a consequence the Bitmint-Bills need to be kept in secure hardware and its security depends on the security level of this hardware. Again there is no risk to the bank who does not care about online or offline world.

For the discussion of the offline world we need to make an assumption that the secure hardware can be considered secure. In this case a Bitmint-Bill will be securely deleted in the sender's secure element after it was confirmed to be received by the receiver.

The attractive multi-device storage and backup facility of digital money is not solvable as easy as in the BitMint online world, however, as the online flavor can always be converted to an offline money the user may determine a certain amount only that s(he) requires for the particular case of offline payments → 5.4 "Moving from world to another".

Moving Bitmint-Bills

Bitmint-Bill will only go from one secure element to another secure element. Since both secure elements will provide a mutual secure session, today's cryptology may well generate the associated security.

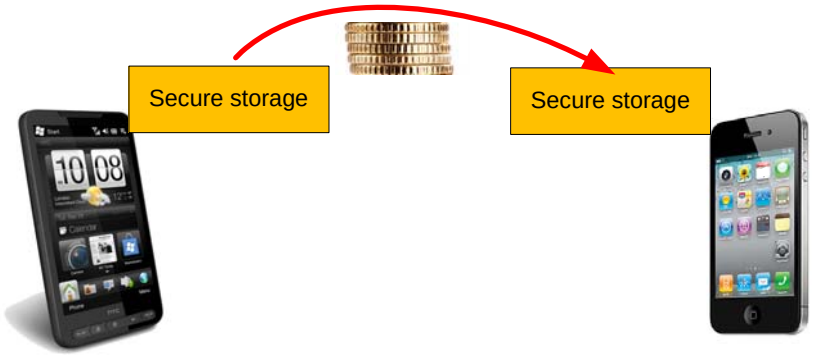


Figure 4 - Offline transfer

Pro's

The advantage of the BitMint offline world is the independence from networks. Online connection may also imply charges that exceed the actual amount of the transaction.

Con's

The disadvantage of the offline world is the mandatory use of secure hardware. That, however, is only a relative disadvantage, any other digital money system mandates this claim nevertheless. BitMint still makes a difference because on breaking the security of secure hardware, the bank does not have any risk as argued above.

The device containing the secure hardware, shall be kept like a classical purse, once being stolen there is an exposure to the amount of offline-stored Bitmint-Bills.

A special case is described in 6.4 "The teleportation problem". It adresses the technical challenge to let Alice's secure element delete a transmitted amount only after she can be 100% sure that Bob received the value.

5.4 Moving from world to another

A Bitmint-Bill may be imported and exported to/from the secure element that represents the offline world. Export is uncritical - the secure element shall simply tag the Bitmint-Bill "unpayable" or even delete it after it has achieved confidence, that the Bitmint-Bill was exported properly.

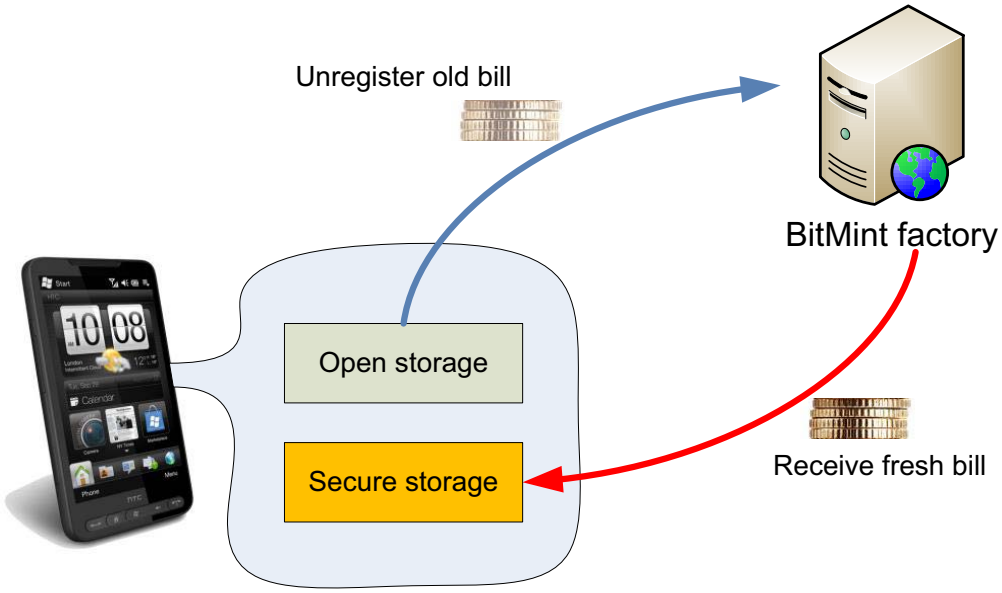


Figure 5 - Moving a Bitmint-Bill to the offline world

To offline world

The import of a Bitmint-Bill into the secure storage demands a mandatory online verification before made available in the secure element. The secure element will itself establish a secure session with the BitMint factory and replace the online Bitmint-Bill by a unique and fresh offline Bitmint-Bill.

Hence further attempts to recharge the same or another secure element with the same (old) online Bitmint-Bill will only result in bad verification and again the online-clone would be useless.

To online world

To move a Bitmint-Bill from the secure storage (offline) into the online-world, there is no server connection necessary because the Bitmint-Bill can be trusted as it comes from the secure storage featuring uniqueness and integrity.

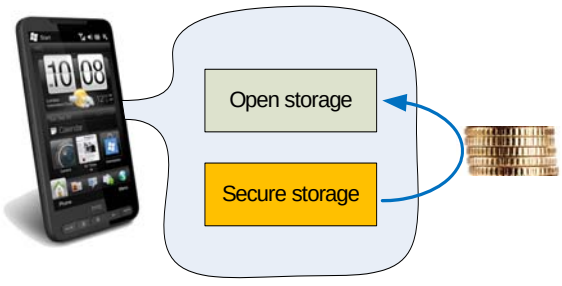


Figure 6 - Moving a Bitmint-Bill to the online world

5.5 Offline or online?

The offline mode is the preferred mode through its better flexibility in situations where online-verification is too expensive (data roaming) or simply not possible. Offline is always available and independent from the local reception quality

Online mode is suggested in association with extended features like Backing up Bitmint-Bills. For instance, a user may have cloned his/her entire purse, which can only be done in the off-secure element variant = online world.

At the time, the user needs to make an offline payment, s(he) shall pick the desired Bitmint-Bills and import them to the offline-world. Of course an online verification is inevitable for the transfer.

Which world to be used

- is up to the user and determined by the risk a user is able to take as a consequence of his (non-/secure) environment.
- depends on the environment and context a user wants to work in

User convenience

The move between these worlds might be supported by applications. Unexperienced users might not even need to understand these ideas but may pay as just as usual and easy without having to care

5.6 Giving a change

As long as the idea of digital coins and bills exists, there is the problem of correct change. In particular in the off-line situation, a bill with the exact required amount cannot be ordered.

BitMint allows to split any Bitmint-Bill into accurate fragments to be used for a correct change. The technical discussion is made in 6.1 “How the Bitmint-Bill is built”.

If a Bitmint-Bill is split into a correct sub-part and a change remainder, both parts are independent Bitmint-Bills with no further impact on the associated security. This can be achieved off-line. The broken parts will contain the hash value of the original Bitmint-Bill which allows the verification system to recognize from which original Bitmint-Bill the split was made.

Together with a position information

"I am a fragment of the original Bitmint-Bill (Hash: xxxx) at <Position Index>)

all information is available to resolve the fragment securely. The hash value does not provide further security. It is used to find the original bill in the database whenever a later verification is launched.

Find more technical discussion in 6.1.2 “Position Index” on page 1-19.

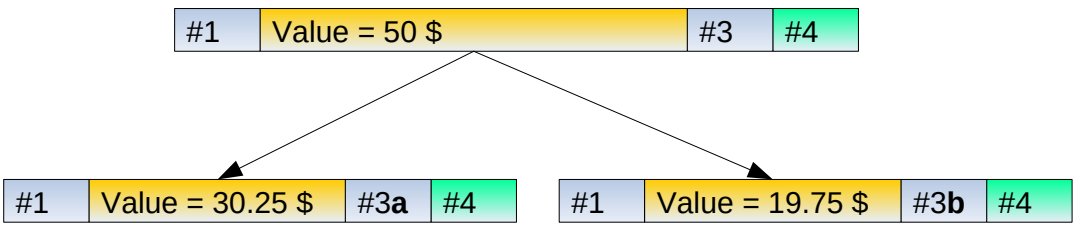


Figure 7 - Splitting a Bitmint-Bill

Figure 7 shows a Bitmint-Bill being split for a change. The value can be split whereas the position information will be different for the fragments to indicate their position in the original bill.

5.7 Money draft

Money draft from ATMs has always been subject to sometimes sensitive charges. Very often money draft is only possible with an ATM of the user's home bank.

Bitmint-Bills draft is possible wherever a network is available. This compares to a universal ATM system independent from home banks and cash issues.

Security aspects

Money draft means to access money on your own account. This is not a business transaction but indeed a service of most sensitive nature. Any attacker who is able to open such a transaction to your account could be thought of drafting Bitmint-Bills. More options are described in 9.3.1 "Cloud-based backup service".

5.8 Using special features of digital money

Through the system of anonymously registered Bitmint-Bills it is possible to attach Attributes to a Bitmint-Bill. These attributes may control the scope of the Bitmint-Bill and provide attractive use cases. Details are discussed in 8 "Extended BitMint features" on page 1-27.

6 Technical details

6.1 How the Bitmint-Bill is built

As said above a Bitmint-Bill is basically a large random number that is stored on a remote system called the BitMint factory. The basic underlaying security depends on the idea that it is not possible to guess such random number which is mathematically expressed by a Collision Probability of nearly zero. In the following the simplest example of the value representation is shown whereas the value of a Bitmint-Bill is represented by the number of bits of the random number (multiplied by a fixed factor, here = 32).

According to that solution the layout of a Bitmint-Bill is basically made of four fields

Figure 8 - Fields in a Bitmint-Bill

<hash> <rnd value> <pos info> <attributes >

Table 1-1. Bitmint-Bill layout

Field	**Size** [bytes]	**Comment**
Hash ID	16	Does not have cryptographic significance, only to speed up the retrieval in the BitMint database
Bitmint-Bill value	N x 32	Random number storing the actual value of N cents.
Position Index	8	**Format:** *StartPos*:4bytes | *Length*:4bytes
Attributes	var.	Attributes as described in 8 “Extended BitMint features”

Hash ID

Hash collision risk

The hash ID is a 16-byte value in order to efficiently identify the Bitmint-Bill in the BitMint database. 16 bytes can address approx. 10^{38} choices, at 10^{11} separated Bitmint-Bills in the field the collision probability is left at 10^{27}.

Figure 2 - Hash field in a Bitmint-Bill

The hash ID is built only over the Bitmint-Bill value which allows to verify that Bitmint-Bill values are 100% collision free in their production.

100% collision free hash

Even with a lower collision probability a collision is not critical. If the BitMint factory produces a Bitmint-Bill, then it may verify the uniqueness of the Bitmint-Bill before issuing. If the hash value is already part of another Bitmint-Bill, the produced Bitmint-Bill will be dropped and a new one will be generated.

Efficient hash storing

The hash value does not necessarily to be expressed as additional 16 bytes. It can be made of the first 16 most significant bytes of the actual Bitmint-Bill value. Since the Bitmint-Bill is made of 32 bytes, there will always be 16 bytes available for the hash value.

Cryptographic strength

The hash value does not need cryptographic strength. Attacks on hash function try to generate a collision, i.e. to find an input B that generates the same input as the original input A of a hash computation. For the BitMint system such an attack would be irrelevant because finding such a collision would not imply its existence as valid Bitmint-Bill in the records of the BitMint factory.

6.1.1 Bitmint-Bill value

Collision-free Value

The Bitmint-Bill is made of a random bit string. This value is produced in the BitMint factory together with the other fields of the Bitmint-Bill and stored on the server database of the BitMint factory. The random number is 100% collision free which can be easily verified through the creation of the Hash ID. If the BitMint factory creates a Bitmint-Bill and tries to store it where it already finds a similar hash value it will dispose the new value and create another one instead.

Figure 3 - Value field in a Bitmint-Bill

The discussion made in 6.3 “Collision Probability” shows that it is practically impossible to find a registered (valid) Bitmint-Bill value by intention or accident.

Length of Bitmint-Bill

The length of the Bitmint-Bill value is 32 x N bytes, whereas N represents the amount to be "printed" in multiples of cents. A cent is considered the smallest unit of the associated currency, regardless whether this actual currency does have other names for their smallest unit.

Hash

The Hash ID is built over the entire Bitmint-Bill, but not over the Attributes. This allows the verification of uniqueness of the hashed value. As the hash is only used for fast indexing, there is no security issue about spanning the value only.

6.1.2 Position Index

The position information describes the fragment of a Bitmint-Bill if it is split for the purpose of change. From the original Bitmint-Bill fragments can be created simply by taking a desired number of N x 32 bits from the original Bitmint-Bill. Since a value is expressed by the length of a Bitmint-Bill, the value is still inherent in any fragment of a Bitmint-Bill.

Figure 4 - Position info field in a Bitmint-Bill

Although the fragmented value alone has the specified quantities of Collision Probability, it would be quite inefficient, to search the fragment in the entire set of stored (=issued) Bitmint-Bills. Therefore the Hash ID is copied to the header of the fragment. Then the position information will be set to the start position of the original Bitmint-Bill. A additional length field is not required since the length is determined by the number of cents (N x 32 bits) from the original Bitmint-Bill.

On verification, the BitMint factory will find the original bill through the attached Hash ID but will then identify the fragmented parts using the position index. If found, the associated number of bits will be blanked in the BitMint’s database. Hence no other verification could be done on any of the concerned bits. Neither can the entire bill be reclaimed.

Offline world

A Bitmint-Bill split can only be done in the BitMint offline world and hence within a secure element. Since the secure element can be trusted, it will only create correct substrings (fragments) with the associated position information. A malicious user cannot tamper with manipulations.

Online world

The BitMint online world mandates the receiver's Online verification before closing any associated deal. Hence the payee cannot manipulate Bitmint-Bills to his personal advantage. In general fragments of a Bitmint-Bill are nothing but another Bitmint-Bill having exactly the same security.

> The Position Index is only an information where to find the value in the BitMint database, it does not imply any monetary information different from an unfragmented Bitmint-Bill.

6.1.3 Attributes

Technically, attributes are fields of additional information that are stored together with the actual Bitmint-Bill. Storing these fields can be a paid service and as such be part of associated Business models.

Figure 5 - Value field in a Bitmint-Bill

Attributes may be used for a large variety of purposes, some of them being listed in 5.8 "Using special features of digital money". Here we only consider attribute's technical representation. Attributes are preferably expressed as structured data. XML is the most attractive format to code attributes. Not all attributes can be set by a user.

Constraints and privileges

Technically attributes may be distinguished by "constraints" and "privileges". A constraint reduces the versatile use of a Bitmint-Bill to a dedicated purpose. An example is parental control - parents may transmit Bitmint-Bills to their children which is constrained such that the children cannot purchase banned material or cigarettes.

A bank may give a credit line constrained to the purpose of spending the money for the car or the property. The bank might even constrain the credit to the payment of a signed associated contract - there are of course other ways to bind a money transfer to a legal document.

Anyway a lot of phantasy is possible for such purpose. From the technical point of view it is relevant to understand, who is allowed to lift a constraint.

Who can lift a constraint?

It is obviously the receiver of the constrained Bitmint-Bill who has interest to lift the constraint to allow wider (mis-)use of the Bitmint-Bill. Let's stay with the example of the parental control constraint. In the BitMint online world it is possible to "see" the Bitmint-Bill, yet any change of parameters (except for a fragmentation) - invalidates the Bitmint-Bill since it will lack correspondence in the BitMint database.

Verify credentials

However, the juvenile could try to reclaim the Bitmint-Bill in the BitMint factory to receive a free exchange in return. To release the constraint, however he needs to verify his credentials (not his identity) to the BitMint factory. The credentials of our juvenile are "may buy anything which is not restricted to underaged". The age verification can only be done by the juvenile's secure element, unless he steals a device with a secure element that has no constraints.

In social life, the juvenile will of course find a out-of-age friend who buys the beer. Cheating on the use case level cannot be entirely covered by technical systems like BitMint. But if it comes to critical levels and banks ban their credit not to be used for gambling, a majority of misuse can certainly be covered.

Attributes do not invalidate digital money, they only control the money flow and exchange for a specified purpose.

Who can set an attribute?

In general, attributes can be set by the owner of a Bitmint-Bill.

A dedicated scheme of access control might be associated to the question who is allowed to change what attribute. For instance, the associated currency cannot be changed.

As a general rule, the owner of a Bitmint-Bill is authorized to assign attributes. As far as this assignment is a constraint, the user will know that he might decrease the attractiveness of the Bitmint-Bill. A receiver might not want to accept attributes, therefore a user might be careful with restrictions.

An attribute will be activated on the first transmission. This means, that attributes, being set by an owner, do not restrict the owner but the next receiver. Accordingly an owner may still change/erase attributes and will not be restricted by his/her own settings.

BitMint offline world

In the BitMint offline world, attributes are associated to a Bitmint-Bill and activated during the next transmission. On reclaiming a Bitmint-Bill, a receiver needs to present his credentials to his secure element (storing the constrained Bitmint-Bill).

As a special service, the receiving device may always warn a receiver on the reception of attributes that s(he) will not be able to cover. A juvenile will be warned on the reception of constrained Bitmint-Bills. A liqueur shop will be warned that he cannot reclaim a Bitmint-Bill of a juvenile. A receiver of Bitmint-Bills will learn, that the Bitmint-Bill that s(he) receives is constrained and by which parameters.

If a Bitmint-Bill from the BitMint offline world is ever to be reclaimed, the BitMint factory will automatically assign the attributes to the Bitmint-Bill to be reclaimed and execute the associated procedures. If the juvenile tries to reclaim parental controlled Bitmint-Bills, he needs to present his/her credentials to the BitMint factory.

BitMint online world

In the BitMint online world, attributes, assigned to a Bitmint-Bill will be linked to the verification record of a Bitmint-Bill immediately. Any user alteration of these attributes during the online-existence (apart from a secure element) will be rejected by the BitMint factory on a reclaim request. As a service, however, the BitMint may "repair" the attribute setting according to its database entry. Then a reclaim or transfer to the BitMint offline world will be possible by presenting the appropriate credentials.

Attributes architecture

The scope of a white paper cannot cover the full architecture of attributes. A full system design shall be made to allow a scalable and flexible use and administration of attributes. Services may evolve that also stimulate attractive Business models.

6.2 Size and Performance

The system has some elegance. For instance, it makes little difference whether a user keeps $100 as a single bill or as 10.000 pieces of 1cent. The $100 value is represented by the same number of bits, whether it is in one or hundreds of pieces. Hence the storage and the network traffic for money transmission depends on the actual amount in question, but not much on the actual fragmentation.

Of course this linearity is not perfect. Any Bitmint-Bill has additional information which adds to the proportional part. There will be software architectures who can compensate the effect. Splitting a $100 Bitmint-Bill into pieces means that every piece has the same <hash> and <attributes>. Hence these values can be stored once and referred to by any children of the original Bitmint-Bill coin internally until the last member disappears.

6.3 Collision Probability

A collision happens, if two or more identical Bitmint-Bills are produced by statistical accident. In such a case, the first of the identical Bitmint-Bills will be paid off on return, but the second (same) number will not be paid since the system considers a second same number as impossible and an invalid attempt to win cash.

Already the collision of the Hash ID wouild lead to problems. The good news are that the Bit-Mint factory can avoid such collisions by 100%. Any generated random number can be tested for collision with presently stored Hash IDs before it is issued. Hence the collision probability equals zero.

6.4 The teleportation problem

The problem of teleportation means to transport a value from A(lice) to B(ob) such that the value shall be deleted on Alice's side if Bob received the value (coin). This is important to avoid that Alice can spent the coin more than once. If the communication channel between Alice and Bob breaks during the transaction, Alice might not receive an ACK from Bob or the ACK may get lost. Alice remains in a state where she does not know whether to delete the coin (forever) or to keep it for retransmission.

The problem to be solved is a secure offline teleportation that avoids the "Two General's Problem".

> The "two generals problem" describes a situation where two generals need to attack a town together in order to win the battle. However the enemy sits exactly between the two armies and the two generals need to send a courier through the enemie's territory to announce the right time of the attack.
>
> The problem occurs if the enemy captures one of the couriers. Courier A sends the message of General A "I will attack on Monday morning". If courier A is caught, General B will not reveive and General A will attack alone - and loose. If courier A, however, succeeds to reach General B, then General B will attack, however, before he sends a courier B back to General A to approve his acknowledgement. General A will not attack if courier B does not arrive, so General B will attack all alone ...
>
> The problem has been proven to be mathematically unsolvable.

At a first glace the problem of safe teleportation looks alike. Alice doesn't know whether Bob received the money until she receives an acknowledgement from Bob. Only then Alice (Alice's secure element) will delete the money sent to Bob. If a communication error disconnects communication, Alice doesn't know whether a.) Bob received the money and she didn't get the ACK or b.) Bob did not even receive the money. Alice's secure element doesn't know whether to delete the amount or not.

One possible solution is shown below.

Both partner own a secure wallet represented by a secure device that does trustable execution of the functions described below. It also provides confidentiality i.e. the data cannot be seen inside the wallet.

1. Alice pays Bob with the coin (C) by a simple transmission of the coin to Bob. However, the coin has a marking that it is not allowed to be spent (Locked flag).

2. Bob sends an ACK to Alice meaning "I received the coin"

3. Alice receives the ACK

4. Alice deletes / invalidates the coin that she transmitted.
5. Alice receives a permission token (PT) from her secure wallet (after deletion) with the meaning "Bob may now spend the coin".
6. Alice sends the permission token (PT) to Bob
7. Bob's secure wallet enables the coin to be spendable.

After Step 3 Alice may delete her original coin because she knows that Bob did receive the coin. Alice only can create the permission token after she has deleted the coin (4).

Whenever the communication breaks, Alice and Bob may re-establish and Alice will send the permission to Bob as often as Bob requires. The permission does not help Alice for anything since she does not own the coin anymore and hence cannot double-spend.

The advantage can be seen already here. Alice may resend the permission token to Bob as often as she wants. Alice cannot spend the old coin anymore but she knows to 100%, that the coin is with Bob.

Even in a very noisy channel, Bob will not close the deal with Alice until he received the permission token. That permission token, however, can be sent by Alice to Bob as often as she wants. It does no more have the requirement of a unique location.

Alice cannot cheat by spending the coin that she sent to Bob because the coin is no more available after she deleted the coin (4). Bob cannot cheat because after he sent his ACK (2), Alice has evidence, that Bob has the coin and she won't send another coin but the permission token TK.

Alice and Bob together cannot cheat in a joint action because it is guaranteed by Bob's ACK, that he received the coin and Alice cannot release (allow payment) with Bob's coin until she deleted her own coin C.

If the secure elements (which do the processing and keep the coins) are broken by either Alice and Bob, they cannot trade in more than the single coin in the back. They could however spent the coin to a third person in offline mode.

This system does not involve a particular states of the payment system. The quality to be payable is attached the coin itself, not to any system state that administrates the coin.

Moreover the protocol is very simple but efficient. Implementation can be done very fast and is also better suited for high certification levels. The protocol is fully off-line compatible and only requires a Peer-2-Peer communication between two partners.

7 Attack scenarios

7.1 Guess a number

Indeed, this is the seed of an attack whereby attackers start exhaustive "return number" retries to hit any correct number.

Therefore the number of bits representing the smallest unit of the BitMint money needs to be large enough to avoid any realistic collision.

The following computation derivatives a conservative approach

- We assume 10 Bio. (10^{10}) attackers each holding 100 cent of the currency. This is already a unrealistic high number of cents, yet a conservative approach justifies this assumption. This results in 10^{12} cents given out at one time.
- It takes approx. 30 msec seconds, to process a refund transaction. This allows about 30 attempts per second.
- A year has 31.536.000 seconds
- Thereof in one year, one attacker can request approx 10^9 requests. We allow processing of 1000 requests in parallel and raise the number of possible requests to 10^{12} per year
- As a consequence, 10^{10} attackers may each place 10^{12} refund requests every year. So the BitMint factory will not allow for more than 10^{22} refund requests per year.

Now we want to find the probability that 10^{22} attacks (1 year) challenge the database which expresses 1c by B bits. The population of the database is 10^{12} pieces of 1c.

As with every challenge the attacker knows more about the content of the database, the situation follows a hypergeometric distribution which corresponds to "sampling without replacement". With every draw the probability to guess a correct number will slightly increase. (http://en.wikipedia.org/wiki/Hypergeometric_distribution)

The formula to compute the probability of hypergeometric distribution is

$$P(X = k) = \frac{\binom{m}{k}\binom{N-m}{n-k}}{\binom{N}{n}} \tag{1-1}$$

with

N is the population size i.e. the maximum number of 1c pieces each expressed by B bits. It follows that $N = 2^B$.

m is the number of success states in the population, in our example the number of available 1c coins on the server (= 10^{12}).

n is the number of draws, in our example the number of attacks per year which was set to 10^{22} (see above).

k is the number of success, in our example k=1 as we stop our attack after the first number was guessed.

Trying to compute P(k=1) was found to be impossible with regular tools (e.g. EXCEL) since the numbers were too high and did exceed EXCELS number range. Using the logarithmic approach (GAMMALN function) slightly improved, but did neither work finally due to the same reason.

Therefore the probability P will have to be conservatively estimated by a modification of the hypergeometric distribution.

In

$$P(X = k) = \frac{\binom{m}{k}\binom{N-m}{n-k}}{\binom{N}{n}} \tag{1-2}$$

we replace (*N*–*m*) by N which increases the probability

$$P'(k=1) = \frac{\binom{m}{1}\binom{N}{n-1}}{\binom{N}{n}} > P(k=1) \tag{1-3}$$

which resolves into

$$P'(k=1) = \frac{m}{\left(\frac{N-(n-1)}{n}\right)} \tag{1-4}$$

For N much larger than n (given in our case) we may approximate (N–(n–1)) by N

$$P'(1) = \frac{m}{\left(\frac{N-(n-1)}{n}\right)} \approx \frac{mn}{N} = P'(1) \tag{1-5}$$

The result simply states that we can approximate the precise hypergeometric distribution by the binomial distribution which corresponds to "sampling with return". This corresponds to a BitMint factory that generates a new random number for every false verification.

This results in the following table

Table 6 - Size of a cent n Bytes/bits to attack one cent

Bytes/cent	Bits B / cent	P	Years to p = 0.5
15	120	0,0076	66
16	128	2.97×10^{-5}	≅17000
20	160	6.9×10^{-15}	7×10^{13}
32	256	8.72×10^{-44}	6×10^{42}
48	388	1.6×10^{-83}	N/A

10^{83} is the estimated number of molecules in the universe. The last row is of academic nature only and shows that it would require 48 Bytes in order to compare to the probability that a person would guess the order number of one molecule out of the entire universe (1 guess only).

To guess 3 cents, each of it expressed by 16 bytes (128 bits) would be of the same order!

A good value to represent 1 cent is therefore a number of 16 bytes. It is very unlikely that values of 1 cent are stored on the server, any larger value would, however, already increase the complexity exponentially. If the entire world population requires about 17000 years to guess one cent at a confidence level of 0.5 (flip coin) then this risk is affordable.

Insurance

Hence an insurance company may insure the collision risk at extraordinarily low rates. As a matter of fact, it would be a most promising business to insure this risk, even with the promise to pay out one additional million $ to anyone who guesses a collision.

Note: Unfortunately this show effect cannot really be executed because people would hand in valid Bitmint-Bills claiming to have them guessed. Since we allow the BitMint online world, it is possible for a user to know the number of a valid coin.

7.2 Denial of value

The most prominent attack that we identified was the dishonest receiver who runs a "Denial of value" attack – only possible in the BitMint online world.

- Alice pays Bob with a valid Bitmint-Bill
- Bob (dishonest) trades the coin to the BitMint Factory but tells Alice, that the BitMint Factory has refused the Bitmint-Bill because it was invalid.
- Giving back the old coin to Alice will not help because now it is indeed invalid and Alice cannot re-verify or if she does she will get a confirmation of Bob's claim.

The actual attack is not on a technical level since the correct technical payment is closed after Alice sent the valid money to Bob. However, Alice could contact the BitMint factory and ask whether her bill (she is allowed to keep a copy) has been verified valid recently. At this point it would be helpful if Bob can still be identified as the last verifier - details would have to be worked out in order to maintain the anonymity aspect.

The full solution to this threat can be developed and it is not the idea of this paper to show the entire countermeasures. In general a.) Bob needs to be identified as the trader of Alice's bill and b.) Alice shall be able to get a report of the status immediately while she is still acting with Bob. The rest of this situation compares to the situation where a merchant denies to deliver to a client, which is a regular legal case and little related to the technology of the payment scheme. These situations are well known from credit card fraud.

7.3 Man-in-the middle (MiM)

This attack has several flavors, The MiM could sit between a peer-2-peer transaction between Bob and Alice. The MiM could also sit between Alice who wants to redeem a valid Bitmint-Bill to the BitMint factory.

Both cases can easily be solved by already standardized authentication protocols. A powerful (IKE based) protocol is the "Privacy Protocol" described in EN14890-1. The basic idea is the exchange of certificates between Alice and the receiver. Alice can recognize the receiver's identity from the certificate and she can therefore know whether the next instance is the MiM or the desired communication partner.

For the BitMint factory there will be one certificate available known to every subscriber.

Note: Even if the associated PrK (private Key) of such certificate would be broken, this is no attack to the money system. There would be some manageable consequences, to communication channels.

Alice will not send money to someone who does not identify as the desired target of transmission. Therefore the MiM cannot enter the communication.

7.4 Stealing money

This is the most obvious attack. An attacker would be interested to read valid Bitmint-Bills from any device, mobile or desktop, where money is stored. Today's state of the art technology is absolutely capable to cover this problems, in general the Bitmint-Bills could be locally encrypted with any encryption technology that users have in place. SmartCards and TPM modules are already available as technology.

Another attack would try to read the Bitmint-Bills after local decryption, e.g. when used for a transaction. This can be solved again by the same technology, but it requires more sophisticated applications which care to re-crypt the encrypted money with the session keys used for any transaction.

The key message is, that this part of protection compares to keeping a classical purse safe and it falls under the responsibility (or system provider) who actually uses the BitMints, the BitMint design itself is not less secure than any other digital money being stored on those devices.

8 Extended BitMint features

The raw Bitmint-Bill may link Attributes in order to associate special characteristics. From the use case point of view these Attributes add features to the Bitmint-Bill which make digital money highly competitive to printed money. As a matter of fact both representations do perfectly combine for their particular use cases.

The chapters below are an extract of many more features that can be used with BitMint, as features are also related to Business models the list of features will increase anyway.

8.1 Currency association

BitMint is not a currency on its own. This is attractive because there is no associated value to Bitmint-Bills but to the associated currency. Bitmint-Bills are always assigned to a particular currency and the value of its bits rises an falls with that currency. As such Bitmint-Bills are not competitive to currencies, only on their representation.

Currency attribute

The currency of a Bitmint-Bill is represented in a *currency* attribute. The currency cannot be changed. Money exchange - like currency change - is possible by an exchange through the BitMint factory. If a Bitmint-Bill is reclaimed with a currency exchange request, then the BitMint factory will reconvert the Bitmint-Bill to real money trade the exchange with an associated bank where it buys the desired currency to the conditions of the money market.

8.2 Backing up Bitmint-Bills

Backup

Backing up your money is an absolute winning point of the BitMint system. In many publications of digital money, the duplication of the anonymous bills and coins is considered as major thread. A duplication would be considered as "printing digital money" because the bank is not supposed to distinguish between two incoming bills as long as they qualify to be genuine by the cryptographic checksum attached.

No risk to the bank

BitMint already explained in the BitMint online world that there is no such risk through the single-occurrence representation of a Bitmint-Bill in the BitMint factory.

If duplication is no problem, then a holder of Bitmint-Bills may move it to the BitMint online world. The Bitmint-Bill can be stored on private data storage (Home PC), in the cloud or on other storage. Of course it is highly recommended that a user protects the backup through encryption. Several applications will be available to provide a secure backup of Bitmint-Bills.

Restoring Bitmint-Bills

If there is a need to recover Bitmint-Bills, e.g. if a mobile device finally breaks, then the client may download his backup to the new device.

Since the old device might not have been broken, but is stolen, the legitimate user may send his backup in the BitMint factory and reclaim a fresh set of bills. Through the mechanisms of the BitMint online world the user cannot cheat by such refresh request while keeping the backup to pay a purchase. The backup is always on the level of the BitMint online world and any receiver of the money verifies the validity before closing a trade.

8.3 Deposit Bitmint-Bills in the cloud

A mechanism which is quite close to the backup of Bitmint-Bills is the "deposit"-use case. The idea of a money depot in the cloud (or as a service of the BitMint factory) solves the problem of keeping around large amounts of cash, in particular in unsafe environment e.g. touristic places with pick-pockets.

With a deposit in the BitMint online world, it is possible to keep only small amounts of digital money in direct access. A stolen mobile device with activated BitMint purse would not expose large sums of money.

Emergency PIN

To recall money from a deposit to the client's mobile device, it is common practice to enter a PIN. The idea of an "emergency PIN" would provide a second PIN which will also work like the original PIN, but in addition it triggers an emergency alarm in the BitMint factory and locks the rest of the depot. Other alarm systems and emergency calls can be associated with the reception of the emergency PIN.

Note: The idea of the emergency PIN is described in many publications and associated patents might be in place or even expired.

Money draft

A particular and attractive use case is the "Bitmint-Bill money draft" described in Money draft. Drafting money from the user's bank account and a particular money deposit in the cloud compare quite well. In both cases the user does not need to buy cash, but only transfers his already owned cash.

Bitmint-Bills are favored for this transfer.

Protect the Bitmint-Bills

With the idea of User assigned money it would be possible to automatically assign a money draft to a dedicated receiver. An attacker cannot draft money since he will not be able to spent it anyway.

As a consequence, even the classical attacks like the "PIN over the shoulder" would not work since the actual use of Bitmint-Bills is dedicated to only the owner.

Stolen Bitmint-Bills

If an attacker steals the Bitmint-Bill purse (e.g. the mobile phone) the user (whose phone was stolen) may immediately call a service number to disable the associated Bitmint-Bills. In the BitMint online world this would be a efficient protection to stolen money.

Offline- or Online world?

The task of cloud-based Bitmint-Bills deposit associates the question whether this is better made in the BitMint online world or the BitMint offline world. Then answer can be given rather straight.

Use the BitMint online world wherever the environment is obviously unsafe. It a mobile device is exposed to be stolen, emergency-disabling downloaded money is easier to realize in the BitMint online world because any trade with the disabled coins would before have to pass an associated online verification.

However, the BitMint online world imposes the risk of stolen Bitmint-Bills through malware. Hence the BitMint online world should be used in connection with Extended BitMint features like User assigned money. This delegates the responsibility of secure money to the Bitmint-Bills and not to the equipment which is hard to be verified as secure enough.

Using the BitMint offline world is very attractive, where the online conditions are bad. However, in this case, the user has to keep his electronic purse (e.g. mobile phone) as safe as s(he) would keep an actual purse. Fraud is possible for an attacker who steals the purse (= mobile device).

Hybrid approach

Another interesting choice is the hybrid approach which stores Bitmint-Bills in the secure element, but still implies an online verification for spending. Such tagged Bitmint-Bills can be invalidated in case of stolen equipment (e.g. mobile phone) but still be kept secure until they are spent for trade.

8.4 Using BitMint attributes

A Bitmint-Bill features Attributes attached to the value which may add particular features to digital money. The associated use cases apply the Bitmint-Bills attributes to the determine the context or purpose of digital money Out of many possibilities we explain two popular use cases in some more detail

- Control payment purpose
- User assigned money

8.4.1 Control payment purpose

There are many situations, where the purpose of payment shall be assigned.

- Parental control context → juveniles shall not buy liqueur or pornographic/violent media.
- Voucher context → money is assigned to be spent on a particular place. e.g. football game or a concert only.
- Therapeutic context → In cooperation with the client, the client might be restricted to spent money only in a pre-defined environment, e.g. a casino might be forbidden.
- Legal context → a government office might bind social support to a particular spending profile whereas the receive is only allowed to spent 10% for luxury but the rest to maintain life quality.
- Budget control → e.g. Parents want to grant her daughter student a particular budget to maintain life with organic food instead of conventional food. If this comes on top of a normal budget in contrast to a restriction, the present will positively stimulate the behavior of the student.

Many examples are possible. The examples do not claim a perfect technical coverage of the designated life aspects, however, in a majority of cases the mechanisms can contribute to the improvement of social life.

8.4.2 User assigned money

Threats on money transfer

User assigned money is in particular relevant for a money transfer in unsafe environment. If a particular receiver can be named for a transfer of Bitmint-Bills, there is a perfect technical evidence, that only the receiver may reclaim the package regardless from the potential fraud and wiretapping on the communication channel on which the money was transferred.

Reclaim process

It is assumed that such money transfer will finally arrive at the designated receiver. The receiver does have a trustable device which allows a regular reclaim procedure with the BitMint factory. To do this, the receiver shall authenticate to the BitMint factory as the legal holder of the designated money transfer. No other attacker in the insecure network will be able to reclaim the money package.

Receiver's mandatory online refresh

User assigned money acts like an offline-account, money is dedicated to a particular holder (account holder). User assigned money cannot be spent directly. Before it needs to be refreshed by the authorized holder to receive spendable bits without the holder designation.

Offline variant

In theBitMint offline world owner-tagged money may received through a secure channel from one secure element to another secure element. If the Bitmint-Bills are assigned to the receiver, they may be passed through several trusted environments (secure elements) until the receiver gets them. Only the receiver's secure element is able to lift the receiver's address constraint from the incoming Bitmint-Bill.

By this, digital money can be carried through several persons without the risk that one of the couriers would use the Bitmint-Bills.

9 Business models

In the following, we discuss some business opportunities that are associated to the BitMint system.

9.1 BitMint factory

The BitMint factory is a synonym for many possible BitMint factories deployed worldwide. There might be many reasons why these BitMint factories should be distributed, they would not even need to be synchronized to avoid collisions since the collision risk is extremely low as discussed in 6.3 "Collision Probability".

One system - different providers

However, BitMint factories need to be connected such that any Bitmint-Bill anywhere in the world being sent for refresh/reclaim can always be answered by the issuing BitMint factory. Finally, since Bitmint-Bills are only a representation of currency, banks will always be involved because they keep the actual accounts of their customers.

Bank's opportunity

Banks are also favored as associates of the BitMint factory and system because they do officially stand for the security of money which is important as long as any other representation of digital money is chosen. Despite his convincing and superiority, BitMint is no exception to the perception of trust through banks.

The BitMint factory (system) has several business opportunities

9.1.1 Float

What is float?

It is an old tradition that bank life from float. Float is profit which is made from temporarily available money. If people buy Bitmint-Bills for real money, this real money will actually arrive at the bank which hosts the BitMint factory. And this money can be used for short term investments (e.g. daily depot) which will buy the bank interest.

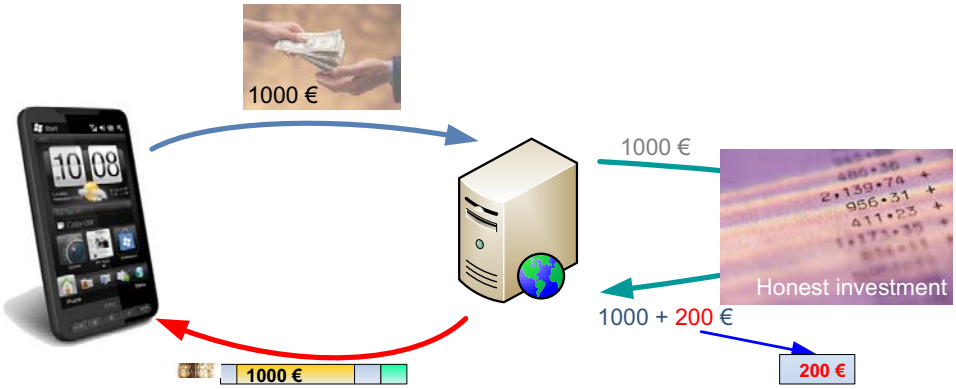


Figure 7 - Business Case - "Float"

Business Case

Living from this interest can be an attractive business case. While the float from the delay of money transfers (money stays some days in the banks) has become rather unpopular (in Europe laws forbid banks to make float) in the BitMint case it can be considered serious. As money in pockets does not pay interest, there will be a social acceptance for the BitMint factory's float business.

Advantages

In particular, if the BitMint does not activate other business cases like Subscription fee or Transaction fee the float is the most promising scheme.

For the user perception and acceptance the float business case might be the most attractive one because he can return a Bitmint-Bill for the same amount that s(he) bought the Bitmint-Bill. Since the float does not address a particular client, the business model is entirely anonymous, which is attractive for the use of Bitmint-Bills.

9.1.2 Subscription fee

Using Bitmint-Bills could be subject to a yearly subscription fee. This would make the BitMint system a membership model. For the ramp up acceptance of the BitMint system such a model would certainly affect the "use it by curiosity"-effect.

Acceptance factor

Since Bitmint-Bills live from the idea, that many people accept them, a slow ramp-up could actually spoil the entire idea. The model could be introduce with a "two first years free" policy.

In general a subscription fee recommended only as third choice, since the Privilege based subscription/transaction fee and the Float model do much better stimulate the user's desire for Bitmint-Bills.

9.1.3 Transaction fee

A transaction could be subject to a transaction fee and by definition this is a bad idea with digital money. Regardless from the actual value of this fee, even it is very low, it might keep off users to accept the system.

Best of fee based models

If a transaction fee is planned, preferably the retailer or the receiver of the money should be charged. This method is known from the credit card system and does not spoil user acceptance as the users make the majority.

Yet problems...

Yet it has to be considered, that unlike the credit card, Bitmint-Bills do not have a clear client/retailer relationship. Money transfer is independent from the role, hence there is an organizational challenge to setup a transaction fee system that is retailer-based.

Privacy threat

There is, however, a significant disadvantage to this business model. If there is a charge on a transaction, the transaction itself can be theoretically traced to the involved parties. Although this can be technically protected, users will always have the perception of being traced. In particular in the BitMint offline world such transaction would have to be linked to the Bitmint-Bills, which is a technical artifact, that spoils the pureness of the BitMint idea.

9.1.4 Reclaim fee / Printing fee

While the actual transfer and payment with Bitmint-Bills could be free of charge, buying new Bitmint-Bills and/or reconversion to actual cash could be subject to a transaction fee.

Stimulates BitMint

The advantage is, that this model stimulates the use of Bitmint-Bills and reduces the exchange of digital money to bank notes. Certainly this is not the best idea since it sacrifices the user acceptance, in particular in the ramp up phase.

Another option would also include the Online verification (get new Bitmint-Bill for an old one) which is an important step in the BitMint online world, however this is recommended second choice because Moving from world to another is one of the attractiveness factors of Bitmint-Bills.

9.1.5 Privilege based subscription/transaction fee

The BitMint system offers a large spectrum of Extended BitMint features. These features may even grow. A privilege based business case would only charge the desire for higher than the (free of charge) base functionality.

References

Privilege based models are often used in open source communities. The actual product is made free as open source software, where a company offers special services (stable versions, consulting, installation, add. tools) around the actual product.

As such these models are very attractive because customers really want to buy the additional privileges.

The disadvantage of these models is in the stronger unpredictability of the actual case compared to an expected transaction based model.

9.2 Which business model to use

In a first approximation we would rather be careful to activate the business cases of Subscription fee or Transaction fee. Many examples in the future were showing that free systems (Internet, Google, etc.) developed to a exponential acceptance just because they are free of use. There is, however, a big opportunity in business by associated services

Associated services may be offered by the BitMint factory but as well as by other service providers (e.g. cloud provider)

Recommended first is Float

From the user perspective, the Float business case will have best perception because the entire BitMint system appears to be with no additional surcharge. Hence the curiosity on a no-cost system will be high and the BitMint system can be deployed quickly.

The second best recommended business case relates to the Privilege based subscription/transaction fee. On a free system, users will be more willingly to pay for additional services but for the base use.

The other models do more relate to classical infrastructure. If banks with this infrastructure (eg. credit card system) find a way of application without affecting the attractiveness of Bitmint-Bills or by compensating the disadvantage through an associated promotion, these cases may live as well.

9.3 Other services

Other providers but BitMint-banks could charge other fees associated to the BitMint system.

9.3.1 Cloud-based backup service

The cloud-based backup service allows to Deposit Bitmint-Bills in the cloud. Cloud providers may offer special access systems to securely feed Bitmint-Bills from the deposit. The service can depend on local architectures (banks, public terminals, secure internet café) or other ideas (which shall not be anticipated). The basic concept and security of the BitMint system is not exposed to such offerings.

9.3.2 Secure money draft service

In unsafe environment, it might be of particular interest to people that money cannot be stolen but is available when needed. A secure money draft service may be booked to setup a list of features for exposed situations

- Emergency PIN
- Emergency PIN with follow up tracing
- Authenticated money draft
- Spending limitations
- Trusted third party service

Out of these examples we want to describe the "Emergency PIN with follow up tracing" in more detail.

Attacking

A person could be forced by a criminal to enter her/his PIN or authorization code to transmit digital money. Since with the outcome of digital money they attack scenarios might change this is a possible scenario in contrast to today's pick-pocket.

Emergency PIN

The victim could enter a working "Emergency PIN" which does about the same service of money transfer, but with limited amounts and in particular with a trace option on the money.

Money trace

If the victim is released, it could call an emergency number an activate the trace. (Before, it could be critical because the criminal might get evidence of the emergency PIN and threaten the victim in consequence).

As such, the traced money could be tagged "invalid" and the criminal is not able to use it, in particular if the money is sent in the BitMint online world. The criminal might be even subject to capture if the police system is sophisticated enough.

9.3.3 Transaction protection service

Trading with an unknown, untrusted merchant 8000 miles distant, a user might hesitate to send money over and at the same time the merchant may be reluctant to send merchandise until the customer paid.

Legal case

An associated service could act as trusted third party which confirms and guarantees the payment to the merchant after the merchandise was received. If the customer denies the reception, the legal fight might have to be taken as usual, however, whatever the court decides, the trusted third party can return the money to either side being found eligible due to the associated sentence.

9.3.4 Other services

More than the above services a likely to be offered. The need to be discussed out of the scope of this document, but the share the idea that a customer is willing to pay for an additional special service that can be realized with Bitmint-Bills.

10 Economical threats and opportunities

This chapter discusses the economical impact of a deployed BitMint system. While the acceptance of Bitmint-Bills is likely to depend on its Free-of-charge availability (→ 9.2 “Which business model to use”) those market players who are currently holding the business streams, will naturally percept a change to Bitmint-Bills from the perspective of their own business stability.

If Bitmint-Bills really come to work globally, and technically spoken they bring everything that will be required, there will be an impact to other systems - it depends on the actual attitude of concerned organization whether to see such changes as threat or as opportunity.

The following discussion focuses the roles of today’s major institutions in order to best address those roles for a peaceful introduction of Bitmint-Bills.

10.1 The role of banks

Banks are the preferred associates of the BitMint factory and system because they do officially stand for the security of money which is important in particular if any other representation of digital money is chosen. Regardless from its convincing parameters and superiority, BitMint is no exception to the perception of trust through banks.

Bitmint-Bills are no own currency

As Bitmint-Bills are only the representation of currency, they are not as much competitive to whatever is done with money today. They just transfer the flexibility of printed cash to electronic cash.

Hence the business case where people required printed cash will be affected by the possibility of 5.7 “Money draft”.

Banks can associate special services to security exposed money draft (like traveller’s cheques today). As their customers may be reached worldwide, Bitmint-Bills can generate a positive customer binding effect.

Currency exchange

Another positive effect relates to currency exchange. Banks can actually give out Bitmint-Bills to their customers in any currency and profit from the typical exchange rates. Again customers will appreciate to receive the service from their home bank in contrast of seeking any other foreign bank for draft and deposit services.

Final idea

Summarizing it appears, that the use of Bitmint-Bills is more an opportunity than any kind of threat to the banks, mainly stimulated by the idea of higher customer binding and the "no risk to the bank" feature of Bitmint-Bills.

10.2 The role of credit card institutes

Credit card institutes are associations of banks. Therefore the advantages described in "The role of banks" above implies the advantages to those who maintain credit card systems. Yet the idea of Bitmint-Bills is a debit paradigm. So the question is - "Will the comfortable use of Bitmint-Bills affect the versatility and popularity of credit card system?".

The answer seems to be two-faced. Regarding the payment comfort and features through its electronic appearance, Bitmint-Bill are supposed to become very attractive for the use of money transactions

On the other hand, the idea of a "credit" has very popular distribution, more in the US than in Europe, but the general idea of a solvency (within acceptable limits) should not be put in question through a use of Bitmint-Bills.

Bitmint-Bill credit paradigm

Therefore the idea of a credit line can be implemented in the BitMint system and the same business model can be kept upright with the versatilely of Bitmint-Bills. There it depends on the flexibility of the credit card institutes to make the best of the BitMint opportunity.

Little economical damage is expected due to the different initial paradigms credit versus debit.

10.3 Internet clearing system's reaction

The next big players that may be concerned are the internet payment systems. Bitmint-Bills are favored for electronic transfer and they offer some account independent transactions. Today, participants need to subscribe to payment services (e.g. PayPal), sometimes pay an associated fee for the service or a percentage when receiving money.

The Bitmint-Bill threat

With Bitmint-Bills, business transactions can be made by two parties without having to subscribe to any payment system. In particular the use in online systems makes payment quite comfortable.

Attacking online-Bitmint-Bills

It needs to be considered, however, that electronic money transaction of Bitmint-Bills will be very attractive to attackers who are going to reclaim/refresh such Bitmint-Bills instantly on the attack. Hence the person that pays will be attacked. The Online verification does not help because it is being redirected to the attacker's advantage.

It follows that the **transmission of Bitmint-Bills needs to be secured**. Bitmint-Bills beyond the protection of secure elements are always an interesting point of attack.

The opportunity

Several countermeasures can be provided (e.g. holder's encryption). The "PayPals" of the future could pick up that issue and provide secure services for the online money transfer. The subscription model might be replaced by a scheme that allows transferred of Bitmint-Bills only on behalf of the two persons involved in a business.

As such, these services could act in the role of a trusted third security party that technically provides the transfer mechanisms and from an economical point of view - could insure such transmission that people can be confident on a safe electronic transfer.

As an internet payment service has the connection to a user's account another possible business direction could be that customers can use this service to buy Bitmint-Bills whenever they need some at any place worldwide.

11 Summary

In our quest for the ultimate digital money we did not expect any system to survive our hard claims. Finally there was one candidate to overperform our filter and we identified BitMint as the only candidate qualifying as a universal digital representation of worldwide currencies. This lead us to further investigation about BitMint's nature and features.

BitMint is a new idea of digital cash. It breaks with all historical conventions of secure money. It solves the "change" problem. And it offers more than just money. BitMint is not a currency on its own, it only is meant to be a cash representation of any existing currency. The advantage is, that Bitmint-Bills do not have their own exchange rate and profit from the stability of their associated currency. Yet the most important advantage of BitMint is its technical attractiveness that there is no risk for the bank. This can be guaranteed.

BitMint is not competitive to bills and coins but it accomplishes aspects that cannot be solved with bits and coins. As such it is supplemental to classical bills and coins like the credit card was when it arrived many years ago. Physical cash in the appearance of coins and bills will still be as attractive as ever before since they address a very instant value exchange that is unique to live without batteries and electronic devices.

BitMint can be competitive to credit cards but it can also accomplish things that credit cards may be dreaming of. The idea of a credit system, realized by cards or digital coins, can have its place in the money market regardless from the representation of money.

Whether to be competitive or cooperative to existing payment systems depends on the integration of BitMint virtual coins and bills into tomorrow's life. Threat or opportunity - it all depends on how BitMint will be acquired in the future and who takes it first to go the steps forward in tomorrow's payment society.

And as it is well known, that "Tomorrow never dies ..." today is exactly the right time to check out what an ultimate solution to the question of digital money may promises for tomorrow.s