

Φ BitMint Mobile

Pay and Get Paid Through Your Phone

Presented by:

The BitMint Team

Amnon Samid, CEO

Amnon@BitMint.com * +972-544-200-400 * 1-571-214-9814

Vision & Strategy

BitMint Mobile is a major component of the global BitMint vision which is based on the realization that money is about to climb into the highest rung in the ladder of abstraction. What started as barter, and continued to weighing precious metal, then to official coins, followed by paper, is now about to leap ahead for the last time. Money is about to assume the form of a binary string, which is media independent, and native to electronic communication. In this new form, digital money, will assume a profound impact on human economies, human societies, and general welfare. One aspect of this grand vision relates to retail, consumer, and general money exchange between friends and strangers around the corner or around the world. Digital money residing on ubiquitous intimate devices, serving as wallets, will exchange money with similar devices everywhere.

The bulk of payments today is in the category of consumer to merchant. In the developed world such payments are by far based on payment cards, while in the third world, these payments are cash based. The vision that underlies this business plan is that in both

categories digitized currencies exchanged between two ubiquitous intimate devices (wallets) can and will take over.

In the developed world the card-based payment is controlled and dictated by Visa and MasterCard, aided by American Express and Discover. It is a mature industry, indeed old. These networks have been very successful in dragging the 'plastic card' introduced in 1958, well into the early years of this century, but technology has finally changed the landscape. Everyone has a cell phone, which is sufficiently advanced to exchange data and money, and which has a much greater computing capacity than any plastic card (EMV included). The dominance of the networks allowed them to squeeze merchants and consumers alike with ever-increasing transactions fees, which further builds an incentive to shift to another payment platform. An efficient digitized cash solution will bring a much-needed relief to thousands of merchants and millions of consumers. This is especially so for small ticket retail, where the new Congressional Durbin amendment levees a choking fee on the merchants.

In the underdeveloped world, banking and financial services are lagging, and the vast majority of payment activity is cash based. This massive trade will be easily exchanged with cash-like virtual currency conveniently stored in mobile devices. Countries in Africa, Asia, and South America will welcome a phone-based cash-like solution. In fact the vast majority of these countries are steeped in cell phones, and already have all sorts of SMS based payment systems.

The idea of BitMint is to apply the far-reaching general concept of BitMint money, as expressed in the granted and pending BitMint patents, and use it for the rather narrow application of phone-to-phone payment with the mint as the only authority, no proxy, and no partners for the basic money exchange. The inherent robustness of the BitMint currency will endow this solution with the winning advantages as it competes with other SMS, phone-to-phone payment systems.

Technology

The BitMint concept is bold and far-reaching. It reshapes money in its highest degree of abstraction: a string of bits. This string of “ones” and “zeros” is media independent, and it flows naturally through the veins of the Internet, and through the myriad of all sorts of communication channels crisscrossing the planet. It allows for money to be stored, millions of dollars on a pinhead size memory, and it makes it possible to backup one’s assets, and safe keep them with the most powerful protection ever devised: encryption. Modern, state of the art, super powerful encryption technology is available to anyone, practically for free, and its protection is more effective than tall walls, steel locks, and battalions of guarding soldiers. Much as the scales, with which traders weighed precious metal as money, greatly impacted ancient economies, and old cultures, so bit-string money will impact payment and banking reality. And as much as minted gold coins improved on the scales and weighing technology, so one would expect a dramatic improvement upon the introduction of bit currency. And as much as banknotes have revolutionized commerce compared to the bags of coins lugged around, so it is prudent to expect that digital currency will revolutionize the reality of trade and exchange, on a global and local levels, for macro as well as micro payments.

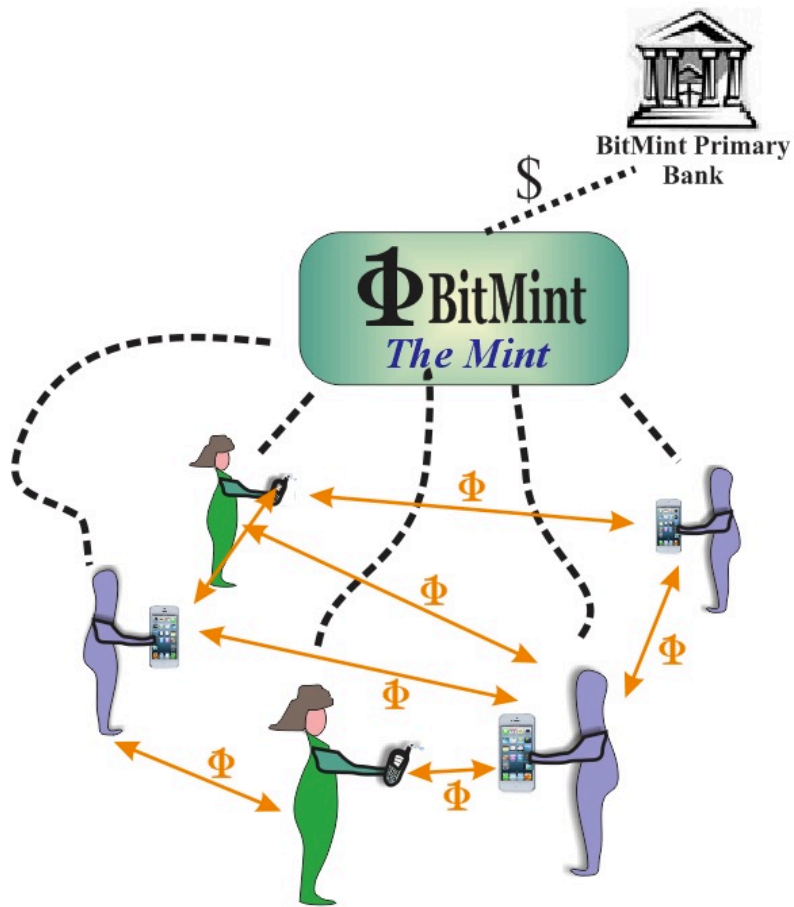


BitMint is NOT Bitcoin

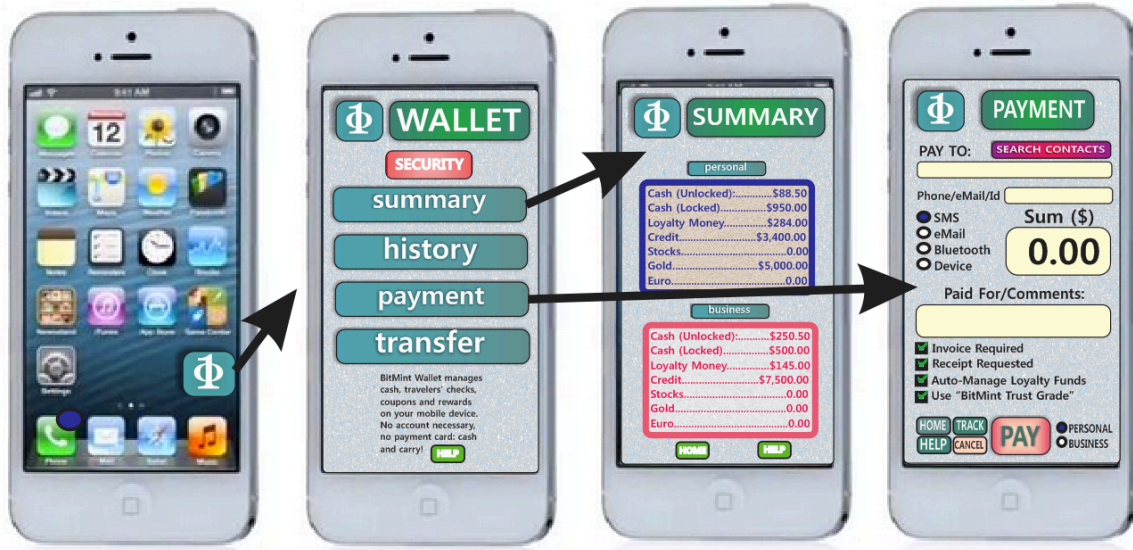
Bitcoin having risen to become the most notorious digital currency – it may sow confusion as to the distinction between it, and BitMint. Despite some name similarity the two entities are very dissimilar. Indeed, they are both digital money, namely expressed as a media-independent string of bits. However the Bitcoin bits are determined by a complicated algorithm designed to insure that fraudsters will not be successful in constructing fake Bitcoin coins, or double spend a bona fide Bitcoin coin. Trust in these algorithms creates value for these strings. The fundamental vulnerability of Bitcoin is the unproven robustness of these algorithms. There is no mathematical proof that assures anyone that a hidden flaw will not surface tomorrow and all the assets vested in the underlying algorithm will melt away. A more prosaic threat appears in the ‘brute force’ of governments and central banks that are not likely to allow their citizens to replace the national currency they control with a new money they can’t control. By contrast, BitMint digital money is nothing more and nothing less than digitized US dollar (or any other currency, or traded commodity). A BitMint string worth 1\$ today, will be worth 1\$ tomorrow. The BitMint string may be regarded as an IOU note, if you will. And as such it does not compete with the dollar, it simply facilitates trade with the dollar.

Why the Phone?

A mindful study of today’s payment landscape clearly points to the omnipresent, ubiquitous cellphone as the modern wallet. This conclusion is equally valid in the developed world, as much as in the undeveloped world. In the latter, phone-payments score big against the only other alternative: old fashioned hand-to-hand cash exchange. In the former, the quintessential credit cards are virtually stuffed into the phone, much as yesterday they were stuffed into the old worn leather wallet. To load the modern smart phone with credit cards is like pulling a motor vehicle with a bunch of horses. The phone has much more computing power than any card will ever have. It has the keyboard, the screen, the familiarity to receive an invoice, send payment, receive a payment, send and accept a receipt, and organize the daily transactions in a perfect efficient order. The phone is inching its way to become the unchallenged modern wallet.



Below is an example of the operating screen to be used by the BitMint Mobile users:



USE

We consider:

- friendly daily exchange
- consumer-merchant experience
- occasional long range stranger exchange
- cross border remittance
- charity
- taxes, tolls, fees, rebates

A brief description of these applications follows: a friendly daily exchange is the person to person occasional payment. One borrows some cash for a day, two order a pizza together, three rent a car for an excursion, a parent passes some spending money to her teenage child. These are all examples for handing over small amounts of money from one friend to another where neither one is a merchant, nor has more than a smartphone for the purpose. Today, the only practical way to effect such occasional payments is with cash or with checks. Most of us don't use checks almost at all, and we certainly don't carry around a checkbook. Cash may still be found in worn leather wallets carried by the older

generation, while the young ones simply do away with the inconvenience of paper bills and metal coins. So while this marketplace is limited, it is an uncovered niche for which BitMint has no competitors.

The consumer-merchant marketplace is by far the largest and most lucrative one, but unlike the former case, is a very competitive field. The well-heeled and long time established networks have dominated this section for decades, and have been impressively successful in remaining on top despite some serious technological challenges. They have the means and the motivation to defeat any challenger. From a marketing standpoint the BitMint approach depends on the market. In third world markets the networks have poor presence, and BitMint will face cash payment competitors offering a variety of SMS based payment solutions. In the developed world, the BitMint campaign is based on the cost difference to the merchant. The networks, exploit their dominance and overcharge and the merchants are desperate to find an alternative, which is what BitMint offers them. No doubt that penetration will be a painful issue, but we have devised a mechanism to exploit the consumer-merchant market without penetration.

Occasionally the Internet brings together far away strangers who wish to enter into a one time transaction. If the seller is no merchant, then check-in-the-mail used to be the only viable alternative to BitMint. PayPal exploited this shortcoming, and is now a huge player. BitMint intends to go further than PayPal, requiring no account registration.

Cross border remittance is half a trillion dollar marketplace world-wide, now dominated by Western Union and MoneyGram who overcharge their customers. The BitMint alternative will have a lot of profit margin to compete with. Yet, there would have to be a per country investment – a local reference bank to carry out the exchange with.

The charity money flow today has a fundamental problem: a large share of the contribution at hand, is directed towards management comfort as opposed to direct help to the needy. The reason is that the money in total first flows to management who then decides on its distribution. The BitMint solution allows for money to be SMS-ed or

emailed directly to the needy. In the future the concept of tethered money will be applied and further offer efficiency to the charity business.

Taxes, tolls and fees: various government taxes and tolls will most comfortably be paid by SMSing the money to the indicated number.

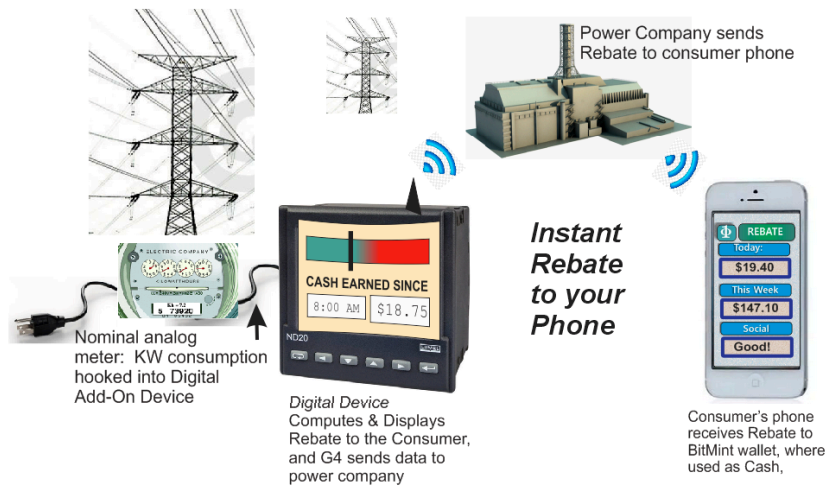
The government is fond of using the tax code to influence public behavior. The result is a bulging, out of control tax code, and questionable results. Using the effect of instant rebate flashed into the consumer phone, ready money – the effect might be much more pronounced. For example, residents who will not set up the thermostat above a

predetermined high-value will be paid a weekly ‘thank you’ money from the government.

Consumers who will use washing machines and dish washers and other high consumption

devices at night time, off peak hours, will see a daily rebate from the

power company. Attendants to a meeting regarding public safety will see a payback, etc.



The Power Company Shares Savings due to optimal usage

Scope, Potential, Vista, Boundaries

The prospect of becoming the mint to the money of the 21st century is quite overwhelming, and admittedly, may sound delusional. We don't envision BitMint to issue all the money in this century, but we do have high hopes for the BitMint platform to prevail as the procedural solution for digital money. We invest our time and money convinced that BitMint, at the end of the day, will serve as the preferred protocol for

digital currencies around the world. The lasting, super-secure attributes of BitMint are not readily understood, but they are there, underlying this high ambition. Having interviewed the BitMint team for an hour and half, overseeing the assigned patent examiner in the US Patent office in Washington DC, the patent supervisor reacted; soon thereafter : *“I have been many years here, and I have not seen something so innovative”*.

When the President and CEO of Giesecke & Devrient, Dr. Krasten Ottenberg, was briefed on BitMint he quipped: *“This is as large as Facebook!”* We have been discussing BitMint with the Federal Reserve, the Bank of Canada, the Bank of China and others. In its full scale we envision an *“Intermint”* that would connect various mints, some issued by governments, some by commercial banks, and industrial corporations.



The web of mints will be comprised of various implementations, of different flavors, and colors, but the simple robust principles of BitMint will underlie them all. In the long run the BitMint concept will sell its proven intellectual property to some, will build turn-key mints to others, and will run mints elsewhere. BitMint is designed with global exchange in mind, with micro and macro payment under consideration, and with utmost regard to the super critical issue of security.

It is therefore that we at BitMint wish to engage with partners that would share the vision, possess the imagination, claim the daring and boldness needed for something so ambitious. Building each step on its former, we intend to prove our way to the full vista of our present vision, and the full reach of BitMint as it evolves in the coming future.

Competition

Superior competition can never be discounted. A more innovative, creative, and imaginative team may offer a better solution to the challenge addressed here, and steal the show. But that fear always applies, and unless there is a clear sense of what such superior competition would be, this risk should be borne as is. Analyzing the spectre of competitive solutions for payments we may distinguish between the developed countries and the third world. In the former case payment languishes under the choke-hold of the major networks (Visa/MC/AmExp). The payment card is ubiquitous, and well entrenched since 1958 when it was first introduced. The system has evolved in complexity, and the necessary payment settlement cycle involves so many parties (all of which expect to be paid) that the burden on the merchant, and hence on the consumer is of such magnitude that the search for an alternative is very aggressive. The world largest retailer, Walmart, has initiated a merchant-wide effort dubbed MCX and aimed at breaking this choke-hold. Others aim for the same. Both the networks, and the alternative seeking efforts are important serious competitors for BitMint Mobile. Why would BitMint prevail?

- Simplicity
- Speed
- Convenience
- Universality
- Security
- Controlled Anonymity

Simplicity: the BitMint concept distinguishes itself in its simplicity. Bit money is purchased from a single source, BitMint, and redeemed there too. BitMint is universally accessible, it works with one primary bank, and any settlements and dispute resolution happen within the BitMint framework, and not via a host of issuers, acquirers, processors, networks, and settlement banks as the case is in the prevailing regimen. It is hard to overemphasize simplicity as a business success asset.

Simplicity also translates to **speed**. Since there is no settlement cycle, there is no settlement delay. In maturity BitMint will work with a delegated hierarchy of authentication nodes so that no meaningful delay is expected for concluding a

transactions. Also, BitMint transactions, for the most part, will be concluded on the basis of a cryptographic dialogue between payer and payee, without the need to wait for a remote authentication center to bless the transaction. This fact implies instant transactions for most cases.

Convenience: BitMint Mobile transactions regard the phone as the wallet, and the money inside the phone as paper bills and coins found in the old fashioned wallet. This spells a conceptual convenience: you pay with money that you hold in your wallet. It's universal cash, simple and convenient compared to a host of payment cards, each stored in the phone (as many solution proposals advocate today). Because BitMint money is a string of bits, it is convenient to pay or get paid whatever the connection: IP, IR, Wi-Fi, NFC, Bluetooth, or anything else.

Universality: BitMint Mobile is a facet of the BitMint platform which amounts to elevating money one more rung in the ladder of abstraction. The digitization of money by BitMint refers to paper money, as paper money refers to gold coins, and as gold coins refer to weighing precious metal with a scale. In short, shaping money into a media independent string of bits, adapts this entity into the modern construction of a communication web, creating new vista for payment, money flow and money storage. The BitMint concept is larger than an easy way for consumers to buy clothing, or furniture. It is universal: it is a way to store money, make macro payments, and exchange values in forms never tried before. This broadness and this universality are the fundamental edge enjoyed by BitMint over the host of quick merchandizing gimmicks that stack up as competition.

Security: payment today is account based, and software negotiated. What passes between payer to payee is not money but software instructions. The payer responds to an instruction to decrement the number representing his available funds, by, say \$10.00. While at the same time a corresponding instruction has the effect of incrementing the number representing the credit available to the payee by \$10.00. For these two transactions to work it is necessary for both payer and payee to expose their identities and their accounts, regardless of how small the transaction. This exposure is the root of

vulnerability that leads hackers to swarm around the business area and steal the attributes of the transactions so that they can abuse the system and fake fraudulent transactions later on. It matters not whether the bank pays back the consumer, or not – cyber stealing is damage that is borne by somebody in the system, and by the end of the day is being paid by the consumer. In particular, a pesky challenge today is to conclusively identify the cyber identity of a party. There are clever ways for a hacker to represent himself as someone else. Fundamentally these vulnerabilities vanish in the BitMint regimen. The money flows from one phone to another, not from one account to another. The recipient needs only to verify that the bits received by him are valid money – regardless of the identity of the payer. The authentication of the payment is provided by one responsible authority – the mint -- no confusion, no shared responsibility. Because no remote account is involved, it is possible to effect the payment by a simple dialogue between payer and payee, voiding the need to wait for any third party before concluding the exchange. BitMint money can be secured as electronic travelers' checks, and therefore one's phone may contain a large amount of money with no risk of loss. This, in turn translates to transaction readiness in times when the networks are down.

Controlled Anonymity: in account based transaction the account owner is eventually identified, and anonymity is only an illusion, in most cases. Also every transaction amounts to money hopping from one known account to another – no anonymity. In the BitMint solution money held in one's phone may be split, and transferred to another, who in turn may transfer it to a third party, etc. No authentication may be invoked, and no exposure of the money flow – anonymity per se. On the other hand, BitMint regimen may be applied with transaction tracking cryptography so that each and every movement is captured and identified. In short, BitMint may adapt to the prevailing laws and regulations and provide as much anonymity as the authorities allow, and no more.

On a broad general view:

BitMint – the idea that one's phone becomes one's wallet is so much more appealing than the age-old idea of carrying around a bunch of plastic cards (sophisticated less – magnetic stripes, or sophisticated more – EMV), whether these cards are put in a leather

wallet, or in a phone wallet. A card cannot compete with the computing power of the phone. The modern cell phone is ubiquitous, intimate, and useful. In our modern culture the phone is our natural wallet, and a string of bits are natural money. BitMint is well positioned to prevail.

Phase I Per-Se Competition

The BitMint Mobile Phase I is focused on offering a simple, easy, convenient, versatile and secure payment between friends, strangers and between consumers and merchants – based on the phone as a wallet. The competition comes from banks who have recently marched into this space (e.g. Capital One); from PayPal who became a huge player by offering simplicity, security, and convenience for friends and strangers to pay each other; from giants like Google who burst into the market with a proprietary wallet; from start-ups like Square who designed a convenient piece of hardware to render the phone into a wallet, and from smart POS terminal companies, like GoPago, who also enable the phone as payment device; from ‘gimmick’ oriented companies like Starbucks who use facial photography, and ‘find friends’ phone option to smooth up the payment process; from large ecosystems like Amazon and Facebook who mint their own coins, and trade with their own currencies. In the third world competition is robust and strong in the form of token based SMS payment systems (e.g. Kenya M-Pesa). The field is crowded, why should BitMint succeed?

BitMint is the only payment solution, which is *cash-like* because with BitMint you *pay and forget*. All the rest, all the other payment solutions eventually rely on a payment card, and several weeks down the road you are obliged to review a statement that contains your purchase today. You are expected to remember shopping that day, and buying what the statement said you bought, as well as paying what the statement claimed you did. This is a burden that is more and more unacceptable for smaller and smaller purchases. When you check out a DVD at Red Box, you use your credit card, and you pay \$1.27 if you return it by 9pm the next day. Some three weeks later you will see a

statement from your credit card with a line item for \$1.27. You will have to scratch your head, what is that? And once you find out – is that charge legitimate? Did I rent a movie on that day? If you use your card in a small bar downtown, chances are there, for the owner to charge you for more drinks than you consumed, and perhaps on a day you have not frequented the bar. The sums are small, and you are likely to not dispute anyway. But with BitMint you pay digital cash on the spot. You receive electronic receipt right away, and you never ever see an invoice, a statement, a demand to pay of any kind. So sleazy vendors cannot cheat you, and admin errors cannot cram up. Moreover, recent US laws allow the network to squeeze high surcharges from small transactions, and merchants are eager for a payment replacement.

PayPal rose to prominence by allowing anyone with an email to become a payment partner. BitMint goes a step further and allows anyone to deal with BitMint cash – no BitMint account needed, email address is helpful, but not necessary. BitMint money can be printed out in bar code, then read back into an electronic device. If you have a cell phone, and you can send and receive SMS – you are on!

Phone based payments in the third world rely on a network of agents who supply tokens to represent money and value, which in turn is SMSed between traders. While these procedures look somewhat similar to BitMint they lack the theoretical foundation for security and convenience offered by BitMint. On the other hand, the BitMint concept will be seen as familiar.

Unlike Facebook and Amazon money, BitMint digitized dollars are universal, and as more and more people and merchants accept them, the more ubiquitous it becomes. Add to this the super security, the tethering, the convenience, and BitMint rises above all its competition, hands down!

Competition beyond Phase I

The conceptual competitive map may be charted according to (i) technology, (ii) markets, and (iii) regulatory compliance.

Technology: The technology aspects of competition may be analyzed according to (1) money representation, (2) money in storage, and (3) money in motion. Each of which may be analyzed per (a) convenience, (b) cost, (c) security.

Conclusively all the traditional competitors represent money as a numeric value held in a computer addressable memory. This means that anyone who managed to hack his way to administrative role in that computer, will have the power to change the number that represent money. Such modification is tantamount to stealing all the money in that computer. By contrast, BitMint represents money as a string of bits. A hacker who changes the bit identity – does not steal the money, he destroys it. Alas, BitMint money may be backed up as many times as desired, and the identity of the money bits may be protected by mathematically secure ciphers, which are guaranteed not to yield to cryptanalysis. This is a fundamental advantage for BitMint over any and all its competitors. Using the common technology of cryptographic hashing and ‘signing’ BitMint money transfers and money storage may be made as secure as desired, and clearly not trail behind any other money transfer or money storage scheme. Cost is comparable.

The non-traditional competitors are the cryptographic currencies (e.g. Bitcoin) which are based on algorithms that may be breached tomorrow. These are speculative currencies. They attract many on account of their anti-government appeal, but they are not serious contenders to replace money as we know it.

Market: In the retail industry the networks and their payment cards rule the seas. In the macro payment, B2B, the banking industry is king. Both dominant forces will not welcome the BitMint innovation. They might use their muscle to suppress it, and therefore we need a high profile partner. In head to head competition, BitMint plans to claim its growing share employing the following strategy: retail – viral growth. One by

one merchants will realize that their competition which signed on to BitMint is by passing the choking interchange fees and transaction fees that the network exact, and more and more will migrate to BitMint. In addition we devised a mechanism to allow consumers to buy from merchants who only recognize payment cards. Basically the idea is for the consumer to trade his BitMint money against a one time branded payment card number that would be acceptable by the merchant. As to the macro payments, the electronic traveler's check option of BitMint will attract merchants to keep their money, highly protected, encrypted on their own computers, rather than risk a bank default, especially as long as the interest on deposits is virtually non-existent. In addition, the ease of emailing money at any sum, as an email attachment, will attract businesses to the BitMint platform, and will put the pressure on the banks to follow suit. In fact, we expect that after an initial attempt to suppress BitMint, both the banks and the networks will change course, and move to acquire a stake in the new technology.

Regulatory Compliance: The financial regulatory arena is highly political, and any new comer should be duly concerned as to the eventuality of being choked by heavy-handed new regulations designed to protect the powers that be. We intend to meet this challenge by acquiring high profile partners and advisors, and by maintaining geographic flexibility as to where we should start.

Appendices

Selected BitMint Attributes/ Aspects

Payment Technology and The Payment Card are Getting a Divorce And Look Who Is Getting Married!

“Plastic” -- that is how the familiar payment card was called -- was introduced in 1958! Think about it, more than half a century ago! Three years later the IBM Selectric typewriter was introduced. Technology has long buried the latter, how long before “plastic” shares this fate? Over the many decades since its introduction the plastic ‘scheme’ bulged in complexity, and amassed half a dozen players: the consumers, the merchants, the issuers, the issuers processors, the acquirers, the acquirer processors, settlement banks, and the networks with their ever more complicated rules. Small wonder that hackers poke holes; card data is routinely stolen, and millions are sucked away. Using plastic one has to first authenticate the card -- that it is bona fide, then to authenticate the card holder -- that he or she are bona fide, and finally to secure a promise to pay, regardless of what the consumer will do later. Hackers have a choice where to come in.

For how long would commerce wait for payment technology to catch up? The Internet allows for merchants to showcase their merchandise in rotating high resolution colorful displays, presented with a full list of specification and attributes. Utility vendors provide comparable pricing, and crowdsourcing packages tell the consumer and the merchant what others are thinking of the same purchase. All is done from home, online, fast and open. And when all is said and done, the consumer is held up with a barrage of stupid questions about his mother’s maiden name, and the city where he was married, often to be falsely rejected because of some overeager suspicion algorithm. Why? Because the card, and the presenter of the card, and the promise to pay, are all part of today’s scheme. The pressure is on, relief is on its way.

What comes around, goes around. Before plastic, trusted customers have simply drawn a “promise to pay” (the familiar check), and walked away with the goods. The check was cashed a day later. That is exactly what BitMint does today using modern cryptography. The paper check is replaced by a string of bits, the presenter of the string proves his bona fide cryptographically, and walks away with the goods. Consumer and Merchant exchange a lightning-fast bilateral crypto-dialogue, and no one is held back with stupid questions as with card technology. And if the buyer chooses not to present his crypto-bona fide, or they are not established yet, then the merchant will instantly send the money (the string of bits) to BitMint for authentication. Just the money (not the identity of the payer), and just to BitMint (no arduous settlement cycles between issuers and acquirers), as it should be. No interchange fees, no transactions fee, no penalty for stepping out of a security code.

The plastic card was invented almost a decade before ARPA started to link networks, and establish the Internet. Isn’t it time for payment to be reinvented with an Internet-compliant

format: The “blood” that flows in the “veins” of the Internet is ‘strings of bits’ -- which is exactly the form of BitMint money.

Payment technology and plastic enjoyed a long and good ride together, but they have reached their limit. A divorce is inevitable. Payment technology has a new suitor: digital currency. Watch for the wedding invitations, coming out soon!

On BitMint Security

BitMint, like any digital currency, immediately lights up the warning signs: security... With all the nice things that can be done with digital money, is it not going to be too risky, too easy for fraudsters to abuse? After all, we have a hard time insuring that paper bills are not counterfeit, how much more challenging is it to prevent bits from being modified, distorted, faked?

Good question. So good that it alone should disqualify Bitcoin, PPcoin and all other ‘*algorithmic*’ currencies. The mathematics of these currencies is daunting, and creates the impression of robustness. Alas, these obscure algorithms, steeped in math as they are, are, in fact, completely naked, in terms of having absolutely no shred of proof that they are effective in what they are designed to do. No reputable cryptographer claims that these algorithms are unbreakable, or are so robust that, he, the cryptographer, will bet his personal wealth on. Neither should you. One need not go any further: algorithmic money is not secure, and should be disqualified.

So how is BitMint different? What is so special about BitMint that allows it to survive where all the algorithmic money fails? The mint that issues BitMint money does not rely on any breakable algorithm. BitMint money is generated through a quantum mechanical purely randomized process. The BitMint money bits are guaranteed to be void of any identifiable pattern, or order, or formula to be cracked. This guarantee comes with the full faith and credit of quantum physics -- the predominant physics of the last 100 years, the most successful theory of science ever. It does not get any better than that.

Now, BitMint procedures use a hefty amount of standard cryptographic tools, that is a fact, but these crypto measures are employed for securing money on your phone, safeguarding a payment in transit, and insuring integrity in various monetary procedures. All these measures protect the BitMint traders. But the value of the money itself is based on the inherent equivocation offered by quantum mechanics, not on any not-breached-yet-algorithm, which will be breached tomorrow. A fraudster that can fake a hundred dollar bill, can eventually debase the currency, and steal anything on sale, offering his counterfeit currency -- that is fundamentally dangerous. But a robber who broke into a safe, and stole the hundred dollar bills in it, can do much less harm. In the digital world of BitMint -- the faking of the currency is protected with the total credibility of quantum physics, and the cracking of a particular safe deposit box is protected by state of the

art cryptography -- boosted by the equivocation of the data. The latter is a fairly technical point which is hard to reduce to a couple of sentences: cracking modern ciphers is based on exploiting subtle patterns in the original data. However, the data that is used to express BitMint coins is totally and completely patternless -- subtle or otherwise, and hence it resists cracking, the way a hard, smooth vertical wall will prevent even a skilled climber from climbing on it. A good climber will exploit tiny cracks, and small protrusions in an otherwise smooth wall, but a completely smooth wall can not be climbed. Similarly BitMint coins resist the efforts of the most powerful crypto-busters.

BitMint is a closed system: you buy the bit money from the mint, and the mint is where you exchange those bits back to dollars. This fact all by itself should placate security worries. It's very easy to write a play and mark it "written by Shakespeare". Quite a few will be fooled by it, but clearly this fraud will not work on Shakespeare himself. Similarly, the mint knows what it mints, and while it is easy to come up with a BitMint coin look-alike, it won't fool the mint.

Security defended and argued with high-tech concepts like 'complete randomization' and 'absence of pattern' require a considerable measure of thought to be convincing. If you wish to enjoy the many benefits offered by BitMint digitized dollars, then invest in convincing yourself of the top security of the money.

Why BitMint, and not any other Digital Currency Solution?

When it comes to digital currency, the question is *who has the best concept?*

Digital money is a media-independent string of bits that is comprised at a minimum of an indication of value, and of an indication of bill-identity. It's obvious that the string will carry its denominated value -- otherwise it is not money. It is equally mandatory for the bit-string to carry a unique identity -- otherwise double payment cannot be prevented.

So, when Alice pays Bob, say \$10.00 by sending him a string of bits. Bob examines the string, reads its denominated value and its identity mark, and then he applies some validation algorithm to satisfy himself that the string is bona-fide.

This validation algorithm cannot be kept a secret, because every payee will have to apply it to validate the money he or she is being paid. The validation algorithm analyzes the pattern of the identities of the bits to verify that it complies with certain rules, and hence is a valid, not a fake, 'coin'.

Whatever the pattern, Fred, the fraudster, knowing the validation algorithm, may construct a string of bits that will pass the validation test. Since Fred knows what exactly is the validation algorithm he can try to fool it, test his trial, try again, test again, until he has a "hit". Regardless of how complicated the algorithm, Fred, using mathematical insight in combination of

increasing computing power has an *unbound probability* to satisfy the validation algorithm. And what is more -- as this currency becomes more popular, and more people use it for ever larger amounts -- Fred's incentive to cryptanalyze the currency is proportionally rising. So just when more and more people rely on this money scheme - one of the many hackers who would attack it, will eventually break it.

And when broken, Fred could construct a string of bits, and pass it on as good money. It's going to be a disaster, because it would not be immediately obvious that one could fake money out of thin air. The fraudsters would silently corrupt the integrity of the digital money, leading to a catastrophic collapse. The consequences of this collapse will be more pronounced, the more popular and wide-spread the system is when it happens.

That is the background on which BitMint was designed.

The foundational premise for BitMint is that any bit pattern that satisfies a validation algorithm may be faked -- *it can't be helped*. So BitMint grabbed the stick from its opposite end: the BitMint coin -- the BitMint bit string -- is utterly patternless. It is strictly and completely devoid of any pattern whatsoever. Here is the clincher: *you cannot find a pattern in a patternless string!*

In fact, the ultimate BitMint design calls for two tiny sources of radioactive material monitored for their activity. For the first source, every nanosecond, when the radiation count is larger than the previous nanosecond, is marked as "1", otherwise, it is marked as "0". For the second source, the opposite would happen. The two streams would then be XORed. The full faith and credit of Quantum Physics guarantees that such a bit string will be of maximum entropy -- of zero pattern.

And since there is no pattern to be second-guessed, the probability hurdle faced by Fred is bound -- *bound!* -- at a laughable negligible measure of 2^{-n} , where n is the bit count.

This is the fundamental superiority of the BitMint solution for Digital Money. The mint is not vulnerable to any future mathematical insight, nor to the specter of super fast computers. As long as the integrity of the mint is preserved -- the money is good, and can't be faked.

And more: since the raw money is totally randomized, not pseudo-randomized but truly randomized, it is the most desirable input for any cryptographic vault in which a user might choose to keep it. You cannot crack a full-featured cipher, regardless of its math, if the input, the plaintext, is totally random.

So the mint is mathematically secure, and the money traders are cryptographically secure.

As soon as the supervisor of the patent examiners in Washington DC understood this point, he quipped: "*I have not seen such an innovative idea in so many years that I am here, examining financial patent applications.*"

When Dr. Karsten Ottenberg, the physicist CEO of Giesecke & Devrient was briefed on this very concept, he wasted no time recognizing its profound business potential and boldly directed G&D

into a contractual partnership with BitMint, LLC. The merit, and the superiority of the BitMint concept has been recognized by the highly regarded technology experts of Giesecke & Devrient when they awarded BitMint the first prize, among twelve finalists invited to Munich, following an international competition for financial innovation.

Rarely is there such an a-priori clear-cut, mathematically backed, advantage to one solution over all others. Take your time to internalize the implications, and then ask yourself: *how can I be part of this unfolding saga?*

References

1. US Patent #6,823,068 The Cryptographic Foundation for BitMint Security
2. "Tethered Money: Digital Currency & Social Innovation" G. Samid, DGS Vitco, 2013
3. "The Battle of the Bits" Lind Pauch, Digital Transactions, June 2013
4. "Digital Currency" cover story, Digital Transactions, July 2013
5. The BitMint website (www.BitMint.com)
6. G. Samid 'BitMint v. Bitcoin' YouTube <http://youtu.be/RuFTGcfh0WE>
7. "Governments Must Co-Opt Bitcoin to Avert Disaster" G. Samid, "The American Banker" June 2013
8. The G&D Website: <http://www.gi-de.com>
9. "The Smartphone Wallet: Understanding the Disruption Ahead" David W. Schropfer TLG Books.
10. "US Payment Handbook" Ben Love 2011
11. "The End of Money" David Wolman, Da Capo Press (February 14, 2012)