Satoshium: Minted Bitcoin

White Paper

Thomas Hartman
<thomashartman1@gmail.com>

Alex Kravets
<kravets@gmail.com>

January 11, 2017
(Draft)

Abstract

Satoshium is a physical bitcoin system specifically made to appeal to non-experts that evokes the user experience and security of gold and silver coins. Like precious metal coins, and unlike nearly all physical bitcoin and hardware wallets to date, Satoshium tokens ("satoshiums") feature safe offline physical transferability. Users don't need to understand addresses, transactions, confirmations, change, fractional amounts, secrets or backups to hold or transact with satoshiums. At the point of sale or transfer, a smartphone verification of circulatability is performed, similar to a gold or silver assay on a coin. This can be performed offline, without an internet connection to the bitcoin blockchain. We introduce the satoshium, a physical bitcoin token that makes owning and circulating bitcoins easy.

1. Introduction

In this section we motivate and give a brief introduction to Satoshium. Section 2 talks about the satoshium coin, section 3 about the default phone client, and section 4 about the overall lifecycle. Subsequent sections handle more technically challenging subject matter such as counterfeit mitigation and security features.

1.1 Bitcoin The Incomprehensible

We propose that the key reason why Bitcoin hasn't seen greater mainstream adoption is its embedding in a computer-mediated online environment where people's expectations are the exact opposite of Bitcoin's actual attributes. Consider a dialog between someone who wants bitcoin ("novice") and someone who wants to help her friend understand bitcoin ("expert").

Novice*:* If it is a file, and it is copyable, how can it be money?
Expert*:* It is the best money ever. Wallets are copyable but the bitcoins controlled by private keys are neither copy-able nor double spendable.
Novice*:* I don't understand but I believe you. Now, if hackers steal my password, can I change it?
Expert*:* If hackers steal your Bitcoin private keys, your Bitcoin is gone forever. Because of this, a lot of people that are new to bitcoin keep their money on exchanges or buy a tracking fund instead.
Novice*:* I'll do that. As long as it's safe. I mean, it is insured and can't be stolen?
Expert*:* No, by that definition, it is not safe.
Novice*:* Well, if my bitcoin gets stolen, I'll just reverse the payment.
Expert*:* Payments are irreversible. Bitcoin's strength is exactly that payments are cash-like. Meaning irreversible. A payment takes about ten minutes to confirm, but once confirmed, it's final.
Novice*:* OK, I need to get in on this price rally, but I definitely don't want to get my bitcoins stolen. How do I open an account, where I am the one in control of the wallet?
Expert*:* Bitcoin doesn't need trusted institutions or accounts, instead each user is their own bank.
Novice*:* Oh, like email. What is my address?
Expert*:* You don't have a specific address. And addresses are not human friendly. You get a wallet and the wallet gives you multiple addresses.
Novice*:* What does it mean for a transaction to be confirmed multiple times ?
Expert*:* Initial and subsequent confirmations ensure that the transaction quickly becomes recognized as final and irreversible by the network. After 6 confirmations or roughly 1 hour, it's customary to consider even very large transactions final.
Novice*:* OK… Another thing is bothering me. A bitcoin is $800 each. When bitcoin takes over the world, how are people supposed to do day-to-day business in $800 chunks?
Expert*:* A bitcoin is divisible into one million bits. We should really talk about 21 trillion bits instead of 21 million bitcoins, but nobody does, although this will change.
Novice*:* Aha. Final question. What does a bitcoin, or a millionth of a bitcoin, a bit thing, or whatever it is, look like?
Expert*:* Well, the things you spend are called transaction outputs but no one looks at these directly. The private key looks like a long hexadecimal number, but it's usually encoded using 58 digits to save space and for readability… you know what… never mind.

1.2 Towards Humane Bitcoin

We believe that to become mainstream as a worldwide savings medium, Bitcoin must be physical.

Taking precious metal coins as the start point in the design space, we endeavor to design a physical bitcoin aimed at non-experts, that shields users from addresses and related low level details of the bitcoin protocol, and is as easy to use *and secure* as bullion gold.

Unlike previous attempts at physical Bitcoin, we propose bitcoin tokens called “satoshiums” that can be safely transferred between untrusted strangers without requiring an understanding of addresses or other protocol complexities such as transactions, confirmations, secrets, backups, change, and fractional amounts.

Satoshiums have a coin form factor incorporating a cryptoprocessor for storing secrets. A client, typically a smartphone, determines fundedness and transferability.

Denominations are standardized and use bits rather than fractional bitcoin.

A satoshium either contains transferable bitcoin with the denomination physically displayed upon it (Minted status), or it is contains no transferable bitcoin (all other statuses). There is no guessing how much bitcoin a minted satoshium has. This all or nothing nature makes the satoshium more like a traditional coin, and greatly simplifies its use. This is an object quite close in spirit to a precious metal coin.

Like precious metal coins, satoshiums are not meant for day to day spending. They are bitcoin containers for onboarding, hodling, and occasional re-selling. To secure a satoshium, hide it, or put it in a safe deposit box.

Like hardware wallets, satoshiums are more secure than general purpose computers and phones, which have large attack surfaces for bitcoin-stealing viruses. Using a cryptoprocessor to lock secrets in a tamper secure way is also far safer than using an easily tampered hologram (e.g. Casascius) or a scratch-off (e.g. Little Bit of Coin).

A satoshium with minted status contains transferable bitcoin. A minted satoshium protects a bitcoin secret that originated on the satoshium, which is unknown to anyone, but convincingly uses entropy provided by the funder. It is also provably funded to the advertised amount, without requiring online connectivity.

Anyone who has a bitcoin wallet can mint and/or redeem a satoshium. We call these users “minters.” Minters help users new to bitcoin (“novices”) own bitcoin easily without relying on trusted third parties -- including the minter, as the minter never learns the bitcoin secret.

After funding, novices can buy, sell, spend and receive minted satoshiums, circulating them hand to hand without touching the blockchain. Since they do not mint or redeem satoshium, novices have no need to understand Bitcoin addresses or related complexities. Novices need only understand how to determine whether a satoshium is minted, using a phone app. A novice can become a minter via a gentle learning curve.

When bitcoin exchanges eventually offer satoshium integration, novices will mint and redeem satoshium directly from an exchange linked bank account without ever coming in contact with a bitcoin address, yet fully controlling their secrets.

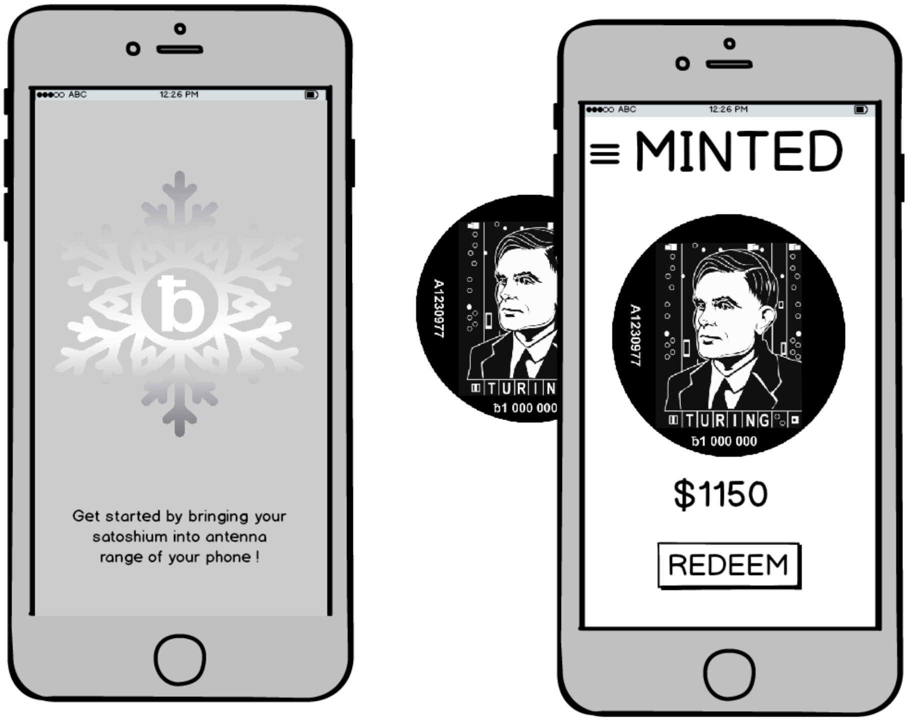


Figure 1. Verification of Minted Status

A smartphone performs minting, verification of minted status, and redemption.

- Minting: Creation of a minted satoshium. (Requires an address, performed by minter)
- Verification of minted status: Determines whether a satoshium contains bitcoin that is transferable. This can be performed offline, that is, without network access to the bitcoin blockchain. (Easy, shields user from addresses, can be performed by novice.)

- Redemption: Moves all value off the satoshium. (Performed by minter.)

Satoshiums are reusable. After redemption, the satoshium can be reminted with a new address and fresh funds. Since satoshiums speak an open protocol, people would be able to keep using satoshiums even if the company dissolved or the phone app somehow became unavailable.

The following competition matrix situates Satoshium among the existing Bitcoin storage solutions. “Easy to use” here means bitcoin can be bought from an untrusted seller without needing to understand bitcoin addresses or other low level details of the protocol.

Types of Bitcoin	**Easy to Use**	**Reusable**	**Transferable**	**Control of Keys**	**No Malware**	**Withdraw Bitcoin**
Satoshium	✓	✓	✓	✓	✓	✓
OpenDime			✓	✓	✓	✓
Physical Bitcoin (Casascius/BTCC)				✓	✓	✓
Web / Phone Wallet		✓		✓		✓
Hardware Wallet		✓		✓	✓	✓
Bitcoin ETF	✓				✓	
Bitcoin Bank (Coinbase)					✓	✓

Figure 2 Bitcoin storage solutions

2 Satoshium

Fundamentally, the satoshium is a bitcoin storage token that must be physically possessed to be used. The appearance, heft and feel of the satoshium should evoke precious metal coins popular with collectors today. It should come in a variety of designs, aiming for collectability. For example satoshiums could feature icons of science, art, cryptography and economics.

Our preferred satoshium implementation repackages the elements of a vanilla contactless smartcard [11] to evoke a precious metal coin -- perhaps something like a high end casino chip. Satoshium has a cryptoprocessor for storing secrets and an antenna for communicating wirelessly. The satoshium needs no battery, as it is powered by NFC magnetic induction or using built-in micro USB, drawing power from an active NFC-enabled smartphone. We assume the coin form factor of NFC cryptoprocessor-based satoshiums throughout the whitepaper, though other form factors are possible.

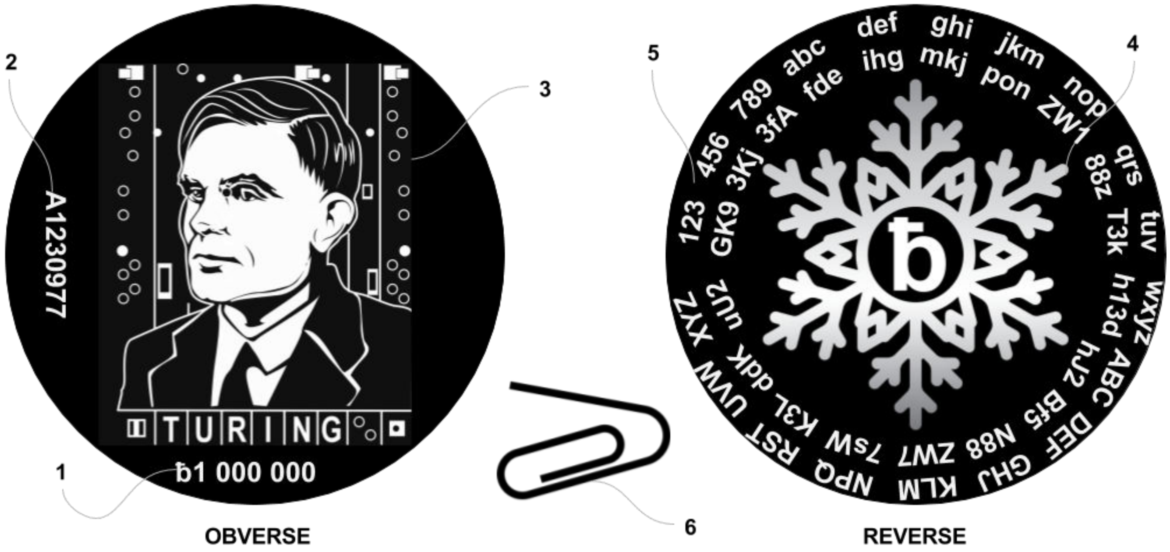

2
3
5
4
A1230977
TURING
ƀ1 000 000
1
6
OBVERSE
REVERSE
123 456 789 abc def ghi jkm nop qrs tuv wxyz ABC DEF GHJ KLM NPQ RST UVW XYZ
GK9 3Kj 3fA fde ihg mkj pon ZW1 88z T3k h13d hJ2 Bf5 N88 ZW7 7sM K3L dqk un2

Figure 3 Satoshium

The satoshium features: Denomination **1**. Series and Serial Number **2**. Portrait **3**. Satoshium Logo **4**. Internal to the satoshium are a Secure Cryptoprocessor, micro USB plug and NFC antenna (not pictured). on-coin security elements include a decoder ring and satoshium button **5**, **6**.

The most important job of the cryptoprocessor is to control access to bitcoin secrets, such that they may never be revealed when the satoshium has minted status. The satoshium should therefore use a cryptoprocessor that performs zeroization of secrets with a high level of probability if an attacker attempts to access cryptographic secrets by invasive probing. FIPS is an industry standard-setting and testing program, and the 140-2 level 4 [5] certification is for cryptoprocessors with strong zeroization mechanisms and related security features appropriate for devices that operate in physically unprotected environments. Ideally a cryptoprocessor with FIPS 140-2 level 4 or a similar certification should be used.

The satoshium responds to requests from a satoshium client device, generally a smartphone. The satoshium proves its genuine-ness using a verifiable cryptographic signature.

Possession of the coin and user participation via the on-coin security elements is required for redemption (see Appendix for details).

2.1 Security Considerations: Satoshium

A satoshium should have a shelf life of over a decade if it is heavily circulated, or longer if it is sitting in climate controlled storage, however just as cash can be burnt so Satoshium can be mechanically destroyed, therefore users should consider redeeming very old satoshiums.

There is about a one percent annual chance of a Carrington-type solar flare event that would damage unprotected electronics on a worldwide scale. So the enclosure should include faraday containment of the cryptoprocessor.

We defer an in depth consideration of counterfeiting to Section 6. We cover security considerations for the on-coin security elements in the Appendix.

3. Smartphone

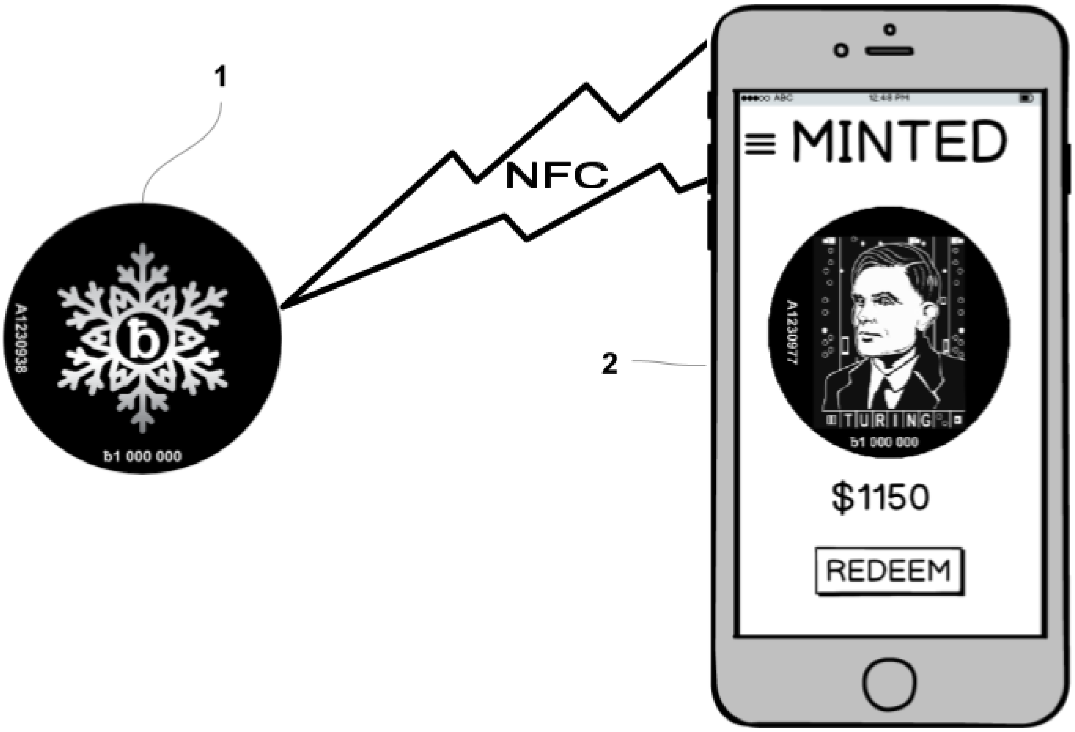


Figure 4 Satoshium communicating with Smartphone

A satoshium **1** communicates with and is powered by a smartphone **2**.

Generically, the device that interfaces with the satoshium is a satoshium client device. Most of the time it will be a phone, so unless it is important to be generic, we usually just write "phone."

The phone stores no secrets, and no bitcoin is lost if the phone is stolen, damaged or malwared. Phones are not paired with satoshiums. Any phone can perform any of the basic lifecycle functions, of which the most important are minting, verification of minted status, and redemption.

Multi-satoshium readers could enable batch minting, asay and and redemption by allowing simultaneous communication with multiple satoshiums from a single satoshium client device.

4. Lifecycle

We first give a high level overview of a satoshium's lifecycle, contextualized by a state diagram covering all the main states and transitions. We call out potential security vulnerabilities for key state transitions, to aid implementers. The security focus is on phone malware, as this seems like the likeliest threat. The Counterfeiting section later considers satoshium malware in depth.

4.1 Overview

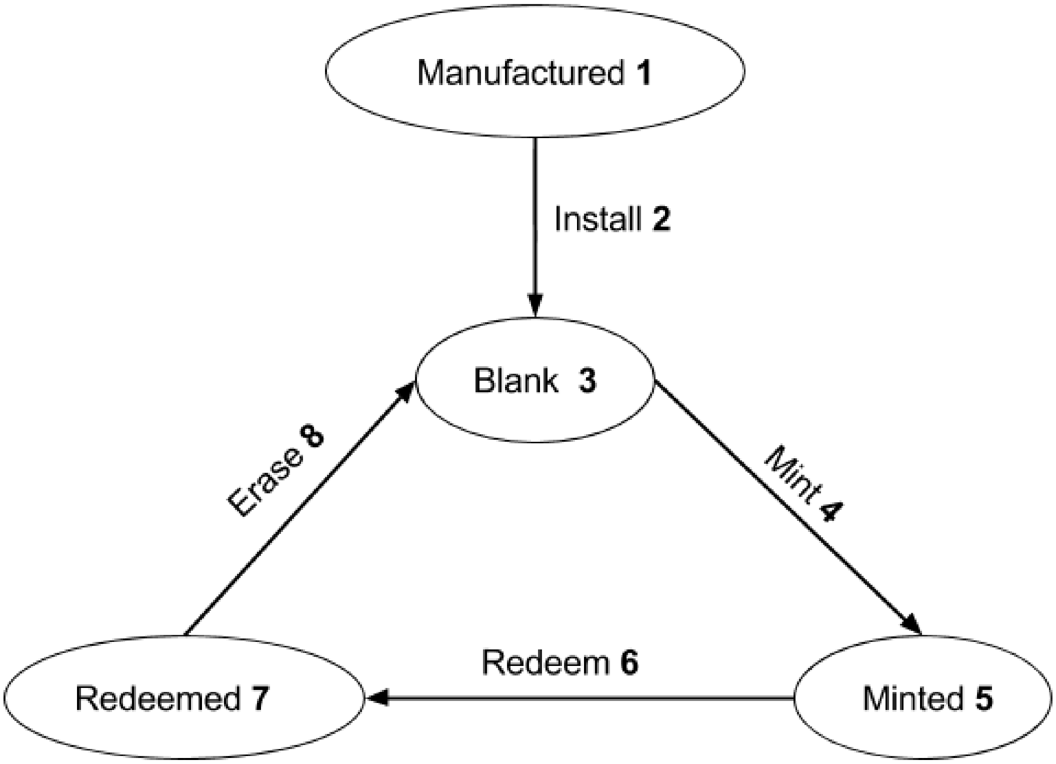


Figure 5 Basic lifecycle of a satoshium

A manufacturer produces a satoshium without any custom software **1**. Satoshium software and indelible data such as identkeys are installed **2**, putting the satoshium into the blank state **3** (section 4.2).

A minter mints the satoshium **4, 5** (section 4.3). Minted satoshiums are secured with a bitcoin secret which is unknown to the minter yet probabilistically likely to use entropy the minter supplied. Minted satoshium also carries a witness of a proof of fundedness which has been checked by the satoshium. The minted satoshium may circulate hand to hand as a container of bearer bitcoin.

Eventually the minted satoshium is redeemed **6** (section 4.5), which puts it into the redeeming status, making it no longer transferable. After the redemption is confirmed on the blockchain the satoshium becomes redeemed **7**, at which point it is safe to erase as no more funds are protected by the secret. Finally, the satoshium can be reset to blank via erasure **8** after which it can be re-minted with a new address.

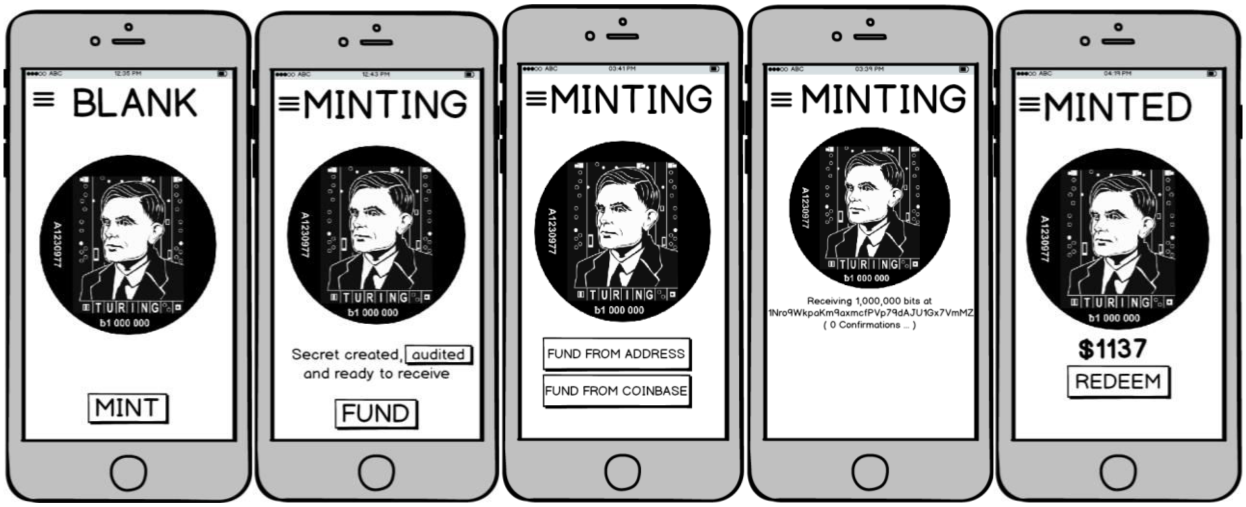
4.2 Installation

A enclosure manufacturer supplies satoshiums to the Satoshium installation facility. These tokens, which have the custom coin-like enclosure and an embedded cryptoprocessor, are in the Manufactured state (**1** in the Lifecycle Diagram above). At the Satoshium facility, the satoshiums are installed with the following non-overwritable information making them blank satoshiums:

- Denomination
- Series Identifier and Serial Number as engraved on the surface.
- Derived Satoshium identity key pair
- Derived Decoder Ring mapping
- Blockchain checkpoint header

The section on Counterfeiting considers secret leakage and malware attacks at installation time.

4.3 Minting



Secret created, audited and ready to receive

Receiving 1,000,000 bits at 1Nro9WkpaKm9axmcfPVp79dAJU1Gx7VmMZ (0 Confirmations ...)

Figure 6 Minting

To mint a satoshium, the minter performs

- Inscription: Generate a bitcoin secret (private key or seed mapping to private key) unknown to the minter but using entropy provided by the minter, with probabilistic evidence that no cheating occurred. Optionally, the minter can view an audit report in which she can verify the entropy she provided was probably used in the bitcoin secret. The minter can enforce an arbitrarily high probability that her entropy was used, with more certainty requiring more time during the inscription phase.
- Funding: Send bitcoin to the address derived from this secret. The satoshium checks an SPV proof of funding before changing its status to minted.

If an exchange integrates with satoshium, as with coinbase in the hypothetical example above, the buyer could fund his satoshium directly from an exchange linked bank account.

4.3.1 Inscription

Inscription is the process of generating a bitcoin secret which is unknown to the minter yet likely to use entropy the minter supplied, in a way that is auditable. This bitcoin secret is used to generate an address for subsequent funding as a minted satoshium, which is communicated to the phone. The inscription protocol ensures that even with the satoshium's platform integrity completely compromised, the attacker cannot steal bitcoins by controlling the bitcoin secret.

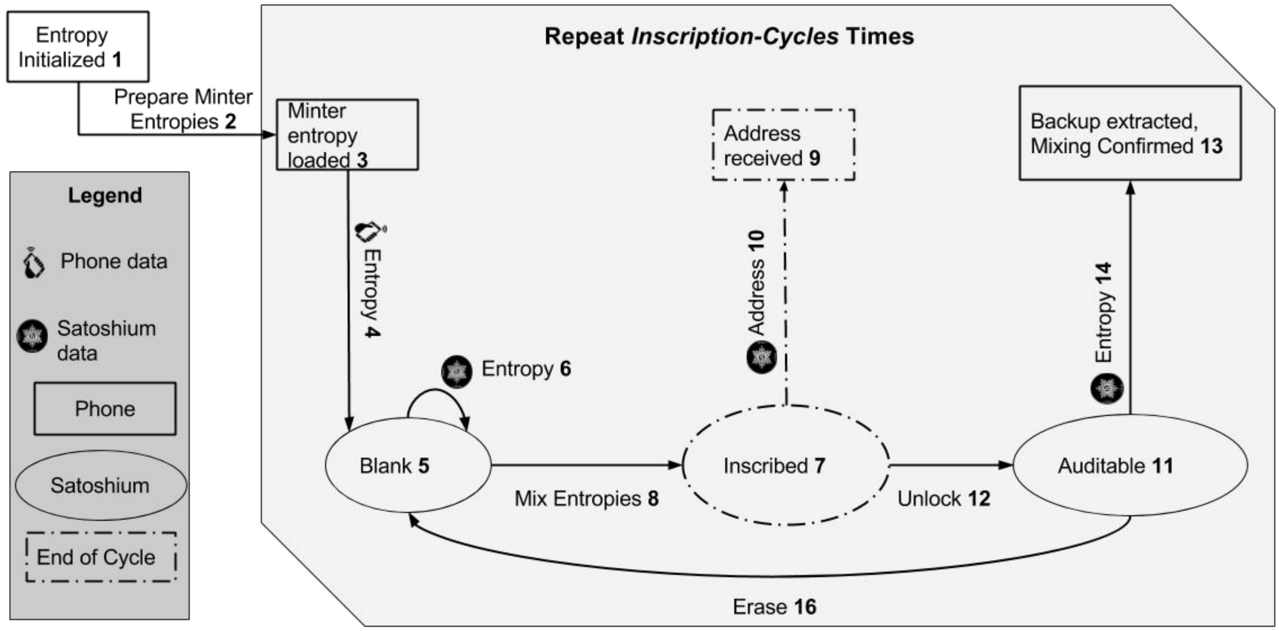


Figure 9 Inscription

The phone prepares for the inscription cycle as follows. A random number is picked -- *Inscription-Cycles* -- which is unknown to the satoshium. The phone generates this many minter entropy strings, which are also unknown to the satoshium. For efficiency, a single master minter entropy seed can be seeded using phone entropy, environmental entropy, and minter supplied random data, and then derived minter entropy strings can be created from the seed using a deterministic pseudo-random process such as repeated hashing. The phone now has minter entropy for inscription prepared and not known to the satoshium **1.**

One by one, the derived minter entropy strings are loaded **2** and used in repeated inscription cycles. This series of inscription cycles will end with the satoshium Inscribed **7** and its address but not its secret revealed to the phone **9**.

The phone **3** sends the next prepared minter entropy string **4** to the blank satoshium. The satoshium generates a satoshium entropy string using the cryptoprocessor random number generator **6**. The two entropy strings are mixed **8** to generate a BIP39 512 bit bitcoin secret [10]. This is used to generate the satoshium address, making the satoshium Inscribed **7**. The address is sent **10** to the phone **8**.

If *Inscription-Cycle*s inscriptions have been performed, the satoshium inscription ends here. Otherwise the phone does more inscription cycles until it has repeated this process *Inscription-Cycles* times.

In the case of more inscriptions, the next step is for the phone to demand that the satoshium unlock **12** its secret satoshium entropy (from **6** earlier), making it Auditable **11.** The satoshium entropy, along with the minter entropy (from **4** earlier) which is already known to the phone, allows the phone to perform a full replay of the deterministic Bitcoin secret generating procedure. The secret can be confirmed by deriving the address and confirming that this is the same address as revealed earlier (in **10**). The satoshium is then erased **16** back to blank **5** and the next cycle is initiated.

Since the satoshium does not know the value of *Inscription-Cycles*, it is likely to be caught lying if it produces bitcoin secrets that do not depend on minter entropy.

After the inscription cycle has been done *Inscription-Cycles* times, the inscription concludes by initiating Funding instead of demanding that the satoshium entropy be revealed.

4.3.2 Funding

The satoshium must be funded, and the funds must be proven to and remembered by the coin.

The Bitcoin network routinely and cheaply serves SPV proofs for arbitrary addresses [8]. Normally an offline SPV wallet would need to be careful that proven funds were not later spent, but the satoshium lifecycle ensures that funds can't be spent prior to redemption so in this case no such caution is needed.

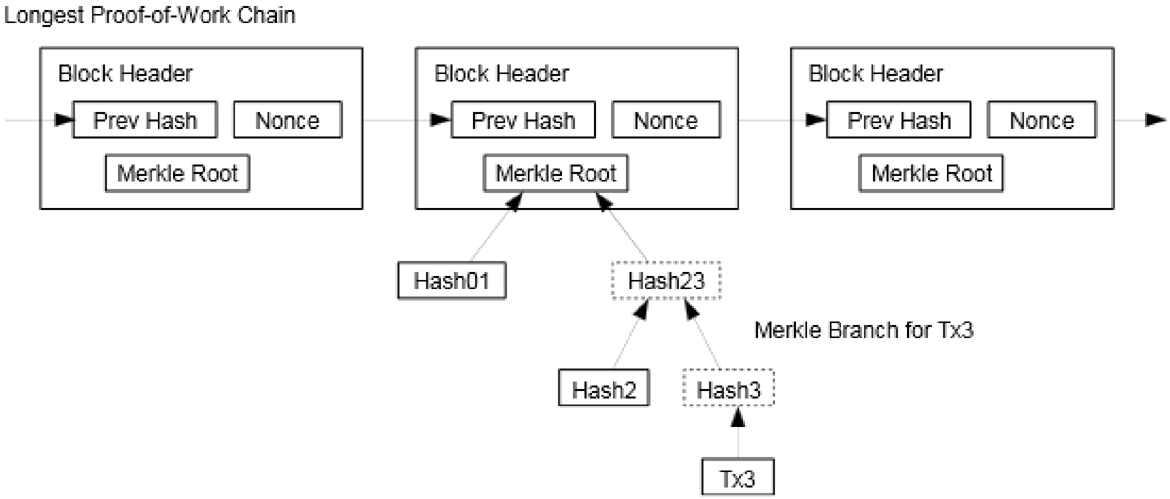


Figure 10 SPV Proof of Sufficient Funds

This Figure (from [1]) shows the highest cumulative difficulty header chain recorded by the Bitcoin network, along with a Merkle Branch of a specific transaction included into one of the headers. The headers and the Merkle Branch depicted constitute an SPV proof of funds by the phone to the satoshium of any address funded by Tx3 [1]. This proof can be made arbitrarily expensive in terms of cumulative energy sacrifice required to create the most recent header, by requiring some threshold cumulative difficulty confirming all headers containing funding transactions. As an implementation note, the satoshium does not need to cache all headers, only the tip.

The SPV proof of sufficient funds is first communicated to and checked by the phone. Then the phone passes this proof to the satoshium, when it is in the Inscribed state. If the proof passes, the satoshium changes its status to minted.

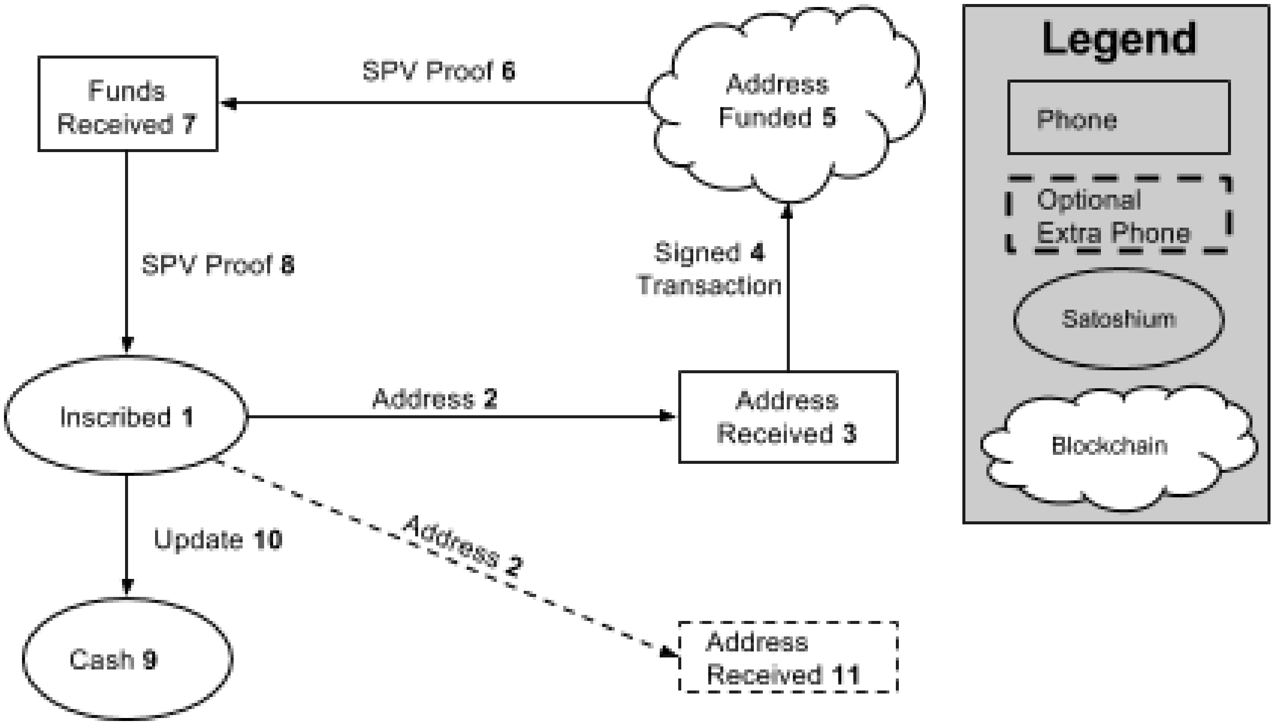


Figure 11 Funding

While in the Inscribed state **1** the satoshium sends the phone the funding address **2,3**. A funding wallet (typically but not necessarily the phone) broadcasts a signed funding transaction **4,** to the Bitcoin network. Eventually the bitcoin network accumulates sufficient cumulative difficulty around the transferred funds to prevent double spends and the address is considered funded **5**. An SPV proof satisfying the cumulative difficulty requirement is requested by the phone and transmitted from peers on the Bitcoin p2p network **6**. After checking the proof the phone believes the funds are real **7**. The proof is serialized and transmitted **8** to the satoshium. After checking the proof itself **10** the satoshium now also believes the funds are real and flips its status to minted **9**.

4.3.3 Security Considerations (Minting)

Before funding, the minter may double check the funding address on a secondary phone or other device, if she wishes to guard against a malwared phone address substitution attack.

4.4 Verification of Minted Status

Precious metal coins are assayed to prevent counterfeiting by a variety of means, as pictured above. The equivalent operation with satoshium uses a phone app, which simply verifies that the satoshium has minted status. Since verification of minted status is easy to learn and can be performed quickly, it is may be done routinely whenever a satoshium changes hands.

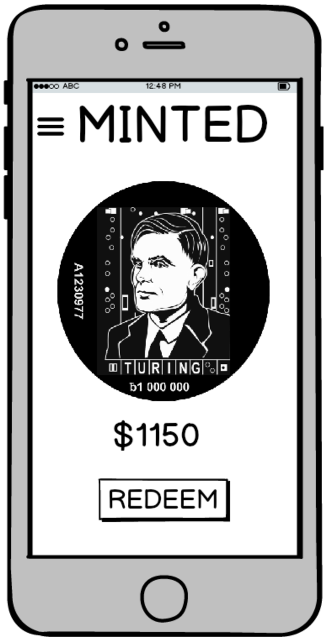


Figure 7 Verification of Minted Status

In Figure 7, a 1,000,000 bit satoshium is verified as minted by a phone. The display of a satoshium coin with the appropriate serial number and denomination indicates that the satoshium has proved its software integrity and genuineness. The phone reports that the satoshium is minted, as well as confirming the denomination and serial number**.** This guarantees the satoshium is funded and no knows the secret. Optionally, if the phone is online, it queries the Bitcoin p2p network for the balance of the address, to corroborate the balance on the blockchain.

The phone app reports if overfunding has occurred during minting; underfunding is impossible.

3.4.1 Security Considerations (Verification of Minted Status)

Trivially, a buyer may be convinced to buy a satoshium without performing verification of minted status first, and pay funded price for an unfunded satoshium. Or a thief posing as a buyer could do a grab-and-run theft during verification of minted status.

The buyer may also be the victim of fraud during verification of minted status if she trust the seller's phone instead of using her own. The seller runs fraud-ware that shows a blank satoshium verifying as minted The buyer believes this, pays, and departs with an unfunded token. The buyer must understand that she should trust a mint verification report only on hardware she controls.

If the phone is online, it checks the bitcoin balance by querying the bitcoin network. If bitcoin on a atoshium with minted status has moved on the blockchain, then something has gone seriously wrong. An attacker has somehow learned the bitcoin secret for the satoshium's address. Perhaps the satoshium's cryptoprocessor secure element lock has been broken[7], or a side channel attack has been discovered to steal the bitcoin secret. Alarms should go off in this case -- literal alarms on the phone, and also a message should be sent that alerts security personnel at satoshium headquarters.

4.5 Redemption

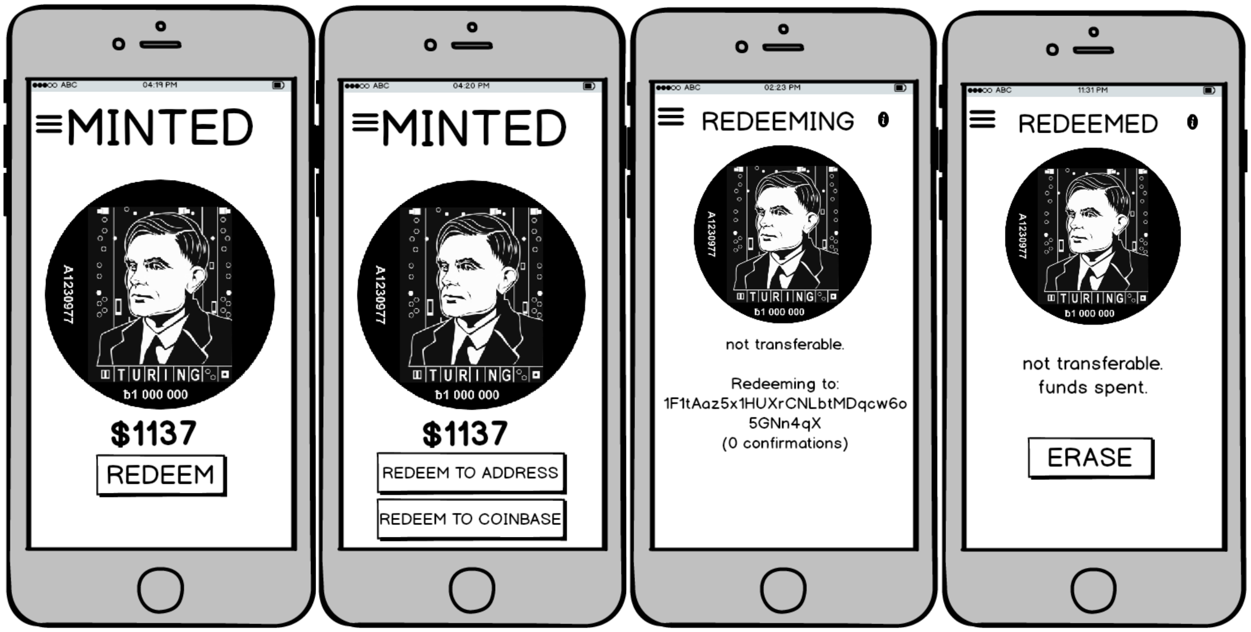


Figure 8 Redemption

Redemption produces a signed transaction that transfers all value to an address specified by the owner. If an exchange integrates with satoshium, as with coinbase in the hypothetical example above, the buyer could redeem his satoshium directly to fiat in an exchange linked bank account, without ever encountering a bitcoin address.

If there was a problem with the redemption, the BIP39 secret can be extracted for troubleshooting (see Appendix).

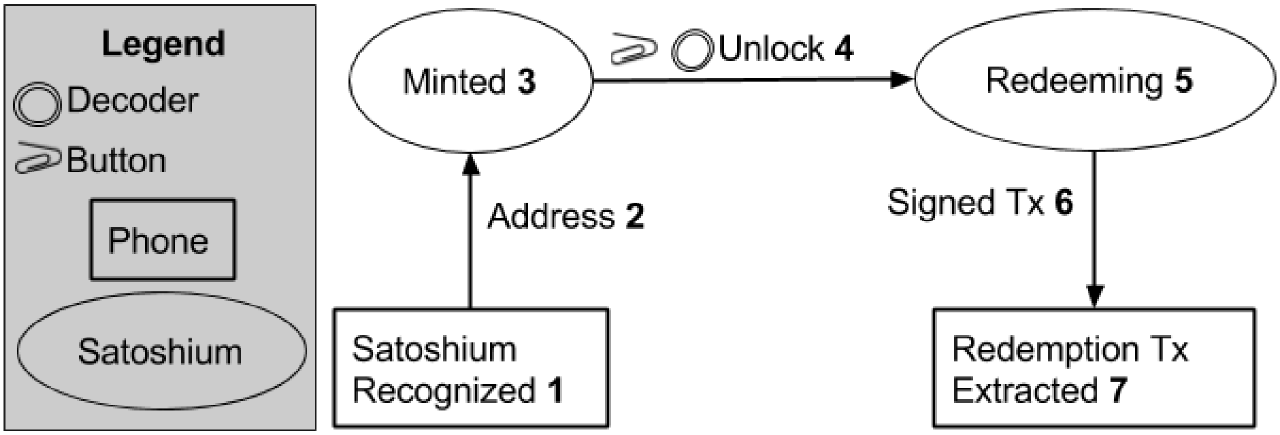


Figure 12 Redeeming

Redemption of a minted satoshium begins when the phone **1** transmits **2** a redemption transaction request **3** to the satoshium, which includes a redemption address. The user has a minute to approve this action using the on-coin security elements **4** (see Appendix section On-Coin Security

Elements)**.** This changes the satoshium's status to redeeming **5**. The redeeming satoshium transmits **6** a signed redemption transaction to the phone **7**. The phone broadcasts the signed transaction to the Bitcoin p2p network.

3.5.1 Security Considerations (Redemption)

See Appendix section Security Considerations, Decoder Ring.

5. Counterfeiting

The phone determines that the satoshium is genuine by challenging it with a nonce, as described in [6]. The satoshium signs the nonce with its identkey and transmits the signature to the phone. The phone checks the signature against the public identkey, and displays the serial number. The serial number is used in deterministic derivation of the coin's identkey, which is one of the factors used by client software to authenticate the satoshium as genuine.

The following section wargames various attacks that try to defeat the above protections.

5.1 Enclosure

This section considers satoshium counterfeiting where the attacker uses stock cryptoprocessor and software, but is able to fake an enclosure.

5.1.1 Tap Attack

An attacker could implant the cryptoprocessor from a genuine satoshium into a counterfeit enclosure. The counterfeit enclosure has a battery and a second malwared processor. The malwared processor must be able to communicate over NFC, transmit cellular data, and know the decoder ring secret. After funding, the malwared processor redeems the funds to an address it controls, enters the appropriate decoder ring secret, and sends the signed transaction over cellular data to the bitcoin p2p network.

All hardware wallets are potentially vulnerable to this attack, for instance by intercepting and replacing hardware that is shipping. However, with traditional hardware wallets, pre-shipping is the only time the attacker has access to a genuine hardware wallet. By contrast, with circulating satoshiums the attacker has a wider window of access during potentially anonymous hand to hand exchanges.

On the other hand, the attacker must not only compromise the phone with malware, but also know the decoder ring secret for the individual satoshium. This attack seems farfetched enough not to assign it undue importance. Its risk can be further minimized by making enclosure counterfeiting and tampering expensive.

5.2 Cryptoprocessor

This section considers counterfeiting where the attacker uses a stock enclosure, but is able to install a fake and/or malwared cryptoprocessor.

5.2.1 Non-redeemable “Minted” Satoshium

To begin with a concrete example: an attacker could create a malwared counterfeit satoshium which acts like a minted satoshium in every way, except it cannot be redeemed. The bitcoin secret of the bad satoshium’s address is known by the attacker. The attacker funds this address in order to pass the verification of minted status, knowing that she can claw back the funds at any time. The attack is discovered on the first redemption attempt. To stretch the effective window of the attack before detection, the attacker should avoid using counterfeits with duplicate addresses or serial numbers, and spread the attack out over a wide area.

5.2.2 Platform Integrity

There are many such potential malware attacks, if platform integrity is not preserved. The key to stopping all such attacks is to enforce platform integrity effectively, so the cost to break platform integrity is higher than the expected revenue from counterfeiting.

Platform Integrity [9] means the software running on some hardware behaves as intended, meaning no malware. The software running on the satoshium and endorsed satoshium client devices should be open sourced, and the satoshium hardware should support a mechanism for verifying platform integrity.

To achieve this, the satoshium uses the Installation Receipts mechanism of Global Platform 2.1+ [13] to create and cache a self certifying cryptographic receipt that attests to the hash of the installed software as observed by the global platform layer underneath at installation time. This hash is signed by a lower level cryptoprocessor fabricator key and the signature encompasses unique identification fields of the cryptoprocessor. This allows the app to conduct a *routine* verification process to ensure that the software running on the crypto processor is bit-for-bit identical to a version built in a clean-room virtual machine and the hash of such build is on a whitelist of valid versions preinstalled in the app. This check should occur whenever the satoshium handshakes with a phone.

5.2.3 Counterfeiting Scenario

We now try to wargame the creation of a counterfeit which can pass the routine platform integrity check. We assume the basic “non redeemable satoshium” attack described previously. We try to consider the most plausible attack scenario, without wandering too far into the weeds.

The satoshium enclosure needs to look genuine. If the attacker is an insider at the enclosure manufacturer, theft or unauthorized manufacture of an enclosure may be feasible if internal controls are weak. Another option is to manufacture counterfeit enclosures.

The enforcement of platform integrity via the Global Platform installation receipts mechanism, together with reproducible builds[2], is sufficiently secure to rule out attacks on stock cryptoprocessor hardware. The cryptoprocessor fabricator has a reputation to protect that is sufficiently valuable to rule out an insider attack at the cryptoprocessor fabricator. We rule out theft of the cryptoprocessor fabricator identity secret, for the same reason. Since the keys are derived and it is possible to effectively protect satoshium root identkeys, we rule out compromise of satoshium root keys unless the attacker is an insider. (We define "insider" as anyone who has access to Satoshium root identkeys.)

This leaves an attack that uses a counterfeit cryptoprocessor in a convincing enclosure, together with either

- Satoshium insider attack with compromise of Satoshium root identkey
- Or non-Satoshium insider attack with compromise of Satoshium derived identkeys via:
    - Industrial espionage at the satoshium facility
    - Or breaking the secure element lock on one or more satoshiums

In all cases, the following costs apply

- Acquiring a genuine looking intact enclosure -- from the enclosure manufacturer, or faked.
- Acquiring a counterfeit cryptoprocessor
- Installing the cryptoprocessor in the enclosure
- Writing and maintaining the cryptoprocessor malware
- Fraudulent sales operation
- Risk of detection and criminal penalties
- Doing all the above while maintaining operational security

If the attacker is not an insider at Satoshium, she must also acquire derived key material, by exfiltration from the secure element or espionage [3].

For an attack to be worth doing, the attacker has to recover all costs inherent in an ongoing counterfeiting operation. The attacker's gain is the value of counterfeit satoshiums that can be sold into general circulation prior to detection and countermeasures, minus attack costs [4].

A useful intuition is that circulation is less safe than hodling. So if the system comes under attack by cryptoprocessor counterfeits, hodling until redemption become more common while hand to hand transfers decrease. An equilibrium emerges between the convenience of circulating physical bitcoin, and the threat of counterfeits. The situation is somewhat analogous to that of precious metals which may also be subject to sophisticated counterfeiting while retaining their usefulness as a store of value.

6. Conclusion

Usability problems are handicapping non-technical would-be users of Bitcoin. Satoshium, a humane physicalization with strong security guarantees, brings bitcoin to the masses, safely. The proposed system guarantees authenticity, locking of secrets, and bitcoin balance satisfying the advertised denomination, enforced at the hardware level by a secure cryptoprocessor. A defense-in-depth anti-counterfeiting strategy to makes economically unattractive even along a success path where satoshiums are someday widely circulated. Satoshiums are attractive to collectors, humane enough to onboard would-be nontechnical hodlers, and circulatable offline in the wild.

7. References

[1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2009.
http://bitcoin.org/bitcoin.pdf

[2] Miron Cuperman. "Gitian: A Secure Source Control Oriented Software Distribution Method" 2009.
http://gitian.org/

[3] Paul Kocher, Joshua Jaffe and Benjamin Jun. "Differential power analysis." 1999.
http://saluc.engr.uconn.edu/refs/sidechannel/kocher99differential.pdf

[4] Elena Quercioli and Lones Smith. "The Economics of Counterfeiting." 2015.
http://lonessmith.com/sites/default/files/ecta10975.pdf

[5] FIPS 140-2 level 4, Wikipedia
https://en.wikipedia.org/wiki/FIPS_140-2#Level_4

[6] Muhammad Saeed, Zeeshan Bilal: "An NFC Based Consumer-Level Counterfeit Detection Framework"
https://pure.royalholloway.ac.uk/portal/files/23032339/Consumer_Level_Counterfeit_detection.pdf

[7] William Jackson. "Engineer shows how to crack a 'secure' TPM chip." 2010.
https://gcn.com/Articles/2010/02/02/Black-Hat-chip-crack-020210.aspx

[8] Mike Hearn, Matt Corallo: Connection Bloom filtering (BIP37)
https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki

[9] Platform Integrity, Wikipedia
https://en.wikipedia.org/wiki/Trusted_Platform_Module#Platform_integrity

[10] Marek Palatinus, Pavol Rusnak, et al: Mnemonic code for generating deterministic keys (BIP39)
https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

[11] Contactless Smartcard, Wikipedia
https://en.wikipedia.org/wiki/Contactless_smart_card

[12] Nermin Hajdarbegovic: "Review: Ledger Wallet Nano Provides Premium Security on a Budget"
http://www.coindesk.com/review-ledger-wallet-nano-provides-premium-security-budget

[13] GlobalPlatform. Card Specification Version 2.2
http://www.win.tue.nl/pinpasjc/docs/GPCardSpec_v2.2.pdf

Appendix

1. On-Coin Security Elements

This section discusses security features of the satoshium that necessitate a user action, in conjunction with physical possession of the coin, for security sensitive operation such as redemption or secret extraction.

1.1 Decoder Ring

The decoder ring is based on the security card mechanism implemented by Ledger Wallet [12] for preventing withdrawal address substitution attacks in its screen-less products, such as the Ledger Nano. The satoshium has this secret engraved on its surface, instead of in a separate security card. Like the ledger nano, the satoshium is protected against phone malware performing malicious redemption, assuming the malware doesn't know the decoder ring secret.

1.1.1 Security Considerations (Decoder Ring)

One possibility is a directed attack, where the attacker's phone has malware. For example, an attacker posing as a buyer performs a verification of minted status. The buyer wears a hidden camera, and uses machine vision to quickly read the secret on the satoshium, and communicate this to her own phone. Then the buyer pretends to perform the verification of minted status, but the malware on her phone is actually doing a redemption using the redemption secret. The buyer's phone has a "problem" with the verification of minted status, the attacker refuses to buy the satoshium, and leaves the point of sale. The victim is left with a blank satoshium.

For this attack, the attacker also has to manage to press the satoshium button the appropriate number of times without the owner noticing.

More problematically in our view, the decoder ring secret could leak, and be used to steal satoshiums in an *undirected* malware attack. Potential decoder ring leakage scenarios:

- With heavily circulated satoshium, many redemption challenges, potentially across multiple infected phones reporting back to the same attacker (or multiple attackers sharing information), could allow an attacker to eventually learn a satoshium's full decoder ring, or enough of the secret for malware to issue a hostile redemption after multiple tries.
- Malware could try to trick the user into placing the decoder ring into the phone camera's field of view and use OCR techniques to try to capture the secret .
- Attackers could try to buy photographs of decoder rings from owners of unfunded satoshiums (but here the attacker herself is likely to get scammed by the seller, who may create fake decoder ring images using image manipulation tools)
- If satoshiums have a high rate of circulation, an attacker could learn many decoder ring secrets, by acting as a high volume collector/dealer and recording the secrets for all satoshiums that pass through her inventory
- Insider theft or espionage. The manufacturer needs to know the decoder at manufacturing time (for engraving) and the satoshium facility needs to know the decoder ring at installation time (see Lifecycle section).

An undirected decoder ring attack requires:

- Knowledge of decoder ring secret
- Phone malware installed
- Confirmation Button pressed the correct number of times to confirm redemption

Examples of potential undirected attacks:

- Malware could trick the user into entering a decoder ring response to an address the attacker controls by couching this along the lines of "This is a routine security check by the Satoshium Team to prove you rightfully own of your bitcoin.... Please enter the decoder ring solution for the following address, and press the button three times for confirmation of your entry... Thank you for your cooperation." (In fact, the user should never press the button except when performing a security sensitive operation.) After the user enters the solution and performs the requested confirmation action, the attacker redeems to this address.
- If the malware has more patience, it could wait for the user to initiate redemption herself, and then man-in-the-middle the redemption request and receive the needed button confirmation from the user, who has no way of knowing an address has been substituted.

High risk / value redemptions should be performed on secure hardware such as a factory reset phone, a computer live booted from cd with boot media provided by satoshium, or a satoshium compatible hardware wallet with a screen.

1.2 Satoshium Button

The satoshium button is used to confirm security sensitive actions. A single button press is used to verify that the button works. This way, a user can reassure herself that the button is working on her own phone, without fear of attack.

Two button presses are used to confirm redemption with address confirmation. This is the primary use of the button, in the most common and safest usage mode.

Three button presses are required for secret extraction and redemption without address confirmation. These operations are escape hatches for troubleshooting in case the decoder ring cannot be read due to damage or there is a problem with an initial redemption. They are more vulnerable to phone malware than the usual redemption operation and not intended during normal use of a satoshium.

It should be easy for a viewer to tell how many times a button is being pressed, both when doing it oneself and when watching a potential attacker. So there is a delay between button presses.

1.2.1 Security Considerations: Satoshium Button

The primary purpose of the satoshium button is to protect against decoder ring-aware malware on untrusted phones during verification of minted status, for example during a sale. With a satoshium button this is safe, so long as the buyer is not permitted to press the satoshium button.

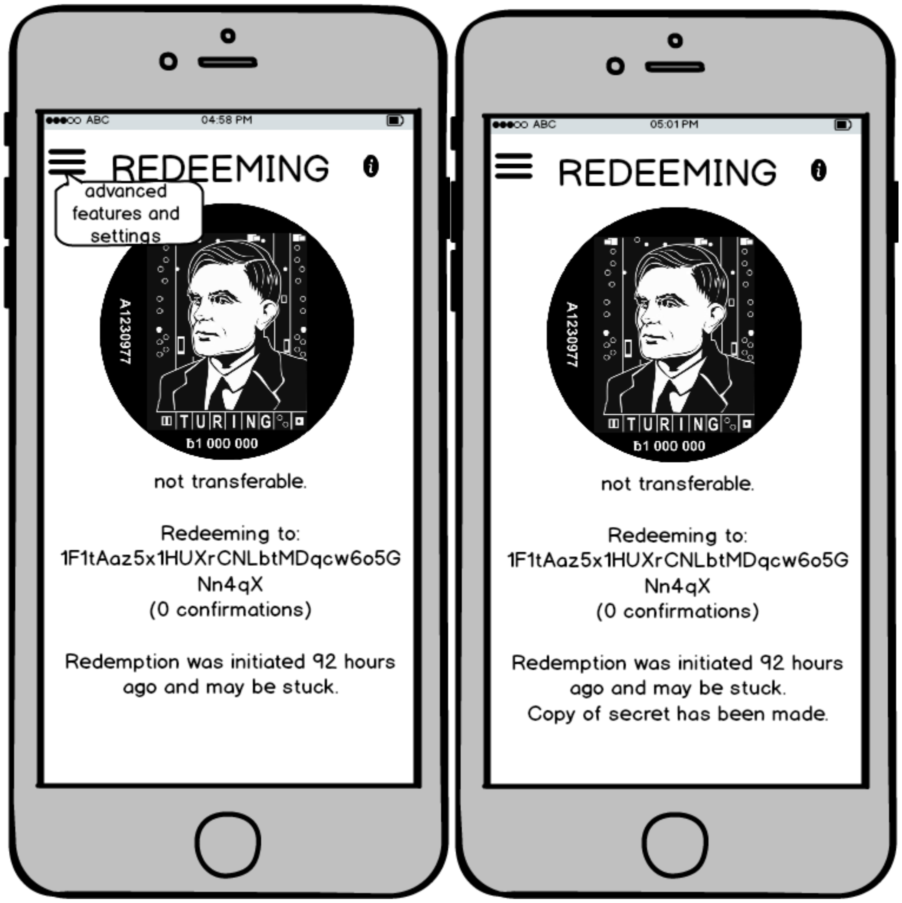
The button cannot protect against malware that knows the decoder ring secret during redemption. For ultra secure operation where this is a concern, see Security Considerations (Decoder Ring).

2 Secret Extraction

Secret extraction destroys transferability and is a potential attack point for malware. It is much less safe than standard redemption. It is also confusing and stressful for inexperienced users. So, it is considered a non-standard usage mode and mildly discouraged via lack of discoverability in the user interface, accessible only via advanced settings.

The extracted secret is a BIP39 mnemonic that can be restored to any satoshium or bitcoin wallet [10].

Secret extraction may be used as a recovery procedure for redemptions gone wrong.



not transferable.

Redeeming to:
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4qX
(0 confirmations)

Redemption was initiated 92 hours ago and may be stuck.

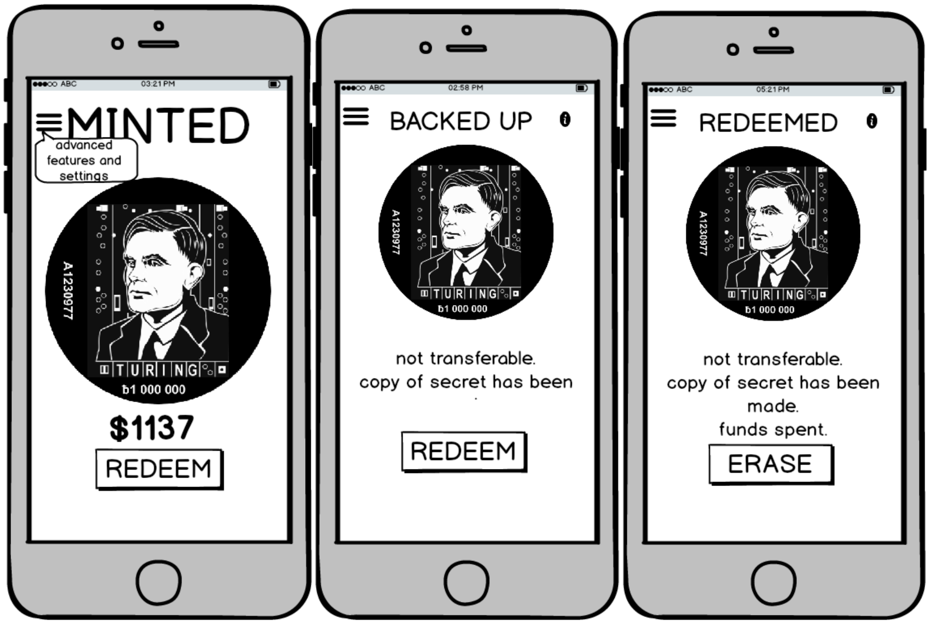
not transferable.

Redeeming to:
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4qX
(0 confirmations)

Redemption was initiated 92 hours ago and may be stuck.
Copy of secret has been made.

Figure 13 Secret Extraction for Troubleshooting Redemption

Advanced users may desire to backup a minted satoshium for peace of mind during long term storage.



not transferable.
copy of secret has been

not transferable.
copy of secret has been
made.
funds spent.

2.2 Security Considerations (Secret Extraction)

Malware is a concern, as the satoshium client, typically a smartphone, could spend the funds to an attacker with the extracted secret. For maximum safety, high value secret extraction should be done on secure hardware (see Security Considerations, Decoder Ring). The same applies to recovery.