Satoshium: Minted Bitcoin

White Paper

Alex Kravets
<kravets@gmail.com>

Thomas Hartman
<thomashartman1@gmail.com>

July 24th, 2017

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 briefly introduce Satoshium. Section 2 addresses the satoshium token, section 3 the default phone client, and section 4 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 their 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 am not following 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*:* 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. But instead of a bank account, you get a wallet with multiple addresses.
Novice*:* Oh, like email. What is my address?
Expert*:* You don't have a specific address. And addresses are not human friendly.
Novice*:* OK... Another thing is bothering me. A bitcoin is $2,800 each. When bitcoin takes over the world, how are people supposed to do day-to-day business in $2,800 chunks?
Expert*:* A bitcoin is divisible into one million bits. We should really talk about 21 trillion bits instead of 21 million bitcoins, and although nobody does that, it 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*:* First of all it's an abstraction so it doesn't have a physical appearance. At the most basic level, to have bitcoin means you control with a secret something called an unspent transaction output, or UTXO for short. That means someone paid you and you haven't spent the output yet.
Novice: I feel dumb.

1.2 Towards Humane Bitcoin

We believe that to become a mainstream savings media, Bitcoin must be available in a physical form.

Taking precious metal coins as the starting point in the design space, we endeavor to design a physical bitcoin that is aimed at non-experts, 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, the Satoshium (uppercase) system uses tokens called "satoshiums" (lowercase) 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. A smartphone app verifies funds and protects against counterfeiting. Satoshiums, being a physical token, can be transferred without an internet connection, which makes them both easy to use and suppression resistant.

Satoshiums have a coin form factor. Denominations are standardized and can can be easily distinguished visually, by size and other characteristics. Satoshiums use bits (1 bit = 100 satoshi) rather than fractional bitcoin.

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

The satoshium incorporates an internal cryptoprocessor for storing secrets. A minted satoshium protects a BIP39 bitcoin secret. This secret is created by the satoshium, but convincingly uses entropy provided by the funder to avoid control of the secret by satoshium insiders or other attackers. The secret is provably unknown to anyone.

Anyone with a bitcoin wallet or an onboarding partner can mint a satoshium. We call these users “minters.” With minted bitcoin, users new to bitcoin (“novices”) can own bitcoin easily without trusting anyone.

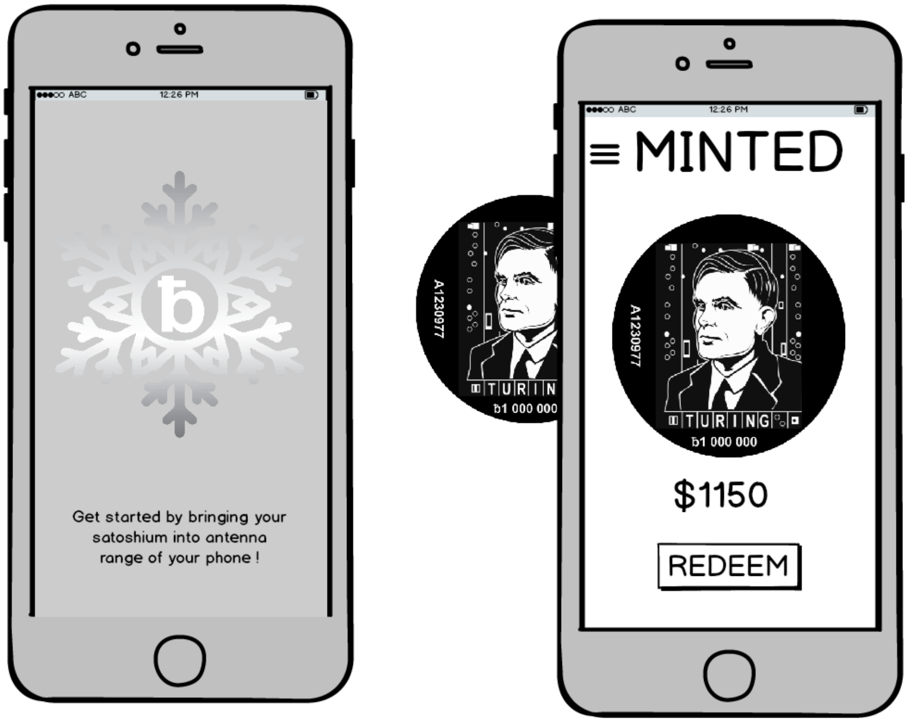
Novices can buy, sell, spend and receive minted satoshiums, circulating them hand-to-hand without touching the blockchain. Since they neither mint nor redeem satoshium, novices have no need to understand Bitcoin addresses or related complexities. A newbie user needs only to understand how to check whether a satoshium is minted using a smartphone app.

While satoshiums can circulate between untrusted strangers, initially most satoshiums will likely “circulate” only once, from minter to novice, after which the satoshium may lie dormant “hodled” for a long period until it is finally redeemed.

For practical purposes, satoshiums are bitcoin containers for onboarding, hodling, and occasional re-selling. To secure a satoshium, hide it, or put it in a safe deposit box. A beginner can become a minter via a gentle learning curve.

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-resistant way is also far safer than using an easily tampered hologram (e.g. Casascius) or worse, a scratch-off like how lotto tickets are sold.

When bitcoin exchanges eventually offer satoshium integration, even novices can mint and redeem satoshium directly from an exchange-linked bank while still fully controlling their secrets.



Get started by bringing your satoshium into antenna range of your phone !

Figure 1. Verification of Minted Status

A smartphone performs:

- Minting: Creation of a minted satoshium.
- 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.

Satoshiums are reusable. After redemption, the satoshium can be re-minted 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.

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		✓		✓	✓	✓
Paper Wallet				✓		✓
Bitcoin ETF	✓				✓	
Bitcoin Bank (Coinbase)					✓	✓

Figure 2 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. Existing solutions could be potentially be made "easy" by working on the usability concerns we have surfaced. We would be very pleased if this came to pass.

We reject “No Malware” for paper wallets, web wallets, and phone wallets because in practice most users do not create or redeem such wallets safely -- which is to say using an air-gapped and vetted installation media such as a Live CD/Bootable OS.

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 [9] 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. There is no custom chip manufacturing for Satoshium. Satoshium uses standard, commodity JavaCard cryptoprocessors. The satoshium needs no battery, as described in section 3 below. We assume the coin form factor of NFC cryptoprocessor-based satoshiums throughout the whitepaper, though other form factors are possible.

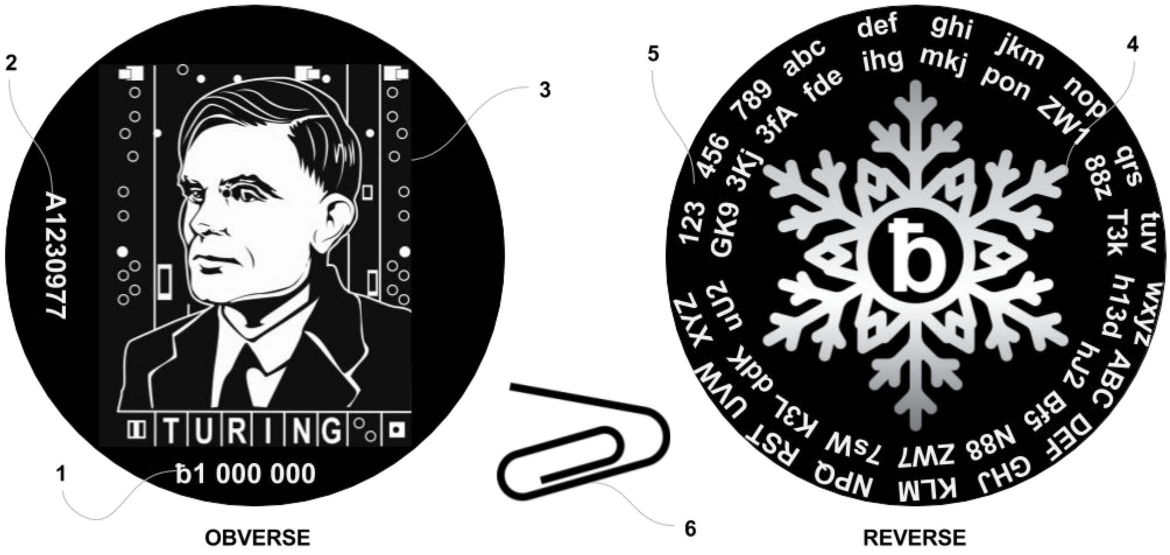

2
3
5
4
A1230977
TURING
ƀ1 000 000
1
6
OBVERSE
REVERSE
def ghi jkm nop qrs tuv wxyz ABC DEF GHJ KLM NPQ RST UVW XYZ 123 456 789 abc
ihg mkj pon ZW1 88z T3k h13d hJ2 B/5 N88 ZWZ 7sW K3L ddk un2 GK9 3Kj 3fA fde
ƀ

Figure 3 Satoshium

The satoshium features: Denomination **1**. Serial Number, which includes a Series identifier **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 secret **5.** and satoshium button **6**.

The cryptoprocessor controls access to the bitcoin secret, such that it may never be revealed when the satoshium has minted status. The satoshium responds to requests from a satoshium client device, generally a smartphone. The satoshium proves its genuine-ness with a cryptographic signature.

Possession of the satoshium 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.

Satoshium identkeys are deterministically derived from parent keys controlled by the Satoshium enterprise. This mitigates the danger of a secure element being compromised. Defeat of a secure element only reveals the key material for that single device.

Compromise of identkeys keys through insider fraud or outsider espionage presents an opportunity for counterfeiting. We defer an in depth consideration of counterfeiting to Section 6.

We cover security considerations for the on-coin security elements in the Appendix.

The satoshium should 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 [3] 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.

3. Smartphone

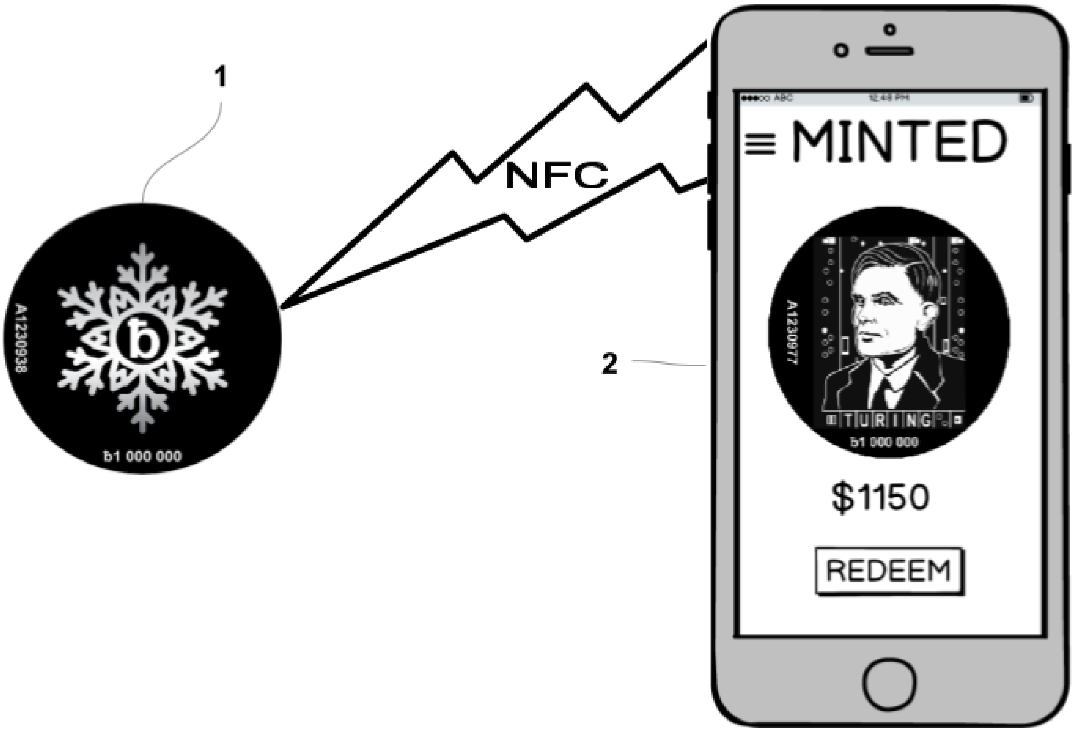


Figure 4 Satoshium communicating with Smartphone

A satoshium **1** communicates with and is powered by a smartphone or a micro USB connection **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 not be generic, we usually just write “phone.”

The phone stores no secrets, and no bitcoin is lost if the phone is stolen, damaged or compromised with malware. 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. To aid implementers we point out potential security vulnerabilities for the key state transitions. The security focus is on phone malware, as this seems to be the likeliest threat. The Counterfeiting section later considers satoshium malware in depth.

4.1 Overview

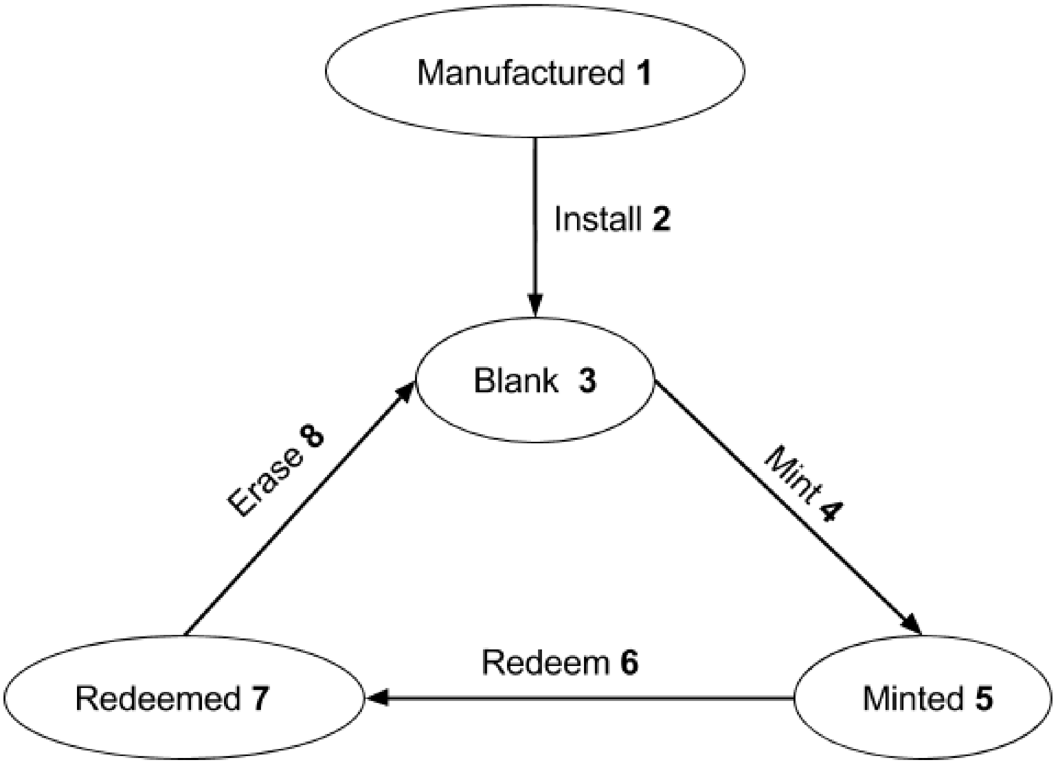


Figure 5 Basic lifecycle of a satoshium

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 back to Blank state via erasure **8** after which it can be re-minted with a new address.

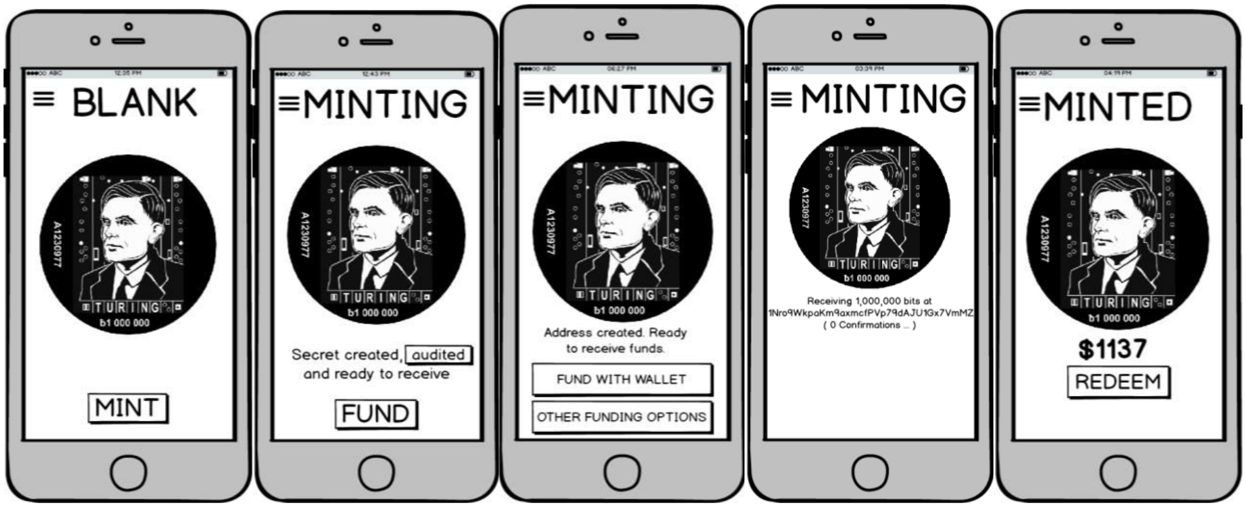
4.2 Installation

An 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
- Serial Number as engraved on the surface.
- Satoshium identkey pair
- 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

Address created. Ready to receive funds.

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 corresponding to this secret. The satoshium checks an SPV proof of funding before changing its status to minted.

When exchanges integrate with satoshium ("other funding options"), buyers will fund satoshium directly with exchange linked bank accounts and avoid ever needing to see or understand bitcoin addresses.

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 in the case of a counterfeit satoshium running malware, the attacker cannot steal bitcoins by controlling the bitcoin secret.

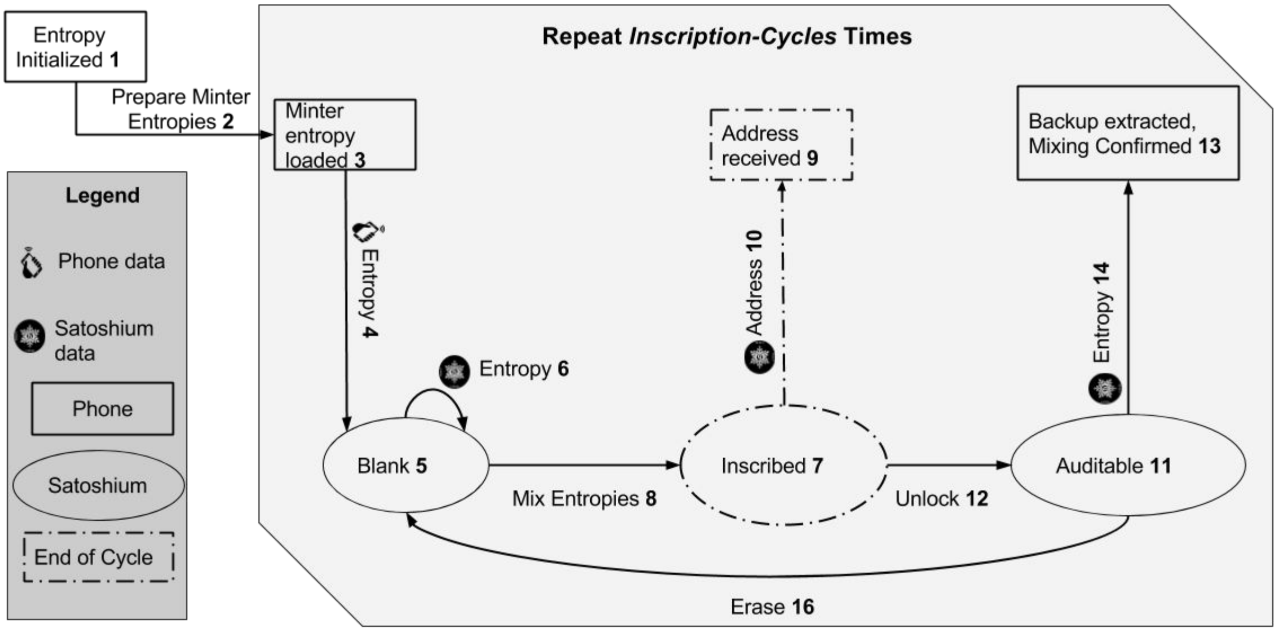


Figure 9 Inscription

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 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 that is prepared and not known to the satoshium **1.**

One by one, the minter entropy strings are loaded **2** and used in repeated inscription cycles. Each inscription cycle except for the last one occurs for the purpose of challenging the satoshium to ensure it isn't cheating. The last inscription cycle ends with the satoshium being Inscribed **7** and its bitcoin address (but not its secret) being revealed to the phone **9**.

For each inscription cycle, 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 (mechanism still to be determined) **8** to generate a BIP39 512 bit bitcoin secret [8]. This is used to generate the bitcoin address, making the satoshium Inscribed **7**. The address is sent **10** to the phone **9**.

If the phone has not yet reached the last inscription cycle then it will 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 computing the bitcoin 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 inscription 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.

Following inscription the Funding part of the minting process is initiated.

4.3.2 Funding

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

The Bitcoin network routinely and cheaply serves SPV proofs for arbitrary addresses [1, 6]. Normally an offline SPV wallet would need to confirm that verified funds were not later spent, but the satoshium lifecycle ensures that minted funds can't be spent so in this case no such confirmation is needed. As an implementation note, since the satoshium only needs to check a single proof from a single action of Minting, the satoshium does not need to cache headers for reuse as the SPV proof progresses .

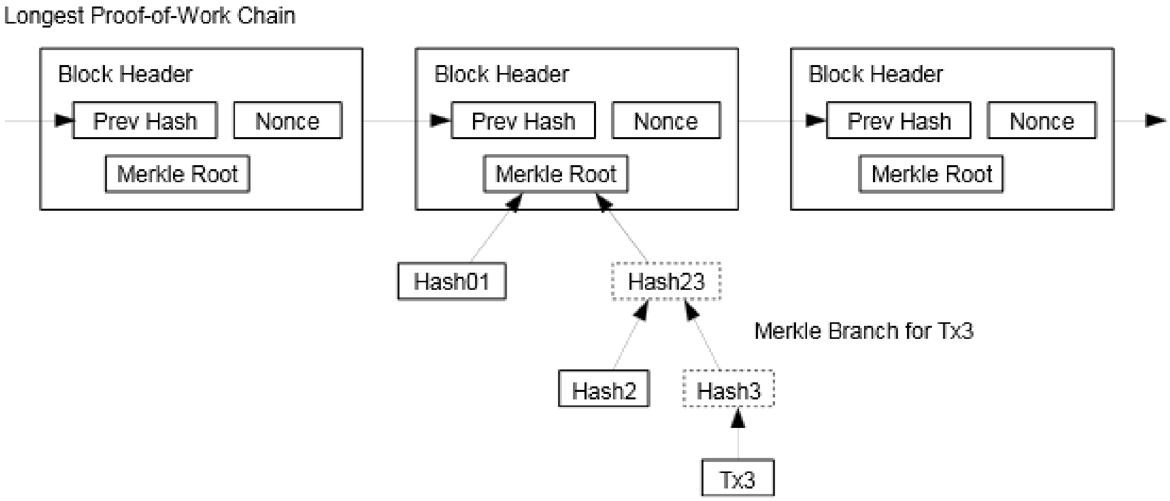


Figure 10 SPV Proof of Sufficient Funds

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 provided by the phone to the satoshium of any address funded by Tx3 [1]. This proof can be made arbitrarily expensive by requiring more confirmations.

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. Satoshium must demand a high number of confirmations to guard against long range attacks where the attacker buys sufficient amount of hashrate in a decade or more in the future to fool the blanks into switching to Minted status after seeing only a few block headers fabricated by future ASICs at the now-ancient difficulty. A requirement for a 1000 block headers built on top of the funding transaction delays minting by roughly a week but makes long range attacks probabilistically infeasible by making them uneconomical.

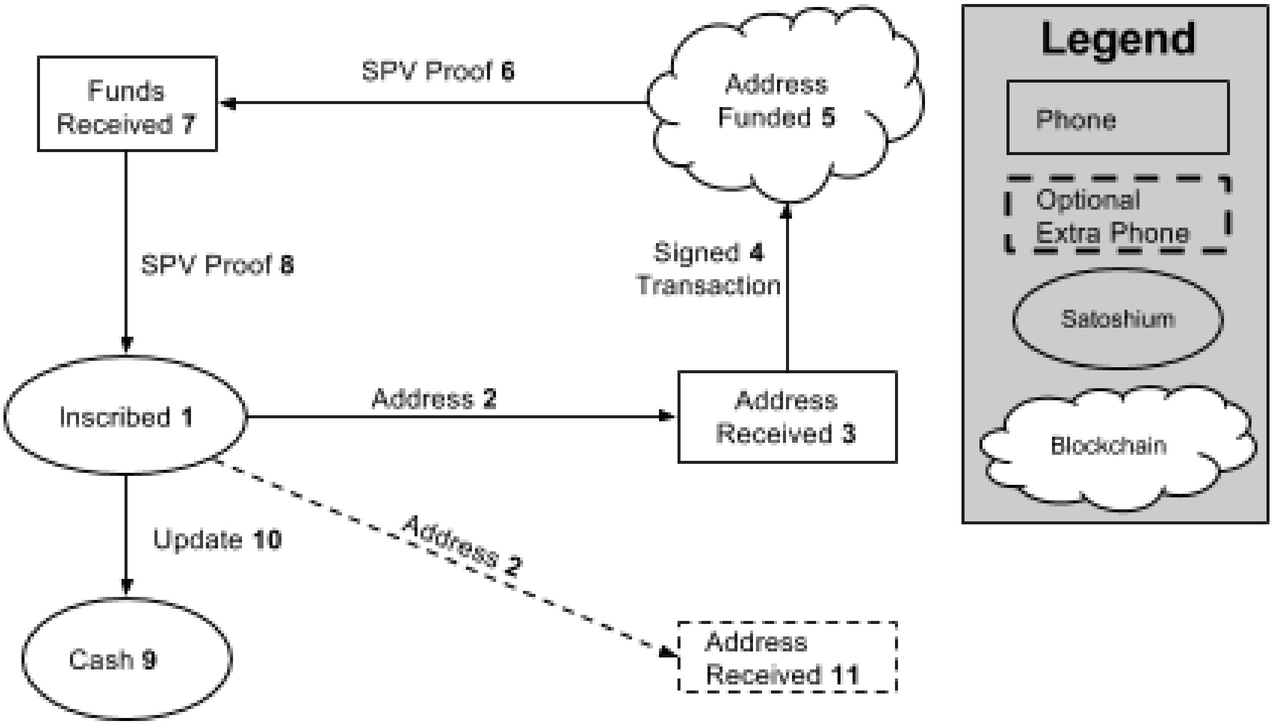


Figure 11 Funding

While in the Inscribed state **1** the satoshium sends the phone **3** the funding address **2**. 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 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 **11** 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. 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 may be done routinely whenever a satoshium changes hands.

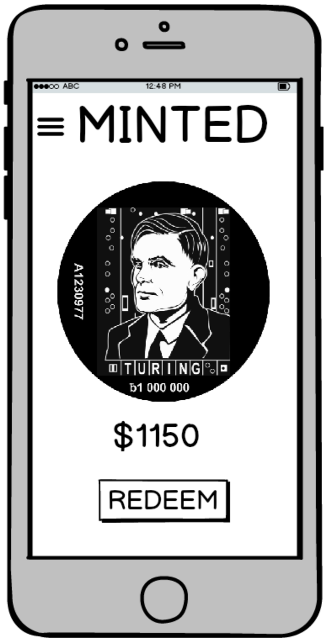


Figure 7 Verification of Minted Status

In Figure 7, a 1,000,000 bit satoshium (not shown) is verified as Minted by a phone. The phone displays a satoshium matching the actual satoshium's serial number and denomination. This indicates that the satoshium has proved its software integrity and genuineness. The phone reports that the satoshium is minted and therefore transferable.

The phone determines that the satoshium is genuine by challenging it with a nonce, as described in [4]. 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 satoshium's identkey. The user can visually verify that the serial number on the satoshium and the serial number on the phone match. All of this is used by client software to authenticate the satoshium as genuine.

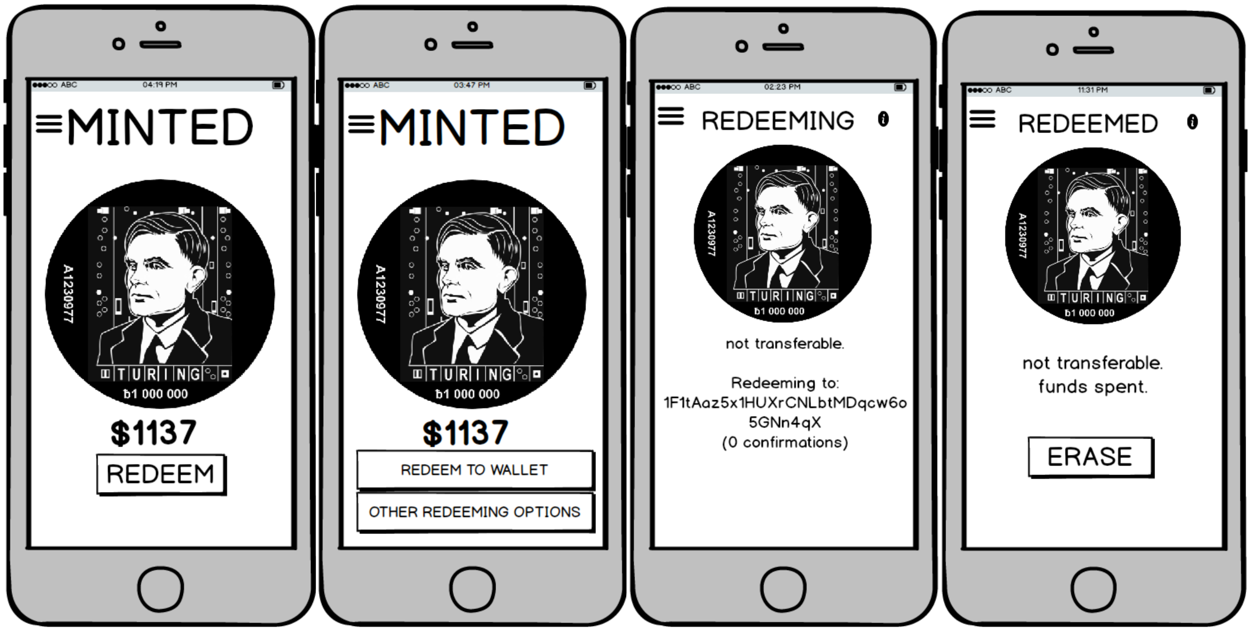
4.4.1 Security Considerations (Verification of Minted Status)

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 buyer might trust a seller's phone, which is running 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.

A thief posing as a buyer could grab the satoshium and run away with it during verification of minted status.

If the phone is online, it checks the bitcoin balance by querying the bitcoin network. If bitcoin on a satoshium 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[5], 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 the Satoshium enterprise.

4.5 Redemption



not transferable.

Redeeming to:
1F1tAaz5x1HUXrCNLbtMDqcw6o
5GNn4qX
(0 confirmations)

not transferable.
funds spent.

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 their satoshium directly to fiat in an exchange-linked bank account, without ever seeing a bitcoin address.

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

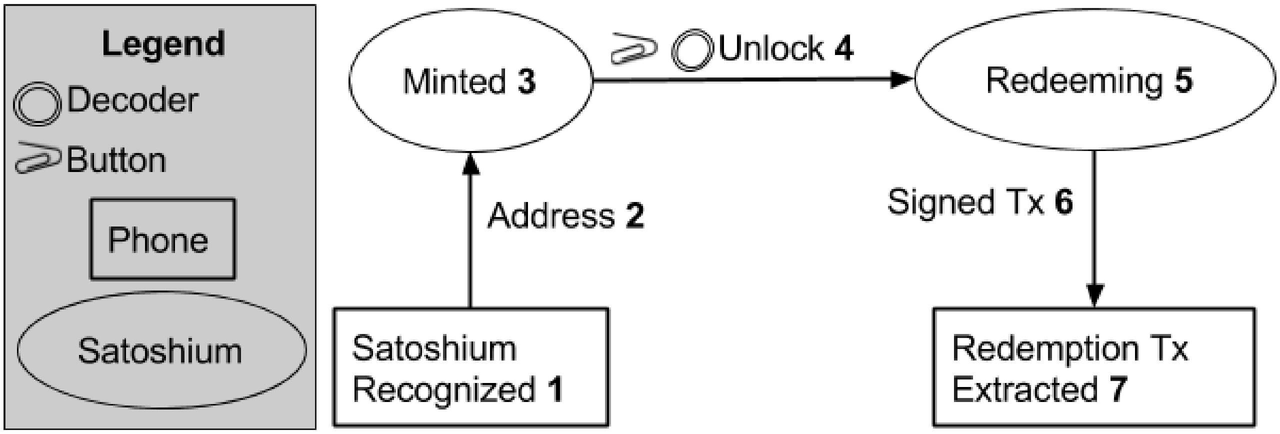


Figure 12 Redeeming

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.

Not pictured: The phone transmits an SPV proof of the confirmed transaction to the satoshium. The satoshium verifies the SPV proof and changes its status to Redeemed. The satoshium can now be safely erased.

4.5.1 Security Considerations (Redemption)

See Appendix section Security Considerations, Decoder Ring.

5. Platform Integrity

Platform Integrity [7] means the software running on some hardware is what it claims to be and not malware. Many potential malware attacks are possible once platform integrity has been compromised. The key to stopping all such attacks is to enforce platform integrity effectively.

To do this, the software running on the satoshium should be open source, with deterministic and reproducible builds [2]

5.1 Attestation

Attestation is a claim by a platform provider that a process running on the platform is actually some software being attested to. The claim is supported by cryptographic evidence: a signature or signatures which can be verified with a well known public key. The signed data is ideally 1) a nonce (random number, to prevent replay attacks) signed by the platform provider (hardware manufacturer or OS packager) to prove that the platform is the one claimed, along with 2) a signed hash of the executable from the packager of the software that they have greenlighted the running software. If the hash can be checked against a reproducible build, users of the software can examine it themselves.

Attestation is a process for cryptographically providing evidence for platform integrity. Attestation as a policy can have a variety of implementation mechanisms, but in general a hash of the binary is necessary and some data must be signed with .

The attestation may provide evidence for trusting the platform itself, or the binary alone. If the hardware layer supports embedding secret key material in a secure element, the attestation may include signing a challenge nonce.

5.2 Self Attestation

A common practice in the software industry is Self Attestation. In this model, the software is signed by the distributor of the software. This is how security sensitive software (e.g., a bitcoin wallet) is typically provided for the vanilla desktop platform.

5.3 Third-Party Attestation

The idea with third-party attestation is to not require trust in the distributor of the software. This requires some other entity (i.e. the third party which is neither end user nor packager of the software) to attest that the software installed is actually the software compiled deterministically from the open source. We call this Third-Party Attestation or TPA.

In this model the attesting third party would be an independent provider of the hardware that Satoshium is implemented on. The user need only trust the provider of the underlying hardware.

5.4 Satoshium Attestation Policy

Satoshiums use a combination of Self Attestation and Third-Party Attestation implementations.

6. Counterfeiting

The following section considers counterfeiting attacks on satoshium.

6.1 Enclosure

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

6.1.1 Enclosure Alteration or Substitution Attacks

The attacker might attempt to substitute one enclosure for another or alter denominations on the enclosure. The defense against such an attack is is similar to what’s used for regular cash. Different denomination could employ different diameters and different design

6.1.2 Tap Attack

An attacker could implant the cryptoprocessor from a genuine satoshium into a counterfeit enclosure. The objective of the Tap Attack is to trick a user into funding this counterfeit device. The counterfeit enclosure has a battery, a second processor that is under the attacker's control and which is programmed with the decoder ring secret, and a physical actuator or some other means for pressing the button that is also under the attacker's control. The attacker's processor must be able to communicate over NFC, transmit cellular data, and know the decoder ring secret. From the satoshium's point of view, the attacker's processor acts like a phone with the satoshium app installed. After funding, the attacker's processor redeems the funds to an address it controls, enters the appropriate decoder ring secret, fakes a button press from the user, 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.

This attack seems farfetched enough not to assign it undue importance. Faking the button press seems particularly challenging.

Since, in addition to the cryptographic proof, the user also determines if the satoshium is genuine by examining its physical appearance, this attack and potentially other enclosure attacks can be further deterred by putting effort into making enclosure counterfeiting and tampering expensive.

6.2 Cryptoprocessor

Platform integrity does not help if the attack takes place at the hardware level.

This section considers counterfeiting where the attacker uses a stock enclosure, but installs a platform integrity subverting malicious cryptoprocessor.

6.2.2 Exfiltration of Secrets Through a Back Door

A malicious cryptoprocessor enclosed in the genuine enclosure could contain a hardware backdoor. For instance, the backdoor might be that if the attacker sends a special secret bytestring, the satoshium responds by revealing all secrets, including identkey and bitcoin secret. Thus equipped, the attacker could purchase circulating satoshiums and then sell them after collecting the secrets. The attacker can then steal the bitcoin off the circulating satoshium, knowing the secret.

Such malicious hardware could also permit arbitrary reprogramming of the putatively write only firmware which determines the behavior of the satoshium, while preserving the integrity certificate for the audited and whitelisted build.

If the satoshium relied on self attestation only, without third party attestation, the satoshium packager could create satoshiums with a software backdoor using stock hardware. Since satoshiums use third party attestation as well, however, such an attack is ruled out.

Ultimately all counterfeiting attacks, including cryptoprocessor counterfeiting, are mitigated by "know your customer" policies -- in the gold coin market rather than banking sense. Due to counterfeiting and legal risk, coin dealers generally generally steer clear of large purchases when the buyer is unknown or has a poor reputation. When a rare coin market develops for satoshium, it may work similarly.

7. 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. Satoshiums are attractive to collectors, humane enough to onboard would-be nontechnical hodlers, and circulatable offline in the wild.

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

[4] 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

[5] 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

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

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

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

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

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

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 satoshium, 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 [10] to prevent 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 being stored 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)

If the decoder ring secret leaks, it could 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

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 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 two button press 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. The button presses do not initiate redemption, but are only for confirmation. If the satoshium is not expecting button presses, this user action is disregarded.

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.

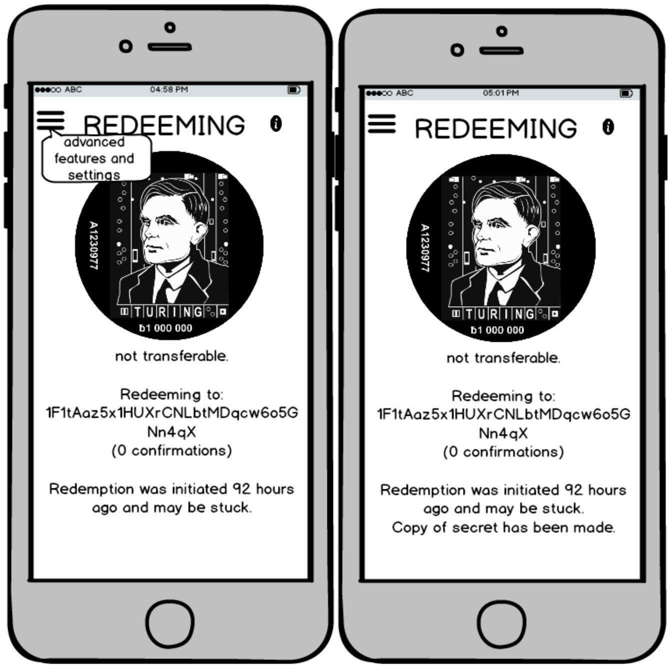
The button cannot protect against users who don’t know the rules about button presses. Phone malware could trick the user into doing the three button press escape hatch sequence by stating "This is a routine security check by the Satoshium Team to prove you rightfully own of your bitcoin.... Please enter the decoder ring solution for the following address, and press the button three times for confirmation of your entry..." (In fact, the user should never press the button more than once except when performing a security sensitive operation.) The attacker can then redeem redeem to an arbitrary address.

Even when used properly, 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 disables 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 12-word BIP39 mnemonic restorable to almost any bitcoin wallet [8]. Secret extraction may be used as a recovery procedure for redemptions gone wrong.



not transferable.

Redeeming to:
1F1tAaz5x1HUXrCNLbtMDqcw6o5G
Nn4qX
(0 confirmations)

Redemption was initiated 92 hours ago and may be stuck.

not transferable.

Redeeming to:
1F1tAaz5x1HUXrCNLbtMDqcw6o5G
Nn4qX
(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 backup a minted satoshium for peace of mind for long term “cold storage”.

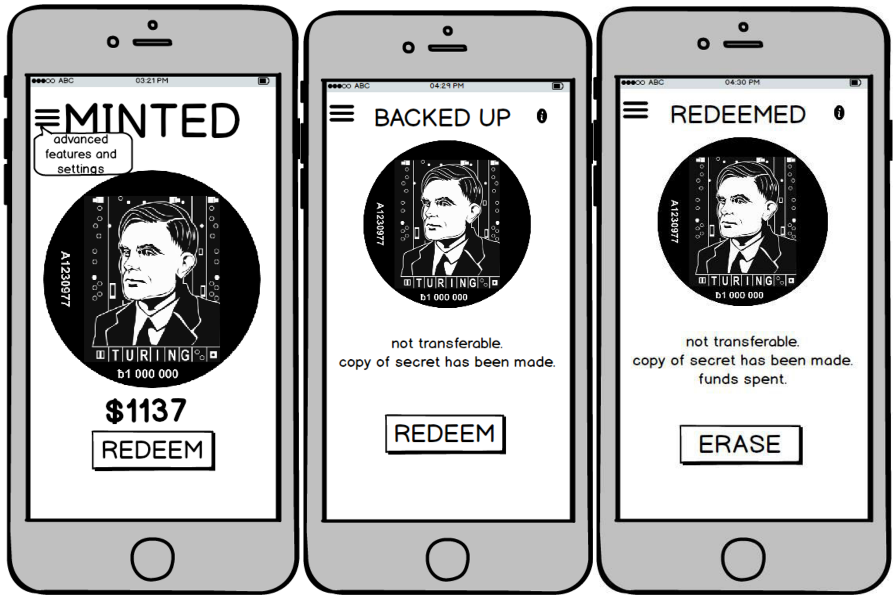


Figure 14 Secret Extraction for Value Extraction

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.