CryptoDelivery™ - Bitcoin Customer Transfer Specification

delivery.crypto.farm

by
Crypto Farm Corp.
CANADA
info@crypto.farm

ABSTRACT

Here we illustrate and explain the full checkout back-end process that occurs when a customer (the buyer) purchases a Bitcoin (BTC) Paper Wallet from the *delivery.crypto.farm* server (the seller). It is designed such that once the Bitcoin has been successfully delivered to the customer, our company does not keep any record or physical trace of the private keys on the printed Paper Wallet, hence the customer purchaser truly is the only one who owns the final asset. They have nothing to worry about for long-term investment storage of the product – even if our company gets "hacked", their BTC is safe and sound. If their Paper Wallet is lost however, so will be the printed BTC value with absolutely no way of recovery. The entire process is done on an isolated cold-storage environment that has never touched the internet, so the chances of a data breach or information leak are eliminated. From initial order through to physical delivery we show this process. We then present and comment on the cryptocurrency security standard adhered to during the process.

ISSN: *pending*

Table of Contents

List of Figures

ISSN: *pending*

1.0 Process Overview

First we define the Printing Schedule, which is used to determine the Paper Wallet loaded value to be delivered to the customer. For example, on a $10,000 CAD order, we load 90%, and the result is a guaranteed delivery of $9,000 worth of BTC at the exact market rate (we don't change any extra exchange fees). We display the Printed Amount instantly on the Paper Wallet GUI (graphical user interface), so the customer knows exactly how much BTC they will be receiving from their order. See Figure 1. This schedule is subject to change:

Wallet Funding Amount ($CAD Equivalent)	Market Value Loaded (BTC Printing Schedule)
100 – 250	70%
250 – 500	72%
500 – 1,000	75%
1,000 – 5,000	80%
5,000 – 10,000	85%
10,000 – 100,000	90%

Figure 1: BTC Printing Schedule 2020 release on *delivery.crypto.farm* server

Once the fiat order amount is determined, the customer can proceed to payment through our processing parter PayPal Canada (they support billing in many local currencies). Customer can choose many options to pay such as VISA and direct Bank account debit, as facilitated by PayPal. We require all PayPal orders to have a verified email and shipping address, hence to further strengthening the order delivery legitimacy and a verified email as to have direct contact with the customer on a known inbox they can open. We proceed to Sec.2 which outlines the printing process and environment.

2.0 Cold-storage Printing

Once customer order funds are confirmed, we begin to manufacture and print their Paper Wallet. We use the most recent copy of Bitcoin Core [1] installed on a formatted Linux machine operating system (OS) of Ubuntu 18.04LTS [2] that has never touched the internet. Figure 2 below outlines the working isolated environment:

ISSN: *pending*

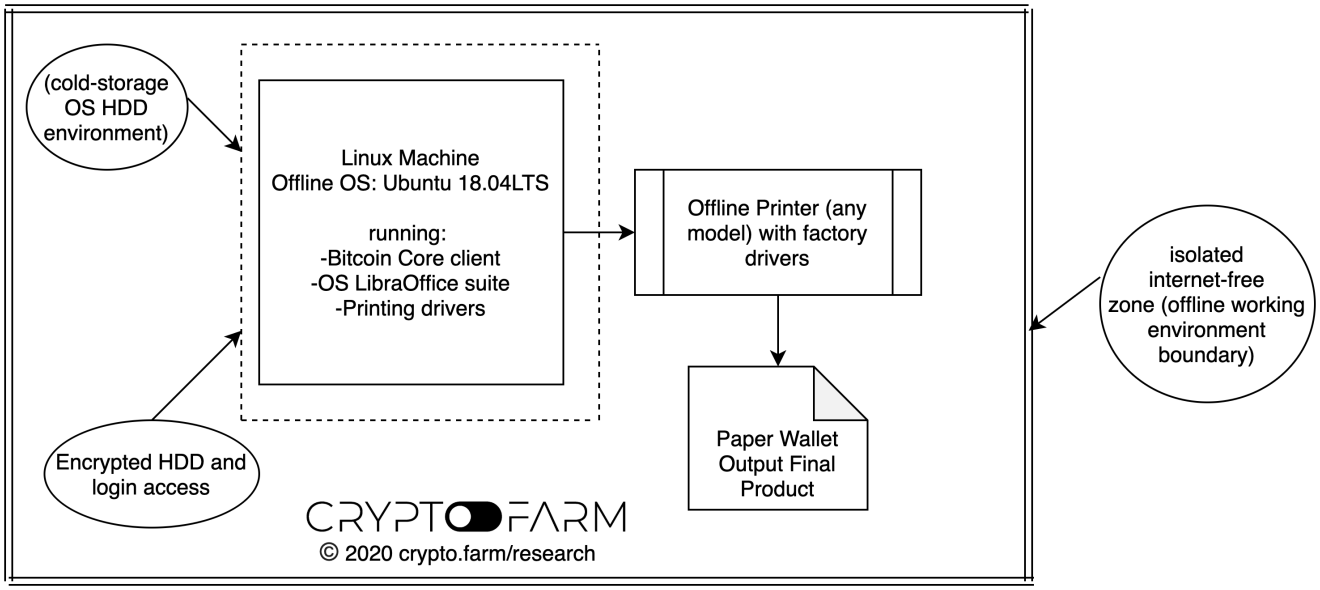

Figure 2: Isolated cold-storage printing environment

Here it can be seen that the actions of generating the public and private key that are printed on the customers Paper Wallet, are done from a totally secure offline environment. Each Paper Wallet gets a unique wallet.dat file and set of keys for printing. Once printed we only record the public address, as that will be used as shown in Sec.3. for delivering the BTC. Once printed the wallet.dat file is deleted with at least a triple-pass scrubbing technique, and hence there is now no physical trace of the private keys on the HDD except now hidden inside the printed Paper Wallet for the customer.

3.0 Delivery Confirmation

We then ship the newly printed Paper Wallet to the customers verified Shipping Details as collected by PayPal during the checkout process. Once the customer has received the wallet in had at their address, there is final instructions included. We ask that they email us from the same verified email as used during checkout, and let us know that they have received the Paper Wallet in good condition. Final step is to then load the real BTC from our company holdings BTC wallet to their public key. This way we are never shipping a loaded Paper Wallet, incase the mail gets lost or stolen, there would be no BTC lost during a failed delivery attempt. Figure 3 illustrates this:

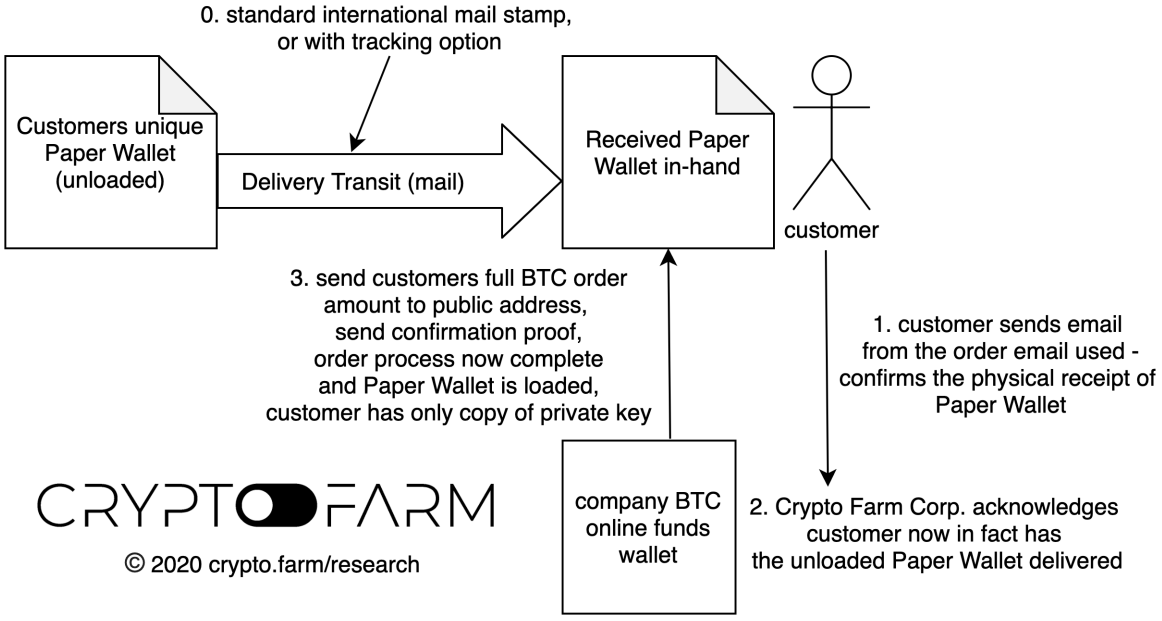

Figure 3: Delivery procedure with customer confirmation logic

Once we get delivery confirmation from the customer, we send a confirmation email showing the complete transfer transaction proof, letting them know they now have their BTC successfully delivered and the only copy of the private key. Customers can then check there public address balance using the following free smartphone apps, by scanning the public address QR code on the open side of the Paper Wallet, and see that they indeed have their Bitcoin now in hand on the Paper Wallet. The order process is now complete and delivery is successful, customer has only copy of the private key.

On Android PlayStore:

“Wealth Check – Bitcoin Wallet Balance and History” by Juraj Kusnier

and on iOS Apple Store:

“Bitcoin Monitor – Market Check” by Leszek Szary

4.0 Delivery Security Standard

We follow with best practices the Cryptocurrency Security Standard (CCSS) to a Level 1 protocol [3]. Here in Figure 4 below, the standard security matrix is presented with relative comments to the CryptoDelivery process:

Security Category	Tech Aspect	Component	Uncertified Protocol	Level 1 Certified Protocol	Company Comment relative for CryptoDelivery
Cryptographic Asset Management Pt.1	Key / Seed Generation	Operator-created Key / Seed	Keys/seeds are issued to the keyholder by another actor	Keys/seeds are created by the key/seed operator themselves	Yes this is done in offline envi. By human operator
		Creation methodology is validated			N/A
		DRBG Compliance	Keys / seeds are created with a non-compliant DRBG	Key/seed is created using a NIST SP 800-90A compliant DRBG	Created with Bitcoin Core 0.18+ protocol DRBG
		Entropy Pool	Keys / seeds are created on system with insufficient entropy	Key/seed is created on a system with sufficient entropy	Yes
	Wallet Creation	Unique address per transaction	Wallets/addresses are reused	Unique addresses are generated for every transaction	Yes
		Multiple keys for signing			N/A
		Redundant key for recovery			N/A
		Deterministic wallets			N/A
		Geographic distribution of keys			N/A
		Organizational distribution of keys			N/A
	Key Storage	Primary keys are stored encrypted	Keys/seeds are stored in plain text	Key/seed is stored with strong encryption	Key is deleted from system once printed, hence only copy is in customers Paper Wallet
		Backup key exists	No key backups exist	Key/seed backup exists	N/A
		Backup key has environmental protection		Key/seed backup is protected from environmental damage	N/A no backup is kept
		Backup key is access-controlled			N/A
		Backup key has tamper-evident seal			N/A
		Backup key is encrypted			N/A
	Key Usage Pt.1	Key access requires user/pass/nth factor	Access to key/seed does not require sufficient factors of authentication to provide adequate security	Access to key/seed requires an identifier and at least 2 other factors (password, MFA token, in-person verification by guard, IP address whitelist, physical key to gain access to secured storage, countersigning organization)	Yes, the initial generation required HDD pass seed (very long), user login pass, and physical office access (3 layers)

ISSN: *pending*

Cryptographic Asset Management Pt.2	Key Usage Pt.2	Keys are only used in a trusted environment	Keys/seeds are used on public/untrusted machines, or in environments where passwords/secrets can be disclosed	Keys/seeds are only used in trusted environments	Yes cold-storage offline envi. See Figure 2
		Operator reference checks	No checks are performed on key/ seed holders	Key/seed holders have references checked	Yes
		Operator ID checks	ID of one or more operators is not established	Key/seed holders have identify verified	Yes
		Operator background checks			Partial, not criminal background check
		Spends are verified before signing			Yes
		No two keys are used on one device	Multiple keys for a single asset used on one device	No two keys belonging to the same wallet are present on any one device	N/A all wallets have unique keys
		DRBG Compliance	Signatures use a non-compliant DRBG and may be susceptible to "dirty signature" vulnerabilities	The 'k' values in digital signatures are created using a NIST SP 800-90A compliant DRBG OR The 'k' values are created deterministically according to RFC 6979	N/A as this is from Bitcoin Core keygen 0.18+ or newer complacence per bitcoin.org source
	Key Compromise Protocol (KCP)	KCP Exists	No staff has the necessary knowledge/experience/training required to rebuild the keys/ wallets when necessary	An employee with knowledge/experience with the system is able to direct staff with appropriate tasks to remove the risk of compromise.	Yes
		KCP Training + Rehearsals			Infrequent
	Keyholder Grant/Revoke Policies & Procedures	Grant/Revoke Procedures/Checklist	No Policy/Procedures in place	Permission changes for incoming/outgoing staff are performed by someone knowledgeable with the system	Yes sysadmin will purge any old staff logins, they would need to physically be in the office to access
		Requests made via Authenticated Communication Channel			N/A simple
		Grant/Revoke Audit Trail			N/A
Operations	Security Audits / Pentests	Security Audit	No proof of security	A developer who is knowledgeable about bitcoin security has assisted in the design and development of the system	Yes
	Data Sanitization Policy (DSP)	DSP Exists	No sanitization is performed on decommissioned media	Staff is aware of how data remains on digital media after deletion, how to securely wipe data, and when secure wiping should be used	Yes they know how to wipe the private keys successfully upon each order print (multiple-pass methods)
		Audit Trail of all media sanitization			N/A
	Proof of Reserve (PoR)	Proof of Reserve Audits	No audit has been performed	A PoR audit has been completed	N/A no funds held in trust
	Audit Logs	Application Audit Logs	No audit logs	Audit logs exist for some actions within the system	Yes linux sys logs only
		Backup of Audit Logs			Infrequent

Figure 4: CCSS compliance matrix of Level 1 standard used during CryptoDelivery process

ISSN: *pending*

5.0 Conclusion

The delivery process is a robust method that protects both the product asset printing supplier (i.e. Crypto Farm Corp. – the seller) and the global customer individual (the buyer). There is no chance of any funds being lost by either party during the delivery process, and most importantly all liability is transferred to the product customer once delivered, as they are the only party who has a copy of the asset private key, and are the true owners of the Bitcoin delivery product. Which is a win-win for everyone, and a great decentralized secure way of doing business.

6.0 References

[1] Bitcoin Core client latest release, retrieved: 22-FEB-20, https://bitcoin.org/en/bitcoin-core/
[2] Ubuntu offical 18.04LTS repository download, retrieved: 22-FEB-20, http://releases.ubuntu.com/18.04/
[3] CCSS open standards security matrix, retrieved: 22-FEB-20, https://cryptoconsortium.github.io/CCSS/Matrix/

ISSN: *pending*