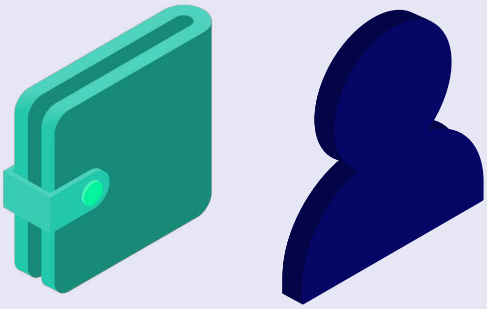
21 ANALYTICS

The Satoshi Test: EXPLAINED

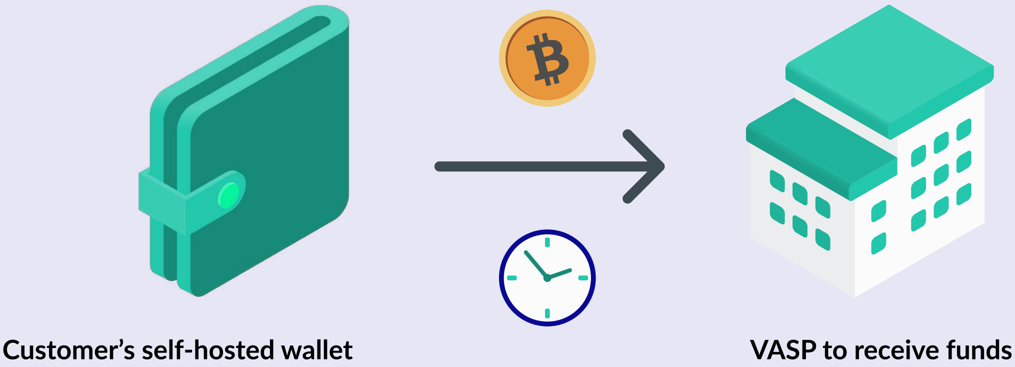
Find out what a Satoshi Test is with an explanation of how it works.
Learn its pros and cons and see what it looks like from a VASP's perspective.

What Is a Satoshi Test?

A Satoshi Test is a method to verify ownership of an address belonging to a VASP customer's self-hosted wallet.

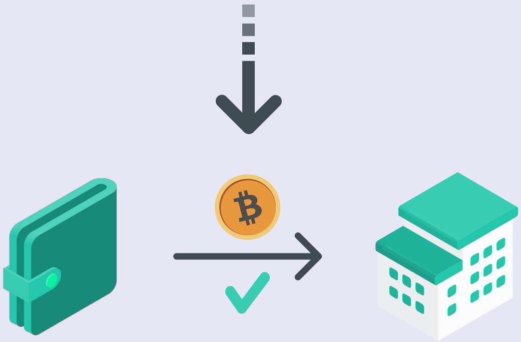


To verify the address's ownership, a small amount of crypto assets (coins), predefined by the VASP, is sent from the wallet owner's address to the VASP within a specific time period.

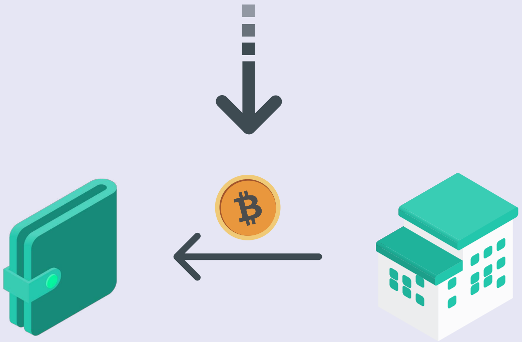


What Is a Satoshi Test?

If the wallet owner can successfully send the coins in the given time frame, it serves as proof of address ownership.



With successful transfers, the wallet user will be reimbursed for the transferred coins. However, the mining fees will not be returned.



If the transaction is unsuccessful for whatever reason, the wallet owner can reattempt the test. The VASP will resend a wallet address and timeframe to complete the test.

The proof is considered invalid if a wallet owner does not complete the transaction in the given timeframe.

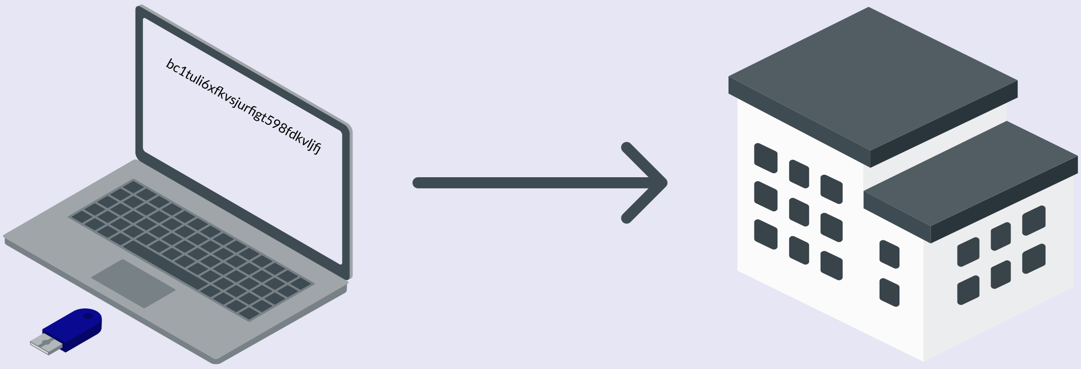
Depending on the VASP's jurisdiction and AML policy, a Satoshi Test only provides a proof for a limited time (e.g. 48 hours) and afterwards has to be repeated, even if the wallet user's address stays the same.

How Does It Work?

A Complete Satoshi Test Step-by-Step

1. The wallet user shares a withdrawal address with the VASP. Even though it’s for a new withdrawal, the address must have a cryptocurrency available to execute the Satoshi Test later.

   The cryptocurrency used must match the currency the wallet owner wishes to transact with.



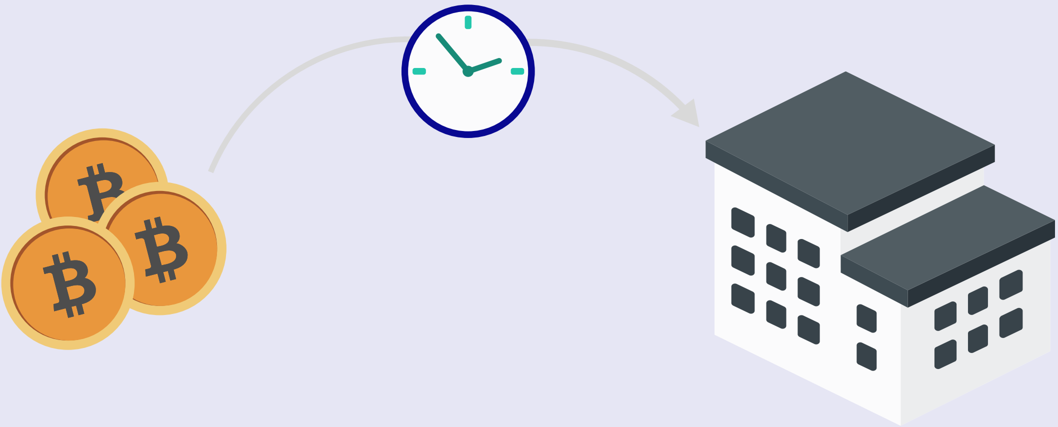
2. The VASP creates a Satoshi Test consisting of the following:

- The VASP’s Test address,
- A random amount, usually valued around USD 1,
- A maximum timeframe (usually between 15min and 48h) for the verification according to the applicable AML policy.

How Does It Work?

A Complete Satoshi Test Step-by-Step

3. This information is then shared with the VASP's customer through the VASP's website or via email/chat.
   The wallet user sends the VASP-defined amount of crypto from their pre-defined withdrawal address to the VASP's deposit address within the specified timeframe.



4. The VASP checks if the transaction has been executed exactly as agreed. If so, the address is whitelisted and ready for transactions. With 21 Travel Rule's live blockchain monitoring, the address is automatically whitelisted.

The Pros & Cons

What Are the Pros?

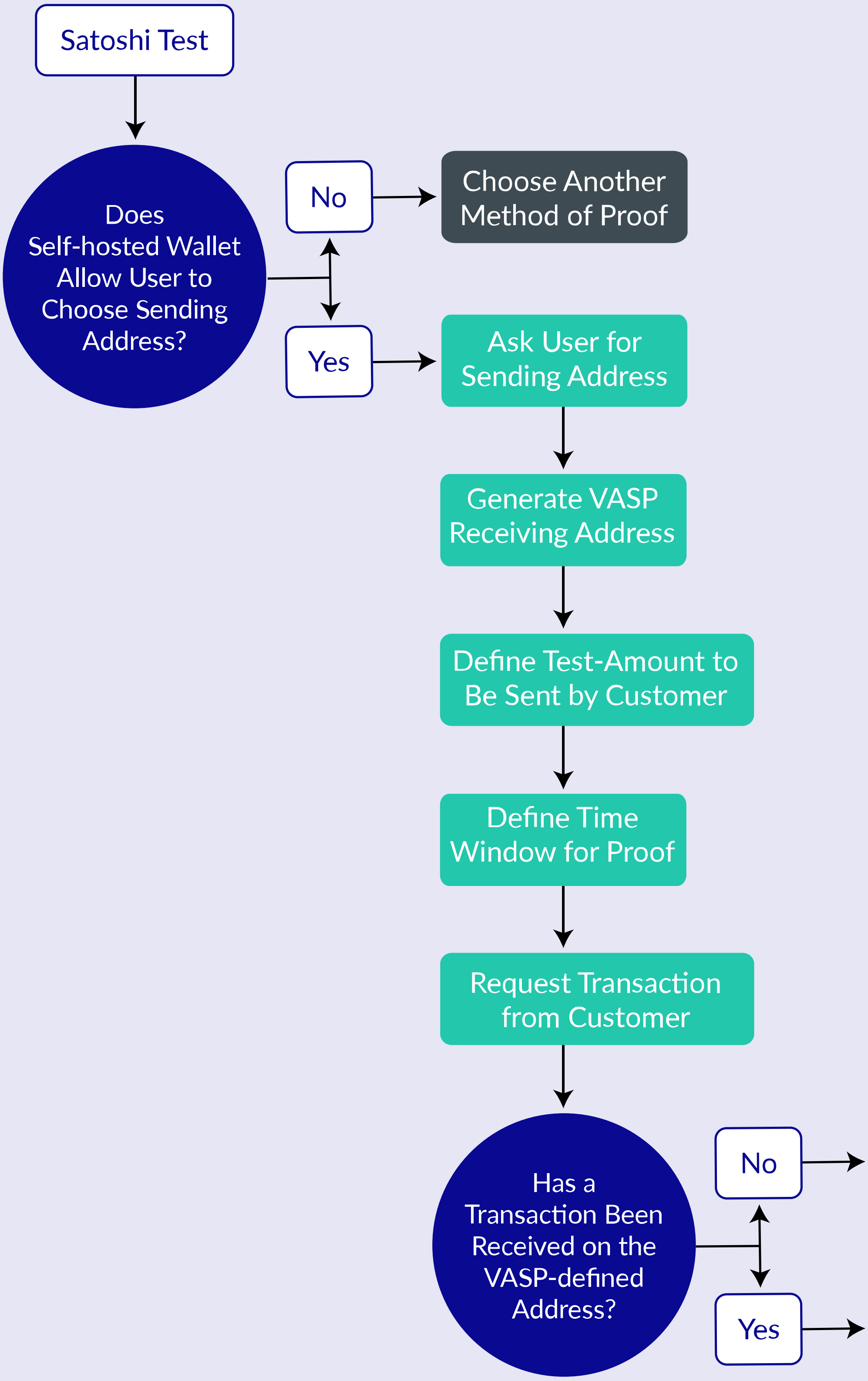
- The process can be automated on the VASP’s side.
- It is safer that visual proofs as it is harder to forge.

What Are the Cons?

- It’s not free. While the transferred amount can be returned, the transaction fees usually are not, and some VASPs will charge wallet users for that process since staff time is needed for review.
  This can encourage address reuse. Which is great to save money, but terrible from a security standpoint.
- Sending from a specific address is difficult with UTXO-based cryptocurrencies, such as Bitcoin, and often not possible with a wallet.
- It is cumbersome, adds friction and offers a poor experience for the end customer, who often requests the VASP’s support to perform it.
- This, too, can encourage address reuse as the VASP’s customer does not want to repeat this burdensome process.
- The process can be slow if it is not fully automated on the VASP’s side, as the VASP’s compliance team needs to review and respond to the proof.

Satoshi Test Workflow

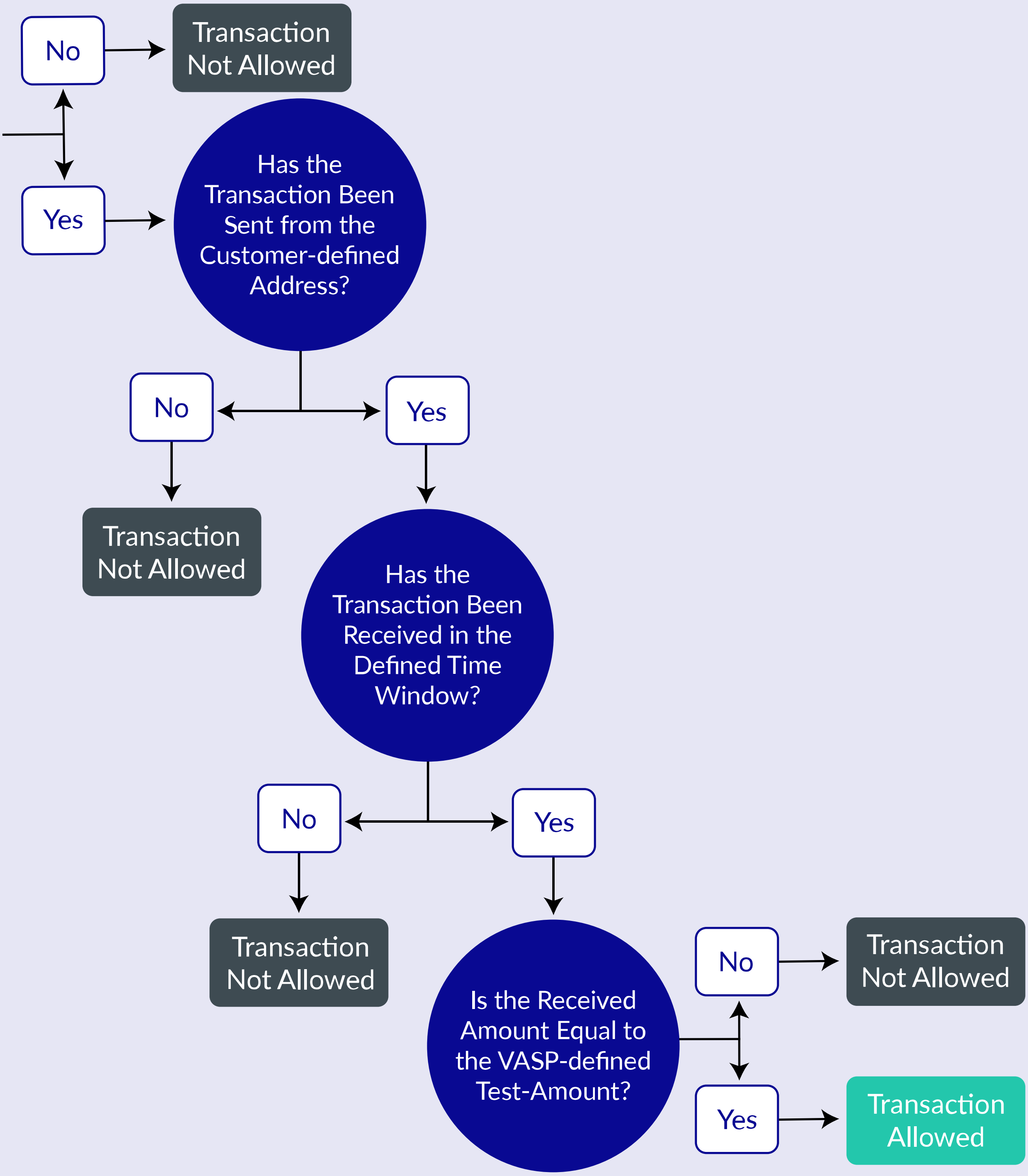
Implement the Satoshi Test into Your Processes: Step-by-Step Decision Tree


Satoshi Test
Does Self-hosted Wallet Allow User to Choose Sending Address?
No
Choose Another Method of Proof
Yes
Ask User for Sending Address
Generate VASP Receiving Address
Define Test-Amount to Be Sent by Customer
Define Time Window for Proof
Request Transaction from Customer
Has a Transaction Been Received on the VASP-defined Address?
No
Yes

21analytics.ch/what-is-a-satoshi-test/

Satoshi Test Workflow

Implement the Satoshi Test into Your Processes: Step-by-Step Decision Tree


No
Transaction Not Allowed
Yes
Has the Transaction Been Sent from the Customer-defined Address?
No
Yes
Transaction Not Allowed
Has the Transaction Been Received in the Defined Time Window?
No
Yes
Transaction Not Allowed
Is the Received Amount Equal to the VASP-defined Test-Amount?
No
Transaction Not Allowed
Yes
Transaction Allowed

About the Author

21 Analytics provides privacy-first Travel Rule compliance software. None of your data is shared with us.

Founded by Bitcoiners who have been working in the blockchain industry since 2014, 21 Analytics leverages its experience to advance our idea of combining compliance with data protection and strengthening privacy for financial intermediaries and their customers.

Request a Demo

This presentation contains information in summary form and is therefore intended for general guidance only. Although prepared with utmost care this publication is not intended to be a substitute for detailed research or professional advice. Therefore, by reading this publication, you agree that no liability for correctness, completeness and/or currentness will be assumed.
It is solely the responsibility of the readers to decide whether and in what form the information made available is relevant for their purposes. 21 Analytics AG accepts no responsibility, and on any specific matter, reference should be made to the appropriate advisor.

2024 21 Analytics AG. All Rights Reserved.