HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

MASTER THESIS

Mr.
Marvin Blaich

Growth by Constancy. Identifying the Impact of Taproot Asset Stablecoins on Bitcoin Adoption

Mittweida, February 2024

Faculty of **Applied Computer Sciences and Biosciences**

MASTER THESIS

Growth by Constancy. Identifying the Impact of Taproot Asset Stablecoins on Bitcoin Adoption

Author:
Marvin Blaich

Course of Study:
Blockchain & Distributed Ledger Technologies (DLT)

Seminar Group:
BC21w1-M

First Examiner:
Prof. Dr. rer. oec. Alexander Knauer

Second Examiner:
Diploma Economist Mario Oettler

Submission:
Mittweida, February 21, 2024

Defense/Evaluation:
Mittweida, 2024

Bibliographic Description:

Blaich, Marvin:
Growth by Constancy. Identifying the Impact of Taproot Asset Stablecoins on Bitcoin Adoption. – 2024. – Page number directories: 17 pages, page number content: 58 pages, page number appendices: 22 pages.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Faculty of Applied Computer Sciences and Biosciences, Master Thesis, 2024

Abstract:

The Taproot Assets protocol is a novel technology that enables the issuance of digital assets on Bitcoin. Since its announcement, the implementation of stablecoins was a predominant use case for its development. In combination with the Lightning Network, a stable asset could generate greater utilization and offer new applications. This potential phenomenon is evaluated statistically in this thesis through quantitative research in the form of an online survey and substantive theoretical studies. Adoption is analyzed based on fundamental theories of Everett M. Rogers' "Diffusion of Innovations". Additionally, other relevant resources are considered to ensure profound transfer of knowledge and reliable results. The findings indicate an increase of Bitcoin adoption since prior novices state a first usage after the integration of Taproot Asset stablecoins. Moreover, further potential is identified by the cumbrousness of the price volatility of bitcoin regarding the use as a means of payment.

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Table of Contents

List of Figures

List of Tables

List of Abbreviations

BRZ	Brazilian Digital
BUSD	Binance USD
DAO	Decentralized autonomous organization
DeFi	Decentralized finance
DOC	Dollar on Chain
ECDSA	Elliptic Curve Digital Signature Algorithm
ETP	Exchange-traded product
L-BTC	Liquid bitcoin
lnd	Lightning Network daemon
MAST	Merkelized Abstract Syntax Tree
MS-SMT	Merkle-Sum Sparse Merkle Tree
NFT	Non-fungible token
POS	Point of sale
P2SH	Pay-to-Script-Hash
P2TR	Pay-to-Taproot
RBTC	Smart Bitcoin
RSK	Rootstock
STX	Stacks
tapd	Taproot Assets daemon
TEUR	Taproot EUR
TUSD	Taproot US dollar
UTXO	Unspent transaction output
USDC	USD Coin
USDt	Liquid Tether USD
USDT	Tether USD

1 Introduction

Constancy can neither grow nor fall. The oxymoron emphasized in the title of this paper combines two blockchain-based technologies and raises the question of whether the constancy of technology A (stablecoins) can facilitate the growth of technology B (Bitcoin[1] adoption). Blockchain technology has so far created a multitude of applications, with Bitcoin being the first to enable the exchange of fully digitized value and the intentional absence of a third party. In this paper, the term " crypto asset" is used in alignment with the nomenclature of the German Banking Act. Accordingly, crypto assets are digital representations of value that are exchanged, stored, and traded electronically, are not issued by a central bank or authority, do not have the legal status of currency or money and are accepted by natural or legal persons (Federal Office of Justice , 2024). The term "digital asset" is used as a synonym, as its definition by the U.S. Internal Revenue Service is identical (IRS, 2023).

In Chapter 2 of this thesis, the fundamentals of the Taproot Assets protocol are explained. On the one hand, this includes the prerequisites, which primarily concern Bitcoin, a significant upgrade of it and the Lightning Network. On the other hand, the Taproot Assets protocol is examined, whereby the creation of assets, their structuring and transfers are analyzed.

In chapter 3, stablecoins are discussed. This is a prominent class of crypto assets in the blockchain ecosystem that can be categorized into three classes depending on their collateralization mechanism. The current landscape and the most common use cases of stablecoins are presented. Ultimately, stablecoins have been introduced to Bitcoin before. Therefore, we look at four different stablecoin projects on Bitcoin and their position in the market.

Chapter 4 describes the purpose of this thesis, including the research question and a hypothesis based on previous theoretical and consistent findings.

In Chapter 5, quantitative research is conducted to identify the impact of Taproot Asset stablecoins on Bitcoin adoption. First, the methodology, including the assessment of data collection and quality criteria, is outlined. To provide a theoretical foundation, the definition of adoption is examined based on fundamental scientific sources. Subsequently, the responses to the questionnaire are evaluated. The survey participants were confronted with the question of Taproot Asset stablecoins on Bitcoin and their opinion and eventual usage

[1] The terms "Bitcoin" and "bitcoin" are used according to their definitions of the reading "Mastering Bitcoin" and the general approach. While "Bitcoin" refers to the entire ecosystem, "bitcoin" describes the native crypto asset being transferred (Antonopoulos, 2021a).

of such an application. The analysis of potential adoption is divided into a status quo view and the prospective impact based on the results.

Chapter 6 describes possible implementation approaches for Taproot Asset stablecoins. Since there are no concepts yet, this part is based entirely on previous theoretical insights gained from stablecoins and the Taproot Assets protocol. For the integration into the Lightning Network, there exist notions that describe how the implementation will proceed, whereupon a scenario is presented.

In chapter 7, we summarize the thesis and the results of the research. Lastly, an outlook is given that can be estimated based on the findings, and further fields of research that can benefit from this study are identified.

2 Foundations of the Taproot Assets Protocol

In this chapter, we examine the Taproot Assets protocol that natively introduces digital assets to Bitcoin. To obtain a comprehensive understanding, its prerequisites are initially addressed. The Taproot Assets protocol is built on the bedrock of two crucial developments: the Lightning Network and the underlying technology of Bitcoin itself. Furthermore, the Taproot update added essential features that lay the foundation for issuing digital assets on Bitcoin. These components play an integral role in the development and operation of the Taproot Assets software. Subsequently, we will dive into the protocol itself and gain an understanding of Taproot Assets and elementary concepts such as universes and asset trees. Since digital values are meant to be exchanged between users, the process of asset transfers within the Bitcoin Taproot Assets ecosystem will finally be observed. This results in an extensive characterization that outlines the foundations of Taproot Assets and the intersection of the technologies involved.

Figure 1: *The Taproot Assets stack (Lightning Labs, 2023a)*

2.1 Prerequisites

This section explains the three preconditioned pillars that are essential to the Taproot Assets protocol. According to its stack, the Taproot Assets daemon (tapd) is dependent on an instance running the Lightning Network daemon (lnd) and a full node accessing the Bitcoin blockchain (Lightning Labs, 2023a). Ultimately, the Bitcoin main network received additional capabilities in a soft fork update, which directly determined the development of the Taproot Assets protocol.

2.1.1 Bitcoin

Bitcoin is a peer-to-peer network for digital payments that does not depend on a central entity. Users can execute transactions with the native crypto asset bitcoin. Based on distributed ledger technology, the network is supported by a decentralized computing infrastructure of individual node operators, each storing its own copy of the blockchain – a record of all transactions processed. The absence of a third party eliminates the necessity of unilateral trust and a single point of failure by relying on protocol design and game-theoretic incentive mechanisms. This requires coordination of state changes between truthful participants under the premise of an insecure, error-prone, and pseudonymous network. (Nakamoto, 2008)

Bitcoin in general provides three types of nodes that have different functionalities and roles within the ecosystem. Lightweight clients do not store the entire blockchain to save on storage space. This requires a simplified method of verifying the validity of a transaction and thus trusting the integrity of other participants who have access to this data. Its main purpose as a wallet application is to transfer and receive bitcoin. Full nodes, however, store the Bitcoin blockchain and have direct access to any transaction since the genesis block. Transactions that are propagated in the network can be verified independently. The most common implementation is the Bitcoin Core reference client, which is also embedded in lnd. Both lnd and tapd require a fully synchronized blockchain to operate properly, making a full node the minimum requirement to access all features of the Lightning Network and the Taproot Assets protocol. Finally, mining nodes run additional software to aggregate unconfirmed transactions into blocks, solve a cryptographic puzzle, and distribute the block in the network. Although they have a significant contribution to the Bitcoin network, we will not cover mining nodes in detail in this thesis. (Antonopoulos, 2021b; Lightning Labs, 2023b)

Every bitcoin transfer is initiated by a transaction that is distributed among all nodes storing the blockchain and checked for validity. This is essential to avoid double spending of the same coin. In a simplified manner, a transaction indicates that Alice assigns an unspent transaction output (UTXO) to Bob's Bitcoin address – which is derived from his public key – and authorizes the transaction with her personal private key. An easily verifiable chain of ownership and a new set of UTXOs are created, while the previous UTXO is invalidated once the block is added to the blockchain. Prior to this, miners build a new candidate block containing all unconfirmed transactions and start solving the cryptographic puzzle, also known as proof-of-work – Bitcoin's consensus algorithm. This requires combining various pieces of information and generating a hash value that aligns with the current target. By adding the hash value of the previous block, the blockchain is built, which guarantees Bitcoin's immutability. Within this process, miners compete against each other, causing the successful miner to broadcast the block, which is verified by other nodes and accepted only if it is valid. (Antonopoulos, 2021c; Nakamoto, 2008)

Therefore, Bitcoin represents the main network that ensures the proper execution and settlement of all on-chain transactions, the truthful behavior of its nodes, and the record keeping of every state alteration. It urges to implement additional software that enables new features or remedies deficits to establish a holistic ecosystem with multiple utilizations. For this reason, technologies such as the Lightning Network and Taproot Assets were developed.

2.1.2 Lightning Network

The Lightning Network is a second layer scaling solution of Bitcoin. It consists of multiple bidirectional payment channels between nodes, creating a meshed system in which users can reach each other through a few hops. Its development was primarily driven by the intentional lack of scalability of the Bitcoin network, which – as a gossip protocol – requires

that any modification to the uniform state of the blockchain must be shared and agreed upon with all participants. In this manner, Bitcoin itself can provide security and maintain decentralization (Poon & Dryja, 2016, p. 1 f.). By abandoning scalability on the first layer and shifting it to the second, Bitcoin overcomes the well-known blockchain trilemma – sometimes also referred to as “scalability trilemma”. This theory was first described by Vitalik Buterin and states that a blockchain network can only achieve a maximum of two of the three properties on its base layer (Buterin, 2017). However, each project has its individual approach to overcoming this challenge and prioritizes the significance of the elements differently.

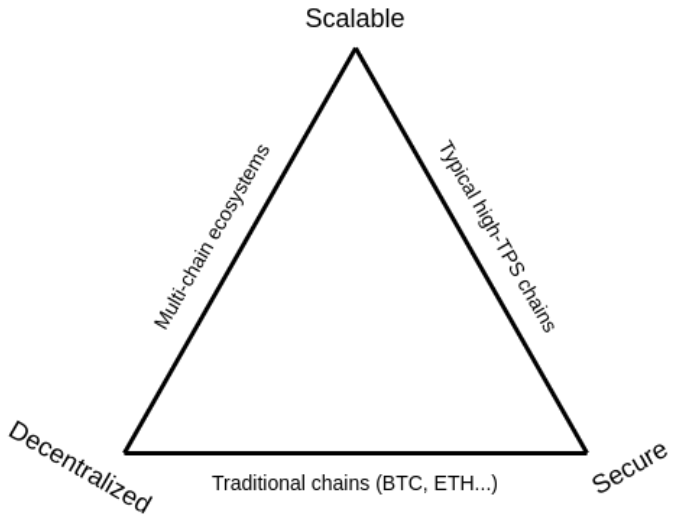


Figure 2: *The blockchain trilemma (Buterin, 2021)*

The Lightning Network enables the creation of off-chain payment channels between nodes through special agreements named 2-of-2 multi-signature addresses. These are constructions that require transactions signed by both participants involved to spend the deposited bitcoin. This initializes the creation of the payment channel and records it on the blockchain. If the counterparties decide to change the allocation of funds, they update the state of the payment channel. This can be done by simply signing and exchanging new transactions and overwriting the previous state. Since it is a bilateral agreement, it is not necessary to broadcast the update to the Bitcoin network. While the two counterparties agree upon the current balance of a mutual payment channel, this is in fact the balance and no conflicts occur. Hence, the counterparties only exchange transaction drafts that can be broadcasted to the main network anytime to close the channel, distribute the bitcoins according to the balance, and inform the network about the final state. In case of disagreement, the protocol provides protection against fraud through game-theoretic incentives and penalties based on cryptography. For instance, if Alice propagates an obsolete state of the payment channel to gain advantage for herself, she will be punished and risks losing all her deposited funds to Bob. (Poon & Dryja, 2016, p. 4 ff.)

Since transactions do not need to be broadcasted to and verified by the entire network, nearly instantaneous transfers of bitcoin are possible, which improves scalability. In

addition, the fees for executing transactions are extremely low as the first layer is not burdened. This also enhances efficiency since unlimited exchanges can be performed off-chain within the scope of the payment channel. If, however, users had to establish a new payment channel with every counterpart they want to interact with, scalability and efficiency would be compromised.

To overcome this, the concept of payment routing was implemented in the Lightning Network. Thus, two parties exchanging bitcoin do not need to be directly linked by a mutual payment channel. Since channels are public, the origin node can construct a path to the receiving node. For instance, if Alice wants to send bitcoin to Carol but only maintains a payment channel to Bob, it is sufficient if Carol also shares a channel with Bob. In this simplified scenario, Bob would serve as an intermediate node, of which there are in fact several. The pathfinding process is subject to various conditions, most notably that the hops and the payment channels in between must hold at least the appropriate amount of transferred bitcoin. (Antonopoulos, Osuntokun, & et al., 2021a)

The Lightning Network is embedded in several software implementations, all of which are compliant with the Basis of Lightning Technology. These are standardized specifications that define how the network operates to harmonize the different solutions and ensure interoperability (Antonopoulos, Osuntokun, & et al., 2021b). One of the software implementations is lnd, developed by Lightning Labs, that also initiated the Taproot Assets protocol. The objective is to merge both technologies allowing Taproot Assets to be integrated into the Lightning Network and to benefit from its capabilities (Lightning Labs, 2023c). Before we go further into the details, we first examine the third prerequisite for the Taproot Assets protocol.

2.1.3 Taproot Update

On November 14, 2021, at block height 709,632, a substantial Bitcoin update named Taproot was launched through a soft fork activation (Bitcoin Optech, 2021). A soft fork is a procedure used by Bitcoin to introduce new features and consensus rules which are supported by a majority of the network, are backwards compatible, and thus do not result in a separation of the blockchain into two branches (Bitcoin Project, n.d.). The update was associated with the adoption of new features that are crucial to the development of the Taproot Assets protocol. In particular, these include Schnorr signatures and Merkelized Abstract Syntax Trees (MAST). We will explore both in this subsection.

Traditionally, Bitcoin's cryptographic scheme for public key generation is the Elliptic Curve Digital Signature Algorithm (ECDSA). Any transfer of bitcoins is based on this technique. The public key (K) is created by computing a product of the randomly generated private key (k) and the constant generator point (G) on the standardized elliptic curve secp256k1: (Antonopoulos, 2021d)

$$K = k * G$$

The security of the equation is guaranteed by a one-way function of the discrete logarithm problem, which cannot be solved for the private key. The Taproot update introduces a novel scheme for generating digital signatures over the same elliptic curve, called Schnorr signature algorithm, that has the same security assumptions as ECDSA. This technique offers numerous advantages without neglecting the security aspects of Bitcoin's cryptography. In particular, the linearity property of the Schnorr signature algorithm allows for more efficient mathematical structures. Simply put, it is possible to add multiple public keys generated from different private keys and perform batch validation with the sum of their generated digital signatures. This enables special multi-signature schemes where bitcoins are sent to the aggregation of the participants' public keys. The threshold signature is then generated in the same way. Both the threshold public key and the threshold signature are indistinguishable from ordinary public keys and signatures. Therefore, it is not publicly ascertainable who the participants are and how many were involved, which enhances privacy. (Wuille, Nick, & et al., 2023)

An even more interesting approach to this linear aggregation mechanism is the generation of a modified public key (Q) by offsetting it with a cryptographic hash commitment (H) to a message (m), as formula I shows hereinafter. To spend the output, a modified private key (q) is created with the same offset as in formula II. This procedure of key pair modification with a specific dataset is called Taptweak. (Bitcoin Optech, 2019)

$$\text{I: } Q = K + H(K|m) * G$$

$$\text{II: } q = k + H(K|m)$$

To fully understand the main purpose of the committed message and its function within the Taptweak, we first need to explain scripts in Bitcoin. Scripts specify the spending conditions of a UTXO defined by the sender of a Bitcoin transaction. As an example, we introduce four different spending conditions for a Bitcoin UTXO:

> *Spending condition 1: Bob produces a valid signature with the corresponding private key.*
>
> *Spending condition 2: 1,000 blocks were added to the blockchain (time-lock) and Alice produces a valid signature.*
>
> *Spending condition 3: two of Alice, Bob and Carol jointly produce a valid signature (multi-signature).*
>
> *Spending condition 4: Carol provides a value that corresponds to a specific hashed secret and produces a valid signature.*

So far, privacy concerns are not considered in this process of Bitcoin. As a result, spending the UTXO would lead to the disclosure of all other spending conditions. For example, if Bob was able to produce a valid signature (spending condition 1), anyone would be able to see that Alice and Carol were also involved in this transaction since it is published on the

blockchain. Furthermore, since all the possible spending conditions must be revealed, complex transactions can become data intensive. (Van Wirdum, 2019)

Nevertheless, to allow multiple spending conditions without exposing the options that have not been used, Taproot uses a technology called MAST. The idea of MASTs was previously discussed by prominent Bitcoin developers and was brought to paper and implemented by Jeremy Rubin, Manali Naik, and Nitya Subramanian (Rubin, Naik, & et al., 2014). Though it has never been integrated into the Bitcoin software ever since. MASTs combine the properties of two technologies already used in Bitcoin today: Merkle Trees and Pay-to-Script-Hash (P2SH) transactions.

Merkle Trees are cryptographic data structures introduced in 1980 by Ralph C. Merkle to authenticate entries within a public file (Merkle, 1980). In Bitcoin, transactions in each block are stored within a Merkle Tree to save storage space, provide confidentiality, and simplify verification. In this process, hashed transaction data is stored in the leaves of a tree structure. The hash values of adjacent transactions are concatenated at each branch and hashed again. Finally, the Merkle root is created, which represents a hash value of all the information within the tree. It is stored in the header of the Bitcoin block and provides a digital fingerprint that ensures the integrity of its entries, consumes minimal storage, and is an efficient way to verify the presence of a transaction within the block while keeping other information secret. The existence of a transaction within the Merkle Tree can be verified by taking its hash value and generating all other hash values up to the root. If it equals the given hash value of the Merkle root, the transaction is in fact included in the block. (Antonopoulos, 2021e)

P2SH is a transaction type of Bitcoin that supports complex scripting (e.g., spending conditions 2, 3 and 4), while the funding address is a fixed-length 20-byte hash. Contrary to the usual scripting system described previously, P2SH shifts the responsibility of providing the conditions to spend the UTXO to the recipient. Hence, Bob defines an arbitrary spending condition in a redeem script, hashes it, and sends the hash value to Alice, who creates the transaction containing Bob’s hashed redeem script. When Bob later provides the script, the UTXO can be spent as it corresponds to the script hash. (Andresen, 2021)

MASTs unify these two technologies and store multiple scripts in a Merkle Tree, where the branches down to its leaves represent different spending paths for the UTXO. The root is a hash value that includes all the spending conditions of the UTXO. Within the Taptweak, the root of the MAST represents the message of the cryptographic hash commitment described above. In addition, Taproot introduces a new type of Bitcoin transaction: Pay-to-Taproot (P2TR). It combines the previously described P2SH with the most basic form of spending a bitcoin: Pay-to-Pubkey (P2PK). This transaction type simply transfers the bitcoin to another user's public key. P2TR supports either key-based or script-based spending of the UTXO. Spending to the public key results in a P2PK transaction, while the cryptographic hash commitment and therefore the MAST of scripts is concealed. If the script-based spending is applied, the selected path is executed within the validation process and ultimately recorded

on the blockchain, while any other option is kept private. Figure 3 shows the structure of a MAST, which is identical to a Merkle Tree: (Wuille, Nick, & et al., 2023)

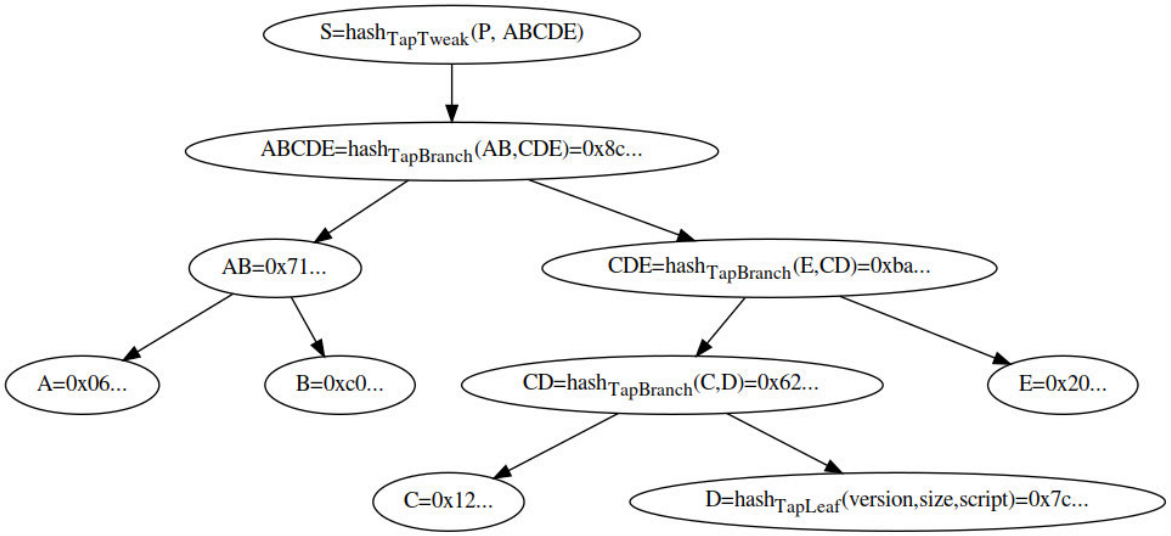


Figure 3: *MAST of scripts for Taproot outputs (Wuille, Nick, & et al., 2023)*

2.2 The Taproot Assets Protocol

The Taproot Assets protocol enables digital assets to be natively integrated into the Bitcoin blockchain. Formerly known as Taro (Taproot Asset Representation Overlay), it incorporates several new elements that are based on the Taproot upgrade and are covered in this section. As an overlay, it depends on the conventions of the Bitcoin protocol, which serves as a backbone and is given special rules for handling Taproot Asset data. In addition to the on-chain issuance and transfer of Taproot Assets, an interconnection with the Lightning Network is planned. This is of particular importance for fungible token such as stablecoins, which potentially are exchanged more regularly due to their uniformity. These are addressed in the chapter 3. (Osuntokun, 2022)

Although the main network alpha version of tapd was released on October 18, 2023, the technology is still under development. Thus, the aspects mentioned in this section may be subject to changes in the future. Users should also be aware of the loss of funds when interacting with the protocol. However, future software improvements will be forward compatible, which ensures that they will not interfere with assets that have already been issued. The alpha version does not yet support the integration of Taproot Assets into the Lightning Network, which will be included in additional updates. (Gentry, 2023)

2.2.1 Taproot Assets

The Taproot Assets protocol enables the issuance of arbitrary digital assets. These can be emitted in the form of “collectibles”, such as non-fungible tokens (NFT), or “normal” assets for the application of fungible tokens (e.g., stablecoins), which we will focus on in this thesis.

However, the application of Taproot Assets is not limited and can have various other representations such as shares or tickets. To encourage adoption, the utilization of Taproot Assets is light-client friendly supporting access for users who do not run their own full node, although this comes with limitations when interacting with the protocol. Besides the integration into the Lightning Network, further updates may bring the incorporation of confidential transactions through zero-knowledge proofs or other prominent technologies. (Lightning Labs, 2023c)

Taproot Assets are designed to significantly operate off-chain in order to avoid large storage requirements or congestion of the memory pool. This is also influenced by the experience of the year 2023, in which many transactions with large storage volumes were sent due to the inscription of Ordinals, which are NFTs on the Bitcoin blockchain. The basic process of transferring Taproot Assets is described later. Since assets can have multiple attributes that expand to large data packages, universes have been created. These are repositories that provide information about a particular Taproot Asset, including transaction data, thus making them comparable to a Bitcoin block explorer. Anytime an on-chain transaction is created, it generates a new proof, resulting in a linear increase in asset proofs. In addition, universes verify the provenance of an asset so that users do not have to trust the originator and can therefore be used as proof of reserves to validate the total amount. (Lightning Labs, 2023d; Osuntokun, 2023a)

2.2.2 Asset Trees

The MAST described in the previous subsection, which was introduced by the Taproot update, is extended within the Taproot Assets protocol by another asset tree: Merkle-Sum Sparse Merkle Tree (MS-SMT). This is a Merkle Tree that has by default 2^{256} leaves, of which empty ones have the value “null” whereas the root contains all the information. MS-SMTs enable a key-value mapping – similar to dictionaries in programming languages – where the information stored in the leaves is linked to its location. A bitmap is created out of this mapping which allows to perform a non-inclusion proof if specific data is not included or has been deleted. Like Merkle Trees, the information in the leaves is hashed to ensure privacy. Since the Bitcoin Improvement Proposal (BIP) of MS-SMTs is still under development, the final implementation can change throughout further processes. Figure 4 illustrates the construction of a MS-SMT: (Osuntokun, 2023b)

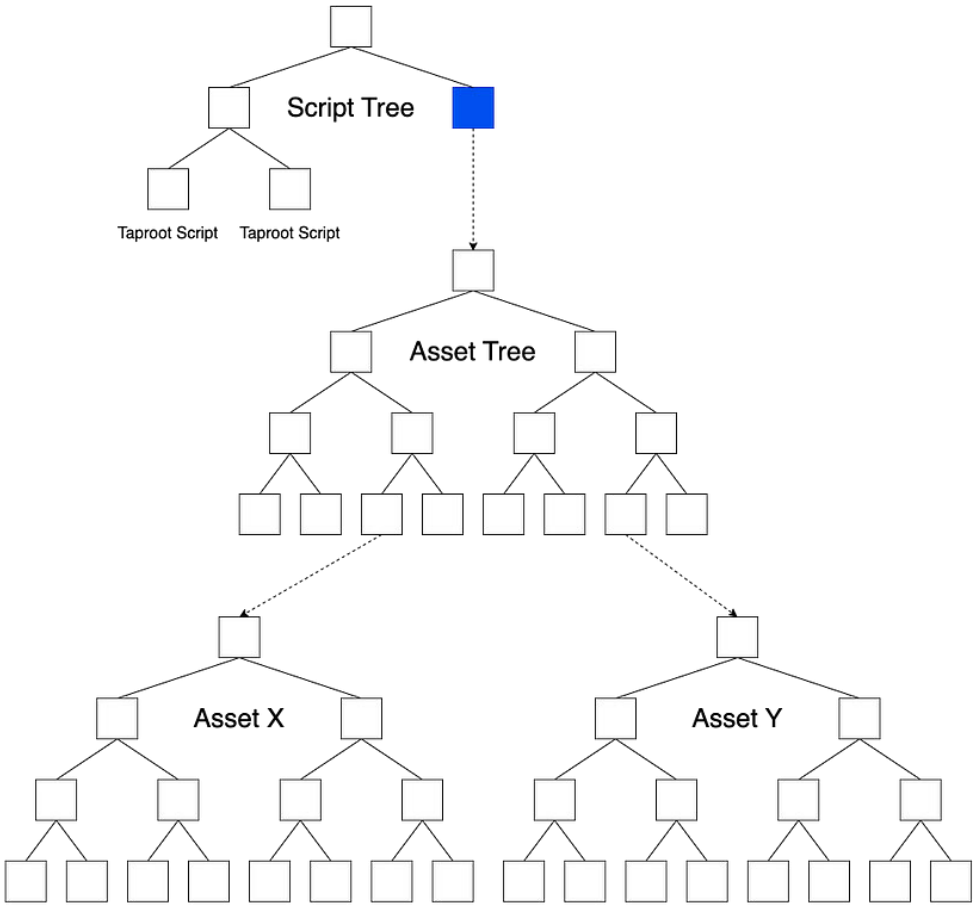


Figure 4: *Taproot Asset MS-SMT (Gondo, 2023)*

The MAST script tree at the top represents the script paths that include all the script-based spending conditions for the UTXO. Its root is committed to within the Taptweak. The asset tree of the Taproot Assets protocol is nested in the script tree and comprises two levels of MS-SMTs. The upper aggregates all the assets in its leaves, each of which constructs a tree on the second level that defines the UTXO sets of a specific asset combined with some data (e.g., asset ID, asset type, amount). The following subsection will focus on the transfer of Taproot Assets between users. (Gondo, 2023)

2.2.3 Asset Transfer

Taproot Assets are being created in a Taproot transaction on the Bitcoin blockchain. Therefore, the asset is assigned a unique asset identifier which makes it distinguishable from others. This issuing transaction does not contain any inputs, however, the outputs can have multiple recipients. Moreover, it is possible to create multiple assets within one issuing transaction. The issuance fills the MS-SMT described earlier of the given asset, where each receiving account (key) is allocated to a leave (value) in which the corresponding amount held by the account is stored. The publication of the issuing transaction and its inclusion into a Bitcoin block confirms the creation of the Taproot Asset. To others this transaction is

indistinguishable from any other Taproot transaction, which enhances the privacy, since only involved users understand its purpose. (Lightning Labs, 2023d)

While the current implementation supports the transfer of Taproot Assets on-chain, the real benefit for stablecoins will be introduced with an integration into payment channels of the Lightning Network. Since this is not yet specified, we will first focus on on-chain transactions and describe possible implementation approaches later. Bitcoin address types generally have specific prefixes, while P2PK addresses start with a "1", P2SH addresses start with a "3" (Antonopoulos, 2021d). Taproot Asset addresses of the main network have the prefix "tapbc" and contain information such as the ID of the asset and the amount to be transferred as well as the tweaked public key, which represents the MAST (Osuntokun, 2023c). When a Taproot Asset is transferred, an address is generated by the recipient and communicated to the sender, who initiates the transaction. However, the protocol still allows some flexibility for the sender to configure this process. To carry out the transaction, the sender creates a new MS-SMT listing the adjusted balances by decreasing or increasing the amounts of the various accounts involved, while the total amount remains unchanged. The transaction must be transferred on-chain and added to a block for the definite confirmation. (Lightning Labs, 2023d)

Taproot Assets are designed to be customizable and therefore offer additional features which have not yet been explained. Due to the peculiarities of a digital asset, it could be necessary to merge or split units. This could be beneficial for the application of NFTs, which – when merged – create a new unique collectible. An example could be the use of this token within the metaverse or the gaming industry. Since this paper is focusing on the implementation of stablecoins through Taproot Assets, we will not examine this in detail. Although, to integrate stablecoins, it is necessary to guarantee fast transfers, a stability mechanism through the extension and contraction of supply as well as further requirements. These will be explored and outlined in chapter 6. To fully understand stablecoins and its current landscape, the next chapter will focus on this type of crypto asset.

3 Exploring Stablecoins

Stablecoins have become one of the largest crypto asset classes amongst blockchain networks. First introduced in 2014, their additional value lies in the promise of stability and an inherent link to the value of a predefined asset. Thus, one unit of the stablecoin can be equal to the value of $1 or any other fiat currency. Although, stablecoins do not have to be linked to a currency but can represent any other asset. The hypothesis is that each unit of the stablecoin can be redeemed at any time for the corresponding value that it is tied to. The classification of stablecoins, which we will focus on in the first section, initially distinguishes between two types: collateralized and uncollateralized stablecoins, whereby the first group is further subdivided into off-chain and on-chain collateralized stablecoins. This ranking also reflects user sentiment towards the current market coverage of the stablecoin landscape, which is discussed later in this chapter. As stablecoins have a large share in terms of market capitalization, they also have an impact on the entire ecosystem including various use cases. Finally, given that the Taproot Assets protocol aims to enable the issuance of stablecoins on the Bitcoin network, we focus on existing solutions that combine these two fields.

3.1 Stablecoin Classification

Stablecoins can be classified according to various characteristics, such as the type of asset they represent or the blockchain network in which they are natively integrated. Generally, the distinction is made according to the type of collateralization. There are currently three different methods, which we will explain in the following subsections. Occasionally these groups are further subdivided or titled differently, but we will focus on the most common procedure. While the first two types attempt to achieve stability through collateralization, the third group does so without the support of underlying assets using a different technique that we will observe later. As we will identify a design for the Taproot Asset stablecoin later in section 6.1, it is crucial to understand the different approaches and benefits of existing stablecoin implementations.

In addition to the blockchain trilemma, there is also the concept of the stablecoin trilemma. Thereby, stablecoin classes can only achieve two of the following three characteristics: stability, (capital) efficiency and decentralization. Both stablecoin classes that apply collateralization have the objective of maintaining relatively stable values. While off-chain models additionally focus on efficiency, on-chain collateralized stablecoins address decentralization. Uncollateralized stablecoins strive to simultaneously target efficiency and decentralization. In the following subsections, this concept will be elaborated in more detail. Figure 5 illustrates the interdependence of the different stablecoin classes and their characteristics: (Zhao, 2023)

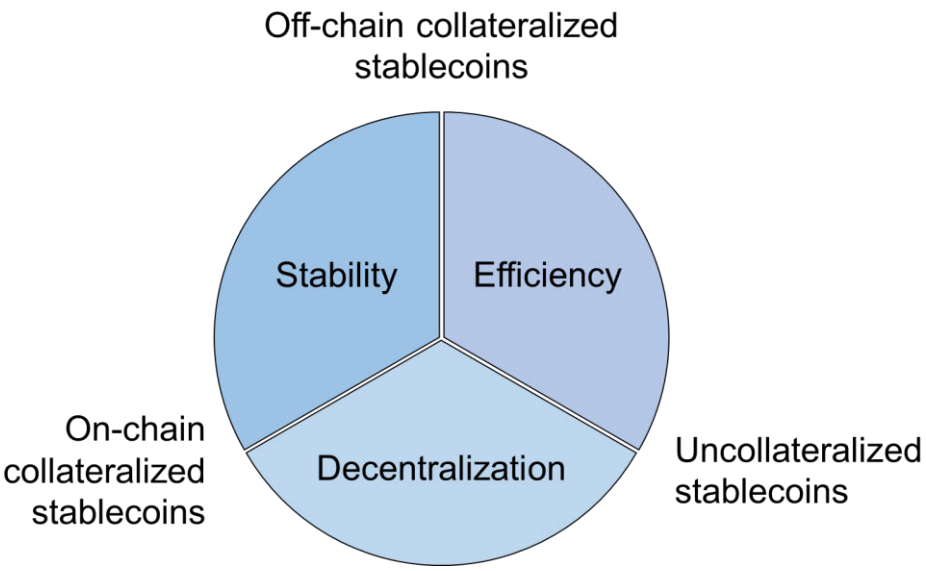


Figure 5: *The stablecoin trilemma per class (own illustration)*

3.1.1 Off-chain collateralized Stablecoins

Off-chain collateralized stablecoins are backed by a reserve of assets that are not recorded on the blockchain, but in a ledger managed by a centralized entity. Most of them represent a fully digitized version of a fiat currency. The collateral mostly comprises financial assets that have a high liquidity ratio but are relatively stable, such as fiat currencies, bank deposits or short-term debt. Overall, the collateral must at least be equal to the value of the current supply to fulfill redemption. This creates a good balance between efficiency and stability, as the issued stablecoins and the collateral are in a 1:1 exchange ratio. Although we only focus on fiat stablecoins in this paper, there also exist ones that represent the value of other assets. One example is Tether Gold, a stablecoin that is pegged to the value of one troy ounce of gold that is physically stored in a vault (Tether Operations Limited, 2022). However, the more widely used stablecoins are fiat-backed stablecoins such as Tether USD (USDT), Circle's USD Coin (USDC) and Binance USD (BUSD), all of which aim to maintain their peg to the US dollar. There are also stablecoins that are pegged to other fiat currencies such as the Euro (e.g., EURC by Circle), but these are less represented on the market. Tether and Circle are examples of custodians that manage the spreadsheet of the respective stablecoin and its collateral. (Mai, 2022)

A typical lifecycle of fiat-backed stablecoins starts with verified users buying the stablecoin directly from the custodian, for example Tether. USDT is issued by a smart contract – a computer program deployed on the blockchain that is executed automatically – and sent to the buyer's address. The holder can now transfer USDT via the blockchain network or use them in decentralized finance (DeFi) applications. These are also smart contracts that enable the utilization of traditional financial services within the blockchain ecosystem. The custodian promises that users can redeem the USDT in fiat currency at any time. In this step of the process, users send their USDT back to the custodian, who burns it and transfers

the same amount of fiat currency back to the user's bank account. It is important to note that only the custodian can issue and remove off-chain collateralized stablecoins, which creates a dependency for users on their integrity. (Tether Operations Limited, n.d.)

Stability is achieved through two coherent mechanisms. Firstly, the promise is given that each unit is redeemable for the equivalent amount of $1, as the value of the supply is hedged by the collateral batch. Secondly, arbitrageurs take advantage of price discrepancies on the secondary market. In the case of fiat stablecoins, the theory says that if the stablecoin-US dollar ratio is above one (stablecoin is worth more than $1), arbitrageurs could exchange their US dollars for stablecoins at the custodian and make a profit by selling them on the secondary market at the prevailing higher price. This increases the supply of the stablecoins, which leads to a price reduction. If the stablecoin-US dollar ratio is below one (stablecoin is worth less than $1), arbitrageurs would redeem their holdings at the custodian, which reduces supply and leads to an increase of the market price. However, if trust in the stablecoin's peg breaks, its holders will exchange it for the promised value, flooding the market with the stablecoin and causing its price to fall. This incident would be comparable to a bank run challenging the quality of the redemption mechanism. Therefore, stablecoin holders must always trust the custodian concerning its management and collateral selection. (Baughman, Carapella, & et al., 2022)

To retain the trust of users, custodians that provide off-chain collateralized stablecoins ensure a high level of transparency by having themselves regularly audited by third parties and providing information about their reserves. As a result, weekly or even daily updates on the collateral reserves are published and updated on their website.

3.1.2 On-chain collateralized Stablecoins

On-chain collateralized stablecoins secure their stability by promising users that the individually deposited collateral can be obtained at any time for the return of the lent assets. Therefore, a few differences to the aforementioned stabilization mechanism of off-chain collateralized stablecoins occur. The collateral that users provide to receive the stablecoin are blockchain-based crypto assets such as Ether – the native crypto asset of Ethereum. Each user independently deposits the collateral in a smart contract provided by an institution. However, users do not have to trust this institution, as it is not a custodian responsible for spreadsheet or collateral management, but rather the program code of the smart contracts. The most popular on-chain collateralized stablecoin is DAI, which was initiated by the MakerDAO project, a decentralized autonomous organization (DAO) in which token holders can participate in the governance process of the protocol to determine its future path. During election periods, MakerDAO governance token holders can, for example, vote on the percentage of the stability fee payable by DAI borrowers to reclaim their collateral. This applies to most on-chain collateralized stablecoins and guarantees decentralized processes of the protocol. Yet, it is important to note that the power in the governance token distribution is not always fully decentralized. Concerning MakerDAO, the top ten addresses hold more

than 43% of the governance token and can thus manipulate elections (Etherscan, 2024a). DAI also aims to maintain a 1:1 peg to the US dollar. Since there is no custodian administering the collateral, which is furthermore filled with rather unstable crypto assets, over-collateralization is required. Hence, users who borrow DAI, for example, must deposit 150% of the value of Ether compared to the corresponding value of DAI as collateral. This compensates for the volatility of the crypto asset. This mechanism also makes on-chain collateralized stablecoins rather capital inefficient. In the future, traditional assets that are tokenized (e.g., blockchain-based bonds) could serve as a more stable on-chain collateral. (Baughman, Carapella, & et al., 2022)

On-chain collateralized stablecoins are created through users depositing crypto assets in a vault provided by a smart contract. Subsequently, a transfer of DAI to the corresponding wallet is initiated. The ratio of over-collateralization depends on the evaluation of risk parameters determined in election periods by governance token holders. After receiving the stablecoin, the user can transfer DAI via the blockchain network or use it for DeFi applications. By returning the borrowed DAI amount and paying the stability fee, the user can withdraw the deposited collateral. However, if the ratio between the collateral and the borrowed DAI enters a predefined zone – i.e., approximating a 1:1 ratio due to collateral depreciation – the vault is liquidated, and the collateral is sold via an automatic auction mechanism to prevent under-collateralization. In both cases, the DAI provided to release the collateral is ultimately burned. (MakerDAO, n.d.)

As there is no central institution that administers the underlying collateral of the stablecoin, other methods must ensure its stability. The protocol itself contains approaches that ensure a 1:1 peg to the US dollar, such as over-collateralization and its liquidation according to the risk profile of the collateral deposited. In addition, MakerDAO governance token holders update the security requirements of DAI and its protocol through election periods. In the event of attacks on the network's infrastructure or DAI's price stability, an emergency shutdown is caused which enables users to immediately withdraw their deposited collateral from the vaults. (MakerDAO, n.d.)

3.1.3 Uncollateralized Stablecoins

Uncollateralized stablecoins – also known as algorithmic stablecoins – do not apply any collateral as the other two categories described above. Although there are different approaches regarding the design of the stabilization mechanism, all projects ultimately leverage economic theory and incentivization through the adjustment of the supply to ensure stability. This can be achieved either directly by using a rebase model or through a coupon model, where other tokens such as bonds or shares are introduced that can be exchanged for the stablecoin at a fixed rate. An example applying the rebase model is Ampleforth, while Terra USD (UST) is an algorithmic stablecoin using the coupon model. It is important to highlight that both projects failed and decoupled from their peg, while UST was even updated and replaced by USTC (CoinMarketCap, 2023a; CoinMarketCap, 2023b). For

simplicity, this thesis will only concentrate on the original project UST. Similar to on-chain collateralized stablecoins, the stabilization mechanism of uncollateralized stablecoins is primarily implemented through the use of smart contracts. Since no collateral management is required, there is theoretically no need for a custodian, which keeps the protocol decentralized. Furthermore, uncollateralized stablecoins are highly capital efficient as users do not need to deposit any assets to use them. However, the security aspects usually pose a challenge since there is no peg to other valuable assets as well as an inherent dependency on the protocol design. For this reason, various projects proposing this type of stabilization mechanism have failed in the past, for example UST or Basis Cash. (Baughman, Carapella, & et al., 2022)

Algorithmic stablecoins are created and destroyed by smart contracts through supply expansion and contraction. Holders can execute transactions on the blockchain network or use them for DeFi applications. Unbacked stablecoins aim to maintain a 1:1 peg to a specific fiat currency, which is predominantly the US dollar. If the price of the stablecoin is $1, the stabilization mechanism functions properly. Only if a disconnection of the value occurs the protocol must adjust in order to regain stability. This happens automatically due to the implementation through smart contracts. If the price of the stablecoin exceeds $1, an expansion of the supply results. This mechanism is based on the fundamental economic theory of market equilibrium. Thus, if the supply of an asset increases while demand remains constant, the equilibrium price decreases. In the event of a decrease in supply, the opposite effect occurs. So, if the price decreases below $1, the protocol burns existing stablecoins, which leads to a contraction of the supply and an appreciation of the price. This technique applies to the rebase model. The coupon model uses a similar approach by incentivizing bond token holders to buy or sell the stablecoin to manage the supply. (Baughman, Carapella, & et al., 2022)

3.2 Stablecoin Landscape and Utilization

Stablecoins have experienced significant growth within the blockchain ecosystem and play a central role in facilitating transactions, providing a store of value, and functioning as a bridge between the volatile crypto markets and traditional finance. At the time of writing, the total market capitalization of stablecoins is around $138 billion. However, at its peak in April 2022, it was almost $190 billion. This was shortly before the failure of the largest algorithmic stablecoin project to date, as mentioned above. As a result, the general trust in stablecoins and their stabilization mechanism was damaged, which led to less utilization. (DefiLlama, 2024)

Market capitalization is calculated by multiplying the current market price of one unit of a crypto asset by the total supply in circulation. Therefore, especially for stablecoins, it is reasonable to conclude that the market capitalization reflects the acceptance or trust that users have towards a particular asset, as its value remains approximately at $1 and only the circulating quantity changes.

Based on the market capitalization of stablecoins, market coverage shows a clear user preference for off-chain collateralized models. Since April 2021, the three largest stablecoins by market capitalization have mostly been USDT, USDC and BUSD, all of which apply off-chain collateralization. The market capitalization of this category amounts to approximately $130 billion, which represents more than 94% of the whole market. After the failure of the uncollateralized stablecoin project Terra USD in May 2022, users primarily shifted their holdings to off-chain collateralized crypto assets, resulting in their dominance. However, these projects also have experienced problems in the recent past. In February 2023, the U.S. Securities and Exchange Commission claimed that BUSD should have been registered as a security, which led to legal problems for Binance and Paxos, the company issuing the stablecoin. In response, Paxos stated that support for the BUSD would end and users would be able to exchange it for fiat currency by a certain date, leading to a reduction of crypto asset holdings (Lang, Wilson, & et al., 2023). In March 2023, funds worth $3.3 billion of Circle were frozen due to the collapse of the Silicon Valley Bank. This announcement led to problems regarding USDC, which broke its peg and traded at 87 cents after users returned assets worth of $2 billion. The price continued to fall due to declining user trust in the stability of the project and further redemptions (Ge Huang, Miao, & et al., 2023). The stablecoin USDT also faced several events where the price decoupled from $1. In May 2022, USDT dropped to 95 cents due to the failure of Terra USD and the distrust in stablecoins in general but was able to readjust to its peg (Browne, 2022). Additionally, the crypto exchange FTX filed for bankruptcy in November 2022, which also led to users redeeming their USDT and a subsequent de-peg (Nicolle & Pan, 2022). Despite the problems of off-chain collateralized stablecoins losing their peg, users' holdings gradually shifted to USDT. As of February 18, 2024, USDT has a market dominance of around 70% and its market capitalization continues to rise, while that of USDC and BUSD is falling. One reason for this could be that the overall market capitalization of stablecoins has been rising since November 2023, which is driving the holdings of USDT. Secondly, users may have more confidence in Tether's business model than other companies issuing off-chain collateralized stablecoins, although USDT also decoupled several times from its peg. (DefiLlama, 2024)

DAI, the most prominent representative of on-chain collateralized stablecoins, has maintained a relatively stable market dominance since April 2021. Similar to USDC, DAI decoupled from its intended value when the Silicon Valley Bank collapsed. At the time, it was trading at less than 90 cents, ultimately returning to $1 and regaining the trust of its holders. On-chain collateralized stablecoins mostly ranked second in terms of market capitalization. Today, their market capitalization is around $7 billion, peaking at almost $15 billion in early 2022. Their dominance of the overall stablecoin market is approximately 5%. (DefiLlama, 2024)

At the beginning of 2022, uncollateralized stablecoins and especially their advocate UST were favored by users and the second most used stablecoin class. However, the failure of the Terra USD project damaged user trust particularly concerning algorithmic stablecoins. The project aimed to maintain the peg of UST by pairing it with another crypto asset named

LUNA. At any time, $1 worth of LUNA could be exchanged for one UST unit and vice versa, regardless of the current price. Thus, holding one unit of LUNA worth $50 can be exchanged for 50 UST, whatever the price. Through this coupon model, stability is regulated. If UST trades at $1.1, arbitrageurs can use the mechanism described above to get 50 UST at $1 by exchanging LUNA for UST and sell them at the current market price, earning them a profit of $5. Due to the excess supply of UST, the price will fall. If UST trades at $0.9, arbitrageurs are incentivized to exchange it for LUNA at a UST price of $1. However, the collapse occurred due to pressure on the price of LUNA, which deterred users from doing this exchange even though UST was trading below $1. As a result, users preferred to exchange UST for fiat, which led to an even greater excess supply, resulting in a further price decrease. Today, FRAX is the largest project according to its market capitalization that employs an uncollateralized mechanism. The total market capitalization of this category peaked at over $23 billion just before the Terra USD crash and has since fallen to around $2 billion. As FRAX is only partially an algorithmic stablecoin and also uses on-chain collateralization, it is apparent that projects are avoiding the absence of collateralization as users have lost trust in them (Frax Finance, 2023). Today, algorithmic stablecoins have a market dominance of approximately 1%, which used to be more than 10%. (DefiLlama, 2024; Briola, Vidal-Tomás, & et al., 2023)

Primarily, stablecoins are used as low-volatility crypto assets that exist on blockchain networks and serve as a bridge between traditional assets (e.g., fiat currency) and other crypto assets (e.g., Bitcoin). From this position, users have various options to utilize their stablecoin holdings. Trading on crypto exchanges (e.g., Binance, Kraken) mostly involves stablecoins. In November 2023, more than 70% of transactions were carried out with USDT (THE BLOCK, 2023). Furthermore, due to their relatively stable value, they could serve as collateral for crypto asset derivative transactions. As they exist on a distributed blockchain network, important use cases exist in the ecosystem of DeFi applications. By providing liquidity of a stablecoin on a decentralized exchange, users can earn money and facilitate the functionality of the protocol as more deposited funds guarantee stable exchange rates. Lending services give users the ability to issue a loan so that others can directly borrow the amount of money in exchange for interest payments that the creditor receives back. However, when using such applications, users must always trust the protocol and the developers behind it. (Adachi, Born, & et al., 2021)

3.3 Existing Fiat Stablecoin Approaches on Bitcoin

Several existing solutions have already approached the combination of stablecoins and Bitcoin. In this section, we discuss these implementations, which include projects such as Stacks, Rootstock (RSK), the Liquid Network and Stablesats. However, it is crucial to note that while these projects target the integration of stablecoins into Bitcoin, their techniques and fundamental designs differ significantly from the paradigm enabled by the Taproot Assets protocol. While the Taproot Assets protocol aims to natively integrate stablecoins into

the Bitcoin network, these projects have different procedures. The consequent subsections examine the different strategies and mechanisms and highlight the differences between their approach and the innovative concept of Taproot Assets.

The project “Stably USD” is neglected in this chapter. It intended to implement a native stablecoin through the BRC-20 Bitcoin token standard – inspired by the ERC-20 Ethereum token standard – established through the Ordinals protocol. The project was announced in May 2023 by several digital publishers. However, there has been no activity since the inscription into the blockchain (Ordiscan, 2024). In addition, the former website no longer exists and can only be accessed via web archives. The plan was to introduce identity verification for users and maintain a 1:1 peg to the US dollar with full collateralization by a custodian (Stably, 2023a). The stablecoin can therefore be classified as an off-chain collateralized model. Stably published monthly reports regarding its assets and the collateral. These reports show that 101,000 units of the stablecoin were booked in May 2023, while in June 2023 the assets have disappeared (Stably, 2023b; Stably, 2023c). Based on these facts, it can be assumed that the project has been canceled. Yet the project website still specifies Bitcoin as a network that will be supported for the integration of Stably USD in the future, thus keeping the approach relevant.

3.3.1 Stacks

Stacks is a blockchain network that aims to complement Bitcoin with smart contracts and decentralized applications. The project includes the homonymous native crypto asset Stacks (STX), whose primary functionalities are in the consensus mechanism of the ecosystem. Since it uses Bitcoin as its base layer, it can be considered a second layer solution – similar to the Lightning Network – that applies the rules and thus the security aspects of its underlying main network. Stacks applies a proof-of-transfer consensus mechanism that selects the miner who creates the next block randomly, but according to their engagement in the Bitcoin network. Thus, the more Bitcoin a stacks miner transfers on the main network, the higher the chance of being selected as the next block producer. The introduction of Stacks' own programming language "Clarity" enables the use of smart contracts and the creation of additional assets such as stablecoins. (Stacks Open Internet Foundation, n.d.)

The Arkadiko protocol is a decentralized application built on Stacks that offers multiple financial services such as exchanges and liquidity providers. It also incorporates the stablecoin USDA and allows users to mint it when depositing STX as collateral. USDA is pegged to the US dollar and can be categorized as an on-chain collateralized stablecoin, similar to its Ethereum-based counterpart DAI. To ensure the safety of the collateral, vaults that are too risky can be liquidated. Thus, if the collateral-asset ratio approximates a 1:1 balance as the value of STX decreases, the vault will ultimately be liquidated. This leads to a higher incentivization of other users to repurchase the collateral (Arkadiko Finance, 2023a). Arkadiko is open-source and managed by the community of governance token holders, who form a DAO and conduct election periods to further the project. (Arkadiko Finance, 2023b)

Since USDA is natively integrated into the Arkadiko protocol, users of this stablecoin must trust not only this project, but also the smart contracts and the programming language Clarity, as well as Stacks itself. Although the project and its stabilization mechanism appear to be a duplicate of MakerDAO and DAI built on Stacks, the stablecoin USDA does not maintain its 1:1 peg to the US dollar. According to crypto asset data provider CoinGecko, the price of USDA has never been able to hold on to this peg and has not been updated since a critical loss of this connection in September 2023 (CoinGecko, 2023a).

3.3.2 Rootstock (RSK)

Rootstock is a smart contract platform that operates as a sidechain of Bitcoin and incorporates its own blockchain. The main goal of its development was to extend the functionality of Bitcoin by enabling smart contracts, decentralized applications and higher scalability while maintaining the security of Bitcoin. This is achieved by creating a bidirectional linked sidechain. When Bitcoin is deposited on RSK, it is locked and becomes "Smart Bitcoin" (RBTC), which can be used to execute smart contracts and access decentralized applications. Thus, RSK does not have its own native token, but uses entitlements on bitcoin as a transitory local asset. Since RBTC itself is pegged to the value of bitcoin, it is itself a stablecoin. However, we will focus on fiat-based stablecoins when examining the existing solutions on Bitcoin. Due to high compatibility and a bridge to Ethereum, both networks are interoperable and can communicate with each other, enabling the conversion of assets across both blockchains. RSK employs a merge-mining consensus mechanism that is linked to that of Bitcoin. This allows miners producing Bitcoin blocks on the main layer to simultaneously produce RSK blocks at almost no marginal cost, as the same hardware can be used. To incentivize Bitcoin miners to participate in RSK mining, they are rewarded in RBTC through transaction fees. (Lerner, 2019)

RSK includes several stablecoins that use different stabilization mechanisms. Three of them are introduced in this subsection. The first is Dollar on Chain (DOC). It aims to maintain its peg to the US dollar and is similar to DAI as it is also an on-chain collateralized stablecoin managed by a DAO whose token holders vote on policies and changes of the project. While DAI's vaults are collateralized with Ether, for example, DOC is kept stable by a collateralization of RBTC and thus indirectly by bitcoin. Users who send RBTC to the vault are rewarded with the corresponding amount of newly minted DOC. As Bitcoin is volatile, the price of RBTC also changes. Therefore, a certain degree of overcollateralization is necessary to keep the value of the RBTC vault higher than the issued DOC. (Carjuzaa, Bokser, & et al., 2019)

RSK's second stablecoin is called XUSD and is issued on the platform BabelFish. It is also an on-chain collateralized stablecoin that aims to maintain its peg to the US dollar. Relevant characteristics of the protocol are updated through election periods of a DAO. Rather than being backed by solely one asset, the vault is collateralized by several stablecoins that exist on the RSK, but also on blockchain networks that provide a bridge to RSK, such as

Ethereum and the Binance Smart Chain. Currently, the vault consists of twelve different stablecoins, which are also selected and monitored by the DAO according to their qualification (Blockscout, 2024a). By depositing one of the recognized stablecoins into the BabelFish protocol, the corresponding amount of XUSD is transferred to the user's wallet address. (BabelFish, 2023)

Lastly, RSK implements an off-chain collateralized stablecoin named Brazilian Digital (BRZ), which is pegged to the Brazilian Real and backed by assets denominated in that same fiat currency. The pool of assets is managed by dedicated reserve managers. The stablecoin is therefore similar to USDT, USDC and BUSD. Although its native blockchain is RSK, there exist bridges to other networks such as Ethereum, Solana and the Binance Smart Chain. Its main purpose is to facilitate the access of companies operating in Brazil to customers and other crypto assets, as well as to hedge their business operations. A potential buyer can obtain BRZ by sending a purchase order to the administering organization, which is the sole custodian that distributes and removes the stablecoin. (BRZ, n.d.)

Similar to the approach of Stacks examined previously, the user must trust the RSK network when using one of the stablecoins described in this subsection. Additionally, most of them have their own protocol policies that need to be considered when interacting with the platform. According to crypto asset data providers CoinGecko and CoinMarketCap, XUSD, DOC and BRZ have maintained relative stability compared to their fiat equivalents (CoinGecko, 2023b; CoinMarketCap, 2023c; CoinGecko, 2023c). They tend to have higher volatility than established stablecoins such as USDT or DAI but have retained their peg value so far. However, as RSK is not a widely known network, the stablecoins are hardly adopted and therefore barely utilized. The smart contract that issues XUSD was created on June 7, 2021, and counts only 20,462 transactions on RSK (Blockscout, 2024a). The number of transactions that apply to the smart contract of DOC, which was already deployed on October 5, 2019, is 17,619 (RSK Explorer, 2024). With regards to BRZ, whose smart contract was published on June 24, 2021, only 34 transactions were recorded, while its instance on Ethereum registered 923 transactions (Blockscout, 2024b; Etherscan, 2024b). Contrary to Tether and Circle, the organization that manages BRZ also does not regularly publish transparent reports of the collateral securing the stablecoin. This further increases the risks for users while holding and interacting with BRZ. All figures mentioned above refer to February 18, 2024. For comparison to these statistics, USDT had 139,723 transactions within one day on January 17, 2024, which is the most recent statistic available (Glassnode Services AG, 2024). This emphasizes that the adoption of Rootstock and its existing stablecoins is low and cannot be associated with other blockchain networks and their projects.

3.3.3 Liquid Network

Similar to RSK, the Liquid Network is an approach that is interoperable with Bitcoin and implements its own independent network as a sidechain to it. Its transitory local asset is "Liquid bitcoin" (L-BTC), which is pegged to bitcoin at a 1:1 ratio. During a peg-in, bitcoin is

locked on the main network and the same amount of L-BTC is issued on the sidechain. In a peg-out, L-BTC is burned on the sidechain while the previously locked bitcoin is released on the main network. The Liquid Network was developed by Blockstream and enables the issuance of individual assets. (Blockstream, 2023a)

The Liquid Network also applies a blockchain for a transparent publication of the transaction history. Contrary to the Bitcoin network, the blocks are not verified by a proof-of-work consensus mechanism, but rather signed by specific members (functionaries) who secure the network. This means that no single member has full control, but the structure is more centralized than Bitcoin itself. As of February 18, 2024, there are a total of 66 members of the federated system "Liquid Foundation" (Blockstream, 2023b). A subset of 15 of these are the functionaries who propose, sign, and distribute blocks to the other nodes in a round-robin fashion. Once eleven of these functionaries have checked and signed the propagated block, it is added to the blockchain. The functionaries are also indispensable for the execution of both peg-in and peg-out. (Blockstream, n.d.)

The Liquid Network includes two stablecoins that can be used when interacting with the platform. In 2019, Liquid Tether (USDt) was launched, which is an off-chain collateralized stablecoin akin to the conventional equivalent of Tether. Users can buy it on different exchanges or perform Liquid-based atomic swaps, where assets (e.g., L-BTC) are traded against each other on the Liquid Network. (Mow, 2019)

Another stablecoin that was introduced by the Canadian exchange "Bull Bitcoin" is Liquid CAD (L-CAD). It is a digital representation of the Canadian dollar and aims to maintain a 1:1 peg to it. L-CAD utilizes off-chain collateralization, where each unit is backed by one Canadian dollar. However, Bull Bitcoin does not provide redemption of L-BTC for its collateral. Therefore, L-BTC must be traded for Bitcoin or, if offered, used as a payment method. (Mow, 2020)

Both stablecoins involve counterparty risks for users towards the intermediary that issues the asset. Overall, the Liquid Network is experiencing a lack of utilization. Currently, most blocks – which are generated every minute – only contain one to seven transactions (Blockstream, 2023c). Compared to Bitcoin, where on average a new block is produced every ten minutes, this would add up to less than 100 transactions in the same duration. The Bitcoin network processes more than 3,000 transactions per block (Mempool.space, 2023). Furthermore, USDt and L-CAD are not very common, although they have been introduced and implemented in the Liquid Network in the years 2019 and 2020.

3.3.4 Stablesats

The last approach of fiat stablecoins on Bitcoin, which we will examine in this section, is entirely different from those described previously, as it does not involve a native asset, nor a transitory local asset issued through a peg-in of bitcoin. Stablesats introduces a synthetic US dollar on the Lightning Network, to which users can exchange their bitcoin through a

perpetual inverse swap administered by a dealer. However, the dealer only holds bitcoin on its books. The objective of this construct is to constantly maintain a 1:1 peg to the US dollar, despite the current price of bitcoin. This implementation eliminates the need of fiat currency or fiat-based stablecoin integration. The exchange occurs in a Bitcoin Lightning wallet that supports the Stablesats software (e.g., Blink wallet). Such a wallet application comprises a bitcoin account and a US dollar account. The bitcoin account represents a typical Bitcoin Lightning wallet. Users can convert their bitcoin holdings at any time to the respective amount of US dollars at the current exchange rate. For example, the bitcoin account contains one million sats (the subunit of bitcoin) and bitcoin is traded at $10,000. As one bitcoin is divided into 100,000,000 sats, the total balance would be $100. Exchanging 500,000 sats would result in the user holding $50 as well as the remaining 500,000 sats. Due to the volatility of bitcoin, the dealer – who guarantees a permanent exchange – must hedge the bitcoin holdings converted to synthetic US dollars. This is accomplished through a bitcoin derivative position that is opened immediately after the exchange. The derivative guarantees redemption at the current price when the exchange happens, regardless of the future price of bitcoin. Such a contract is also known as a short position, where the financial instrument replicates the opposite of the actual asset. Thus, if the price of bitcoin falls, the dealer's holdings decrease by the same percentage, while the derivative increases, so that they counterbalance each other. The perpetual inverse swap achieves this with without specifying a settlement date for the position. Consequently, the exchange can take place at any time in the future. (Galoy, 2023; Burtey, 2023)

Stablesats comprises an approach that, contrary to the other projects, cannot be evaluated regarding its stability, since it does not incorporate its own token. However, users need to be aware of counterparty risks, too, when interacting with the platform. Firstly, users must trust Galoy, the company behind Stablesats, and its business model. The custodial Blink wallet also must be trusted when depositing bitcoin holdings. According to their website, most of the user funds are managed securely in multi-signature structures and cold storages that have no connection to the internet (Blink, 2023a). As both applications are developed open-source, this risk can be reduced partially due to the involvement of the community. Secondly, and more importantly, the exchange acts as a counterparty, that can collapse. If this happens, the derivative may not be recoverable and the user’s US dollar account in the wallet therefore worthless. Furthermore, issues may occur with the derivative itself, as the position could be closed, leading to a situation where the US dollar accounts are underhedged. The dealer must therefore establish a new contract in order to secure its holdings. Overall, it is necessary to mention that Stablesats is still relatively new whereas the risks described here must be evaluated and further risks need to be identified. So far synthetic US dollars on the Bitcoin Lightning Network are only implemented via Stablesats in the Blink wallet. Thus, the interoperability of this solution is limited and users that want to hold it must download the mobile application. However, transferring from the US dollar account to other wallet applications is feasible since both can communicate over the Lightning Network. Within this transaction the amount of synthetic US dollar transferred is exchanged to the corresponding number of bitcoin and sent to the wallet of the recipient. (Blink, 2023b)

4 Research Objective

In this study, our primary objective is to determine the impact of Taproot Asset stablecoins on Bitcoin adoption. Therefore, we employ a combination of substantive studies and standardized data gathering methods. On the theoretical side, the foundational research on diffusion and adoption by Everett M. Rogers is used to support the practical procedure. Quantitative research in the form of a survey was chosen to determine the potential for adoption. The central research question addressed in this paper is:

> **What is the current adoption of the Bitcoin network and bitcoin as a means of payment and how do stablecoins on Bitcoin influence that?**

In the preceding chapters, the foundations of the Taproot Assets protocol were discussed. Certain prerequisites were established in advance and are crucial for its development. Among these, Bitcoin forms the backbone of these technologies. The soft fork integration of the Taproot update has extended its capabilities with relevant features. In addition, the Taproot Assets protocol relies on the Lightning Labs software implementation of the Lightning Network. Ultimately, the Taproot Assets protocol and its specifications were investigated with the objective of facilitating stablecoin integration.

Stablecoins were explained in more detail in the subsequent chapter. This crypto asset class can be divided into three categories, which we have highlighted in a separate section. In the following, an overview of the current stablecoin landscape was depicted. Lastly, there were already combinations of stablecoins and Bitcoin before the invention of Taproot Assets. However, these are either not natively integrated and therefore require an additional network or do not use any token at all.

In conclusion, the required theoretical principles were described to address the challenges described in the research question. Furthermore, these fundamentals and their characteristics lead to the following hypothesis: the combination of a decentralized network that can process transactions fast and crypto assets that have low volatility, like stablecoins, could improve the utilization of Bitcoin.

5 Identifying Bitcoin Adoption

In this chapter, we will analyze the potential that the proposed implementation of Taproot Asset stablecoins could have on the adoption of Bitcoin. The first section describes the methodology selected to determine these metrics. In order to obtain a representative and statistically evaluable result, quantitative research based on a survey was applied. The conditions of the design and data collection are explained, followed by a review of the quality of the responses. In a second step, adoption is explored theoretically, and an overview of the concept and terminology is provided based on the work "Diffusion of Innovations" by Everett M. Rogers. The innovation-decision process is explained, which serves as an essential reference for the evaluation. The third section is divided into the current state of adoption, which is also analyzed based on previous statistics, and the potential impact according to the results of the questionnaire. All findings relate to the deadline of the survey on January 6, 2024. The tables included in this chapter are own illustrations created with the data set *Survey Statistics.sav* (Appendix E) and the software *IBM SPSS Statistics Data Document*.

5.1 Methodology

This section provides fundamental information on the quantitative research model that was selected to determine the impact of Taproot Asset stablecoins on Bitcoin adoption. It explains crucial concepts and comprises proper statistical procedures that were applied to ensure reliable results. This is important to substantiate the research question and thus the objective of the thesis.

5.1.1 Data Collection and Questionnaire Design

The survey was conducted in a digital format using Microsoft Forms, with a hyperlink shared with the target group for participation. The survey was published for five weeks, and participation was requested repeatedly. The questionnaire was developed according to the ten rules of question wording defined by Rolf Porst. In the study, Porst explains that the questions and response options should be phrased neutrally, contain simple terms and should not be excessively long or complex. In addition, the survey must not include any information that the participants may not have. (Porst, 2000)

To ensure all participants were on an equal level of knowledge, the questionnaire included sections that provided general information about Bitcoin, the Lightning Network and Taproot Assets. This ensured that everyone could participate, regardless of their Bitcoin knowledge. However, the general acceptance of blockchain technology and crypto assets is still in its

infancy. According to statistics from the data aggregator Statista, there were merely 428.6 million users of crypto assets globally in 2022 (Statista Market Insights, 2024a). In Germany, users totaled 10.9 million in the same year (Statista Market Insights, 2024c). This shows that there are still many people who have not yet had any experience with this technology. As it is a niche topic, asking people with low awareness of its functionalities and advantages to participate would not support the validity of the survey results. Therefore, a segmentation was performed to address the intended target group of participants with a background in blockchain technology and Bitcoin. Accordingly, the results can only be applied to this homogeneous group, but within the blockchain ecosystem they can be extrapolated to a larger sample of users. Hence, a partial generalizability of the results in this particular group can be attested. The overall generalizability for a community of heterogeneous people cannot be guaranteed. First of all, the acceptance and knowledge must grow in order to be able to undertake such a survey on a larger scale. Lastly, the questionnaire features branching, which leads participants to different paths depending on their decisions. However, all branches address the same issues. Appendix A illustrates the survey question path and along with the questions and results of Appendix B, provides a better understanding of the questionnaire structure.

The questionnaire was distributed to students of different cohorts of the master's degree program "Blockchain & Distributed Ledger Technologies" at University of Applied Sciences Mittweida. Moreover, it was published on the social media platform LinkedIn, which also predominantly includes contacts who are engaged in the blockchain ecosystem. Finally, the survey was posted in the Slack channels of DeFi Talents, Bitcoin Talents – both of which are programs of the Frankfurt School Blockchain Center – and the LND Developer Community of Lightning Labs. A total of 57 participants completed the questionnaire. Table 5 in the appendix shows the demographics of the respondents and their experience with Bitcoin. Of the 57 participants, a majority of 46 (80.7%) were male and 10 (17.5%) were female. Although this difference is conspicuous and uneven, this distribution reflects the gender composition in the blockchain ecosystem, which is dominated by male users. Most participants were between the ages of 24 and 34 (24; 42.1%) and had a master's degree as their highest educational achievement (31; 54.4%). A majority of 28 (49.1%) attendees are employed full-time. Regarding the participants' experience with Bitcoin, 25 (43.9%) would consider their knowledge to be advanced, while 40 (70.2%) have already used the Bitcoin network.

All extended tables and calculations can be viewed in Appendix C. Alternatively, they can be recomputed using the syntax code (Appendix D) and the SPSS file *Survey Statistics.sav* (Appendix E) digitally attached to this thesis.

5.1.2 Quality Criteria

Considering the results of the survey, it is important to review the quality of the results. Such an assessment is based on three central quality criteria: objectivity, reliability, and validity.

All of them are analyzed in this subsection. Objectivity refers to the independence of the participants' decisions, which predominantly includes the influence of the interviewer. As the quantitative research is conducted as a digital survey, the influence of the interviewer can only be exerted indirectly through the formulation of the survey, comprising questions and informative sections. As previously described, the design of the questionnaire was based on Rolf Porst's rules of question wording. Accordingly, the articulation concerning the questions and the information provided to the participants was selected and formulated neutrally. The introductions to the main subjects of the survey contained the same evidence-based information for each participant. These were primarily added so that a potential knowledge advantage of certain participants could be excluded. Furthermore, all survey participants received the same questionnaire. In order to minimize the researcher's bias, the evaluation of the results is conducted using the statistical data analytics software SPSS in a standardized manner based on the actual number of options selected by the participants. (Rammstedt, 2004, p. 2 ff.)

Reliability expresses the accuracy by which an attribute is measured by the questionnaire. Accordingly, the repetition of the survey under the exact same conditions must lead to the same results. Of course, this can only be analyzed in a hypothetical scenario, as two different measurements cannot produce exactly the same results, in particular due to changes in information and knowledge. The reliability of the survey results is determined by quantifying their consistency. Cunningham, Preacher et al. describe it as “the homogeneity of responses to all items within a particular measure” (Cunningham, Preacher, & et al., 2001, p. 166). More specifically we calculate the internal consistency and whether certain items (questions) measure the construct defined by the research question. (Rammstedt, 2004, p. 5 ff.)

The research question aims to identify the influence of stablecoins on the utilization of Bitcoin reflecting on its current adoption. Therefore, only items that relate to this construct and – due to branching – were answered by all participants can be considered. The split-half test was applied, which separates the items into two groups that are compared with each other. Resulting from the research question, these comprise the following six items: (Rammstedt, 2004, p. 9)

First half:

(A) Based on your knowledge, do you consider bitcoin as money?

(B) The price volatility of bitcoin is high. Do you consider this to be a problem if an asset is supposed to be a means of payment?

(C) Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior?

Second half:

(D) Have you used the Bitcoin network before (e.g., create a wallet, do a transaction, operation of a full node)?

(E) Do you consider the integration of stablecoins to be an improvement for Bitcoin?

(F) Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?

Based on the aforementioned items, the split-half test calculates a Spearman-Brown reliability coefficient r_{tt} of 0.75 (Table 7). Due to the split, only half of the values are incorporated in the calculation. Therefore, an adjustment through test duplication can be applied with the following formula: (Rammstedt, 2004, p. 10)

$$corr\ r_{tt} = \frac{2 * r_{tt}}{1 + r_{tt}}$$

This results in a corrected reliability coefficient corr r_{tt} of 0.857. According to statistical theory, a calculated reliability value of more than 0.8 is considered satisfactory (Rammstedt, 2004, p. 15).

Validity is the degree of accuracy by which a method is suitable for measuring the intended characteristic. This implies that the survey results represent what is to be researched and thus serve as a measurement for the research question. In concrete terms, we determine the construct validity. Two constructs that deviate from the research question were identified, each represented by two items, as follows: (Rammstedt, 2004, p. 16 ff.)

Bitcoin utilization:

(C) Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior?

(D) Have you used the Bitcoin network before (e.g., create a wallet, do a transaction, operation of a full node)?

Stablecoin utilization:

(E) Do you consider the integration of stablecoins to be an improvement for Bitcoin?

(F) Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?

Accordingly, an inter-item correlation matrix can be generated based on the calculation of Kendall's tau-b coefficient in SPSS (Rammstedt, 2004, p. 18 ff.). This method is used for

items of an ordinal scale level and compares them with each other (Laerd Statistics, n.d.). The following abridged version of Table 8 shows the results between the items:

	Bitcoin utilization		Stablecoin utilization	
	(C)	*(D)*	*(E)*	*(F)*
(C)	-			
(D)	0,092	-		
(E)	0,345	-0,051	-	
(F)	0,679	0,029	0,454	-

Table 1: *Inter-item correlation matrix with Kendall's tau-b coefficient*

The coefficient ranges between -1 and +1 and expresses the correlation between two variables. A result of -1 would therefore indicate a fully negative correlation, while a Kendall's tau-b coefficient of +1 describes a perfect positive correlation and values close to 0 indicate indifference between the variables. According to Neyman, the labeled values in Table 1 represent a significant correlation, since their level of significance is less or close to 0.01 (Neyman, 1976). First, a null hypothesis is established, which assumes that there is no correlation between the two variables. The level of significance determines the probability of accepted uncertainty that the null hypothesis is still correct and is set at 1% in this calculation (Tenny & Abdelgawad, 2023). The distinct positive correlation of *(C)* and *(F)* shows that the consent to one item has a positive influence on the other and vice-versa. In this case, it can be inferred that participants who tend to increase their use of bitcoin through the integration of stablecoins also increase their use of stablecoins. As a result, the overall usage of Bitcoin increases. A medium positive correlation can be identified between the items *(E)* and *(F)* within the construct. This implies that attendees who consider the integration of stablecoins to be an improvement also endorse regarding its utilization. The effectual positive correlation of *(C)* and *(E)* further supports this assumption. With regard to the findings, it is feasible to assume that the selected methods in fact measure characteristics that deviate from the research question.

5.2 Adoption in Theory

To gain a broader understanding of the theory of adoption, we refer to one of the most prominent works, "Diffusion of Innovations" by Everett M. Rogers. According to Rogers, „diffusion is the process by which an innovation is communicated through certain channels over time among the members of a social system" (Rogers, 1962, p. 5). This process therefore comprises (1) an innovation, (2) an individual that has knowledge or experience of using this innovation, (3) another individual that has a lack of this knowledge and has no experience, and (4) a communication channel through which these individuals interact with each other (Rogers, 1962, p. 17). In addition to the term "innovations", Rogers also refers to "technologies" in his theory, both of which can be applied to Bitcoin in terms of revolutionizing the peer-to-peer exchange of value without the necessity of an intermediary

(Rogers, 1962, p. 12). Furthermore, Rogers defines adoption as “a decision to use and implement a new idea” (Rogers, 1962, p. XVIII). It is the affirmative result of the innovation-decision process, which we will examine in the following subsection. The opposite and adverse option is the rejection of the innovation or technology. According to the process of diffusion described above, more individuals with knowledge about Bitcoin would inevitably lead to the establishment of more communication channels and thus more interaction between aware and unaware individuals. As a result, more novices would be faced with the decision to accept or reject Bitcoin, which eventually depends on the key attributes of the innovation explained subsequently.

5.2.1 The Innovation-Decision Process

Individuals that discover an innovation or technology start with a minimal level of knowledge and a sudden event triggers the personal interest of acquiring information to reduce uncertainty. Such an introduction can occur by chance or through communication channels. This stage of the innovation-decision process is known as *knowledge*. The individual becomes aware of the innovation and receives information about it. It involves familiarization with the new technology and developing an initial understanding of its features and benefits. While the knowledge in the first phase is rather cognitive, the *persuasion* includes affective knowledge. The individual actively seeks additional information about the innovation until an attitude is formed. This occurs through the evaluation of advantages and disadvantages and potential needs that the innovation could satisfy. The *decision* stage is the conclusion of the previous information gathering and opinion-forming phase. In this stage, the individual is faced with the decision-making based on the available knowledge. Therefore, the outcome of the persuasion process predominantly influences the decision. Although there are two extremes, acceptance and rejection, the individual can also take a more neutral position or even gradually change their attitude towards the other option. If the individual decides to adopt the innovation, this leads to its *implementation*. This phase concerns overcoming obstacles, adapting to change, and integrating the innovation into daily routines. *Confirmation* is the final stage of the innovation-decision process. The individual compares the adopted innovation with the previous approach that was superseded. As described above, the individual's choice can either be final or switch to the other extreme. For example, an individual can form a negative attitude towards an innovation, but then develop further interest in it and finally adopt it (later adoption). The contrary decision process is called discontinuance. When an individual's decision is final, they seek reinforcement and reassurance through their own experiences or feedback from others. Throughout all stages, there are communication channels between individuals for the exchange of knowledge. Figure 6 illustrates the innovation-decision process described above: (Rogers, 1962, p. 164 ff.)

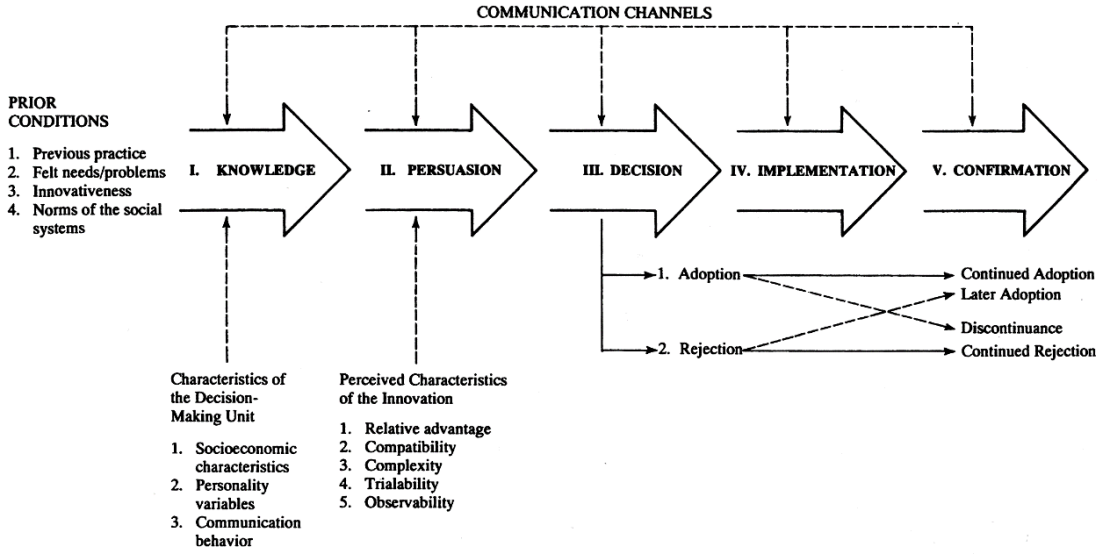


Figure 6: *The innovation-decision process (Rogers, 1962, p. 165)*

In his theory of the Diffusion of Innovations, Rogers identified five key attributes that influence the rate of adoption of an innovation within a population. These attributes play a crucial role in shaping individuals' perceptions and decisions regarding the adoption of an innovation or technology. This can be applied to Bitcoin and further translated to the results of the survey. *Relative advantage* refers to the perceived superiority of an innovation over existing alternatives that the individual has previously used. An innovation is more likely to be adopted if it offers clear advantages in terms of efficiency, effectiveness, or other benefits. The greater the perceived relative advantage, the more rapid the adoption is expected to be. *Compatibility* indicates the extent to which an innovation is consistent with the existing values, practices and needs of potential users. The higher the compatibility between the existing practice and the innovation, the lower the uncertainty. This results in a higher degree of adoption, as the innovation can be integrated more smoothly into the existing social and cultural context. *Complexity* relates to the perceived difficulty of understanding and using an innovation. Innovations that are perceived as simple and user-friendly are more likely to be adopted more quickly. Reduced complexity lowers the barriers to adoption and makes the innovation more appealing to a broader audience. *Trialability* is the extent to which a person can experiment with or test the innovation before fully committing to it. Innovations that allow a trial period or limited use enable potential adopters to assess the benefits of the innovation and its suitability for their needs, thereby reducing the risk associated with adoption. The *observability* of an innovation refers to the visibility of the results for other potential adopters. When the positive results of adopting an innovation are easily observable by the community, a social influence is created which encourages others to embrace it. Observability plays a significant role in the diffusion process as it fosters the mechanisms of social learning and imitation within a population. (Rogers, 1962, p. 211 ff.)

5.2.2 Adopter Categories

According to Rogers and the Diffusion of Innovations, a population can be divided into subgroups that have different characteristics and attitudes towards an innovation. Rogers refers to them as adopter categories and classifies individuals based on their willingness and readiness to accept new innovations. There are five adopter categories, which are also illustrated in Figure 7. *Innovators* are the fastest adopters, who are described as venturesome and make up around 2.5% of the population. Innovators are adventurous risk takers who embrace new ideas and technologies prematurely despite uncertainty. They play a crucial role in the early stages of innovation diffusion. Furthermore, *early adopters* represent around 13.5% of the population and are considered respectable. These individuals are opinion leaders in their social circles and are quick to embrace new innovations. Hence, they serve as role models for other potential users who obtain their information from this group. The early adopter forms a bridge between the innovators and the following cohort. The *early majority* constitutes 34% of the population and has deliberate characteristics. Members of the early majority adopt innovations before the average person in a social system is aware of the innovation. Their decision-making process takes longer and relies on the experiences of others before they embrace an innovation or technology. The *late majority* is similar in size (34%) to the early majority and is described as skeptical. This means that they begin studying an innovation only after the average person in the social system has already completed the adoption process. These individuals take a more cautious approach to adopting innovations. They rely on proven success stories and are often influenced by social pressure. For the late majority, almost any kind of uncertainty needs to be removed for them to adopt an innovation. The *laggards* make up the last 16% of the population and are referred to as traditional. They are resistant to change and are the last to adopt new innovations. Laggards are deeply rooted in existing practices and are hesitant to adopt anything new as their attitude is predominantly oriented towards the past. By the time this category has adopted a technology, it may have already been superseded by another innovation. (Rogers, 1962, p. 245 ff.)

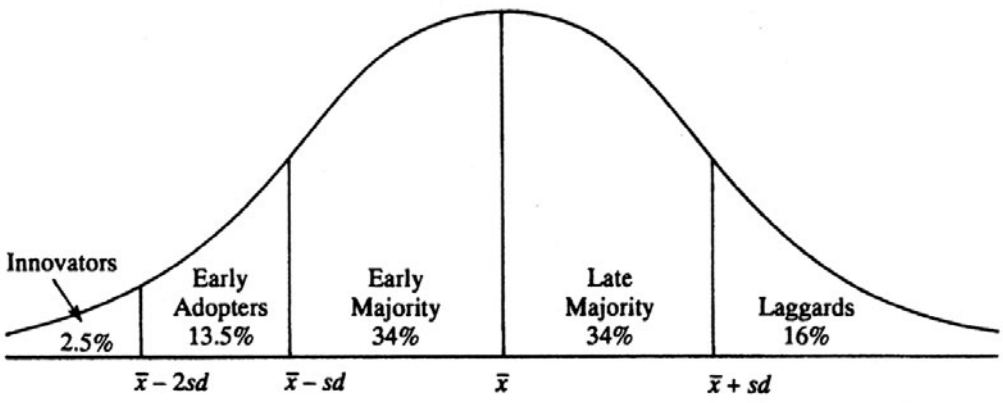


Figure 7: *Adopter categories (Rogers, 1962, p. 247)*

This categorization provides a valuable framework for evaluating the dynamics of Bitcoin adoption, determining the current state and gaining insights into the potential development.

By categorizing individuals into these groups, it is possible to analyze the prevailing attitudes, motivations and behaviors related to Bitcoin. In the subsequent section, a comprehensive examination of Bitcoin adoption is conducted by evaluating the results of the quantitative research.

5.3 Results

After testing the quality criteria of the survey and gaining a comprehensive understanding of adoption in theory, we will analyze the survey results in this section. In order to assess the potential impact, we first need to determine the current state of adoption. Subsequently, we can compare this situation with the results of the survey and create scenarios of how these could affect the future utilization of the Bitcoin network, its native asset bitcoin and integrated stablecoins. Thereby, we focus on statistics describing global and specifically German data. Roger's Diffusion of Innovations theory assists in determining whether users would accept or reject the integration of stablecoins into Bitcoin and what the implications would be. At this point, it is important to emphasize that the survey does not explicitly take into account how stablecoins will be integrated into Bitcoin, as this has not yet been determined and to keep the questionnaire more general and uncomplicated. This also applies to this section. We will further evaluate on that in chapter 6.

5.3.1 Current State of Adoption

Referring to the market capitalization, Bitcoin has ever since been the largest crypto asset (CoinGecko, 2024). This figure is, however, only of limited relevance as an indicator for the acceptance of Bitcoin. Therefore, we consider identifying relevant statistics that could testify the adoption through different information on the conjunction of Bitcoin and the public. The analysis below is based on figures concerning the global population by the U.S. Census Bureau (U.S. Census Bureau, 2024). According to the data of Statista, there were 426.8 million users of crypto assets in 2023 on a global scale (Statista Market Insights, 2024a). This adds up to a global saturation of 5.3%. The almost same figure was published by the crypto asset payment provider Triple-A which specifically analyzes the holders of crypto assets (Triple-A, 2023). Furthermore, data of the crypto asset exchange Crypto.com reports 425 million owners of crypto assets in December 2022 (Crypto.com, 2023). Since bitcoin only makes up for a part of these user balances, it is necessary to identify the proportionate ownership of the average person in bitcoin compared to their whole crypto asset portfolio. The same statistic of Crypto.com shows that 219 million respondents claimed to hold bitcoin, which represents 52% (Crypto.com, 2023). In comparison to the global saturation this result in 2.8% of bitcoin holders in the year 2023. According to the adopter categories of Rogers, the innovators are fully engaged in Bitcoin while the early adopters are beginning to hold bitcoin. However, there are also more pessimistic statistics that state only 106 million bitcoin owners (Buy Bitcoin Worldwide, 2023). This would only result in 1.3% of bitcoin holders and thus half of the innovators were adopting it.

For the population of Germany, analysis by Statista was used (Statista Market Insights, 2024b). According to another research of that data aggregator, in 2023 there were approximately 15 million users of crypto assets in Germany, which is a national saturation of 17.7% and an increase of 4.4 percentage points compared to 2022 (Statista Market Insights, 2024c). A statistic from Triple-A of the year 2022 only counts 5.8% of crypto asset holders. Although this number differs much from the analysis of Statista, the holders doubled within one year compared to 2021 (Triple-A, 2022). Hence, for the year 2023 it could be assumed that the figure is at least double-digit. The specific type of usage is not defined in detail by the research of Statista and only calculates the "number of customers or accounts" (Statista Market Insights, 2024c). As the usage and holding of a crypto asset both imply having an account, these evaluations can be compared with each other. The only alternative would be receiving crypto asset through a direct blockchain transaction in order to not have an account. However, this will be neglected here. As the objective of this subsection is to identify Bitcoin adoption – not crypto asset adoption – the statistics of Triple-A furthermore states that in the year 2022 there were roughly 69.4% of crypto asset owners that held bitcoin (Triple-A, 2022). If we compare this with the recent crypto asset analysis of Statista described above, there would have been 12.3% of bitcoin holders in Germany in 2023. Applied to the more pessimistic results of the Triple-A statistics itself, and the assumption that the numbers would further double from 2022 to 2023 (11.6% of crypto asset holders), there would have been 8.1% of bitcoin holders in the year 2023 (Triple-A, 2022). Compared to the global setting, the German market can be considered more matured. In accordance with Rogers' adopter categories, all innovators in Germany already adopted Bitcoin in terms of simply holding its native asset. Additionally, more than two-thirds – or at least almost the half in the pessimistic scenario – of the early adopters joined them so far.

Yet this only represents the owners of bitcoin and does not testify the utilization of Bitcoin as a payment network and other applications. A report of FIS Global indicates that merely 0.2% of the e-commerce payments in 2022 were executed using crypto assets (FIS, 2023, p. 24). The statistic, however, does not disaggregate this figure nor particularize payments using the Bitcoin network. Therefore, we can only expect that a subset of it was performed using bitcoin. The report further states that 77% of the respondents buy crypto assets for investment purposes while 18% would use them to purchase goods or services (FIS, 2023, p. 23). Data from a statistic of PYMNTS and BitPay that was collected in the USA in 2021 reveals that a shift concerning crypto asset payments could happen due to younger, more technically skilled users. According to this, the younger the generation that a person is assigned to, the higher the percentage of already performed purchases with crypto assets for any kind of product category. For those who did not purchase anything with crypto assets so far, more than 92% on average across all generations could imagine doing so (PYMNTS & BitPay, 2021, p. 7 f.). If we strictly equate adoption with the actual use of Bitcoin, we need to apply the percentage of people considering making payments with it (18%) to the previously identified holders. Accordingly, global adoption would amount to 0.5% (pessimistic: 0.2%), while adoption in Germany would be 2.2% (pessimistic: 1.5%). In terms of making payments, both globally and in Germany, only the innovators would have adopted Bitcoin.

However, since owning Bitcoin also implies certain usage, this broader interpretation is considered equivalent to adoption in this paper.

Furthermore, the barriers to adoption, hindering people that do not own crypto assets to pay with them, were analyzed in the statistic. Far ahead, the response that was given the most was the lack of knowledge (75%), followed by missing acceptance (33.3%) and volatility (25.2%) (PYMNTS & BitPay, 2021, p. 16). Since a majority of the attendees of the survey used within this thesis would consider their knowledge above average it is not possible to reflect on that. As described before, blockchain technology is still in its beginnings and has low adoption rates, which demonstrates that the figure above is not unfounded. However, information resources are primarily digitally available and therefore open to anyone with an internet connection. This can be seen as highly progressive and enhances the learning process, compared to more traditional circumstances that may require guidance or less accessible sources. In addition, there are plenty of free programs and courses that interested users can enroll to. The inhibition that is created due to the volatility of bitcoin and was mentioned by the respondents could be remedied through the implementation of Taproot Asset stablecoins. We will examine this in more detail in the next subsection. Regarding the acceptance of payments with bitcoin, the coverage indeed is still low. As of February 18, 2024, there are 10,548 merchants globally and 1,118 in Germany that accept payments in bitcoin (Coinpages, 2024; BTC Map, 2024). Once again this shows that Germany is leading when it comes to adoption, although the number of outlets is little and can almost be neglected compared to the overall availability of merchants. The questionnaire of the survey also comprises a query that intends to identify whether Bitcoin payment adoption in the future is initiated through customers demanding it or merchants offering it. The results are nearly balanced as 28 (49.1%) responded that customers must further demand this payment method and 29 (50.9%) voted that merchants must facilitate this (Table 9).

In order to identify the current adoption of Bitcoin within the survey, the participants were asked to rate their usage of the Bitcoin main network as well as bitcoin as means of payment. The responses are illustrated in Table 10 and Table 11. Obviously only participants were asked, that stated that they have used the Bitcoin network or respectively bitcoin as a means of payment before. Thereby 19 (47.5%) of a total of 40 participants stated that they use the Bitcoin network occasionally (several times) while in summary 18 (45%) use it regularly (daily, weekly, monthly). More explicit results apply for the usage of bitcoin as a means of payment. For this question 12 (57.1%) of a total of 21 participants responded that they occasionally pay with bitcoin and 7 (33.3%) do so regularly. This also implies that 17 (29.8%) attendees have not used the Bitcoin network before and 36 (63.2%) have not used bitcoin as a means of payment. The predominant reason for not considering the future usage of Bitcoin at all is its price volatility (87.5%), which was chosen by 7 of 8 participants (Table 12). Secondly and thirdly were the missing knowledge and a lack of trust (both 50%). Furthermore, the research group was split into those who used Bitcoin before and those who claimed to not have. Both of them were confronted with the question why they do not consider the use of bitcoin as a means of payment (Table 13 and Table 14). In summary

price volatility was once again the key motive which was mentioned by 10 of 13 (76.9%) participants. With regards to the attendees who used the Bitcoin network before, a majority of 6 (66.7%) votes claimed other reasons. However, these are also primarily focused on its volatility and that they rather see bitcoin as an investment. One participant that used Bitcoin before stated a lack of trust. This also applies to a person that has not used Bitcoin before and two others that do not understand it. Across all 21 participants that were asked these questions, a minority indicated that they consider Bitcoin or using bitcoin as a means of payment as “insecure” or “fraudulent”. This further raises the question, whether the participants consider bitcoin as money (Table 15). As a result, 36 (63.2%) agreed to that, while 21 (36.8%) would refuse this statement. Similar to previously, the participants that negated this question were asked for the reasons of that choice (Table 16). Once again, a majority of 16 (76.2%) justified their response with the price volatility of bitcoin, closely followed by the lack of acceptance which was indicated by 15 (71.4%) attendees. 7 (33.3%) other reasons were specified regarding this question, which predominantly addressed bitcoin’s function as an investment or a store of value as well as lack of regulation. Ultimately, 4 (19%) participants cited complexity as an obstacle for a consideration as money.

Another indicator we can use to identify the total Bitcoin adoption is the global coverage of ATMs to buy and sell crypto assets. According to the data provider Coin ATM Radar, there currently exist 36,131 crypto asset ATMs worldwide. Although the number had its peak in August 2022 with over 39,000 machines and had a slight decrease since then, the number continuously grows again since the mid of 2023 (Coin ATM Radar, 2024a). The decrease predominantly occurred due to a reduction of ATMs in the USA, which is also the largest market with currently almost 30,000 installed machines (Coin ATM Radar, 2024b). In order to express the growth rate, Coin ATM Radar specifies a daily installation rate of more than 46 ATMs globally on average (Coin ATM Radar, 2024c). Almost all of the ATMs support the purchase and selling of bitcoin, which is by far the most represented crypto asset (Coin ATM Radar, 2024d).

On January 10, 2024, the Chair of the U.S. Securities and Exchange Commission released a statement concerning the approval of the listing and trading of 11 spot exchange-traded products (ETP) representing the price of bitcoin (Gensler, 2024). Although, this turning point brings institutional investors and more unaware retail investors into the market, it does not have a direct influence on the adoption of Bitcoin, as buyers do not directly invest into bitcoin but rather in a financial asset construct. Investors are only interested in the actual price representation of bitcoin and not in its additional functionalities and therefore primarily consider it as an investment. Since the ETP provider purchases bitcoin and delegates the shares to the investors, this does not represent a direct holding. Hence, users have no authorization over their bitcoin and cannot withdraw nor transfer them. This also implies that the Bitcoin network is not or barely used, as the only on-chain transaction performed is to the provider’s personal custody solution or a third-party custodian. However, the general adoption in terms of public awareness and knowledge could be enhanced indirectly due to the approval.

The adoption of Bitcoin, crypto assets and blockchain technology in general is still in its infancy. We have identified that there is a deviation between global and German adoption. However, both of them are only used by a small subgroup of the population. According to Rogers, innovators and in parts early adopters have adopted Bitcoin. Nevertheless, specifically early adopters have influence on potential adopters due to their status as opinion leaders and role models for others, resulting in more potential for Bitcoin. Consecutively, we will further elaborate on these implications.

5.3.2 Possible Impacts

The adoption of Bitcoin can be affected by several activities such as a growth in public knowledge, increasing on-chain transactions or more people using it as a payment network. Since Taproot Asset stablecoins are intended to maintain stability, they can be used as a store of value and means of payment based on Bitcoin technology. In order to estimate the overall potential of users switching from traditional electronic payments to Bitcoin payments, it is required to identify the current saturation of electronic payments. Therefore, the introductory question of the survey determined the frequencies that the attendees pay with a debit or credit card or utilize mobile payments (e.g., smartphone or smartwatch) at a physical point of sale (POS), given that this payment method is offered by the retailer. As payments at an online store primarily are electronically, this question is redundant, and the result can therefore be assumed as at least the frequencies of payments at a physical POS. The majority of 66.7% of the attendees would pay electronically every time, while another 29.8% would consider doing so often. Only 3.5% do sometimes choose electronic payments. The options “rarely” and “never” were not selected by any attendee (Table 17). In summary this statistic shows that a preference for electronic payment methods exists, which describes a fundamental potential for the utilization of Bitcoin payments. This can be substantiated based on the results of the research by FIS Global. According to that, in the year 2022 only 2% of the e-commerce and 16% of the POS transactions globally were performed using cash. These figures are expected to further decrease until 2026, while payments with a digital wallet are reckoned to grow the most (FIS, 2023, p. 8).

An approach of demonstrating the prospective potential of bitcoin as a means of payment is by comparing the results of participants who used Bitcoin before with those who have not (Table 18 and Table 19). While 52.5% of the people who utilized Bitcoin before also used bitcoin as a means of payment, there are a little more potential users of 55.6%, who could imagine doing so in the future, although these are no definite answers. As a result, the use of bitcoin as a means of payment could increase in the future. On the other hand, the answers could also be influenced by a lack of experience with Bitcoin technology. Participants that did not have prior usage of Bitcoin could misconceive its functionalities and might have a euphemistic imagination.

In the previous subsection we have discussed several reasons of the respondents for not using bitcoin as a means of payment. The predominant challenge of this is the price

volatility. However, this does not affect the Bitcoin network itself. The integration of stablecoins could mitigate this problem. In accordance with the previous comparison, we contrast attendees that used bitcoin as a means of payment before with those who did not regarding their appraisal of the cumbrousness of the price volatility. 42.9% of the survey participants that already paid with bitcoin agreed with this statement, whereas a majority of 57.1% is not bothered by the price volatility (Table 20). In contrast, participants that have no experience in using bitcoin as a means of payment voted differently. This group consists of persons that used the Bitcoin network before and those that did not use Bitcoin at all (Table 22). In this evaluation, 73.3% of the participants stated that the price volatility of bitcoin is cumbersome while 26.7% did not have a problem with it. This represents a distinct discrepancy between these groups and reveals a potential for a less volatile and therefore more stable crypto asset. Nevertheless, from this statistic we could also interpret that people who used bitcoin as a means of payment are not worried about the price fluctuations. It is evident that if as a person uses bitcoin more frequently for purchases, an average price emerges which levels out. In order to check this assumption, we generate a crosstabulation of these items (Table 21). It illustrates the relation that survey participants who used bitcoin as a means of payment more regularly, are likely to not have issues with its price volatility. Hence, the percentages shown in the crosstabulation of individuals that used Bitcoin before, are ascending, while those of nonusers are descending. If a person paid with bitcoin only once or occasionally, they rather rate the price volatility as cumbersome. Ultimately, 55.6% of the participants claimed the cumbrousness of the price volatility of bitcoin, compared to 44.4% who did not criticize this (Table 23). This further substantiates the necessity for a stable crypto asset that could serve as a means of payment. In comparison, these figures show a discrepancy to a more general question regarding the problems of a highly volatile asset that aims to be used as a means of payment. The results are shown in Table 24. In this analysis, 91.2% claimed that an intense volatility is considered cumbersome for such an asset. Although the results represent the same tendency but to a different extent, the deviation cannot be deduced.

Despite of that, the volatility in fact is still the central issue that was mentioned by the participants. This raises the question whether the integration of stablecoins could be an improvement for Bitcoin (Table 25). Overall, 52 (91.2%) respondents would agree with that statement, of which 15 (26.3%) consider stablecoins on Bitcoin to be definitely advancing. Only 5 (7%) participants do not find this to be improving for Bitcoin, of which 1 (1.8%) absolutely disagrees. In order to understand the reasons for their rejection of Bitcoin-based stablecoins, these respondents were further interrogated. According to their answers, they either prefer using bitcoin itself, stablecoin solutions of other blockchain networks or do not recognize the difference from fiat currencies and thus the added value. Though, this statistic shows a clear dominance of individuals that would endorse an integration of stablecoins into the Bitcoin network, which we will further examine in the following.

To identify the impact of the integration of stablecoins into Bitcoin, the survey participants were asked how their behavior would change based on their current usage of the Bitcoin

network. This was specified on both, the expected use of bitcoin and integrated stablecoins (Table 26 and Table 27). The statistics represent similar results as for most attendees the utilization would probably stay the same. Though, there are a lot more participants that expect a higher usage of both, bitcoin and integrated stablecoins, than those who would use them less. The results could be interpreted as an increase in the use of Bitcoin. However, the results of this question must be treated with caution, as the usage of something that does not yet exist cannot decrease after its introduction. This also applies to similar usage, which would indicate disuse. Specifically for this question, it was assumed that the survey participants were expressing their opinion on the potential use of Bitcoin-based stablecoins.

The adoption of Bitcoin grows when previous nonusers start demanding it. Therefore, an interesting evaluation is the combination of prior Bitcoin usage and the appraisal of a future stablecoin integration regarding its capabilities of enhancing the technology. According to the results of that statistic, 100% of the nonusers consider the stablecoin integration to be an improvement. For attendees that already used Bitcoin 87.5% would agree with that, while 12.5% would do not see this inclusion as a benefit. Table 2 illustrates the results:

Do you consider the integration of stablecoins to be an improvement for Bitcoin? * Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)? Crosstabulation

			Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?		
			Yes	No	Total
Do you consider the integration of stablecoins to be an improvement for Bitcoin?	Definitely	Count	11	4	15
		% within column	27,5%	23,5%	26,3%
	Probably	Count	24	13	37
		% within column	60,0%	76,5%	64,9%
	Probably not	Count	4	0	4
		% within column	10,0%	0,0%	7,0%
	Definitely not	Count	1	0	1
		% within column	2,5%	0,0%	1,8%
Total		Count	40	17	57
		% within column	100,0%	100,0%	100,0%

Table 2: *Usage of Bitcoin vs. improvement through stablecoin integration*

Despite that the findings above show a clear tendency, there is always a difference between noticing the benefits of something and considering its usage. To correct this obscurity, we further contrast the prior Bitcoin experience with the potential use of integrated stablecoins based on the opinion of the participants. The results show that 7 (41.2%) of the nonusers would endorse the use of stablecoins. Based on the total set of answers these respondents would represent 12.3%. Moreover, 42.5% of the individuals that are already conversant with Bitcoin could imagine increasing this usage behavior. In summary this results in 42.1% of the participants that agree to a higher use of the Bitcoin network once stablecoins are introduced. Though, it is necessary to mention that there is an unpredictable difference between

claimed behavior and actual behavior. The answers given in a survey that describe a theoretical scenario usually differ from real practice. This is typical for statistical research and also applies to the chosen methodology, as the use of an application that has not yet been launched cannot be tested. Hence, the results must be interpreted cautiously. The majority of 54.4% would not change their behavior regarding Bitcoin when stablecoins are included. Ultimately a minority of 3.5% would even reduce their usage or reject the innovation. Since more participants mentioned an increase in using Bitcoin, this can be construed as an expansion of adoption. Table 3 below shows the total results in a crosstabulation:

Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins? * Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)? Crosstabulation

			Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?		
			Yes	No	Total
Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?	Higher usage of the Bitcoin network and integrated stablecoins	Count	17	7	24
		% within column	42,5%	41,2%	42,1%
	Probably the same usage of the Bitcoin network and integrated stablecoins	Count	22	9	31
		% within column	55,0%	52,9%	54,4%
	Lower usage of the Bitcoin network and integrated stablecoins	Count	1	1	2
		% within column	2,5%	5,9%	3,5%
Total		Count	40	17	57
		% within column	100,0%	100,0%	100,0%

Table 3: *Prior Bitcoin usage vs. potential usage of integrated stablecoins*

Next, we apply this evaluation to the future use of bitcoin as a means of payment after a potential integration of stablecoins and compare it to the prior utilization of Bitcoin. The resulting crosstabulation shows similar findings to the previous ones. 5 (29.4%) of the current nonusers could imagine using bitcoin as a means of payment in the future. Based on the whole dataset this number adds up to 8.8%. In total there are 20 (35.1%) survey participants that would increase their use of bitcoin as a means of payment, of which 15 have had prior experience. The majority of 61.4% would neither increase nor reduce their behavior on the utilization of bitcoin as a means of payment. Lastly, 3.5% would consider reducing their use of bitcoin as a means of payment, if stablecoins were introduced. All results are illustrated consecutively in Table 4:

Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior? * Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)? Crosstabulation

			Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?		
			Yes	No	Total
Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior?	Higher usage of the Bitcoin network and bitcoin	Count	15	5	20
		% within column	37,5%	29,4%	35,1%
	Probably the same usage of the Bitcoin network and bitcoin	Count	24	11	35
		% within column	60,0%	64,7%	61,4%
	Lower usage of the Bitcoin network and bitcoin	Count	1	1	2
		% within column	2,5%	5,9%	3,5%
Total		Count	40	17	57
		% within column	100,0%	100,0%	100,0%

Table 4: *Prior Bitcoin usage vs. potential usage of bitcoin as a means of payment*

An extended and combined version of Table 3 and Table 4 can be found in Table 29. It serves as a comprehensive overview to determine the potential growth in adoption following the integration of stablecoins. Nonusers in particular are a useful group for this evaluation. Overall, survey respondents included 8 (14%) people who expect to increase their overall use of Bitcoin network. Previously, 40 respondents indicated that they had used Bitcoin before, representing a potential increase of 20%. As they have no experience with the technology, this number can be identified as potential novices to Bitcoin. Of these participants, 3 would use specifically integrated stablecoins, 1 would prefer bitcoin and 4 would use both solutions. In addition, 19 (33.3%) survey respondents who already have experience with Bitcoin would expand their use of the network. This includes 4 respondents who favor the use of integrated stablecoins, 2 who would expand their use of bitcoin and 13 who would increase their use of both technologies. As seen in the previous subsection, a majority of survey participants that do not intend to use bitcoin as a means of payment or the Bitcoin network at all substantiated this with the price volatility. In summary, 14 (24.6%) attendees stated this as a reason (Table 12, Table 13 and Table 14). Of these, 10 (17.5%) have not used the Bitcoin network before. Compared to the potential novices described before, that consider a higher usage after the integration of stablecoins, this figure is slightly bigger and demonstrates that there might be even more potential.

In the previous subsection we have differentiated the current adoption into a broader and a stricter interpretation. While the broader determined the holding of bitcoin as a state of adoption, the stricter interpretation only took into account the respondents that made payments with it. Since the questionnaire primarily focused on making payments, we compare the results with the figures representing this aspect. However, the holding of bitcoin also includes a certain level of Bitcoin utilization. For this reason, we will carefully assess this evaluation as an ideal scenario. The stricter interpretation of current individuals using bitcoin as a means of payments added up to 0.5% (pessimistic: 0.2%) globally and 2.2% (pessimistic: 1.5%) for Germany. The evaluation showed that there were 5 (8.8%) novices that

claimed using bitcoin as a means of payment after the integration of stablecoins. As a result, the adoption could grow up to 9.3% (pessimistic: 9%) globally and 11% (pessimistic: 10.3%) for Germany. According to the theory of Rogers, this could lead to progress for the adoption which would reach the early adopters. Regarding the broader interpretation, worldwide 2.8% (pessimistic: 1.3%) have used Bitcoin while in Germany the figures added up to 12.3% (pessimistic: 8.1%). The evaluation of the survey showed that 8 (14%) novices stated that they would begin utilizing Bitcoin. In summary this could lead to an adoption of 16.8% (pessimistic: 15.3%) globally and 26.3% (pessimistic: 22.1%) in Germany. For the broader and ideal scenario, the integration of stablecoins already holds interest for the early majority according to the theory of Rogers. Overall, this results in a range of 0.2% to 16.8% for the whole world and 1.5% to 26.3% for Germany. The evaluation of the survey can be applied to the statistics of the previous subsection describing the current adoption, since both apply to the same geographical group. The survey included German attendees (University of Applied Sciences Mittweida) as well as an international audience (Slack channels, LinkedIn). A detailed disaggregation for this was not conducted. Nevertheless, the figures of potential and actual adoption differ significantly. For transparency reasons, it is important to point out the causes that could be responsible for this discrepancy. Firstly, the research methodology that was used to identify the potential adoption addressed a target group of participants with a background in blockchain technology and Bitcoin, which did not apply to the studies that analyzed the current adoption. Secondly, once stablecoins are integrated into Bitcoin and survey participants are confronted with the challenge of whether they use the technology, their claimed behavior might differ from their actual behavior. Thirdly, we assumed that Bitcoin owners not only deposit Bitcoin as an investment, but also use it for some purpose.

In the previous subsection, we also analyzed statistics that are not directly affected by a possible stablecoin integration. For example, the market capitalization of Bitcoin is a metric that will not necessarily change because of this development. Furthermore, the introduction of stablecoins has no direct impact on the number of available ATMs. While it is possible that the stablecoin can be purchased at such a machine, there must be a clear advantage for the individual to use such a service despite the possibility of buying it online. Since identity verification is required (“know your customer”) and exchange fees apply, the stablecoin integration may not increase the number of ATMs. Similarly, the ability to make POS payments must have a competitive advantage over current payment methods. For example, merchants could offer such payments to attract new customers.

Finally, we revisit the five key attributes of Rogers that influence the rate of adoption of an innovation within a population and apply this to Bitcoin and the findings. As described above, a relative advantage must be identified that distinguishes the use of bitcoin as a means of payment. The technical possibility is proven by the existing availability in shops. One relative advantage could be lower transaction costs. According to 77.4% of merchants who accept crypto asset payments, fees are lower, while none of them claimed they are higher (PYMNTS & BitPay, 2022, p. 21). This is substantiated by the fact that the average processing fee for credit card payments is between 1.5 % and 3.5 % and the costs for online

transactions start at a minimum of 2.9 % (Leonard & Bottorff, 2023). In comparison, off-chain transactions via the Bitcoin Lightning Network only cost a few sats, which is the equivalent of a fraction to a few cents. A relative advantage for traditional payment methods is their usability, which might still be complex with crypto assets. Within the target group of the survey, 6 (10.5%) participants stated that they do not use Bitcoin because they do not understand it (Table 12 and Table 14). On a broader scale the complexity, however, is still a barrier for merchants to offer payments using crypto assets. Difficulties predominantly arise with the implementation of wallets (67.9%), technical skills of employees (44%) or private key handling (42.2%) (PYMNTS & BitPay, 2022, p. 23). This also applies to users who refuse to buy crypto assets due to a lack of knowledge (PYMNTS & BitPay, 2021, p. 16). On a technical level, blockchain-based transactions are eventually more complex than traditional payments. This could be mitigated through service providers offering payment processing or wallet applications with a simple usability. The current applications already support user-friendly features that hardly differ from other payment methods and ensure appropriate compatibility. This allows payments to be made by scanning a QR code or via NFC-enabled devices such as smartphones, which also applies to credit and debit cards. The usage of Bitcoin is permissionless, which enables low barriers to entry for users and a high degree of trialability. This does not apply to traditional finance, where processes are more elaborate. As seen in previous statistics, setting up a wallet and performing transactions might be more complex for beginners. Nevertheless, each user can test the functionalities themselves or, in rare instances, in various digital and physical stores mentioned above. Due to the transparency of Bitcoin, its observability can be considered as ideal. Though, details are limited, and it cannot directly be identified if a transaction is a purchase at a store or a simple exchange between two individuals and who participated since accounts are pseudonymous. The results of a transfer are visible to anyone, which does not apply to traditional finance. As the technology still has low public awareness, this attribute must further develop.

According to Rogers' innovation decision process, new technologies always lead to some level of adoption. Some individuals entering the Bitcoin adoption process may conclude that they reject Bitcoin. We have analyzed various reasons for this decision in this chapter. In contrast, some survey participants decide to adopt Bitcoin in the future once stablecoins are introduced. This was evaluated based on different statistics. Ultimately, the development of the recent years and the research results show that Bitcoin is gaining adoption, which also leads to more communication channels and discussions. Whether the integration of stablecoins actually improves the adoption of Bitcoin will become clear when this application is launched. The next chapter examines how such an implementation could be designed.

6 Implementation Approaches

At the time of writing, Lightning Labs has already released the alpha version of tapd for the main network, which supports the on-chain issuance and functionality of Taproot Assets. However, the implementation into the Lightning Network as well as concrete concepts of stablecoins are still awaited and remain purely theoretical models. Rapid prototyping tools such as "Polar" allow users to get an impression of what the combination of these technologies could look like (Gentry, 2023). In this chapter, we will therefore attempt to illustrate possible implementation approaches for Taproot Asset stablecoins and their integration into the Lightning Network.

6.1 Stablecoin Design

In section 3.1 we have discussed different stablecoin classes which we will refer to in this section. Nevertheless, it is also necessary to consider the historical performance data. Uncollateralized stablecoins are very difficult in their configuration, as their stability primarily depends on the algorithm adjusting the supply. If this mechanism is based on a reasonable framework, stability could be achieved. Due to earlier de-pegs, which also led to several collapses, they are not a proper representation of stability. As previously shown, this is also reflected in the number of users holding uncollateralized stablecoins. Therefore, we will not consider uncollateralized stablecoins in this section when conceptualizing designs. Instead, a hypothetical scenario is created in which Taproot US dollar (TUSD) is a stablecoin that aims to achieve a 1:1 peg to that same fiat currency by utilizing collateralized approaches as a stability mechanism. The proposals presented in this section do not claim to be complete and are merely suggestions for the implementation.

6.1.1 Off-chain collateralized Approach

Beginning with the most prominent stablecoin class applying off-chain collateralization, at first a custodian such as Tether and Circle that issues TUSD is required. The custodian therefore must operate a full node that runs tapd to interact with the protocol. Since Taproot Assets are light-client friendly, users do not need to operate a full node themselves. The minting of TUSD is initiated through tapd whereas the creation happens through an on-chain transaction. Thereby it is important that a *group_key* is assigned to TUSD. This option establishes an asset group so that the supply can be expanded in the future within that group (Tsagkarelis, 2023). Consequently, users must buy TUSD directly from the custodian, that executes a new on-chain Taproot transaction. It includes the asset in its MAST and the held amount of TUSD per account in its MS-SMT. Compared to Tether, this could be performed without the need of complex smart contracts, as the incoming payment of users

triggers the on-chain transaction. Furthermore, since multiple asset assignments can happen within one transaction, this process is efficient, and batches of issuances can be executed similar to an emission. Contrary to minting, the object *asset_group* provides the functionality to burn specific assets, which enables the reduction of the supply (Harvey-Buschel, 2023). In this process users send their crypto assets to the address of the custodian, that destroys the TUSD. Due to the promised 1:1 exchange rate the user account is rewarded with the corresponding amount of US dollar. Ultimately, only transactions signed by the custodian can increase or decrease the supply. Users can transfer TUSD to other addresses within the scope of their holdings. Such transactions cannot change the amount of assets in circulation to prevent inflationary traits. The management of the collateral devolves on the custodian, that has to choose the underlying assets for TUSD with a high liquidity ratio and that are stable in value. Regular third-party audits and transparent reports ensure the collateralization of TUSD and thus the trust of users in the stablecoin project. Universes enable proof of reserves so that users can obtain protocol-based data for TUSD and compare it with the information provided by the custodian (Harvey-Buschel, 2023). The issuer can create a proof file for a specific Taproot Asset, the provenance of which users can verify to confirm its authenticity (Gugger, 2023). Moreover, secondary markets could emerge through the listing of TUSD on peer-to-peer exchanges, where arbitrageurs utilize price discrepancies to stabilize the rate (Bitcoin.org, 2024).

Since the business model of off-chain collateralized stablecoins is primarily managed without the necessity of the blockchain network, TUSD could be implemented using this mechanism. However, there are still challenges regarding its design. Firstly, the initial purpose of Bitcoin was to create a payment system that does not rely on centralized entities. However, off-chain collateralized stablecoins require a custodian to manage the reserve assets. Risks can be minimized by demanding regular and transparent information that is publicly available. Nevertheless, the integrity of the intermediary and the business model is still not guaranteed, as the reports could be falsified. Ultimately, this has no impact on Bitcoin itself, but contradicts its idea. Users that want to utilize TUSD therefore sacrifice the decentralization that the underlying network provides. Furthermore, especially in difficult situations, off-chain collateralized stablecoins decouple from their intended peg. Large projects such as USDT and USDC might regain the trust of users, but smaller and new projects could collapse in such scenarios. One solution could be the approach of Stablesats, which has already been described. If TUSD is traded on secondary markets, exchanges could also offer perpetual inverse swaps. Such derivatives already exist for Tether’s stablecoin USDT (Poloniex, n.d.). TUSD could be additionally hedged in this manner by the custodian investing in such products. This could further strengthen user trust in TUSD due to a better security mechanism, as each unit is collateralized not only by the reserve but also by the derivative. Should the stablecoin decouple from its peg, users would still be eligible to redeem their crypto asset for the promised 1:1 exchange rate. The drop of TUSD leads to an increase of the derivative. If the reserves somehow fail and TUSD is under-collateralized, the short position could be used to make up for losses. If the reserve holds, the custodian could cover own losses by selling perpetual inverse swaps. This of course leads to more complexity, higher costs and

the risks associated with the Stablesats approach. In this case, however, the inclusion of another custodian could reduce the overall counterparty risk, as both of them would have to default for TUSD to collapse.

6.1.2 On-chain collateralized Approach

The more complex implementation approach of a native stablecoin on Bitcoin is through on-chain collateralization. This is because there is almost no component that solely operates without the dependence on the blockchain network. The management of the collateral, the supply as well as governance processes all occur on-chain. While current implementations exist on more interoperable networks like Ethereum, this could be a challenge for Bitcoin. Compared to that, the Bitcoin script language is limited regarding its functionality due to a missing “Turing completeness”. This means it is not possible to do difficult operations such as loops and rather supposed to execute simple stack-based processes. Complex structures like smart contracts are also not supported. In this way Bitcoin maintains a robust security and still can perform different types of transactions up to more extensive applications like the Lightning Network. (Antonopoulos, 2021f)

However, we can still design a theoretical approach that could implement an on-chain collateralized stablecoin. Bitcoin transactions fundamentally consist of a locking script that defines specific spending conditions, and an unlocking script that fulfills these conditions to do the transfer (Antonopoulos, 2021g). This concept is similar to the conventional technique of on-chain collateralized stablecoins, where the reserve assets are locked in a vault and only unlocked if the borrower returns the lent amount and if applicable an additional fee. If a user deposits bitcoin into the vault, this represents the locking script, whereas the return of the borrowed TUSD is a condition of the unlocking script, which triggers the redemption of the deposited bitcoin. Once again, the variables *group_key* and *asset_group* are required to manage the fluctuating supply of TUSD. Trading could also take place on secondary peer-to-peer markets. Furthermore, other assets can also be deposited, which are implemented through the Taproot Assets protocol. Hence, asset-referenced token or electronic money token which are digital representations of traditional assets or currencies could also be applied in the future (European Union, 2023, p. 44). As a result, more stable assets could cover the collateral of TUSD and eliminate the necessity of over-collateralization.

Since an on-chain stablecoin design does not include a centralized entity, governance processes must be administered by the community. As with DAI, a governance token that allows holders to vote could be implemented using the Taproot Assets protocol. The more difficult task is to delegate voting periods on the blockchain without relying on smart contracts. In the past, soft forks were implemented after a certain hash rate controlled by the miners indicated support or rejection of a potential update. This is done by signaling, whereby the miners vote by adding the old or new version number to their produced blocks (Bit2Me, 2020). Signaling could be a method for token holders to express their stance. To inform the public of their decision, an on-chain transaction could be carried out. However,

this would temporarily burden the blockchain and high transaction costs would arise during election periods. Ultimately, token holders could be prevented from voting. Elections could also take place off-chain on a separate website or application where token holders verify their eligibility for the election period. The results could be published in an on-chain transaction within a Merkle tree allowing each voter to verify the integrity of their personal vote. Yet decentralization could be weakened due to centralized structures. Ultimately, it is more difficult to design a proposal for on-chain collateralized stablecoins.

6.2 Lightning Network Integration

Unlike the stablecoin design, the integration of Taproot Assets into the Lightning Network was already intended when the project was announced. Due to fast processing and low fees, this was an obvious decision. Bitcoin remains the backbone for both technologies, while Taproot Assets utilize the Lightning Network infrastructure. At the time of writing, the on-chain functionalities of the main network of the Taproot Assets protocol are already integrated, while the use of the Lightning Network is still outstanding (Gentry, 2023). In the future, Taproot Assets – and thus also stablecoins – will be used to create payment channels, as is already possible with bitcoin. As a result, stablecoins can be transferred and routed via the Lightning Network, while bitcoin serves as a universal platform asset to pay routing fees, similar to Ether when paying for gas fees. Nevertheless, conventional off-chain bitcoin transactions are still possible. Transferring Taproot Assets on the Lightning Network can be done via a homogeneous route. However, this requires all nodes to hold the corresponding asset. To increase interoperability, heterogeneous routes can be established in which the participating nodes do not need to hold the transferred asset in order to function as routing nodes. This process requires specific "edge nodes" that are directly connected to the sender or recipient of the transaction and exchange bitcoin for the asset. Nodes in between simply route bitcoin. In fact, payments can include different assets, as Figure 8 shows. Eric could create an invoice in which he requests a certain amount of Taproot EUR (TEUR) from Alice and presents it to her. Despite of that, Alice can still initiate the payment to Eric with her TUSD balance at a predefined exchange rate. Bob and Dave, who act as edge nodes in this setup, specify their exchange rate and convert the asset into bitcoin and vice-versa. Carol acts as an ordinary routing node on the Lightning Network and has no interaction with Taproot Assets. (Lightning Labs, 2023e)

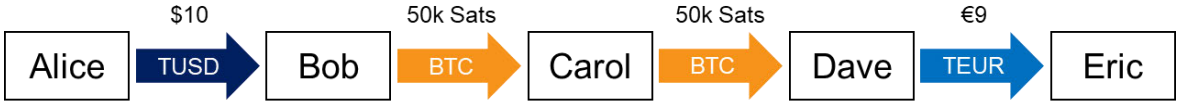


Figure 8: *Routing of multiple Taproot Asset stablecoins (Lightning Labs, 2023e)*

The exchange of bitcoin and the Taproot Asset stablecoin is enabled through atomic swaps (Lightning Labs, 2023c). These are methods that are already used in the Lightning Network in the form of hash time-locked contracts. The exchanging transactions are blocked until

either the preimage of a given hash value is provided or until a certain time has elapsed (Cointelegraph, 2023). The first option executes the exchange of bitcoin and the asset, while the second either does nothing or reverts everything. In the example, Bob exchanges the TUSD received from Alice for bitcoin, which he forwards to Carol. Since Carol functions as a standard routing node, she sends the bitcoin to the next hop, which is operated by Dave, who in turn converts bitcoin into TEUR and transfers it to Eric. Each edge node can set its own exchange rate or use the reference rates of the public exchanges. This also creates competition between the edge nodes, as the sender can select the least expensive route. Overall, routing is still dependent on the amount of value held in each payment channel. However, since the nodes can now hold multiple assets, this restriction is more flexible and not only the assets held in bitcoin are included in the capacity. (Lightning Labs, 2023e)

Nevertheless, to function properly and establish routes, funds must be held available in payment channels. This leads to liquidity issues as the respective amount must be deposited in multiple channels and the funds cannot be used for other purposes. Since the Lightning Network enables cost-efficient transactions, node operators do not earn much from routing fees. Edge nodes could therefore become relevant in the future as they create a business model that makes it profitable to hold funds available. As of February 18, 2024, Lightning nodes hold an average capacity of 0.325 bitcoin (approx. $16,800). Although the distribution is relatively concentrated, the 50th percentile of nodes holds 0.05 bitcoin (approx. $260), while the 75th percentile manages 0.035 bitcoin (approx. $1,800). The average channel capacity provides further information about the management of off-chain funds. Payment channels currently maintain a capacity of 0.083 bitcoin (approx. $4,300). The 50th percentile of payment channels holds 0.02 bitcoin (approx. $1,000) and the 75th percentile includes 0.055 bitcoin (approx. $2,800). These figures show that even larger payments could be processed via the Lightning Network. Eventually, the distribution leads to a more centralized structure, as nodes with higher capacities tend to aggregate larger values and maintain more payment channels, while smaller nodes become obsolete. This impairs the decentralized approach of Bitcoin. (1ML, 2024)

The Lightning Network still needs to be further evaluated and developed. An October 2023 research report by River – a Bitcoin financial services provider – states that the volume of routed transactions via the Lightning Network has increased by 1,212% in two years. Most of the transfers concern values of less than 1,000 sats (approx. $0.48) which are classified as micropayments. Larger payments are used less frequently, which especially applies to daily purchases. However, this could also be due to the use of bitcoin and could change with the integration of stablecoins. On River's Lightning nodes, a transaction success rate of over 98% on average was recorded. The predominant reasons for transactions failing are the absence of a proper route or a timeout when searching for a route. Insufficient funds and incorrect payment details are rarely represented. A second payment attempt could at least reduce the possibility of a timeout if a route can be found. Ultimately, it is necessary to mention that due to the volatility of bitcoin, the exchange values expressed in this section will vary in the future and should not be taken for granted. (River, October 2023)

7 Conclusion

The research of this thesis dealt with the idea of Taproot Assets and their potential influence on the Bitcoin network adoption. Theoretical concepts of the prerequisites of this technology were explained comprehensively to establish a profound knowledge base. Although different types of assets could be created, the research focused on the crypto asset class of stablecoins, which were examined in detail. Since the Taproot Assets protocol is still under development, a survey was conducted to gain insights into the potential utilization of the attendees. The questionnaire concentrated on the prior and current use of the Bitcoin network as well as bitcoin as a means of payment and reasons for not doing so. As stablecoins introduce a crypto asset with low volatility, the issues with price fluctuations were addressed. Ultimately the potential adoption of Bitcoin was analyzed in a hypothetical scenario where Taproot Asset stablecoins already exist. It the following section we will once again revisit the most important results identified in this thesis. Subsequently, we draw an outlook and determine research fields that could benefit from the findings of this paper and must be analyzed to fully grasp the subject.

7.1 Summary of Research Findings

In the analysis of the current state of the adoption of Bitcoin and other crypto assets, the results showed an increase over the previous years. This evaluation comprised the holders of crypto assets but also the usage for example as a means of payment. Furthermore, statistic indicates that this development will continue in the future since younger generations rather sympathize with these technologies. However, based on global and country-specific population data the adoption rate is still low. More detailed investigations regarding the refusal of Bitcoin depicted that the price volatility is the most prominent reason. The implementation of Taproot Asset stablecoins could rectify such challenges.

Overall, a majority considers the integration of stablecoins as an improvement for Bitcoin. The prospective adoption was determined by evaluating the change of (potential) users' behavior in a scenario where Taproot Asset stablecoins have been implemented into Bitcoin. Although, most survey participants would continue with the same usage behavior regarding integrated stablecoins or bitcoin, there were a lot more attendees that would increase their use than those who would reduce it. For integrated stablecoins this number was even higher than for bitcoin. In particular the group of nonusers are essential for the measurement of the adoption rate. Based on the survey results, there were more nonusers that would start utilizing Bitcoin than those who would reject it. The analysis of the current state of the adoption of Bitcoin allowed to make a distinction between different aspects. On the one hand data merely analyzed the bitcoin holders while other considered the real use

of it. On the other hand, global as well as German results were examined. Since the results of different statistics differed, a more pessimistic scenario was illustrated next to a more optimistic one. These aspects were incorporated and served as a basis for the analysis of the future transformation. In result various figures were determined, that express a growth of the adoption rates once Taproot Asset stablecoins are integrated into Bitcoin. Since the research primarily included survey participants that have a background in blockchain technology and Bitcoin, the results can only be applied to this target group.

The actual consequences will be documented after the launch of native stablecoins on Bitcoin. Within the thesis, the potential was demonstrated as well as the benefits of such a technology. Traditional payment systems exist and work perfectly fine but collect fees from merchants that are hidden for the ultimate consumer due to cost allocation. The combination of Taproot Asset stablecoins and the Bitcoin Lightning Network could be a solution to that problem. These technologies combine a stable crypto asset with fast and cost-efficient transactions. However, these methods are still under development and must first establish themselves. The Lightning Network must be tested comprehensively and rolled out for larger payments as previously shown. In order to keep the original intention of Bitcoin, the solution should keep the third-party dependence to a minimum.

7.2 Outlook and Areas for further Research

On October 18, 2023, the launch of the main network of the Taproot Assets protocol was announced. With this, the support of on-chain functionalities and the issuance of assets are possible. According to the latest posting from Lightning Labs, almost 2,000 assets have been minted on the test network (Gentry, 2023). Statistics about the main network, which will be published in the future, will show how it has been accessed. The next step is the implementation of a connection to the Lightning Network, which Lightning Labs is currently working on. As described in chapter 6, the theoretical design for this integration already exists. So far, there are no concepts for the development of stablecoins using Taproot Assets. This must be further evaluated in feasibility studies and elaborated on what is important for potential users. In particular, the choice of collateralization and the exact design of this approach must be determined. Multiple solutions already exist and have been presented in this thesis. However, these do not represent an effective stabilization mechanism. Furthermore, problems arise due to centralization or difficulties in the conception. Ultimately, a tradeoff must be reached that guarantees stability while satisfying user requirements.

In order to determine the actual adoption of blockchain technology, crypto assets and Bitcoin, it is necessary to continue with the research and analyze the usage of the different applications. Based on the results of the survey, this research should be extended to a larger target group, including more unaware participants and their perception of such an approach. Once stablecoins are introduced to Bitcoin, field investigations must be conducted that go beyond quantitative research. These results are more reliable due to their

practical approach. Based on this analysis, it is possible to identify whether users would actually be willing to pay with crypto assets, as stated in the survey. Another interesting analysis is the actual comparison of such an application with existing payment services regarding their usability and whether people would prefer such a solution. This investigation must also include people who are not yet familiar with blockchain technology. Although blockchain technology is still under development, the improvement of applications will continue. Furthermore, users do not need to completely understand the technology behind it. Similar to the internet or current payment systems, which can be used without being aware of underlying processes. The usability could therefore evolve to current financial applications and eventually reach a level where they hardly differ from each other. At this point, people take other advantages into consideration, such as the cost benefit, disintermediation, or an easy onboarding process.

8 Bibliography

1ML. (2024, February 18). *Real-Time Lightning Network Statistics*. Retrieved February 18, 2024, from https://1ml.com/statistics

Adachi, M., Born, A., & et al. (2021, November 17). *The expanding functions and uses of stablecoins*. Retrieved December 16, 2023, from https://www.ecb.europa.eu/pub/financial-stability/fsr/focus/2021/html/ecb.fsrbox202111_04~45293c08fc.en.html#:~:text=In%20addition%20to%20acting%20as,trading%20platforms%20involved%20a%20stablecoin.

Andresen, G. (2021, December 12). *BIP 16: Pay to Script Hash*. Retrieved October 23, 2023, from https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki

Antonopoulos, A. M. (2021a, October 25). *What Is Bitcoin?* Retrieved August 23, 2023, from https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch01.asciidoc#what-is-bitcoin

Antonopoulos, A. M. (2021b, October 25). *The Bitcoin Network*. Retrieved August 23, 2023, from https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch08.asciidoc#the-bitcoin-network

Antonopoulos, A. M. (2021c, October 25). *Bitcoin Transactions*. Retrieved August 23, 2023, from https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch02.asciidoc#bitcoin-transactions

Antonopoulos, A. M. (2021d, October 25). *Keys, Addresses*. Retrieved September 15, 2023, from https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch04.asciidoc#keys-addresses

Antonopoulos, A. M. (2021e, October 25). *Merkle Trees*. Retrieved October 23, 2023, from https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch09.asciidoc#merkle-trees

Antonopoulos, A. M. (2021f, October 25). *Transaction Scripts and Script Language*. Retrieved January 10, 2024, from https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06.asciidoc#transaction-scripts-and-script-language

Antonopoulos, A. M. (2021g, October 25). *Script Construction (Lock + Unlock)*. Retrieved January 17, 2024, from https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06.asciidoc#script-construction-lock--unlock

Antonopoulos, A. M., Osuntokun, O., & et al. (2021a, November 19). *Introduction to Onion Routing of HTLCs*. Retrieved August 24, 2023, from https://github.com/lnbook/lnbook/blob/develop/10_onion_routing.asciidoc#introduction-to-onion-routing-of-htlcs

Antonopoulos, A. M., Osuntokun, O., & et al. (2021b, November 19). *Lightning Node Software*. Retrieved August 28, 2023, from https://github.com/lnbook/lnbook/blob/develop/04_node_client.asciidoc#lightning-node-software

Arkadiko Finance. (2023a, February 28). *Liquidations*. Retrieved December 18, 2023, from https://docs.arkadiko.finance/protocol/auctions

Arkadiko Finance. (2023b, February 28). *Introduction*. Retrieved December 18, 2023, from https://docs.arkadiko.finance/

BabelFish. (2023, November 28). *What is BabelFish*. Retrieved December 23, 2023, from https://babelfish.gitbook.io/the-babelfish-gitbook/getting-started/what-is-babelfish

Baughman, G., Carapella, F., & et al. (2022, December 16). *The stable in stablecoins*. Retrieved November 27, 2023, from https://www.federalreserve.gov/econres/notes/feds-notes/the-stable-in-stablecoins-20221216.html

Bit2Me. (2020, May 15). *What is a MASF?* Retrieved February 5, 2024, from https://academy.bit2me.com/en/what-is-a-masf/

Bitcoin Optech. (2019, September). *Optech Schnorr/Taproot Workshop*. Retrieved October 2, 2023, from https://bitcoinops.org/img/posts/taproot-workshop/taproot-workshop.pdf

Bitcoin Optech. (2021, November 17). *Bitcoin Optech Newsletter #175*. Retrieved September 4, 2023, from https://bitcoinops.org/en/newsletters/2021/11/17/

Bitcoin Project. (n.d.). *Block Chain*. Retrieved February 16, 2024, from https://developer.bitcoin.org/devguide/block_chain.html#block-chain

Bitcoin.org. (2024, January 3). *Bitcoin Exchanges*. Retrieved January 3, 2024, from https://bitcoin.org/en/exchanges#p2p

Blink. (2023a, December 31). *Security*. Retrieved December 31, 2023, from https://www.blink.sv/en/security

Blink. (2023b, August 15). *Stablesats*. Retrieved December 31, 2023, from https://faq.blink.sv/stablesats

Blockscout. (2024a, February 18). *XUSD Contract details*. Retrieved February 18, 2024, from https://rootstock.blockscout.com/address/0x1440d19436bEEaf8517896bffB957A88ec95a00F

Blockscout. (2024b, February 18). *BRZ Contract details*. Retrieved February 18, 2024, from https://rootstock.blockscout.com/address/0xE355C280131dfaf18Bf1C3648aEE3c396Db6B5Fd

Blockstream. (2023a, October). *Technical Overview*. Retrieved December 25, 2023, from https://docs.liquid.net/docs/technical-overview

Blockstream. (2023b, December 25). *The Liquid Network*. Retrieved December 25, 2023, from https://liquid.net/

Blockstream. (2023c, December 25). *Blockstream Explorer*. Retrieved December 25, 2023, from https://blockstream.info/liquid/

Blockstream. (n.d.). *What is a Liquid Network functionary?* Retrieved December 25, 2023, from https://help.blockstream.com/hc/en-us/articles/900003264706-What-is-a-Liquid-Network-functionary-

Briola, A., Vidal-Tomás, D., & et al. (2023, January). Anatomy of a Stablecoin's failure: The Terra-Luna case. *Finance Research Letters, Volume 51*. Retrieved December 11, 2023, from https://www.sciencedirect.com/science/article/abs/pii/S1544612322005359

Browne, R. (2022, May 12). *The world's biggest stablecoin has dropped below its $1 peg*. Retrieved December 11, 2023, from https://www.cnbc.com/2022/05/12/tether-usdt-stablecoin-drops-below-1-peg.html

BRZ. (n.d.). *BRZ Token Whitepaper*. Retrieved December 23, 2023, from https://www.brztoken.io/files/white_paper_BRZ_2023.pdf

BTC Map. (2024, February 18). *Dashboard*. Retrieved February 18, 2024, from https://btcmap.org/dashboard

Burtey, N. (2023, February 5). *Dealer*. Retrieved December 31, 2023, from https://github.com/GaloyMoney/dealer

Buterin, V. (2017, December 31). *Sharding FAQ*. Retrieved August 25, 2023, from https://vitalik.ca/general/2017/12/31/sharding_faq.html

Buterin, V. (2021, April 7). *Why sharding is great: demystifying the technical properties*. Retrieved August 25, 2023, from https://vitalik.ca/general/2021/04/07/sharding.html

Buy Bitcoin Worldwide. (2023). *How Many People Own & Use Bitcoin?* Retrieved January 24, 2024, from https://buybitcoinworldwide.com/how-many-bitcoin-users/

Carjuzaa, M., Bokser, A., & et al. (2019, September 19). *Money On Chain Stablecoin Protocol Collateralized with Bitcoin*. Retrieved December 23, 2023, from https://drive.google.com/file/d/10HIs1T4pD5MFSGjr-pnPrPD29DpFYKZN/view

Coin ATM Radar. (2024a, February 18). *Bitcoin ATM Installations Growth*. Retrieved February 18, 2024, from https://coinatmradar.com/charts/growth/

Coin ATM Radar. (2024b, February 18). *Bitcoin ATM Installations Growth (United States)*. Retrieved February 18, 2024, from https://coinatmradar.com/charts/growth/united-states/

Coin ATM Radar. (2024c, February 18). *Speed of Crypto ATM Installations*. Retrieved February 18, 2024, from https://coinatmradar.com/charts/gauge/

Coin ATM Radar. (2024d, February 18). *Crypto ATM Supported Cryptocurrencies*. Retrieved February 18, 2024, from https://coinatmradar.com/charts/cryptocurrency-share/

CoinGecko. (2023a, December 18). *Arkadiko USDA*. Retrieved December 18, 2023, from https://www.coingecko.com/en/coins/arkadiko-usda

CoinGecko. (2023b, December 23). *XUSD (BabelFish)*. Retrieved December 23, 2023, from https://www.coingecko.com/en/coins/xusd-babelfish

CoinGecko. (2023c, December 23). *Brazilian Digital*. Retrieved December 23, 2023, from https://www.coingecko.com/en/coins/brazilian-digital-token

CoinGecko. (2024, January 24). *Global Cryptocurrency Market Cap Charts*. Retrieved January 24, 2024, from https://www.coingecko.com/en/global-charts

CoinMarketCap. (2023a, December 21). *Ampleforth*. Retrieved December 21, 2023, from https://coinmarketcap.com/currencies/ampleforth/

CoinMarketCap. (2023b, December 21). *TerraClassicUSD*. Retrieved December 21, 2023, from https://coinmarketcap.com/currencies/terrausd/

CoinMarketCap. (2023c, December 23). *Dollar on Chain*. Retrieved December 23, 2023, from https://coinmarketcap.com/currencies/dollar-on-chain/

Coinpages. (2024, February 18). *In Deutschland mit Bitcoin bezahlen – wo geht das?* Retrieved February 18, 2024, from https://coinpages.io/location/deutschland/

Cointelegraph. (2023, June 29). *What is an atomic swap, and how does it work?* Retrieved February 8, 2024, from https://cointelegraph.com/explained/what-is-an-atomic-swap-and-how-does-it-work

Crypto.com. (2023, January 19). *Global Cryptocurrency Owners Grow to 425 million through 2022*. Retrieved January 24, 2024, from https://crypto.com/company-news/global-cryptocurrency-owners-grow-to-425-million-through-2022

Cunningham, W. A., Preacher, K. J., & et al. (2001, March). *Implicit attitude measures: consistency, stability, and convergent validity*. Retrieved January 13, 2024, from https://journals.sagepub.com/doi/10.1111/1467-9280.00328

DefiLlama. (2024, February 17). *Stablecoins Market Cap*. Retrieved February 17, 2024, from https://defillama.com/stablecoins

Etherscan. (2024a, February 17). *Maker Token Holders*. Retrieved February 17, 2024, from https://etherscan.io/token/tokenholderchart/0x9f8f72aa9304c8b593d555f12ef6589cc3a579a2?range=10

Etherscan. (2024b, February 18). *Contract BRZ*. Retrieved February 18, 2024, from https://etherscan.io/address/0x01d33fd36ec67c6ada32cf36b31e88ee190b1839

European Union. (2023). *REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Retrieved January 17, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114

Federal Office of Justice . (2024, February 14). *German Banking Act (Kreditwesengesetz - KWG)*. Retrieved from https://www.gesetze-im-internet.de/kredwg/__1.html

FIS. (2023). *The Global Payments Report 2023.* Retrieved from https://www.fisglobal.com/-/media/fisglobal/files/campaigns/global-payments%20report/FIS_TheGlobalPaymentsReport_2023.pdf

Frax Finance. (2023, September 7). *AMO Overview*. Retrieved December 11, 2023, from https://docs.frax.finance/amo/overview

Galoy. (2023, December 31). *Stablesats*. Retrieved December 31, 2023, from https://stablesats.com/

Ge Huang, V., Miao, H., & et al. (2023, March 11). *Circle's USDC Stablecoin Breaks Peg With $3.3 Billion Stuck at Silicon Valley Bank*. Retrieved December 11, 2023, from https://www.wsj.com/articles/crypto-investors-cash-out-2-billion-in-usd-coin-after-bank-collapse-1338a80f

Gensler, G. (2024, January 10). *Statement on the Approval of Spot Bitcoin Exchange-Traded Products*. Retrieved January 28, 2024, from https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023

Gentry, R. (2023, October 18). *Taproot Assets on Mainnet: A New Era for Bitcoin and Beyond*. Retrieved October 30, 2023, from https://lightning.engineering/posts/2023-10-18-taproot-assets-v0.3/

Glassnode Services AG. (2024, January 17). *Tether: Number of Transfers*. Retrieved February 18, 2024, from https://studio.glassnode.com/metrics?a=USDT&category=Network%20Stats&m=transactions.TransfersCount&s=1700611200&u=1700693999&zoom=

Gondo, H. (2023, June 9). *Understanding Taproot Assets Protocol*. Retrieved Ocotber 30, 2023, from https://medium.com/nayuta-en/understanding-taproot-assets-protocol-e2dfe3fc1e07

Gugger, O. (2023, December 12). *Universe.proto*. Retrieved January 5, 2024, from https://github.com/lightninglabs/taproot-assets/blob/f8843faab242da4b9b47fa99f154fe282ecf9001/taprpc/universerpc/universe.proto

Harvey-Buschel, J. (2023, November 28). *Taprootassets.proto*. Retrieved January 3, 2024, from https://github.com/lightninglabs/taproot-assets/blob/76bb5ae01fc0aa147233f332c468943f8c47b053/taprpc/taprootassets.proto

IRS. (2023, September 29). *Digital Assets*. Retrieved February 14, 2024, from https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets

Laerd Statistics. (n.d.). *Kendall's Tau-b using SPSS Statistics*. Retrieved January 15, 2024, from https://statistics.laerd.com/spss-tutorials/kendalls-tau-b-using-spss-statistics.php#:~:text=Kendall's%20tau%2Db%20(%CF%84b,at%20least%20an%20ordinal%20scale.

Lang, H., Wilson, T., & et al. (2023, February 14). *Binance stablecoin backer says U.S. SEC has labeled token an unregistered security*. Retrieved December 11, 2023, from https://www.reuters.com/technology/binance-stablecoin-backer-ordered-stop-issuing-token-binance-ceo-2023-02-13/

Leonard, K., & Bottorff, C. (2023, December 1). *Credit Card Processing Fees (2024 Guide)*. Retrieved December 2, 2024, from https://www.forbes.com/advisor/business/credit-card-processing-fees/

Lerner, S. (2019, January 29). *Rootstock Whitepaper*. Retrieved December 18, 2023, from https://rootstock.io/static/a79b27d4889409602174df4710102056/RS-whitepaper.pdf

Lightning Labs. (2023a, August 17). *The Taproot Assets Stack*. Retrieved August 23, 2023, from https://github.com/lightninglabs/taproot-assets#the-taproot-assets-stack

Lightning Labs. (2023b, August 17). *Initialization*. Retrieved August 23, 2023, from https://github.com/lightninglabs/taproot-assets#initialization

Lightning Labs. (2023c, May 16). *Taproot Assets*. Retrieved August 28, 2023, from https://docs.lightning.engineering/the-lightning-network/taproot-assets

Lightning Labs. (2023d, August 17). *Taproot Assets Protocol*. Retrieved November 1, 2023, from https://docs.lightning.engineering/the-lightning-network/taproot-assets/taproot-assets-protocol

Lightning Labs. (2023e, June). *Taproot Assets on Lightning*. Retrieved February 6, 2024, from https://docs.lightning.engineering/the-lightning-network/taproot-assets/taproot-assets-on-lightning

Mai, H. (2022, June). *Stablecoins - DeFi, Libra and beyond*. Retrieved November 27, 2023, from https://www.suerf.org/suerf-policy-brief/48391/stablecoins-defi-libra-and-beyond

MakerDAO. (n.d.). *The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System*. Retrieved December 8, 2023, from https://makerdao.com/en/whitepaper

Mempool.space. (2023, December 25). *Bitcoin Mempool*. Retrieved December 25, 2023, from https://mempool.space/

Merkle, R. C. (1980, April 16). *Protocols for public Key Cryptosystems*. Retrieved October 23, 2023, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6233691

Mow, S. (2019, July 29). *Tether Lands on the Liquid Network*. Retrieved December 25, 2023, from https://blog.blockstream.com/en-tether-lands-on-the-liquid-network/

Mow, S. (2020, April 2). *Bull Bitcoin Launches L-CAD on the Liquid Network*. Retrieved December 25, 2023, from https://blog.liquid.net/bull-bitcoin-launches-l-cad-on-the-liquid-network/

Nakamoto, S. (2008, October 31). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved August 23, 2023, from https://bitcoin.org/bitcoin.pdf

Neyman, J. (1976). The emergence of mathematical statistics. In *On the history of statistics and probability.* Berkeley, California: M. Dekker. Retrieved from https://openlibrary.org/works/OL18334563W/On_the_history_of_statistics_and_probability?edition=key%3A/books/OL5206547M

Nicolle, E., & Pan, D. (2022, November 10). *Tether Dips Below $1 as FTX Fallout Continues to Roil Markets*. Retrieved December 11, 2023, from https://www.bnnbloomberg.ca/tether-dips-below-1-as-ftx-fallout-continues-to-roil-markets-1.1844519

Ordiscan. (2024, February 12). *Inscription #8,727,192*. Retrieved February 12, 2024, from https://ordiscan.com/inscription/8727192

Osuntokun, O. (2022, Juni 22). *A Taproot-Native Asset Overlay - Bitcoin Miami 22*. Retrieved October 25, 2023, from https://docs.google.com/presentation/d/1YgMG4MOjs5dHhlf77Zh0WOENXqB0JTV8ZarVjS8slyk/edit#slide=id.g121572c76e7_4_124

Osuntokun, O. (2023a, October 17). *TAP: Taproot Assets Protocol*. Retrieved November 6, 2023, from https://github.com/Roasbeef/bips/blob/bip-tap/bip-tap.mediawiki

Osuntokun, O. (2023b, Ocotber 17). *Merkle Sum Sparse Merkle Trees*. Retrieved November 2, 2023, from https://github.com/Roasbeef/bips/blob/bip-tap/bip-tap-ms-smt.mediawiki

Osuntokun, O. (2023c, October 17). *Taproot Asset On Chain Addresses*. Retrieved November 6, 2023, from https://github.com/Roasbeef/bips/blob/bip-tap/bip-tap-addr.mediawiki

Poloniex. (n.d.). *What is USDT Collateralized Perpetual contract?* Retrieved January 7, 2024, from https://support.poloniex.com/hc/en-us/articles/360051798754-What-is-USDT-Collateralized-Perpetual-contract-

Poon, J., & Dryja, T. (2016, January 14). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Retrieved August 25, 2023, from https://lightning.network/lightning-network-paper.pdf

Porst, R. (2000). *Question Wording – Zur Formulierung von Fragebogen-Fragen*. Retrieved January 11, 2024, from https://www.gesis.org/fileadmin/upload/forschung/publikationen/gesis_reihen/howto/how-to2rp.pdf

PYMNTS & BitPay. (2021). *Cryptocurrency Payments Report.* USA. Retrieved from https://www.pymnts.com/wp-content/uploads/2021/05/PYMNTS-Cryptocurrency-Payments-Report-May-2021.pdf

PYMNTS & BitPay. (2022, June). *Paying With Cryptocurrency.* Retrieved February 4, 2024, from https://www.pymnts.com/wp-content/uploads/2022/06/PYMNTS-Paying-With-Cryptocurrency-June-2022.pdf

Rammstedt, B. (2004). *Zur Bestimmung der Güte von Multi-Item-Skalen: eine Einführung*. Retrieved January 8, 2024, from https://www.ssoar.info/ssoar/bitstream/handle/document/20144/ssoar-2004-rammstedt-zur_bestimmung_der_gute_von.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2004-rammstedt-zur_bestimmung_der_gute_von.pdf

River. (October 2023). *Lightning Report.* Retrieved February 12, 2024, from https://river.com/learn/files/river-lightning-report-2023.pdf

Rogers, E. M. (1962). *Diffusion of Innovations.* New York: A Division of Macmillan Publishing Co., Inc.

RSK Explorer. (2024, February 18). *Dollar On Chain*. Retrieved February 18, 2024, from https://explorer.rsk.co/address/0xe700691da7b9851f2f35f8b8182c69c53ccad9db?__tab=transactions

Rubin, J., Naik, M., & et al. (2014, December 14). *Merkelized Abstract Syntax Trees*. Retrieved October 06, 2023, from https://www.mit.edu/~jlrubin/public/pdfs/858report.pdf

Stably. (2023a, June 3). *What is #USD?* (T. W. Machine, Editor) Retrieved February 12, 2024, from https://web.archive.org/web/20230603051123/https://stably.io/brc20-usd/

Stably. (2023b, May 31). *Independent Accountant's Report*. Retrieved February 12, 2024, from https://files.stably.io/attestations/2023-05-Stably-Attestation(2023.06.01).pdf

Stably. (2023c, June 30). *Independent Accountant's Report*. Retrieved February 12, 2024, from https://files.stably.io/attestations/2023-06-Stably-Attestation.pdf

Stacks Open Internet Foundation. (n.d.). *Stacks: A Bitcoin Layer for Smart Contracts*. Retrieved December 17, 2023, from https://stx.is/nakamoto

Statista Market Insights. (2024a, January). *Cryptocurrencies*. Retrieved January 26, 2024, from https://www.statista.com/outlook/dmo/fintech/digital-assets/cryptocurrencies/worldwide?currency=usd#users

Statista Market Insights. (2024b, January 2024). *Bevölkerung - Einwohnerzahl von Deutschland von 1990 bis 2023*. Retrieved 26 January, from https://de.statista.com/statistik/daten/studie/2861/umfrage/entwicklung-der-gesamtbevoelkerung-deutschlands/

Statista Market Insights. (2024c, January). *Cryptocurrencies*. Retrieved January 26, 2024, from https://www.statista.com/outlook/dmo/fintech/digital-assets/cryptocurrencies/germany?currency=usd#users

Tenny, S., & Abdelgawad, I. (2023, November 23). *Statistical Significance*. Retrieved January 15, 2024, from https://www.ncbi.nlm.nih.gov/books/NBK459346/#:~:text=A%20study%20is%20statistically%20significant,not%20a%20statistically%20significant%20result.

Tether Operations Limited. (2022, January 28). *Tether Gold - A Digital Token Backed by Physical Gold* . Retrieved November 27, 2023, from https://gold.tether.to/Tether%20Gold%20Whitepaper.pdf

Tether Operations Limited. (n.d.). *How it works*. Retrieved December 4, 2023, from https://tether.to/en/how-it-works

THE BLOCK. (2023, December 16). *Share of Trade Volume by Pair Denomination*. Retrieved December 16, 2023, from https://www.theblock.co/data/crypto-markets/spot/share-of-trade-volume-by-pair-denomination

Triple-A. (2022). *Cryptocurrency adoption in Germany in 2022*. Retrieved January 26, 2024, from https://triple-a.io/crypto-ownership-germany-2022/

Triple-A. (2023). *Cryptocurrency Ownership Data*. Retrieved January 24, 2024, from https://triple-a.io/crypto-ownership-data/

Tsagkarelis, G. (2023, November 21). *Mint.proto*. Retrieved January 3, 2024, from https://github.com/lightninglabs/taproot-assets/blob/76bb5ae01fc0aa147233f332c468943f8c47b053/taprpc/mintrpc/mint.protoM

U.S. Census Bureau. (2024, January 26). *International Database (IDB)*. Retrieved January 26, 2024, from https://www.census.gov/data-tools/demo/idb/#/dashboard?COUNTRY_YEAR=2024&COUNTRY_YR_ANIM=2024&menu=countryViz&CCODE_SINGLE=**

Van Wirdum, A. (2019, January 24). *TAPROOT IS COMING: WHAT IT IS, AND HOW IT WILL BENEFIT BITCOIN*. Retrieved October 23, 2023, from https://bitcoinmagazine.com/technical/taproot-coming-what-it-and-how-it-will-benefit-bitcoin

Wuille, P., Nick, J., & et al. (2023, April 20). *BIP 340: Schnorr Signatures for secp256k1*. Retrieved September 24, 2023, from https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki

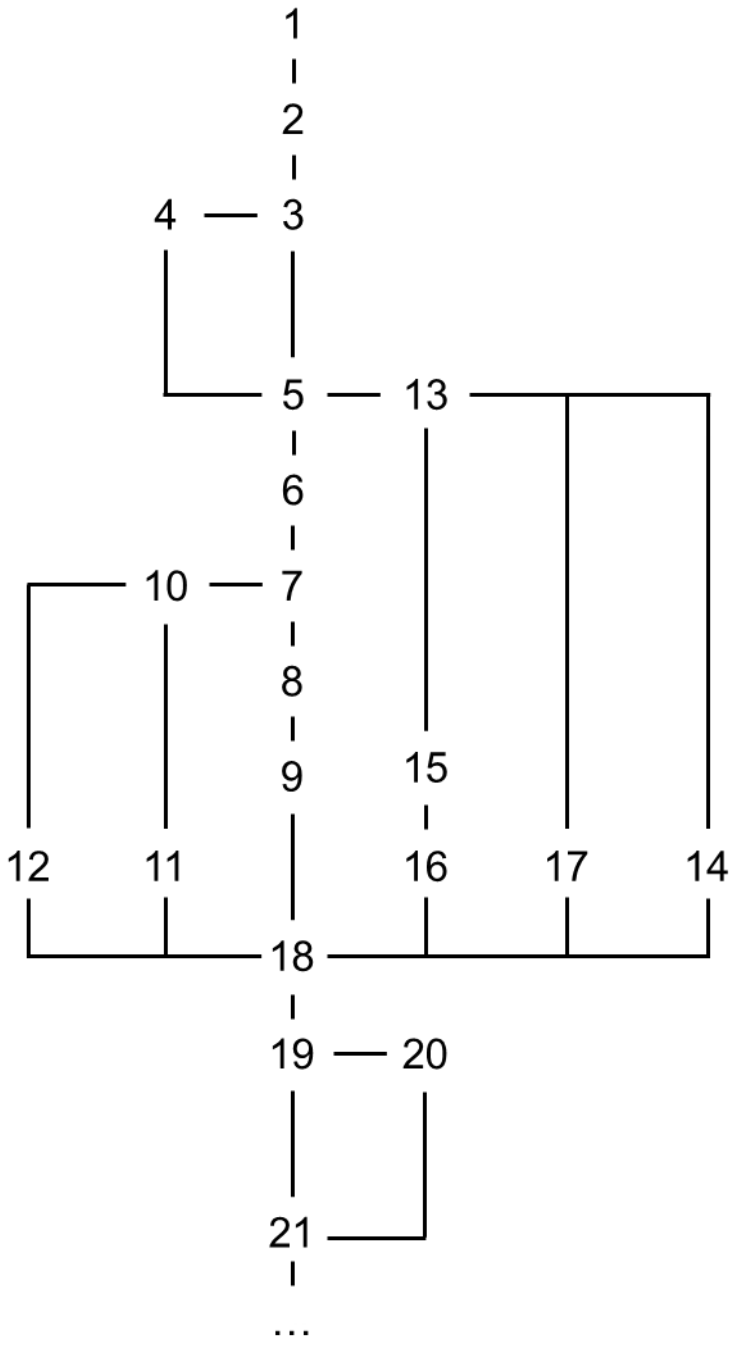
Wuille, P., Nick, J., & et al. (2023, June 29). *BIP 341: Taproot: SegWit version 1 spending rules*. Retrieved October 23, 2023, from https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

Zhao, M. (2023, March 17). *Holding Steady: The Rise of Stablecoins*. Retrieved January 1, 2024, from https://www.grayscale.com/research/reports/holding-steady-the-rise-of-stablecoins

Appendix

Appendix A: Survey Question Path

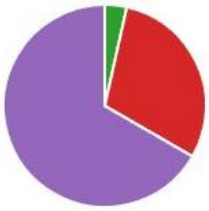
This survey question path was created to simplify the understanding of the questionnaire's structure. The figures refer to the numbering in Appendix B.



Appendix B: Survey Questions and Results

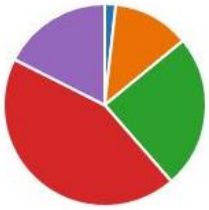
1. How often do you use electronic payments (debit/credit card, mobile payments) at a physical point of sale (e.g. supermarket) if offered by the retailer?

Never	0
Rarely	0
Sometimes	2
Often	17
Every time	38



2. How would you rate your knowledge about Bitcoin before starting this survey?

No knowledge	1
Little knowledge	7
Average knowledge	14
Advanced knowledge	25
Excellent knowledge	10

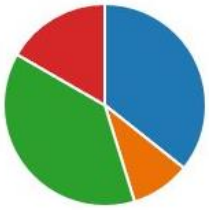


3. Based on your knowledge, do you consider bitcoin as money?

Yes	36
No	21

4. Why not?

Few merchants offer bitcoin as a...	15
Complexity	4
Price volatility	16
Other	7



5. Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?

Yes	40
No	17

6. If yes, how often?

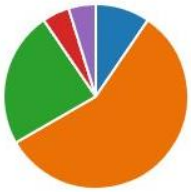
Only one time	3
Several times	19
Monthly	9
Weekly	4
Daily	5

7. Have you used bitcoin as a means of payment so far (e.g., paying for goods or services)?

Yes	21
No	19

8. If yes, how often?

Only one time	2
Several times	12
Monthly	5
Weekly	1
Daily	1



9. Did the price bother you when paying?

Yes	9
No	12

10. If not, do you consider using it in the future?

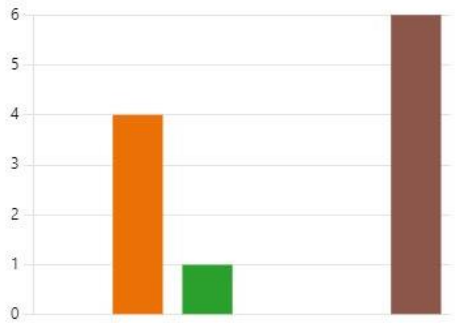
Definitely	3
Probably	7
Probably not	7
Definitely not	2

11. Would the price bother you when paying?

Yes	7
No	3

12. Why not?

Insecurity	0
Price volatility	4
I do not trust it	1
I do not understand it	0
Scam/fraud	0
Other	6

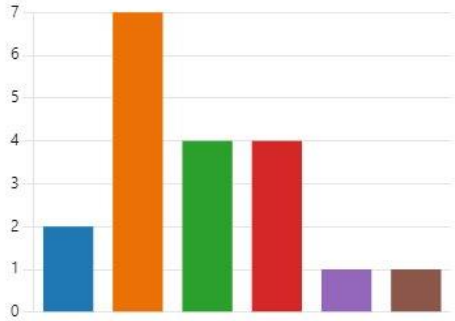


13. If not, do you consider using it in the future?

Definitely	1
Probably	8
Probably not	8
Definitely not	0

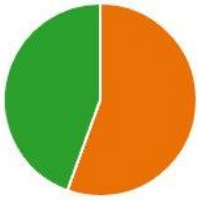
14. Why not?

Insecurity	2
Price volatility	7
I do not trust it	4
I do not understand it	4
Scam/fraud	1
Other	1



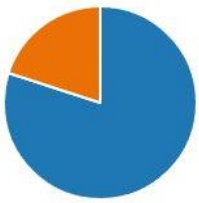
15. Would you consider using bitcoin as a means of payment (e.g., paying for goods or services)?

Definitely	0
Probably	5
Probably not	4
Definitely not	0



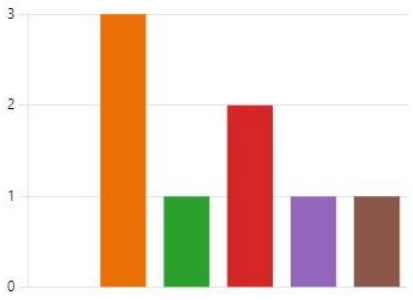
16. Would the price bother you when paying?

Yes	4
No	1



17. Why not?

Insecurity	0
Price volatility	3
I do not trust it	1
I do not understand it	2
Scam/fraud	1
Other	1

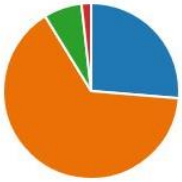


18. The price volatility of bitcoin is high. Do you consider this to be a problem if an asset is supposed to be a means of payment?

Yes	52
No	5

19. Do you consider the integration of stablecoins to be an improvement for Bitcoin?

Definitely	15
Probably	37
Probably not	4
Definitely not	1



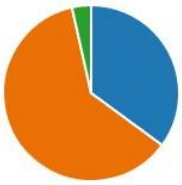
20. Why not?

5
Responses

Latest Responses

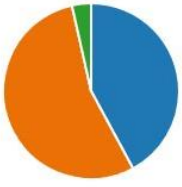
21. Based on your current usage of the Bitcoin network and **bitcoin** as a means of payment, how would the integration of stablecoins influence your behavior?

Higher usage of the Bitcoin net...	20
Probably the same usage of the ...	35
Lower usage of the Bitcoin netw...	2



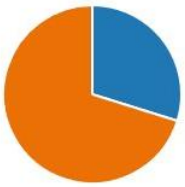
22. Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on **integrated stablecoins**?

Higher usage of the Bitcoin net...	24
Probably the same usage of the ...	31
Lower usage of the Bitcoin netw...	2



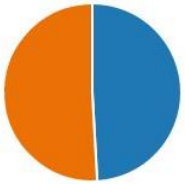
23. Bitcoin maximalists would say "this is Bitcoin on the front but fiat (stablecoins) on the back". Would you consider this to be an issue?

Yes	17
No	40



24. Chicken or the egg: Does adoption start with customers demanding bitcoin as a means of payment or merchants offering it as a payment option?

Customers demanding bitcoin p...	28
Merchants offering bitcoin pay...	29



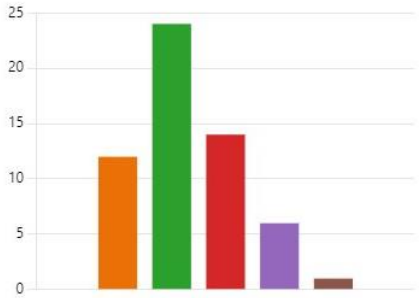
25. Do you have any additional comments regarding the integration of stablecoins into Bitcoin?

5
Responses

Latest Responses

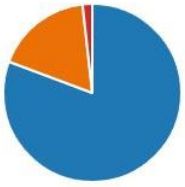
26. How old are you?

Under 18	0
18-24	12
25-34	24
35-44	14
45-54	6
55-64	1
65 and over	0



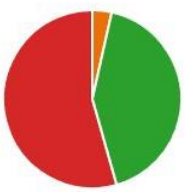
27. What gender do you identify with?

Male	46
Female	10
Non-binary	0
Prefer not to say	1



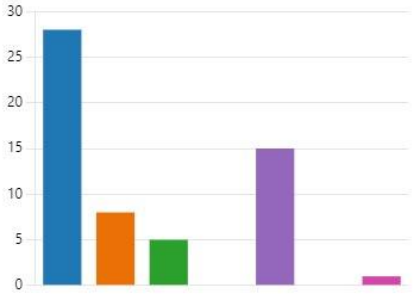
28. What is your highest educational qualification?

Less than high school	0
High school	2
Bachelor's degree	24
Postgraduate degree (Master's,...	31



29. What is your current employment status?

Employed full-time	28
Employed part-time	8
Self-employed	5
Unemployed	0
Student	15
Retired	0
Other	1



Appendix C: Extended Tables

The tables of this appendix are own illustrations created with the data set *Survey Statistics.sav* and the software *IBM SPSS Statistics Data Document*.

Table 5: *Respondent demographics and experience with Bitcoin*

Demographic variables	**Categories**	**Frequency (percentage) N = 57**
Gender	Male	46 (80.7)
	Female	10 (17.5)
	Prefer not to say	1 (1.8)
Age	18-24	12 (21.1)
	24-34	24 (42.1)
	34-44	14 (24.6)
	45-54	6 (10.5)
	55-64	1 (1.8)
Education	High School	2 (3.5)
	Bachelor's degree	24 (42.1)
	Postgraduate degree (Master's, Ph.D, etc.)	31 (54.4)
Employment	Employed full-time	28 (49.1)
	Employed part-time	8 (14.0)
	Self-employed	5 (8.8)
	Student	15 (26.3)
	Other	1 (1.8)
How would you rate your knowledge about Bitcoin before starting this survey?	Excellent knowledge	10 (17.5)
	Advanced knowledge	25 (43.9)
	Average knowledge	14 (24.6)
	Little knowledge	7 (12.3)
	No knowledge	1 (1.8)
Have you used the Bitcoin network before?	Yes	40 (70.2)
	No	17 (29.8)

Table 6: *Bitcoin usage statistics*

Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	40	70,2	70,2	70,2
	No	17	29,8	29,8	100,0
	Total	57	100,0	100,0	

Table 7: *Reliability statistics*

Reliability Statistics

Cronbach's Alpha	Part 1	Value	,247
		N of Items	3[a]
	Part 2	Value	,083
		N of Items	3[b]
	Total N of Items		6
Correlation Between Forms			,600
Spearman-Brown Coefficient	Equal Length		,750
	Unequal Length		,750
Guttman Split-Half Coefficient			,749

a. The items are: Based on your knowledge, do you consider bitcoin as money?, The price volatility of bitcoin is high. Do you consider this to be a problem if an asset is supposed to be a means of payment?, Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior?.

b. The items are: Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?, Do you consider the integration of stablecoins to be an improvement for Bitcoin?, Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?.

Table 8: *Correlations*

Correlations

			Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior?	Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?	Do you consider the integration of stablecoins to be an improvement for Bitcoin?	Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?
Kendall's tau_b	Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior?	Correlation Coefficient	--			
		Sig. (2-tailed)	.			
		N	57			
	Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?	Correlation Coefficient	,092	--		
		Sig. (2-tailed)	,486	.		
		N	57	57		
	Do you consider the integration of stablecoins to be an improvement for Bitcoin?	Correlation Coefficient	,345**	-,051	--	
		Sig. (2-tailed)	,007	,694	.	
		N	57	57	57	
	Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?	Correlation Coefficient	,679**	,029	,454**	--
		Sig. (2-tailed)	<,001	,826	<,001	.
		N	57	57	57	57

**. Correlation is significant at the 0.01 level (2-tailed).

Table 9: *Adoption driver: customers vs. merchants*

Chicken or the egg: Does adoption start with customers demanding bitcoin as a means of payment or merchants offering it as a payment option?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Customers demanding bitcoin payments	28	49,1	49,1	49,1
	Merchants offering bitcoin payments	29	50,9	50,9	100,0
	Total	57	100,0	100,0	

Table 10: *Bitcoin network usage frequency statistics*

If you have used the Bitcoin network before, how often?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Daily	5	8,8	12,5	12,5
	Weekly	4	7,0	10,0	22,5
	Monthly	9	15,8	22,5	45,0
	Several times	19	33,3	47,5	92,5
	Only one time	3	5,3	7,5	100,0
	Total	40	70,2	100,0	
Missing	System	17	29,8		
Total		57	100,0		

Table 11: *bitcoin as means of payment usage frequency statistics*

If you have used bitcoin as a means of payment so far, how often?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Daily	1	1,8	4,8	4,8
	Weekly	1	1,8	4,8	9,5
	Monthly	5	8,8	23,8	33,3
	Several times	12	21,1	57,1	90,5
	Only one time	2	3,5	9,5	100,0
	Total	21	36,8	100,0	
Missing	System	36	63,2		
Total		57	100,0		

Table 12: *Reasons for not using Bitcoin at all in the future*

Why do you not consider using Bitcoin at all in the future?

		Responses		Percent of Cases
		N	Percent	
$Q_4_2_1SUM[a]	Insecurity	2	10,5%	25,0%
	Price volatility	7	36,8%	87,5%
	I do not trust it	4	21,1%	50,0%
	I do not understand it	4	21,1%	50,0%
	Scam/fraud	1	5,3%	12,5%
	Other	1	5,3%	12,5%
Total		19	100,0%	237,5%

a. Dichotomy group tabulated at value 1.

Table 13: *Reasons for rejecting bitcoin as a means of payment (used Bitcoin)*

Why do you not consider using bitcoin as a means of payment in the future?

		Responses		Percent of Cases
		N	Percent	
$Q_4_1_1_2_2SUM[a]	Insecurity	0	0,0%	0,0%
	Price volatility	4	36,4%	44,4%
	I do not trust it	1	9,1%	11,1%
	I do not understand it	0	0,0%	0,0%
	Scam/fraud	0	0,0%	0,0%
	Other	6	54,5%	66,7%
Total		11	100,0%	122,2%

a. Dichotomy group tabulated at value 1.

Table 14: *Reasons for rejecting bitcoin as a means of payment (not used Bitcoin)*

If you have not used the Bitcoin network so far, but consider using it in the future, why would you not consider using bitcoin as a means of payment?

		Responses		Percent of Cases
		N	Percent	
$Q_4_2_2_2SUM[a]	Insecurity	0	0,0%	0,0%
	Price volatility	3	37,5%	75,0%
	I do not trust it	1	12,5%	25,0%
	I do not understand it	2	25,0%	50,0%
	Scam/fraud	1	12,5%	25,0%
	Other	1	12,5%	25,0%
Total		8	100,0%	200,0%

a. Dichotomy group tabulated at value 1.

Table 15: *bitcoin is money statistics*

Based on your knowledge, do you consider bitcoin as money?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	36	63,2	63,2	63,2
	No	21	36,8	36,8	100,0
	Total	57	100,0	100,0	

Table 16: *Reasons for not considering bitcoin as money*

Why do you not consider bitcoin as money?

		Responses		Percent of Cases
		N	Percent	
$Q_3_1SUM[a]	Few merchants offer bitcoin as a payment option	15	35,7%	71,4%
	Complexity	4	9,5%	19,0%
	Prive volatility	16	38,1%	76,2%
	Other	7	16,7%	33,3%
Total		42	100,0%	200,0%

a. Dichotomy group tabulated at value 1.

Table 17: *Electronic payment usage statistics*

How often do you use electronic payments (debit/credit card, mobile payments) at a physical point of sale (e.g. supermarket) if offered by the retailer?

	N	%
Every time	38	66,7%
Often	17	29,8%
Sometimes	2	3,5%
Rarely	0	0
Never	0	0

Table 18: *Consideration usage bitcoin as means of payment (used Bitcoin)*

Have you used bitcoin as a means of payment so far (e.g., paying for goods or services)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	21	36,8	52,5	52,5
	No	19	33,3	47,5	100,0
	Total	40	70,2	100,0	
Missing	System	17	29,8		
Total		57	100,0		

Table 19: *Consideration usage bitcoin as means of payment (not used Bitcoin)*

If you have not used the Bitcoin network so far, but consider using it in the future, would you also consider using bitcoin as a means of payment?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Definitely	0	0	0	0
	Probably	5	8,8	55,6	55,6
	Probably not	4	7,0	44,4	100,0
	Definitely not	0	0	0	100,0
	Total	9	15,8	100,0	
Missing	System	48	84,2		
Total		57	100,0		

Table 20: *Price cumbrousness of bitcoin (used as a means of payment before)*

If you have used bitcoin as a means of payment so far, did the price bother you when paying?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	9	15,8	42,9	42,9
	No	12	21,1	57,1	100,0
	Total	21	36,8	100,0	
Missing	System	36	63,2		
Total		57	100,0		

Table 21: *Frequency bitcoin as means of payment vs. price volatility cumbrousness*

If you have used bitcoin as a means of payment so far, how often? * If you have used bitcoin as a means of payment so far, did the price bother you when paying? Crosstabulation

			If you have used bitcoin as a means of payment so far, did the price bother you when paying?		
			Yes	No	Total
If you have used bitcoin as a means of payment so far, how often?	Daily	Count	0	1	1
		% within row	0,0%	100,0%	100,0%
	Weekly	Count	0	1	1
		% within row	0,0%	100,0%	100,0%
	Monthly	Count	2	3	5
		% within row	40,0%	60,0%	100,0%
	Several times	Count	5	7	12
		% within row	41,7%	58,3%	100,0%
	Only one time	Count	2	0	2
		% within row	100,0%	0,0%	100,0%
Total		Count	9	12	21
		% within row	42,9%	57,1%	100,0%

Table 22: *Price cumbrousness of bitcoin (not used as a means of payment before)*

Summarized: If you have not used bitcoin as a means of payment so far, would the price bother you when paying?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	11	19,3	73,3	73,3
	No	4	7,0	26,7	100,0
	Total	15	26,3	100,0	
Missing	System	42	73,7		
Total		57	100,0		

Table 23: *Total price cumbrousness of bitcoin*

Summarized: Does the price bother you when paying with bitcoin?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	20	35,1	55,6	55,6
	No	16	28,1	44,4	100,0
	Total	36	63,2	100,0	
Missing	System	21	36,8		
Total		57	100,0		

Table 24: *Appraisal of price volatility of asset as means of payment*

The price volatility of bitcoin is high. Do you consider this to be a problem if an asset is supposed to be a means of payment?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	52	91,2	91,2	91,2
	No	5	8,8	8,8	100,0
	Total	57	100,0	100,0	

Table 25: *Appraisal of stablecoin integration as an improvement*

Do you consider the integration of stablecoins to be an improvement for Bitcoin?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Definitely	15	26,3	26,3	26,3
	Probably	37	64,9	64,9	91,2
	Probably not	4	7,0	7,0	98,2
	Definitely not	1	1,8	1,8	100,0
	Total	57	100,0	100,0	

Table 26: *Usage of bitcoin as means of payment after stablecoin integration*

Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Higher usage of the Bitcoin network and bitcoin	20	35,1	35,1	35,1
	Probably the same usage of the Bitcoin network and bitcoin	35	61,4	61,4	96,5
	Lower usage of the Bitcoin network and bitcoin	2	3,5	3,5	100,0
	Total	57	100,0	100,0	

Table 27: *Usage of integrated stablecoins after stablecoin integration*

Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Higher usage of the Bitcoin network and integrated stablecoins	24	42,1	42,1	42,1
	Probably the same usage of the Bitcoin network and integrated stablecoins	31	54,4	54,4	96,5
	Lower usage of the Bitcoin network and integrated stablecoins	2	3,5	3,5	100,0
	Total	57	100,0	100,0	

Table 28: *Potential usage of integrated stablecoins vs. price volatility cumbrousness*

Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins? * Summarized: Does the price bother you when paying with bitcoin? Crosstabulation

			Summarized: Does the price bother you when paying with bitcoin?		
			Yes	No	Total
Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?	Higher usage of the Bitcoin network and integrated stablecoins	Count	11	7	18
		% within column	55,0%	43,8%	50,0%
	Probably the same usage of the Bitcoin network and integrated stablecoins	Count	8	9	17
		% within column	40,0%	56,3%	47,2%
	Lower usage of the Bitcoin network and integrated stablecoins	Count	1	0	1
		% within column	5,0%	0,0%	2,8%
Total		Count	20	16	36
		% within column	100,0%	100,0%	100,0%

Table 29: *Usage of stablecoins vs. usage of bitcoin vs. prior Bitcoin usage*

Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins? * Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior? * Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)? Crosstabulation

Count

Have you used the Bitcoin network before (e.g. create a wallet, do a transaction, operation of a full node)?			Based on your current usage of the Bitcoin network and bitcoin as a means of payment, how would the integration of stablecoins influence your behavior?			
			Higher usage of the Bitcoin network and bitcoin	Probably the same usage of the Bitcoin network and bitcoin	Lower usage of the Bitcoin network and bitcoin	Total
Yes	Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?	Higher usage of the Bitcoin network and integrated stablecoins	13	4	0	17
		Probably the same usage of the Bitcoin network and integrated stablecoins	2	20	0	22
		Lower usage of the Bitcoin network and integrated stablecoins	0	0	1	1
	Total		15	24	1	40
No	Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?	Higher usage of the Bitcoin network and integrated stablecoins	4	3	0	7
		Probably the same usage of the Bitcoin network and integrated stablecoins	1	8	0	9
		Lower usage of the Bitcoin network and integrated stablecoins	0	0	1	1
	Total		5	11	1	17
Total	Based on your current usage of the Bitcoin network, how would the integration of stablecoins influence your behavior on integrated stablecoins?	Higher usage of the Bitcoin network and integrated stablecoins	17	7	0	24
		Probably the same usage of the Bitcoin network and integrated stablecoins	3	28	0	31
		Lower usage of the Bitcoin network and integrated stablecoins	0	0	2	2
	Total		20	35	2	57

Appendix D: SPSS Syntax Code

```
* Table 2 crosstab of Table 6 and Table 25.
CROSSTABS
  /TABLES=Q_6 BY Q_4
  /FORMAT=AVALUE TABLES
  /CELLS=COUNT COLUMN
  /COUNT ROUND CELL.


* Table 3 crosstab of Table 6 and Table 27.
CROSSTABS
  /TABLES=Q_8 BY Q_4
  /FORMAT=AVALUE TABLES
  /CELLS=COUNT COLUMN
  /COUNT ROUND CELL.


* Table 4 crosstab Table 6 of and Table 26.
CROSSTABS
  /TABLES=Q_7 BY Q_4
  /FORMAT=AVALUE TABLES
  /CELLS=COUNT COLUMN
  /COUNT ROUND CELL.


* Table 5 to Table 6 respondent demographics and experience with Bitcoin.
DATASET ACTIVATE DataSet1.
FREQUENCIES VARIABLES=Gender Age Education Employment Q_2R Q_4
  /ORDER=ANALYSIS.
OUTPUT MODIFY
  /SELECT TABLES
  /IF COMMANDS=["Frequencies(LAST)"] SUBTYPES="Frequencies"
  /TABLECELLS SELECT=[VALIDPERCENT CUMULATIVEPERCENT] APPLYTO=COL-
UMN HIDE=YES
  /TABLECELLS SELECT=[TOTAL] SELECTCONDITION=PARENT(VALID MISSING)
APPLYTO=ROW HIDE=YES
  /TABLECELLS SELECT=[VALID] APPLYTO=ROWHEADER UNGROUP=YES
  /TABLECELLS SELECT=[PERCENT] SELECTDIMENSION=COLUMNS FOR-
MAT="PCT" APPLYTO=COLUMN
  /TABLECELLS SELECT=[COUNT] APPLYTO=COLUMNHEADER REPLACE="N"
  /TABLECELLS SELECT=[PERCENT] APPLYTO=COLUMNHEADER REPLACE="%".


* Table 7 reliability (internal consistency) split-half test.
DATASET ACTIVATE DataSet1.
RELIABILITY
  /VARIABLES=Q_3 Q_5 Q_7 Q_4 Q_6C Q_8
  /SCALE('ALL VARIABLES') ALL
  /MODEL=SPLIT.
```

```
* Table 8 construct validity (inter-item correlation) Kendall's tau-b.
NONPAR CORR
  /VARIABLES=Q_7 Q_4 Q_6 Q_8
  /PRINT=KENDALL TWOTAIL NOSIG LOWER
  /MISSING=PAIRWISE.


* Table 9 frequencies of adoption driver: customers vs. merchants.
FREQUENCIES VARIABLES=Q_10
  /STATISTICS=SUM
  /ORDER=ANALYSIS.


* Table 10 frequencies of Bitcoin network usage.
FREQUENCIES VARIABLES=Q_4_1R
  /STATISTICS=SUM
  /ORDER=ANALYSIS.


* Table 11 frequencies of bitcoin as means of payment.
FREQUENCIES VARIABLES=Q_4_1_1_1R
  /STATISTICS=SUM
  /ORDER=ANALYSIS.


* Table 12 frequencies of "why do you not consider using Bitcoin at all in the future?".
DATASET ACTIVATE DataSet1.
MULT RESPONSE GROUPS=$Q_4_2_1SUM (q_4_2_1a q_4_2_1b q_4_2_1c q_4_2_1d
q_4_2_1e q_4_2_1f (1))
  /FREQUENCIES=$Q_4_2_1SUM.


* Table 13 frequencies of "why do you not consider using bitcoin as a means of payment
in the future?".
MULT RESPONSE GROUPS=$Q_4_1_1_2_2SUM (q_4_1_1_2_2a q_4_1_1_2_2b
q_4_1_1_2_2c q_4_1_1_2_2d
    q_4_1_1_2_2e q_4_1_1_2_2f (1))
  /FREQUENCIES=$Q_4_1_1_2_2SUM.


* Table 14 frequencies of "if you have not used the Bitcoin network so far, but consider us-
ing it in the future, why would you not consider using bitcoin as a means of payment?".
MULT RESPONSE GROUPS=$Q_4_2_2_2SUM (q_4_2_2_2a q_4_2_2_2b q_4_2_2_2c
q_4_2_2_2d q_4_2_2_2e
    q_4_2_2_2f (1))
  /FREQUENCIES=$Q_4_2_2_2SUM.


* Table 15 frequencies of "is bitcoin money?".
FREQUENCIES VARIABLES=Q_3
  /STATISTICS=SUM
  /ORDER=ANALYSIS.
```

```
* Table 16 frequencies of “why do you not consider bitcoin as money?”.
MULT RESPONSE GROUPS=$Q_3_1SUM (q_3_1a q_3_1b q_3_1c q_3_1d (1))
  /FREQUENCIES=$Q_3_1SUM.


* Table 17 frequencies of electronic payment usage.
FREQUENCIES VARIABLES=Q_1R
  /ORDER=ANALYSIS.
OUTPUT MODIFY
  /SELECT TABLES
  /IF COMMANDS=["Frequencies(LAST)"] SUBTYPES="Frequencies"
  /TABLECELLS SELECT=[VALIDPERCENT CUMULATIVEPERCENT] APPLYTO=COL-
UMN HIDE=YES
  /TABLECELLS SELECT=[TOTAL] SELECTCONDITION=PARENT(VALID MISSING)
APPLYTO=ROW HIDE=YES
  /TABLECELLS SELECT=[VALID] APPLYTO=ROWHEADER UNGROUP=YES
  /TABLECELLS SELECT=[PERCENT] SELECTDIMENSION=COLUMNS FOR-
MAT="PCT" APPLYTO=COLUMN
  /TABLECELLS SELECT=[COUNT] APPLYTO=COLUMNHEADER REPLACE="N"
  /TABLECELLS SELECT=[PERCENT] APPLYTO=COLUMNHEADER REPLACE="%".


* Table 18 frequencies of bitcoin as a means of payment usage, prior Bitcoin usage.
FREQUENCIES VARIABLES=Q_4_1_1
  /ORDER=ANALYSIS.


* Table 19 frequencies of bitcoin as a means of payment usage, no prior Bitcoin usage.
FREQUENCIES VARIABLES=Q_4_2_2
  /ORDER=ANALYSIS.


* Table 20 frequencies of bitcoin price cumbrousness, used as a means of payment be-
fore.
FREQUENCIES VARIABLES=Q_4_1_1_1_1
  /ORDER=ANALYSIS.


* Table 21 crosstab of Table 11 and Table 20.
CROSSTABS
  /TABLES=Q_4_1_1_1R BY Q_4_1_1_1_1
  /FORMAT=AVALUE TABLES
  /CELLS=COUNT ROW
  /COUNT ROUND CELL.


* Table 22 frequencies of bitcoin price cumbrousness, not used as a means of payment
before.
FREQUENCIES VARIABLES=PriceCumbrousness
  /ORDER=ANALYSIS.
```

```
* Table 23 overall frequencies of bitcoin price cumbrousness.
FREQUENCIES VARIABLES=PriceBother
  /ORDER=ANALYSIS.


* Table 24 frequencies appraisal of price volatility of asset as means of payment.
FREQUENCIES VARIABLES=Q_5
  /ORDER=ANALYSIS.


* Table 25 frequencies appraisal of stablecoin integration as an improvement.
FREQUENCIES VARIABLES=Q_6
  /ORDER=ANALYSIS.


* Table 26 frequencies usage of bitcoin as means of payment after stablecoin integration.
FREQUENCIES VARIABLES=Q_7
  /ORDER=ANALYSIS.


* Table 27 frequencies usage of integrated stablecoins as means of payment after stable-
coin integration.
FREQUENCIES VARIABLES=Q_8
  /ORDER=ANALYSIS.


* Table 28 crosstab of Table 23 and Table 27.
CROSSTABS
  /TABLES=Q_8 BY PriceBother
  /FORMAT=AVALUE TABLES
  /CELLS=COUNT COLUMN
  /COUNT ROUND CELL.


* Table 29 crosstab of Table 6, Table 26 and Table 27.
CROSSTABS
  /TABLES=Q_8 BY Q_7 BY Q_4
  /FORMAT=AVALUE TABLES
  /CELLS=COUNT
  /COUNT ROUND CELL.
```

Appendix E: Digital Appendixes

IBM SPSS Statistics Data Document: *Survey Statistics.sav*
Microsoft Excel Survey Results: *Survey Results.xlsx*

Statutory Declaration in Lieu of an Oath

I – Marvin Blaich – do hereby declare in lieu of an oath that I have composed the presented paper independently on my own and without any other resources than the ones indicated.

All thoughts taken directly or indirectly from external sources are properly denoted as such.

This paper has neither been previously submitted to another authority nor has it been published yet.

Mittweida, February 21, 2024

Marvin Blaich