# Towards Atomic Cross-Chain Token Transfers: State of the Art and Open Questions within TAST

**Research** · August 2018

CITATION
1

READS
13

**4 authors**, including:

Michael Borkowski
TU Wien
**15** PUBLICATIONS **57** CITATIONS
SEE PROFILE

Stefan Schulte
TU Wien
**123** PUBLICATIONS **856** CITATIONS
SEE PROFILE

# Towards Atomic Cross-Chain Token Transfers: State of the Art and Open Questions within TAST

Michael Borkowski*, Daniel McDonald‡, Christoph Ritzer‡, Stefan Schulte*

* Distributed Systems Group
TU Wien, Vienna, Austria
{m.borkowski, s.schulte}@infosys.tuwien.ac.at

‡ Pantos GmbH
Vienna, Austria

***Abstract*—Cryptocurrencies share a broad overall purpose, enabling distributed, decentralized and trustless transfers of value. Nevertheless, the various blockchains upon which each cryptocurrency is implemented remain, for the most part, unconnected. While approaches for atomic swaps (the secure exchange of tokens on one chain for another) are emerging, there is still no documented implentation of such a system that adheres to cryptocurrency's orientation toward decentralisation and trustlessness. In this paper, we propose the concept of atomic cross-chain token transfers, which will connect various blockchains, foster collaboration between various stakeholders, and to mitigate risk to end users of a specific blockchain.**

**This paper reviews the current state of the art, both in terms of blockchains and atomic swap technologies. More specifically, we survey twenty of the most prominent blockchains, as well as fourteen currently operational or forthcoming cryptocurrency systems, discussing their features and potential usability for atomic cross-chain token transfers. We then identify several open key challenges for such token transfers, and discuss potential directions of research.**

## I. Introduction

Blockchain and cryptocurrency systems have recently gained significant interest in finance and economics, research, and public attention in general [64]. Bitcoin [37], the first implementation of a blockchain protocol, has not only demonstrated the utility of decentralized ledgers as cryptocurrency systems, but through its rapid rise in interest and value, sparked significant investment into blockchain/cryptocurrency-related research and development, ranging from adding new layers to Bitcoin itself [60], proposing improvements to the Bitcoin codebase [33], or the development of entirely new blockchains [62]. At the same time, increased attention has been given to use-cases for blockchains beyond cryptocurrencies, such as runtime verification for business processes [44].

Today, the blockchain/cryptocurrency landscape is rich and varied, comprised of technologies ranging from simple forks and slight modifications of Bitcoin or other blockchains, to radical new technologies that remove, augment or alter elementary parts of the original blockchain protocol. The level of public and commercial investment in the blockchain space is indicative both the enormous impact of the technology, and of a broad range of potential implications for the economy of the future.

Despite general positive momentum, however, structural problems exist within the blockchain community. Namely, far more development has centred on the creation of new blockchains and currencies than on the ways in which blockchains could potentially interact or connect. For users, this means that value cannot easily shift from one chain to another without the existence of a trusted third party, acting as a broker or exchange—a notion that is antithetical to the original purpose of blockchains themselves. At the same time, the current landscape an ever-increasing number of unconnected cryptocurrencies exposes users to numerous kinds of risks. First, bugs or security vulnerabilities in poorly tested new codebases may increase the likelihood of theft or destruction of coins. Second, fraudulent new blockchains can attract investment for a product that is never intended to be developed. Third, volatility in the value of a given cryptocurrency, coupled with a lack of liquidity, can leave users with no option but to hold a rapidly depreciating asset.

The currently fractured space also has consequences for blockchain developers and development more generally. For example, novel technologies in the blockchain field face the challenge of finding a sufficient amount of users for their proposed technology (e.g., a novel blockchain, or a methodology based on an existing blockchain). Since consensus plays a key role in blockchain technologies, failing to reach a critical mass of users can significantly hinder or completely prevent the development of new projects.

We propose to approach these challenges by creating a platform for blockchain interoperability, in which assets can be moved between numerous blockchains at-will, in real-time and without the risk of loss of funds. The development of such a platform will, in turn, foster connection between various cryptocurrency communities and developers, and foster further innovation within the blockchain space more generally.

This platform for blockchain interoperability is realized within the Token Atomic Swap Technology (TAST) research project[1]. TAST aims to survey possible technologies used within such a platform, to define requirements, and to find solutions to approaching the problem of fragmentation within the blockchain domain. TAST aims to create an interoperability platform through the introduction of a cross-blockchain

White Paper; May 2018, revised version 1.2, August 2018.

[1] http://www.infosys.tuwien.ac.at/tast/

token called PAN, which is transferable between blockchains. A user holding PAN tokens on one blockchain can freely transfer these tokens to another blockchain.

In this white paper, we give an overview of the stages and goals of the TAST project. First, we provide a description of the goals and background of TAST, including a discussion of various blockchains and other related projects. We then identify challenges for implementing atomic cross-chain token transfers, and discuss possible implementation strategies.

The remainder of this paper is structured as follows: Section II presents the TAST project and its goals. Section III provides background information required for the concept of cross-chain atomic token transfers. Section IV presents the current state of the art, presenting the most prominent blockchains together with the most relevant ongoing and operational projects in the blockchain domain. Section V then discusses the challenges and open problems identified. Finally, Section VI provides a brief summary and conclusion.

## II. TAST Project Goals

On a conceptual level, TAST aims to reduce the fragmentation of digital currency markets by introducing a cross-chain token, PAN, which can be freely transferred between blockchains in a decentralized manner. This token is not only a store of value and a means of exchange, but also a means of increasing standardization and interoperability development goals across the blockchain community, and encouraging co-operation between various projects in the crypto-economy.

PAN is planned to be among the first blockchain-independent tokens. Users holding PAN will not bear the risk of variations in price of different blockchain currencies. Instead, the value of PAN tokens is envisioned to remain the same, independent of the blockchain on which the tokens currently reside. Additional advantages of such an approach include the possibility of near-real-time arbitrage when using PAN as a trading asset between native cryptocurrencies, and using the distribution of PAN to determine the significance of individual blockchains, resulting in a significance metric called the *blockchain domination index*.

TAST therefore aims to propose a technology for defining, issuing and transferring tokens in a blockchain-independent way. Since every blockchain has its own features and specifics, this is done by first identifying these specifics, and defining requirements for cross-blockchain token transfers. From this, TAST will propose a concrete technical approach for performing these transfers, and demonstrate this approach in a prototype, using the PAN token as a proof of concept.

At the heart of interoperation between blockchains lies the necessity of swapping assets between one blockchain and another. Currently, users can use either centralized exchanges, or decentralized solutions [50]. Centralized exchanges are operated by a single entity, where users carry the risk of default or attack on the exchange operator, or on malicious activity, i.e., theft of funds by the exchange operator. Decentralized solutions avoid this problem by removing the central entity, instead facilitating direct transactions between multiple users, each of whom wishes to trade. In order to assert trust in the solution, it must ultimately be decentralized, and therefore not dependent on a single central instance.

Current state of the art for asset exchanges shows many operational solutions for swapping assets within a single blockchain, e.g., distributed exchanges for tokens on the Ethereum blockchain [18, 22, 56]. However, as we will show in Section IV-B, there are only a few approaches for cross-chain transfers and swaps, and none of them have reached production maturity or mass adoption. TAST therefore aims to provide an approach for such cross-chain atomic transfers.

## III. Background

This section gives an overview of aspects relevant to the TAST project. It is not within the scope of this paper to define or discuss the technology of blockchains itself, which has already been explained in detail elsewhere [37, 52, 64]. Nevertheless, specific questions like the definition and types of digital assets or swaps are discussed in the following sections.

### A. Digital Assets

In the context of this paper, *digital asset* describes any tradeable entity available on a blockchain. This can either be a unit of *currency* native to a given blockchain (e.g., Bitcoins on the Bitcoin blockchain [37], or Ether on the Ethereum blockchain [62]), or so-called *tokens*, which are tradeable units used in addition to native currencies of a given blockchain. These tokens are also called *User-Issued Assets* (UIAs) [47].

The way of representing UIAs differs between various blockchains. In some cases, UIAs have not been foreseen in the original definition of a given blockchain. For instance, originally, only Bitcoin was tradeable on the Bitcoin blockchain. The possibility of trading other digital assets has been added by third-party projects such as CounterParty [15] or Omni-Layer [60], which add a digital asset platform piggybacking on top of the Bitcoin blockchain. In other words, transactions using techniques such as CounterParty contain regular Bitcoin transactions (at least the miner's fee, which is necessary to give incentive to the miners to include the transaction in a block), and contain additional transaction data which represents UIA transfers, for instance, specified by CounterParty. To nodes unaware of CounterParty, such transactions simply look like regular Bitcoin transactions, since the additional data is formatted in a way that causes it to be disregarded by such nodes. These UIAs are sometimes called *colored coins* [6], due to the original idea of *coloring* (marking) individual currency units [45] and its implementations [12, 17]. However, more recent approaches no longer follow the original idea, and instead use the so-called `OP_RETURN` opcode [14, 41, 60]. This method allows arbitrary data (i.e., payload) to be appended to a Bitcoin transaction.

In addition to the techniques described above, other blockchains allow native solutions. For instance, one of the features of the Ethereum blockchain are so-called *smart contracts* [62], which allows for arbitrary Turing-complete code to be executed in a decentralized manner. In other words, all

nodes execute the same code deterministically, and the effects of this execution can again cause transactions on the Ethereum blockchain. These smart contracts can be used to create UIAs. Since many UIAs share common functionality (e.g., definition of tokens, issuance, trading), a common interface has been proposed for this functionality in an Ethereum Request for Comment (ERC) [54], which was followed by an Ethereum Improvement Proposal (EIP) [55]. This EIP has been accepted and is therefore regarded as a *standard*. Due to the number of the original ERC (20), this standard is commonly called ERC20[2]. Tokens complying to ERC20 implement a well-defined set of functions which can be used independently of the concrete token, for instance by wallet applications. A backwards-compatible extension of ERC20 has been proposed in January 2018 as ERC827 [30].

Finally, UIAs can be an explicit part of the definition of the blockchain itself, as it is the case for Waves [57] or Nxt [40]. In these cases, no additional smart contracts are required to implement UIAs, but the functionality is implemented natively by the blockchain itself.

Some digital assets traded on blockchains are *fungible*, a property originating from the field of economics, describing that money has no labels [51]. Fungibility of digital assets implies that an asset is only defined by its quantity (e.g., 1.0 Bitcoin), and not by its origin or situation (e.g., *a specific* Bitcoin). The fungibility of digital assets is decided by their definition on the blockchain. For instance, Ethereum uses the so-called *account balance* model, which removes any explicit connection between outgoing and incoming transactions. In contrast, the Bitcoin blockchain uses the *Unspent Transaction Output* (UTXO) model [3]. This binds the input side of a transaction to the output side of another transaction, which adds at least partial traceability, and therefore non-fungibility, which serves as a basis for the initial proposals of colored coins [45]. Furthermore, assets are non-dividable at a given level. While fractions of units are possible (e.g., a transfer of 0.03 Bitcoin), all digital assets considered in this paper have a single smallest unit, beyond which they cannot be divided. For Bitcoin, this is called a satoshi and equals to $10^{-8}$ Bitcoin.

### B. Asset Swaps

The term *swap* is used to denote an exchange of one asset with another [20]. Swaps between two parties are of particular interest, since generally, each party of a swap bears the risk of the other party defaulting. While swapping one currency for another within the domain of a single user can certainly be of interest, we focus on swaps between two or more different parties, and assume no trust between these parties.

There are various classifications for swaps. In the simplest case, users $A$ and $B$ hold assets $X$ and $Y$, respectively, on a given blockchain. $A$ and $B$ then agree to exchange a specific amount of each asset for the other. Therefore, the target of the swap is for $A$ to acquire $Y$, and for $B$ to acquire $X$. However, when transferring $X$ to $B$ using a regular transaction, $A$ bears the risk of $B$ simply refusing to transfer $Y$. Since $A$ has already transferred the funds, they can only be accessed using the private key of $B$, and are not recoverable for $A$. Similarly, if $B$ sends the funds first, the same scenario is possible, and $B$ is at risk of losing all funds.

It is therefore in the interest of both swapping parties to ensure that the funds at risk are not lost during the process. More specifically, after an agreement on the terms, the swap should either be performed in its entirety, i.e., all terms, including all payments, must be fulfilled, or no transaction must take place[3]. This property is called *atomicity*, and is related to the homonymous property in programming languages [19]. Consequently, swaps which are guaranteed to be either completed in their entirety, or not executed at all, are called *atomic swaps*.

In addition to the described scenario, atomic swaps can be performed in a multitude of variations and forms: atomic swaps can be performed across different blockchains, and between more than two users. Additionally, fungible assets can be swapped for functional assets, for instance, a given asset representing a certain price can be atomically swapped for a token representing ownership or rental rights with respect to a physical object, such as a car. Atomic swaps in any of these cases pose certain challenges with regards to the protocol being used, including the functional requirement of atomicity (how to ensure no party loses a significant amount of funds if another party behaves adversely), but also practical questions like matching (how to find partners suitable for atomic swaps).

## IV. State of the Art

In this section, we present an overview of existing technologies. We first survey blockchains and describe each blockchain with regards to suitability for our purposes in Section IV-A, and then give an overview of existing or upcoming projects related to our work in Section IV-B.

Note that information about present technologies discussed in this paper is sourced from various kinds of previous work. While some projects have underlying peer-reviewed academic publications, others are merely described on a website, or even in source code. Furthermore, in certain cases, it is not trivial to distinguish between features already supported, features planned, but not yet implemented, and purely envisioned features. For the sake of completeness, all technologies encountered are included in this paper, and information about various aspects and features for each of these technologies is taken from the most reliable source available for the given technology, to the best of our knowledge. Furthermore, due to the rapidly changing landscape of cryptocurrencies and blockchains in general, technologies are subject to change and new technologies and solutions are introduced on a frequent basis.

[2]While the standard is formally called EIP20, the name ERC20 is still commonly used to designate these tokens. For the sake of clarity, we follow this nomenclature. Alternative spellings are EIP-20 or ERC-20, respectively.

TABLE I
OVERVIEW OF PROMINENT BLOCKCHAINS

| | Chain | Native Asset | Symbol | Consensus | UIA Support | Smart Contracts | Comments |
|---|---|---|---|---|---|---|---|
| [37] | Bitcoin | Bitcoin | BTC, XBT | PoW | No | Simple (Script) | |
| [37] | Bitcoin Cash | Bitcoin Cash | BCH | PoW | No | Simple (Script) | Bitcoin Fork |
| [33] | Litecoin | Litecoin | LTC | PoW | No | Simple (Script) | Bitcoin Fork |
| [16] | Dash | Dash | DASH | PoW | No | Simple (Script) | Litecoin Fork |
| [62] | Ethereum | Ether | ETH | PoW | Smart Contracts | Turing-Complete (EVM) | ETH/ETC Fork |
| [5] | Ethereum Classic | Classic Ether | ETC | PoW | Smart Contracts | Turing-Complete (EVM) | ETH/ETC Fork |
| [28] | Komodo | Komodo Coin | KMD | Delayed PoW | Partial | Planned | |
| [46] | Monero | Monero | XMR | PoW | No | No | |
| [40] | Nxt | Nxt | NXT | PoS | Native | No | |
| [26] | Ardor | ARDR | ARDR | PoS | Native | Smart Transactions | Evolved from Nxt |
| [23] | Ignis | IGNIS | IGNIS | PoS | Native | Smart Transactions | Ardor child chain |
| [57] | Waves | Waves | WAVES | PoS | Native | Planned (Rideon) | |
| [38] | NEM | XEM | XEM | PoS/PoI | Native | No | |
| [61] | Catapult | XEM | XEM | PoS/PoI | Native | Planned, Simple | NEM development |
| [32] | Lisk | Lisk | LSK | Delegated PoS | No | Planned (JS) | |
| [9] | Cardano | Ada | ADA | PoS [27] | Planned | Planned | |
| [39] | Neo | Neo | NEO | dBFT | Native | Turing-Complete (NeoVM) | |
| [43] | IOTA | iota | IOTA | none (DAG) | No | No | |
| [48] | Ripple | Ripple | XRP | RPCA | Native | Planned (Codius) | |
| [35] | Stellar | Lumen | XLM | FBA [35] | Native | Turing-Complete (JS) | |

### A. Blockchains

In this section, we give a brief overview of the most relevant existing blockchains. A summary is shown in Table I, where the name of the blockchain and the currency, the consensus protocol and the support for UIAs and smart contracts are described. Note that due to the amount of blockchains in existence, this list is not exhaustive. Instead, we focus on blockchains with a certain prevalence, which also allow for other types of assets to enable the envisioned interoperability between blockchains. As a base selection set, we consider all blockchains where the respective native currency has a market capitalization of over two billion dollars[4]. From this set, we select blockchains suitable for token transfers, and discuss their properties.

As described in Sections I and III-A, the first blockchain used as a basis for a cryptocurrency, *Bitcoin* [37], played a seminal role in blockchain development. The Bitcoin blockchain natively supports only one asset type (Bitcoin). However, there are third-party approaches to use Bitcoin to transfer other types of assets, as described in Section III-A. Bitcoin uses Proof of Work (PoW) as its consensus mechanism, and uses a stack-based, non-Turing-complete scripting language called *Script* [2]. A hard fork in the Bitcoin blockchain caused the emergence of a new blockchain, forking off Bitcoin, called *Bitcoin Cash*. Furthermore, *Litecoin* [33] is a fork of Bitcoin, with the main goal of reducing the block generation time, as well as a different algorithm used for hashing (SHA-256). *Dash* [16] is a fork of Litecoin, which uses a concept of Masternodes instead of a single-tier network, and also proposes additional privacy features.

*Ethereum* [62] is another prominent blockchain. It is mostly known for its virtual machine, called the Ethereum Virtual Machine (EVM), which enables smart contracts on the blockchain. In contrast to Bitcoin, EVM is Turing-complete, and allows any deterministic algorithm to be executed by the network. It currently uses PoW as its consensus algorithm, but is planned to use Proof of Stake (PoS) at some point in the future [8]. Smart contracts for Ethereum are often written in the *Solidity* language [21]. Ethereum uses its native currency *Ether*. Execution of smart contracts consumes an execution fee called *Gas*, which is paid for using Ether. Apart from Ether, Ethereum does not natively recognize UIAs; however, smart contracts can be used to define, issue, and transfer tokens, as described in Section III-A. Ethereum has also seen a hard fork, yielding Ethereum and *Ethereum Classic* [5].

The *Komodo* project [28] offers an approach that is novel in that it uses *notarization*, which results in a *delayed PoW* consensus. Any disagreement amongst the nodes is resolved by using periodic backups stored in a trusted blockchain. More concretely, the Komodo blockchain is notarized on another blockchain, currently Bitcoin. Komodo nodes elected by a stake-weighted vote decide which blockchain to notarize to, however, the technical documentation does not discuss this process in detail. It is also not defined how the selection takes place, only that the notary nodes must be chosen "wisely". Komodo proposes a solution to facilitate and speed up the creation of new blockchains by notarizing them against Komodo, providing ultimately the security of the blockchain to which Komodo notarizes (currently Bitcoin) to those new blockchains. Unfortunately, while the Komodo white pa-

[3]The latter requirement is sometimes relaxed to a certain degree [28], to allow for minimal investment fees which are lost in case of default.

[4]Time of data acquisition: April 2018

per [28] proposes interesting features and a novel platform, it lacks significant technical details (e.g., how Bitcoin funds necessary for notarization are obtained).

While Komodo does not explicitly support UIAs on its blockchain, its utility to create additional blockchains, notarized on Komodo, hints at the possibility of at least partial support. Furthermore, Komodo claims that users can use smart contract functionality of Bitcoin, but specific details of what constitutes this functionality and the implementation on Komodo are not presented. Furthermore, the effects of switching notorization platform on smart contract execution do not appear to be have considered or described. *Monero*, a cryptocurrency based on the CryptoNote protocol [46], also uses PoW as a consensus protocol. It provides additional privacy compared to Bitcoin by increasing the fungibility of coins, but does not provide smart contract features due to security and privacy concerns.

*Nxt* [40] and *Waves* [57] are two blockchains natively implementing UIAs. While both blockchains currently do not support smart contracts, Waves shows ongoing development in this regard [29]. The implementation of smart contracts is planned in two stages, first supporting non-Turing-complete smart contracts by implementing specific capabilities, intended to cover most everyday use cases, and then extending functionality to include Turing-complete smart contracts [58, 59]. Jelurida, the company developing Nxt, has also created a novel blockchain platform called *Ardor* [26], which serves as a platform for child-blockchains, such as the *Ignis* blockchain [23]. Ardor supports so-called *smart transactions* [26], which pose a limited set of boolean operators (AND, OR, NOT) to create a composite voting model. This very simple form of smart contracts is also inherited to Ignis.

*NEM* [38] is a blockchain introducing the XEM currency, which uses Proof of Importance (PoI), a consensus algorithm extending PoS. The difference between PoI and PoS is that the *importance* score in PoI is calculated from both the amount of currency held in an account (like in PoS), but also the amount of performed transactions, which adds incentive to network members to not only hold currency, but to actively carry out transactions. The NEM blockchain has native support for UIAs in the form of so-called Mosaics. On-chain smart contracts are not supported by design, but a novel development of a blockchain engine as a fork of NEM, called Catapult [10, 61], aims to allow for a certain set of functionalities similar to smart contracts. NEM also natively supportes atomic cross-chain swaps [53]. *Lisk* [32] uses Delegated PoS, which means that network users can elect a number of delegates, which are responsible for finding consensus. The election is weighted based on the amount of LSK held by the voter. Lisk does not support UIAs, and does not currently support smart contracts, though they are planned to be supported using JavaScript. The *Cardano* blockchain, with its native currency Ada, uses the Ouroboros PoS protocol [27]. It currently does not support smart contracts, even though they are planned in the future [9]. However, Cardano is planned to natively support UIAs [13].

There exist relatively new blockchains, such as *Neo* [39], with the native Neo currency, which is another blockchain proposing smart contracts, native UIAs in addition to the native currency, and a novel consensus protocol called Delegated Byzantine Fault Tolerant mechanism (dBFT). Neo uses NeoVM as a Turing-complete virtual machine, supporting smart contracts. Neo plans a cross-chain token transfer protocol called NeoX, however, no technical details to this plan are publicly available. Furthermore, *IOTA* [43] proposes a cryptocurrency not based on a blockchain. Instead, a directed acyclic graph (DAG) is used, where each transaction approves two previous transactions. Coins have been created in the genesis of IOTA, and are not being mined. Interestingly, no consensus protocol is required, and nodes work mostly independently of each other. Instead, a resolution algorithm is proposed to resolve conflicting transactions, such as double spending. Apart from IOTA, the *Ripple* [48] is the only cryptocurrency discussed in this paper with a pre-created amount of assets released at the genesis. All Ripple in circulation has been issued by Ripple Inc., the company developing the blockchain. This relatively centralized paradigm has been a source of criticism [7]. Ripple supports UIAs representing any kind of asset, i.e., other cryptocurrencies, fiat currencies, or any other form of value, however, these assets cannot be transferred freely between users. Instead, a chain of trust by bridge and compliance servers is required. Therefore, this blockchain is not discussed in more detail in this paper. Due to the same reasons, Stellar [35], which started as a fork of Ripple, but has been re-written in the process, is not further discussed in this paper. Ripple plans to support smart contracts using Codius [11], and Stellar supports JavaScript smart contracts.

### B. Projects

In addition to giving an overview of the most prominent blockchains, we also review current projects and approaches related to TAST. This includes cross-blockchain currencies, decentralized exchange (DEX) projects, and on-chain token layers. A summary is provided in Table II, where several properties of the approaches are shown. The protocol type describes the kind of communication model proposed or used, i.e., smart contracts (marked as SC, or ETH-SC for Ethereum smart contracts), off-chain peer-to-peer communication (marked as P2P), data embedded in transactions (marked Tx), or standalone blockchains (marked as sBC).

*1) Metronome and Republic Protocol:* To the best of our knowledge, the project closest to TAST is *Metronome* [36], which is designed to be a cross-chain currency (MTN). Metronome is currently in pre-launch state, with an estimated launch date of June 2018. Metronome proposes the feature of cross-chain portability: a user transferring MTN from one blockchain to another can do so by destroying tokens on the source blockchain in a provable and controlled way, receiving a *proof of exit* receipt. This receipt can then be used on the target blockchain to call the Metronome contracts, which yield MTN on the target blockchain. In other words, while MTN tokens on both blockchains are technically not the same token,

TABLE II
OVERVIEW OF RELATED PROJECTS

| | Name | Type | Protocol | State | Chain | Token |
|---|---|---|---|---|---|---|
| [36] | Metronome | Cross-chain asset (destroy-and-issue transactions) | ETH-SC | Planned June 2018 | Multi (ETH) | MTN |
| [63] | Republic | Dark pool DEX | P2P | Prototype | Multi | REN |
| [28] | BarterDEX | DEX for the Komodo project (atomic, cross-chain) | P2P | Prototype | Multi (KMD) | KMD |
| [4] | Bisq | DEX including fiat, arbiters with 2-out-of-3 escrow | P2P | Operational | Multi | BSQ |
| [34] | KyberNetwork | DEX with distributed reserves | ETH-SC | Beta | Ethereum | KNC |
| [56] | 0x | DEX for ERC20 tokens | ETH-SC | Operational | Ethereum | ZRX |
| [18] | EtherDelta | DEX for ERC20 tokens | ETH-SC | Operational | Ethereum | EDT |
| [22] | IDEX | DEX for ERC20 tokens | ETH-SC | Operational | Ethereum | IDXM |
| [1] | Altcoin.io | DEX with atomic cross-chain swaps | SC | Planned | Multi | |
| [24] | Internet of Coins | DEX with atomic cross-chain swaps | P2P | Planned | Multi | HYBRID |
| [60] | OmniLayer | Token layer on Bitcoin | Tx | Operational | Bitcoin | OMNI |
| [15] | Counterparty | Token layer on Bitcoin | Tx | Operational | Bitcoin | XCP |
| [41] | OpenAssets | Token layer on Bitcoin | Tx | Operational | Bitcoin | OPA |
| [31] | RootStock | Smart contracts protocol on Bitcoin | sBC | Operational | Bitcoin | SBTC |

they are treated like one type of asset. Metronome uses on-chain communication using Ethereum smart contracts.

The Metronome documentation [36] puts strong focus on the economic side of the tokens, discussing the initial supply, market capitalization, and price developments. Furthermore, the document discusses four Ethereum smart contracts, which comprise the Metronome system (MTN Token and Ledger, Auctions Contract, Proceeds Contract, Autonomous Converter Contract). However, it is not clear from the document how this is implemented in other blockchains, more specifically in blockchains not supporting smart contracts, or blockchains not supporting UIAs.

The *Republic protocol* [63] is a comparable project, proposing a dark pool DEX with atomic swaps. Dark pool refers to the fact that orders in the DEX are secret, and can only be reconstructed by nodes matching the orders. The details, i.e., the order amount, type of assets etc., cannot be determined by unrelated nodes. The Republic protocol uses an Ethereum smart contract called the *Registrar* to arrange nodes into a network topology that makes it unreasonably difficult for attackers to acquire enough order fragments to reconstruct the order. The Republic protocol uses the Shamir Secret Sharing Scheme [49] to split orders. Furthermore, the Republic protocol uses atomic swaps for order fulfillment, executed over the Republic Swarm Network, a decentralized peer-to-peer network.

*2) BarterDEX: BarterDEX* is a part of the Komodo project [28], and constitutes a DEX for trading cryptocurrencies without counterparty risk, i.e., risk of failure to pay of a centralized exchange. BarterDEX promises an end-to-end solution, including order matching, trade clearing, settlement, atomic swaps, and a peer-to-peer protocol defined for negotiating between trading partners. BarterDEX is currently in beta operation. The DEX can be used to exchange tokens issued on the Komodo platform. BarterDEX proposes the usage of liquidity nodes, which make their profit from the spread between bid and ask orders, and enhance market liquidity. BarterDEX entails certain features like order matching, and atomic swaps. Unfortunately, in the Komodo documentation [28], many features are only presented on a conceptual level, with important technical details referred to only obliquely or omitted entirely.

*3) Bisq: Bisq* [4] is another DEX implementation, which also allows for exchange from and to fiat currencies. Bisq is operational. In contrast to BarterDEX, Bisq uses a 2-out-of-3 multisignature escrow service. This means that a swap is not atomic, but locked in a multisignature transaction, requiring two signature partners to be unlocked. This can be either the two trading partners, in case of agreement, or, in case of disagreement, one trading partner, and an arbiter. In the protocol proposed by Bisq, both partners select at least one arbiter, and in case of a dispute, an arbiter is selected in a semi-random way (derived from the transaction hash). This arbiter then reviews proofs provided by both parties and unlocks the respective transaction. Arbiters receive a fee, regardless of whether an agreement was reached or not, as an incentive for participation. This off-chain settling with on-chain settlement realization allows for trading of fiat currencies in addition to cryptocurrencies. Bisq employs a peer-to-peer protocol for order matching, arbiter selection and execution, and does not pose limitations on the blockchains or assets traded. Current efforts within Bisq are towards the creation of a Bisq Decentralized Autonomous Organization (DAO) [42].

*4) KyberNetwork and Altcoin.io: KyberNetwork* [34] is an on-chain protocol for instant exchange of digital assets. Currently, KyberNetwork is operating on the Ethereum blockchain, but it is planned to be extended beyond this blockchain to accommodate other assets. The KyberNetwork itself consists of smart contracts, which are responsible for maintaining the actual exchange, as well as maintaining the asset reserves necessary to ensure liquidity. The asset reserves are maintained by reserve managers, which earn from the spread of an exchange transaction. KyberNetwork guarantees both the security of funds and atomicity of transactions. KyberNetwork proposes the usage of a KyberNetwork Crystal (KNC) token as a reverse-fee paid by the reserves in order to be able to participate. For every executed exchange, a given

amount of KNC is destroyed, i.e., taken out of circulation. A related project, *Altcoin.io* [1], is a planned DEX, envisioning the usage of atomic cross-chain swaps. Currently, Altcoin.io uses on-chain communication in the form of smart contracts, but also plans to use off-chain peer-to-peer communication.

*5) 0x Protocol, EtherDelta and IDEX: 0x* [56] is a protocol for decentralized exchange of ERC20 tokens on the Ethereum blockchain. Its key features are its decentralized nature, and the control of fees similar to how fees are controlled in regular transactions. The fees are determined by the maker, but ultimately the decision of including the order in the order book is done by the relayers, i.e., the network. However, 0x is limited to the Ethereum blockchain and to ERC20 tokens. Similar to 0x, *EtherDelta* [18] is a decentralized exchange for ERC20 tokens on the Ethereum blockchain. The main difference between 0x and EtherDelta is the concept of *Relayers* in 0x. *IDEX* [22] is another operational DEX for ERC20 tokens.

*6) Internet of Coins: Internet of Coins* (IoC) [25, 24] promises a decentralized exchange, facilitating atomic swaps to perform cross-chain exchanges. The proposed architecture involves a network daemon (the HYBRID daemon *hybridd*) and gives several architectural features of the system. The main feature described is a self-regulating market, including blockchain-agnostic tokens, issued by IoC, serving as a vehicle for decentralized swaps of value from one blockchain to another. This is claimed to diversify portfolio risks across different blockchains.

In the proposed architecture, the HYBRID daemon is communicating with other HYBRID daemons using a peer-to-peer network. Fundamentally, IoC is similar to BarterDEX [28] and Bisq [4] in that it employs a peer-to-peer communication layer independent from and above the blockchain. Like Bisq, IoC claims to be blockchain-agnostic.

*7) On-Blockchain Layers:* Several projects use technologies which create a layer on top of an existing blockchain. This is done in a transparent way, i.e., to the underlying blockchain, the transactions look like regular transactions.

**OmniLayer, Counterparty and OpenAssets** There exist various approaches for adding a UIA layer to the Bitcoin blockchain, most notably *OmniLayer* [60] (formerly Mastercoin), *CounterParty* [15], and *OpenAssets* [41]. All of these protocols are implementations of the *colored coins* approach [45] (see Section III-A). Functionally similar to ERC20 on Ethereum, they allow coins to be marked as a certain asset (colored), and then traded independently of Bitcoin. The difference between UIAs on Ethereum (e.g., ERC20 tokens) and colored coins lies in the fact that UIAs on Ethereum are implemented as smart contracts using EVM, and therefore do not require extensions of the native blockchain, while colored coin approaches require additional logic for parsing transactions. All three approaches build on top of the Bitcoin blockchain, and are currently operational.

**RootStock** A compatibility layer to run EVM smart contracts using the Bitcoin blockchain is proposed by *RootStock* [31], using a separate blockchain and currency called Smart BTC (SBTC). RootStock proposes a 2-way-peg between BTC and SBTC. This is done by locking BTCs when BTCs are to be exchanged for SBTCs, and unlocking in the reverse case. Since RootStock is completely compatible to EVM, conceptually, ERC20 token issuing is possible on the RootStock blockchain.

## V. Challenges and Open Questions

The realization of cross-chain token transfers within TAST depends heavily on the used underlying blockchain technology, as well as various technical aspects. In this section, discuss the major challenges and currently open questions within the TAST research project, namely:

- How are the tokens issued on the blockchains? Is a fixed pool of issued tokens used, or are they re-issued on a regular basis?
- How are tokens disabled as they are leaving the blockchain? Are tokens destroyed, locked, or stored in a special wallet or contract?
- Are tokens re-balanced across blockchains to maintain liquidity, and if so, how often and by which entity?
- Which blockchains are suitable for cross-chain token transfers?
- Which features (e.g., native UIAs, smart contracts, Turing-completeness) are required from a blockchain to support token transfers as proposed by TAST?
- Can cross-chain transfers be realized despite lack of Turing-complete smart contracts?

### A. Issuance and Handling of Portable Tokens

A crucial challenge is the decision regarding how the concrete implementation of cross-chain tokens is to be realized. Regular tokens, e.g., ERC20 tokens on the Ethereum blockchain, are issued using either a fixed supply of tokens, or a variable supply, where the rules of issuance (minting) of tokens are regulated in the smart contracts constituting the token. The only project surveyed in this work promising a cross-chain token is Metronome [36]. Metronome proposes the MTN token, which is portable across blockchains. This portability is realized using smart contracts. For minting, a *Daily Supply Lot* is proposed which mints 2,880 MTN tokens per day, adjusted for each blockchain on a pro rata basis. In other words, if two blockchains carry two amounts $A$ and $B$ of MTN, respectively, the minting rates per day are set to be $\frac{A}{A+B}$ and $\frac{B}{A+B}$, respectively.

The portability of MTN is realized by changing the amount of tokens in circulation on each blockchain. Considering a transfer of $n$ tokens between blockchains $\mathcal{A}$ and $\mathcal{B}$, the change of supply of MTN is realized by the user creating a *proof of exit* on $\mathcal{A}$, which confirms the reduction of the supply of $\mathcal{A}$ by $n$. This proof of exit can then be used on $\mathcal{B}$ to claim $n$ tokens. Metronome currently does not specify the technical details of this process, or how the proof of exit is verified on $\mathcal{B}$.

Both the removal of tokens from $\mathcal{A}$ and the creation of tokens on $\mathcal{B}$ can be realized in several different ways. The exit

of tokens from $\mathcal{A}$ can be implemented by actually destroying tokens, rendering them unusable, or by locking the tokens into an account only accessible by providing another proof of exit from a transaction back to $\mathcal{A}$. Another possibility includes uniquely identifying each token, and maintaining a list of current blockchain locations for each token on each possible blockchain. Similarly, claiming MTN on $\mathcal{B}$ in exchange for a proof of exit receipt can be realized either by minting new MTN on $\mathcal{B}$, unlocking previously locked MTN, or by changing the internally tracked location of certain (unique) MTN tokens to $\mathcal{B}$.

### B. Cross-Chain Proof

When $n$ tokens are transferred between blockchains, e.g., from account $a$ on $\mathcal{A}$ to account $b$ on $\mathcal{B}$, the receiving blockchain $\mathcal{B}$ must validate a number of facts:

- The account $a$ is in possession of $n$ tokens.
- The account $b$ wants to receive $n$ tokens from $a$ (either because $a$ and $b$ belong to the same person, or because the owner of $b$ has agreed to the transfer).
- The account $a$ will not spend the $n$ tokens dedicated for the transfer in another way (by transferring them to another account on $\mathcal{A}$, to another account on $\mathcal{B}$, or by transferring them to a third blockchain $\mathcal{C}$).

The second condition can be regarded as optional, assuming that the possession of tokens is always a benefit to the receiver. However, the other conditions must be verifiable by the target blockchain $\mathcal{B}$ using the proof of exit receipt.

We are currently investigating possible implementation of cross-chain proofs. Generally, smart contracts on one blockchain are not able to access information stored on another blockchain, but solutions are conceptually possible due to the decentralized nature of blockchain systems in general. One possible approach includes using an additional token and the reversal of proof: while proof of exit might not be possible due to the aforementioned limitation, it might be possible to force the claimer of tokens on $\mathcal{B}$ to publicly disclose information which can be used by anyone else to destroy the tokens on $\mathcal{A}$.

Another concept includes a semi-central authority publicly signing transfers. While the signing process is still centralized (there is one trusted central authority, or a set of such authorities), the signing is publicly verifiable, and any invalid signature can be detected by anyone.

### C. Selection of Blockchains

Another crucial task is the selection of concrete blockchains for cross-chain token transfers. In Table I, we have identified several blockchains which would potentially be candidates for such transfers. Native support for UIAs is provided by Nxt, Ardor/Ignis, Waves, NEM/Catapult, and Neo. Ethereum and Ethereum Classic support tokens through smart contracts.

Turing-complete smart contracts are currently supported by Ethereum, Ethereum Classic, and Neo. Simple scripts are supported by Bitcoin and Bitcoin Cash and its derivatives (e.g. Litecoin, Dash), as well as by Ardor/Ignis (smart transactions).

We propose to select Ethereum as the first blockchain for cross-chain token transfers, since it supports both Turing-complete smart contracts and UIAs through ERC20. Additionally, we consider possible counterpart blockchains:

**Ethereum Classic** Sharing codebases, Ethereum and Ethereum Classic are a promising choice for a blockchain pair for performing cross-chain token transfers. Just like Ethereum, Ethereum Classic supports Turing-complete smart contracts, and UIAs using the ERC20 standard.

**Bitcoin** UIAs are not supported natively on Bitcoin, and transaction capabilities are limited to relatively simple scripts. Challenges for adopting Bitcoin include the necessary utilization of on-blockchain token layers [14, 60], and the limited Script language. The same challenges apply to Litecoin and Dash.

**Neo** supports writing smart contracts in languages including C#, VB.Net, F#, Java, Kotlin, and Python. A challenge to Neo is the high cost of creating a smart contract. However, once created, Neo might provide a smart contract development platform similar to Ethereum.

**Waves** does not currently support smart contracts, but this feature is planned for the near future [59]. Challenges for Waves include the feasibility of cross-chain token transfers using Waves' initial, non-Turing-complete smart contract capabilities, before their deployment of Turing-complete smart contracts.

## VI. Conclusion

In this white paper, we have highlighted the need for token transfers across blockchains, and presented an argument that cross-chain token transfers can potentially foster cooperation within the fragmented blockchain ecosystem, while also reducing various end-user risks. At the same time, we have provided an extensive review of the current state of the art, both discussing present blockchains together with their features and details, and given an overview of the most prominent cryptocurrency projects. Furthermore, we have described the overarching aim, scope and goals of the TAST research project, and provided an overview of the currently open questions and challenges within TAST. Finally, we provided an outlook on possible solutions to these emerging questions.

## Disclaimer

Information provided in this paper is the result of research, based on publicly available resources of varying quality. Popular use of cryptocurrencies includes investment and speculation on price developments of currencies and assets. However, the goal of this paper is to describe technical aspects relevant for TAST. Economic considerations or future price developments are therefore not discussed. Technologies are described from a purely technical point of view. Therefore, the contents of this paper do not constitute advice, information, predictions, or recommendations for investment.


## Acknowledgment

The work presented in this paper has received funding from Pantos GmbH within the TAST research project.

## References


[1] *Altcoin.io - Decentralized Exchange*. URL: https://preview.altcoin.io/lite-paper.pdf. White Paper. Accessed 2018-04-20.

[2] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. *Enabling blockchain innovations with pegged sidechains*. 2014. URL: http://kevinriggen.com/files/sidechains.pdf. White Paper. Accessed 2018-05-17.

[3] M. Bartoletti and L. Pompianu. "An analysis of Bitcoin OP_RETURN metadata". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2017, pp. 218–230.

[4] C. Beams. *Bisq - The peer-to-peer bitcoin exchange*. URL: https://github.com/bisq-network/bisq-docs/blob/master/exchange/whitepaper.adoc. White Paper. Accessed 2018-04-19.

[5] M. Beck. *Into the Ether with Ethereum Classic*. 2017. URL: https://ethereumclassic.github.io/assets/etc-thesis.pdf. White Paper. Accessed 2018-04-13.

[6] *Bitcoin Wiki: Colored Coins*. URL: https://en.bitcoin.it/wiki/Colored_Coins. Website. Accessed 2018-04-13.

[7] V. Buterin. *Ripple is Officially Open Source*. 2013. URL: https://bitcoinmagazine.com/articles/ripple-is-officially-open-source-1380246874/. Accessed 2018-04-13.

[8] V. Buterin and V. Griffith. *Casper the Friendly Finality Gadget*. 2017. URL: http://arxiv.org/abs/1710.09437. White Paper.

[9] *Cardano Roadmap*. URL: https://cardanoroadmap.com/. Website. Accessed 2018-04-13.

[10] *Catapult*. URL: https://github.com/catapult-project/catapult. GitHub Repository. Accessed 2018-06-01.

[11] *Codius - Open-Source Hosting Platform for Smart Programs*. URL: https://codius.org. Website. Accessed 2018-04-19.

[12] *ColoredCoins.org*. URL: http://coloredcoins.org/. Website. Accessed 2018-04-13.

[13] B. Colwell. *Cardano: The HOT New Crypto That Accepts Its Social Nature*. 2017. URL: https://briandcolwell.com/2017/10/cardano-the-hot-new-crypto-that-accepts-its-social-nature/.html. Website. Version 2017-10-05. Accessed 2018-04-19.

[14] Counterparty. *Counterparty*. URL: https://counterparty.io/docs/. Website. Accessed 2018-04-13.

[15] Counterparty. *Counterparty Protocol Specification*. 2017. URL: https://github.com/CounterpartyXCP/Documentation/blob/master/Developers/protocol_specification.md. White Paper. Accessed 2018-04-13.

[16] E. Duffield and D. Diaz. *Dash: A Privacy-Centric Crypto-Currency*. 2015. URL: https://github.com/dashpay/dash/wiki/Whitepaper. 2018 Revision. Accessed 2018-04-13.

[17] *EPOBC*. 2015. URL: https://github.com/chromaway/ngcccbase/wiki/EPOBC_simple. Website. Accessed 2018-04-13.

[18] *EtherDelta*. URL: https://etherdelta.com/#PPT-ETH. Website. Accessed 2018-04-20.

[19] C. Flanagan and S. Qadeer. "A Type and Effect System for Atomicity". In: *SIGPLAN Not.* 38.5 (2003), pp. 338–349. ISSN: 0362-1340.

[20] M. Herlihy. *Atomic Cross-Chain Swaps*. 2018. URL: http://arxiv.org/abs/1801.09515. White Paper. Accessed 2018-04-13.

[21] Y. Hirai. "Defining the ethereum virtual machine for interactive theorem provers". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2017, pp. 520–535.

[22] *IDEX - Decentralized Ethereum Asset Exchange*. URL: https://idex.market/. Website. Accessed 2018-04-20.

[23] *Ignis - The First Child Chain*. URL: https://www.ardorplatform.org/ignis%5C%E2%5C%80%5C%94first-childchain. Website. Accessed 2018-04-20.

[24] *Internet of Coins: Hybrid Assets for Peer-to-Peer Intersystemic Value Transfer*. 2014. URL: https://internetofcoins.org/whitepaper_ioc.pdf. White Paper. Version 1.0, 2015-12-15. Accessed 2018-04-19.

[25] *Internet of Coins — Open and decentralized cryptocurrency platform*. URL: https://www.internetofcoins.org/. Website. Accessed 2018-04-20.

[26] *Jelurida Whitepaper*. URL: https://www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf. White Paper. Accessed 2018-04-20.

[27] A. Kiayias, A. Russell, B. David, and R. Oliynykov. "Ouroboros: A provably secure proof-of-stake blockchain protocol". In: *Annual International Cryptology Conference*. Springer. 2017, pp. 357–388.

[28] *Komodo An Advanced Blockchain Technology, Focused on Freedom*. 2018. URL: https://komodoplatform.com/wp-content/uploads/2018/03/2018-03-12-Komodo-White-Paper-Full.pdf. White Paper. Version 2018-03-12. Accessed 2018-04-13.

[29] G. Kostarev. *Waves roundup for 2017*. 2017. URL: https://blog.wavesplatform.com/waves-roundup-for-2017-d48905d6adf8. Blog. Version 2017-12-28. Accessed 2018-04-13.

[30] A. Lemble. *ERC827 Token Standard (ERC20 Extension)*. 2018. URL: https://github.com/ethereum/EIPs/issues/827. GitHub Issue. Accessed 2018-04-13.

[31] S. D. Lerner. *RSK: Bitcoin powered Smart Contracts*. 2015. URL: https://bravenewcoin.com/assets/Whitepapers/RootstockWhitePaperv9-Overview.pdf. White Paper. Revision 9, 2015-11-19. Accessed 2018-04-19.

[32] *Lisk Documentation*. URL: https://lisk.io/documentation. Website. Accessed 2018-04-19.

[33] *Litecoin*. URL: https://litecoin.org/. Website. Accessed 2018-04-13.

[34] L. Luu and Y. Velner. *KyberNetwork: A trustless decentralized exchange and payment service*. 2017. URL: https://home.kyber.network/assets/KyberNetworkWhitepaper.pdf. White Paper. Version 0.8, 2017-08-27. Accessed 2018-04-19.

[35] D. Mazières. *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*. URL: https://www.stellar.org/papers/stellar-consensus-protocol.pdf. White Paper. Accessed 2018-04-13.

[36] *Metronome: Owner's Manual*. URL: https://www.metronome.io/pdf/owners_manual.pdf. White Paper. Version 0.967, 2018-04-17. Accessed 2018-04-19.

[37] S. Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2008. White Paper.

[38] *NEM: Technical Reference*. 2018. URL: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf. White Paper. Version 1.2.1, 2018-02-23. Accessed 2018-04-19.

[39] *NEO White Paper*. URL: https://github.com/neo-project/docs/blob/master/en-us/index.md. White Paper. Accessed 2018-04-13.

[40] Nxt Community. *Nxt Whitepaper*. 2014. URL: https://www.dropbox.com/s/cbuwrorf672c0yy/NxtWhitepaper_v122_rev4.pdf. White Paper. Revision 4, Version 1.2.2. Accessed 2018-04-13.

[41] *OpenAssets*. URL: https://github.com/OpenAssets. Website. Accessed 2018-04-13.

[42] *Phase Zero: A Plan for Bootstrapping the Bisq DAO*. URL: https://docs.bisq.network/dao/phase-zero.html. White Paper. Accessed 2018-04-19.

[43] S. Popov. *The Tangle*. 2017. URL: https://iota.org/IOTA_Whitepaper.pdf. White Paper. Version 1.3. Accessed 2018-04-13.

[44] C. Prybila, S. Schulte, C. Hochreiner, and I. Weber. "Runtime verification for business processes utilizing the Bitcoin blockchain". In: *Future Generation Computer Systems* (2017).

[45] M. Rosenfeld. *Overview of Colored Coins*. 2012. URL: https://bitcoil.co.il/BitcoinX.pdf. White Paper. Accessed 2018-04-13.

[46] N. van Saberhagen. *Cryptonote v 2.0*. 2013. URL: https://cryptonote.org/whitepaper.pdf. White Paper. Accessed 2018-04-13.

[47] F. Schuh and D. Larimer. *BitShares 2.0: Financial Smart Contract Platform*. 2015. URL: https://www.weusecoins.com/assets/pdf/library/Bitshares%5C%20Financial%5C%20Platform.pdf. White Paper. Accessed 2018-04-19.

[48] D. Schwartz, N. Youngs, and A. Britto. *The Ripple Protocol Consensus Algorithm*. 2014. URL: https://ripple.com/files/ripple_consensus_whitepaper.pdf. White Paper.

[49] A. Shamir. "How to share a secret". In: *Communications of the ACM* 22.11 (1979), pp. 612–613.

[50] M. Swan. *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 2015.

[51] R. H. Thaler. "Anomalies: Saving, fungibility, and mental accounts". In: *Journal of economic perspectives* 4.1 (1990), pp. 193–205.

[52] F. Tschorsch and B. Scheuermann. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies". In: *IEEE Communications Surveys Tutorials* 18.3 (2016), pp. 2084–2123. ISSN: 1553-877X.

[53] *Using secret lock transaction for atomic cross-chain swap*. URL: https://nemtech.github.io/guides/transaction/using-secret-lock-transaction-for-atomic-cross-chain-swap.html. Website. Accessed 2018-06-01.

[54] F. Vogelsteller. *Token standard*. 2015. URL: https://github.com/ethereum/EIPs/issues/20. GitHub Issue. Accessed 2018-04-13.

[55] F. Vogelsteller and V. Buterin. *ERC-20 Token Standard*. 2015. URL: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md. GitHub Site. Accessed 2018-04-13.

[56] W. Warren and A. Bandeali. *0x: An open protocol for decentralized exchange on the Ethereum blockchain*. URL: https://0xproject.com/pdfs/0x_white_paper.pdf. White Paper. Accessed 2018-04-19.

[57] WAVES Platform. *WAVES Whitepaper*. 2016. URL: https://wesdewayne.files.wordpress.com/2017/05/waves-whitepaper.pdf. White Paper. Accessed 2018-04-13.

[58] *Waves Smart Contracts*. 2018. URL: https://wavesplatform.com/files/docs/white_paper_waves_smart_contracts.pdf. White Paper. Version 2018-04-03. Accessed 2018-04-26.

[59] *Waves Smart Contracts. What to Expect and When*. 2018. URL: https://blog.wavesplatform.com/waves-smart-contracts-what-to-expect-and-when-489563a95ca3. Blog. Version 2018-04-18. Accessed 2018-04-26.

[60] J. Willett, M. Hidskes, D. Johnston, R. Gross, and M. Schneider. *Omni Protocol Specification*. 2017. URL: https://github.com/OmniLayer/spec. Version 0.5. Accessed 2018-04-13.

[61] L. Wong. *NEM Catapult*. 2016. URL: https://nem.io/wp-content/themes/nem/files/catapultwhitepaper.pdf. White Paper. Accessed 2018-04-26.

[62] G. Wood. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. 2018. URL: https://ethereum.github.io/yellowpaper/paper.pdf. White Paper. Accessed 2018-04-13.

[63] T. Zhang and L. Wang. *Republic Protocol: A decentralized dark pool exchange providing atomic swaps for Ethereum-based assets and Bitcoin.* URL: https://releases.republicprotocol.com/whitepaper/1.0.0/whitepaper_1.0.0.pdf. White Paper. Version 2017-12-18. Accessed 2018-04-20.

[64] A. Zohar. "Bitcoin: under the hood". In: *Communications of the ACM* 58.9 (2015), pp. 104–113.