AtoX Whitepaper

December 12, 2018

Contents

Abstract

Current, truly decentralized exchanges suffer from slow transaction speed and/or poor scalability. Scalable solutions have been constructed, but usually pay the price of either a limited amount of trade-pairs available or centralized modules like a centralized order book, which is susceptible to manipulation. We present an architecture for a truly decentralized cryptocurrency exchange without the above-mentioned drawbacks. At its core, we utilize cross-lightning-transactions, a process enabling parties to exchange value across almost arbitrary blockchains with the scalability of the lightning network, as well as exchange-rate determination via an off-chain order-book stored on IPFS. Taking ecological impact into consideration, we employ an energy-efficient consensus mechanism while mitigating graph-theoretical issues by design.

1 Introduction

This paper intends to provide an overview of the AtoX blockchain architecture and the functionality of its corresponding AXC currency. Section 2 covers a theoretical background laying the foundations of our language used to describe transaction scripts in section 3 and cross-lightning Transactions in section 4. Section 5 describes the functionality of the order book. Section 6 describes the different types of nodes creating the cross-lightning network and section 7 explains the contruction of block rewards.

Previous Work. In 2013, Tiernan proposed an atomic cross-chain swap protocol via Hashed Timelock Contracts [1]. However, the protocol could not be implemented up until recently, when the activation of the Segragated Witness Consensus layer (SegWit) in 2017 [2] fixed transaction malleability. SegWit

also enabled Poon's and Dryja's Lighning Network [3] to operate safely on the Bitcoin blockchain [4]. The InterPlanetary File System (IPFS), a distributed file system with build-in version control enabled efficient storage of data on blockchains via content-addressed hyper links [5].

Part I

Technical Underlyings

2 Basics

From a technical point of view, the AtoX Blockchain can be thought of as a labeled state transition system whose states are recorded on a public ledger. The explanation below should be taken with a grain of salt as some details have been left out in order to keep matters concise.

2.1 Keys and signatures

We will use the classical, well known Elliptic Curve Digital Signature Algorithm (ECDSA) defined by [6] with the Secp256k1 parameters proposed in [7] which have been used extensively by major blockchain architectures such as Bitcoin and Ethereum. A **private key** is an integer $d \in [1, n-1]$, where n is mandated by the Secp256k1 standard. A public key is generated from this private key. We denote the **public key generation function** as

$$PK : [1, n-1] \to \mathbf{Z},$$

so that **public keys** are of the form

$$Q := PK(d).$$

An address is generated from this public key, but since generation of that address can be seen as a well defined mapping we will simplify and assume the address to equal the public key for explanatory purposes.

2.2 Transactions

Inspired by the Bitcoin transaction architecture and the fact that most cryptocurrencies have at least the same functionality (if not more), we construct our transactions as follows.

Let $v, l \in \mathbf{N}_0$. We call v the **version number** and l the **TimeLock**. The version number will show which transaction standard the transaction will satisfy. This makes it possible to introduce new standards for transactions while keeping old standards backwards-compatible. The usage of TimeLocks will be explained in detail in a later chapter. An **input** is a tuple

$$inp = (PrTX, ind, ScrSig),$$

where we call $PrTX$ **previous transaction reference**, ind **output index** and $ScrSig$ **Signature script**. Let $1 \leq n \in \mathbf{N}$. A **list of inputs** is an n-tuple $I = I_{1 \leq i \leq n}$, where I_i is an input for all $1 \leq i \leq n$. An **output** is a tuple

$$out = (PKS, amt),$$

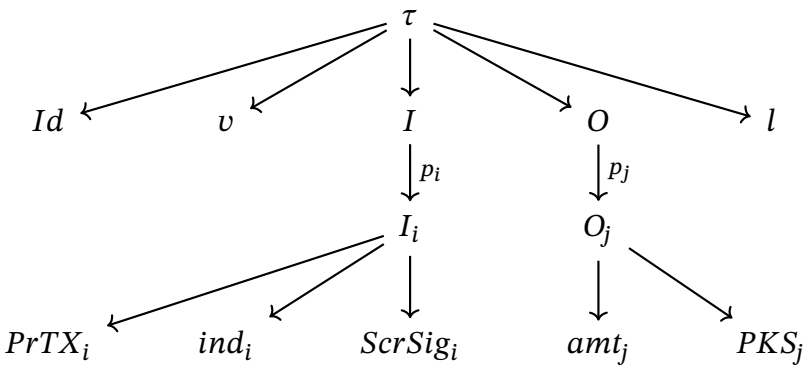
where we call PKS **PubKey script** and amt **amount**. Let $1 \leq m \in \mathbf{N}$. A **list of outputs** is defined as an m-tuple $O = O_{1 \leq j \leq m}$, where each O_i is an output. We can now describe a **transaction** τ as a 5-tuple

$$\tau = (Id, v, I, O, l),$$

where

$$Id = H(v, I, O, l)$$

denotes the image of an injective **TXID generation function** H, which denotes a cryptographic hash function. A visualization is given below. We use the notation p_i for the projection on the i-th component.



We define the **set of inputs in** τ as

$$Ins_\tau := \{x_{1\leq i\leq 3} | x_i = p_i(p_j(p_3(\tau))), 1 \leq j \leq n_\tau\}.$$

Note, how each element of Ins_τ is an input as defined above. The **set of outputs in** τ is

$$Outs_\tau := \{y_{1\leq i\leq 2} | y_i = p_i(p_j(p_4(\tau))), 1 \leq j \leq m_\tau\}.$$

Again, the elements of $Outs_\tau$ consists of outputs as described above. We write

$$\Lambda := \{\tau | \tau \text{ is a transaction}\}$$

for the **space of transactions**. Let $SCRSIG$ denote the space of all possible script signatures. Then a PKS is a binary function, i.e.

$$PKS : SCRSIG \to \{0, 1\}.$$

We will later use these binary functions extensively to specify various useful transactions in section 3.

2.3 The labeled state transition system

We can now construct a labeled state transition system $(S, \Lambda, \rightarrow)$ defined by the following properties:

1. S is a set of states, where each state $s \in S$ is a finite set of tuples (Id, O), where Id is a TXID and O a list of outputs.

2. Λ is a space of transactions.

3. $\rightarrow \subseteq S \times \Lambda \times S$ is a set of labeled state transition functions. The exact set for our construction is given by

   $\rightarrow := \{(p, \tau, q) \in S \times \Lambda \times S |\ (p, \tau, q)$ satisfies the three conditions below.$\}$.

   (i) There exists a (finite) subset $U \subseteq p$ such that there exists a 1-1 map $f : U \rightarrow Ins_\tau$ satisfying

   $$p_1(u) = p_1(f(u))$$
   $$p_2(u) = p_{p_2(f(u))}(p_3(H^{-1}(p_1(u))))$$

   for all $u \in U$. In other words, the references in τ all reference to elements in p.

   (ii) The equation

   $$(p_2(p_2(u)))(p_3(f(u))) = 1$$

   holds for all $u \in U$, i.e. the input script signatures must lie in $p_2(p_2(u))^{-1}(1)$.

   (iii) The inequality

   $$\sum_{u \in U} p_1(p_2(u)) \geq \sum_{1 \leq i \leq m_\tau} p_1(p_i(p_4(\tau)))$$

   holds, i.e. the total amount of the output amounts in τ must be smaller than the total amount of the outputs in U.

(iv) The equation

$$q = (p \setminus U) \cup \{(Id, O_j) | Id = Id_\tau, O_j \in Outs_\tau$$

holds, i.e. the elements of p which get referenced to in Ins_τ are substituted by tuples corresponding to the outputs of τ.

We will use the notation $p \xrightarrow{\tau} q \coloneqq (p, \tau, q) \in \rightarrow$ for elements of this set.

3 Scripts

We will now construct different *ScrSig*s and *PKS* functions. For a labeled state transition function $p \xrightarrow{\tau} q \in \rightarrow$ the input scripts in $p_3(Ins_\tau)$ must lie in the *PKS* preimage of 1. Since these input scripts and the *PKS* functions are defined by code, we can construct useful protocols. The following examples are written in Bitcoin Script. However, since Bitcoin scripts essentially represent a subset of scripts written in Solidity (Ethereums script language), every statement holds for Solidity scripts as well.

3.1 Multisignature contracts

A let $1 \leq n, m \in \mathbf{N}$. An *n-m-multisignature contract* or *n-m-***multisig** is an output with a PKS of the form

$$PKS(y) = \begin{cases} 1, & \text{if } n \text{ out of } m \text{ signatures are valid,} \\ 0, & \text{else.} \end{cases}$$

A 2-2-multisig *PKS* can be created as follows:

```
2
< Q_1 >
```

```
< Q_2 >
2
OP_CHECKMULTISIG
```

with a corresponding *ScrSig* (in another transaction referencing the output which contains PKS above) like this:

```
OP_0
< sgn_Q_1 >
< sgn_Q_2 >
```

3.2 HashLocked contracts

A *HashLocked contract* or *HLC* is an output with a PKS of the form

$$PKS(y) = \begin{cases} 1, & \text{if } H(y) = H(x), \\ 0, & \text{else,} \end{cases}$$

where H denotes a cryptographic hash function. An example of a HashLocked contract *PKS* in the Bitcoin script language looks like this:

```
[HASHOP]
< H(x) >
OP_EQUAL
```

Here `[HASHOP]` is either `OP_SHA256` or `OP_HASH160`. The corresponding *ScrSig* would be a one-liner:

```
< x >
```

3.3 Hashed TimeLock contracts

A **Hashed TimeLock contract** or **HTLC** is a transaction τ with a non-zero lock time, i.e. $l_\tau \geq 0$, and a PKS in at least one output of the form

$$PKS(y) = \begin{cases} 1, & \text{if } H(y) = H(x) \text{ and the locktime expired,} \\ 0, & \text{else,} \end{cases}$$

where H denotes a cryptographic hash function. A HTLC in Bitcoin script could look like this:

```
OP_IF
[HASHOP]
<digest>
OP_EQUALVERIFY
OP_DUP
OP_HASH160
<seller pubkey hash>
OP_ELSE
<num>
[TIMEOUTOP]
OP_DROP
OP_DUP
OP_HASH160
<buyer pubkey hash>
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```

Here `[TIMEOUTOP]` is either

`OP_CHECKSEQUENCEVERIFY` or `OP_CHECKLOCKTIMEVERIFY`.

4 Cross-lightning transactions

One of the core features of the AtoX blockchain are cross-lightning transactions. In order to explain these, we will first talk about atomic cross-chain transactions and the lightning network.

4.1 Atomic cross-chain swaps

An **atomic cross-chain swap** or **ACCS** is a protocol designed to enable an exchange of value between two different blockchains. The specific protocol we use was first described by Noel Tiernan [1].

Let $(S, \Lambda, \rightarrow)$ and $(S', \Lambda', \rightarrow')$ be to different blockchains. Two parties P_1 and P_2 wishing to exchange $0 \leq n \in \mathbf{N}$ coins on the first blockchain to $0 \leq m \in \mathbf{N}$ coins on the second blockchain generate two transactions each on their respective blockchain, i.e P_1 generates $\tau_1, \tau_2 \in \Lambda$ and P_2 generates $\tau_3', \tau_4' \in \Lambda'$ of the structure below. Let $0 \leq 2c \in \mathbf{N}$ and $x \in \mathbf{Z}$ a secret random integer,

generated by P_1. Ids and versions are left out and we also ignore fees:

$$
\begin{aligned}
I_{\tau_1} &= \text{wherever } P_1 \text{ got his coins from} \\
O_{\tau_1} &= (n, (sgn_{P_2}, x || sgn_{P_1}, sgn_{P_2})) \\
l_{\tau_1} &= 0 \\
I_{\tau_2} &= ((Id_{\tau_1}, 0, (sgn_{P_1}, sgn_{P_2}))) \\
O_{\tau_2} &= (n, sgn_{P_1}) \\
l_{\tau_2} &= 2c \\
I_{\tau_3} &= \text{wherever } P_2 \text{ got his coins from} \\
O_{\tau_3} &= (m, (sgn_{P_1}, x || sgn_{P_1}, sgn_{P_2})) \\
l_{\tau_3} &= 0 \\
I_{\tau_4} &= ((Id_{\tau_3}, 0, (sgn_{P_1}, sgn_{P_2}))) \\
O_{\tau_4} &= (m, sgn_{P_2}) \\
l_{\tau_4} &= c
\end{aligned}
$$

Note, that τ_2 and τ_4 need to be exchanged between parties, so that the inputs contain the necessary signatures. Then τ_1 and τ_3 are submitted to their respective blockchains. If P_1 reveals x to generate a transaction claiming the output of τ_3, P_2 can do the same with τ_1. Otherwise, parties can reclaim their funds by pushing τ_2 and τ_4, respectively. Example code for the τ_1 output script:

```
OP_IF
// Refund for Q_1
2 < Q_1 > < Q_2 > 2 OP_CHECKMULTISIGVERIFY
OP_ELSE
// Ordinary claim for Q_2
OP_HASH160 < H(x) > OP_EQUAL < Q_2 > OP_CHECKSIGVERIFY
OP_ENDIF
```

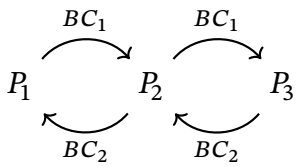
The code for the τ_2 refund transaction is a 2-2-multisig input script, with the output mapping to P_1s address.

4.2 Lightning channels

The specifics of the lightning network implementation can be found in [8]. The concept is described in Poon's and Dryja's paper [3]. In short, two parties open a so called lightning channel which freezes an amount of value on a blockchain. The parties now generate off-chain transactions to redefine their shares of the frozen amount. Although a mutual closure of the channel is cheaper, a one-sided closure is possible as well. Channels can be chained together via HTLCs, allowing almost instant transaction speed.

4.3 Cross-lightning swaps

By issuing atomic swaps in off-chain lightning channels it becomes possible to exchange value across lightning networks on different blockchains. This lets the cross-lightning network operate at speeds comparable to centralized exchanges without users having to trust a third party. A schematic visualization is given below with three parties P_1, P_2 and P_3, with P_1 and P_2 being connected via two channels in two lightning networks on two different blockchains, and P_2 and P_3 being connected via two channels on the same two lightning networks.



5 The order book

We utilize a decentralized, off-chain order book built on top of IPFS, which is a P2P system for retrieving and sharing IPFS objects. IPFS employs a Merkle DAG system to ensure all permanently stored data is unique and tamper-proof.

5.1 IPFS

An *IPFS object* can be seen as a tuple (d, l), where d represents a **blob of unstructured binary data** ($\leq$ 256 kb) and l an **array of link structures**. The link structures are 3-tuples of the form (N, H, S), where N denotes the **name of the link**, H the **hash of the linked IPFS object** and S the **size of the linked IPFS object**. Supernodes store three files for every exchange pair, which will be updated continuously.

1. A file containing the order book; only Valid orders (described below) will be written to the order book, partially executed orders will be updated and executed orders will be deleted.

2. A file containing successful orders, which will be overwritten continuously; this is needed to calculate exchange rates. Because IPFS tracks versions over time just like a Git repository, the old exchange rates can be extracted, making it possible to display a graph of historical exchange rates.

3. A file containing a list of lightning nodes currently active in the cross-lightning network.

If a party P_1 pushes an order wishing to exchange $0 \geq c \in \mathbf{Q}$ coins on blockchain A to coins on blockchain B to the order book, the following steps will run (in the order given below):

```
Test, if P_1 is connected to a registered BC_A lightning node
Test, if P_1 is connected to a registered BC_B lightning node
Test, if P_1 is connected to a registered AtoX lightning node
Test, if P_1 has at least m coins on BC_A
Test, if P_1 paid its order book fees
```

Snapshots of the orderbook are stored on the AtoX blockchain.

6 Types of nodes

We differentiate between four types of parties within the cross-lightning swap network, namely users, regular nodes, entitled regular nodes and supernodes.

We will first give an overview of the piece of software commonly known as 'multiwallet' (which we provide in the form of the AtoX Swap App) and then explain the roles of the aforementioned parties.

6.1 Multiwallets

A **wallet** is a piece of software implementing the deterministic functions mapping private keys of a cryptocurrency to their corresponding public keys and addresses. Using these functions a wallet may, given a specific private key, reconstruct the corresponding address and conveniently display the amounts of funds available to that address to the individual in possession of the private key by adding the amounts of transaction outputs which have not yet been spent. A wallet may also reconstruct the payment history of that address stored on the blockchain.

While the opening and closing transactions of lightning channel setups are stored on their respective blockchains, the off-chain rebalancing contracts are

not. This means if an individual loses its off-chain transaction history of a still opened lightning channel (e.g. because of corruption of the physical device storing that information) the funds in that lightning channel are frozen until the other party one-sidedly closes the channel. If both parties lose their off-chain history, the funds will be lost forever. Therefore individuals are encouraged to only connect to parties trusted to have proper safety measures in the form of e.g. physical data backup.

A **multiwallet** is a collection of multiple wallets together with the ability to issue cross lightning transactions, which make it possible to swap value connected to the addresses in the sub-wallets. A multiwallet gives an individual information about 'all their manageable available in one place'. For conservative individuals, a multiwallet together with cross-lightning swaps may give the experience of more of a currency 'exchange', rather than a 'stock trade'. For the adventurous individual a multiwallet may provide the experience of a trading platform by displaying historical exchange rates and other metrics of interest.

On the surface our multiwallet does not seem different from other multiwallets. However, since the exchanges between currencies within our multiwallet are not executed by a centralized exchange our approach is significantly more secure for the end user: All private keys stay in the hand of the user and there are no 'hackable' exchange servers. The only way a malicious party might obtain an individual's funds is by getting hold of their private keys, which could be compared to someone stealing a PIN in terms of a traditional banking context.

Users of the official multiwallet will pay 0.2 percent of each transaction's value in AXC to the cross lightning network.

6.2 Users

A **user** is a party able to issue transactions to the cross-lightning network. A user may be a person interacting with the cross-lightning network via a multi-wallet app (such as the AtoX Swap App) on a smartphone. A user may also be an instance of a trading algorithm connected to the cross lightning network, automatically executing trades by issuing cross-lightning transactions.

6.3 Regular nodes

A **regular node** is a physical device acting as an entry point to the cross-lightning network for users. A regular node does not need significant amounts of computing power since we do not utilize a proof-of-work (POW) concept. However, a regular node should still have access to a strong, stable internet connection as it will be utilized as a vertice in the cross-lightning network and as such be expected to be up and running continuously, acting as middleman for cross-lightning swaps. Regular nodes are expected to be continuously connected to at least one supernode, a concept which will be explained in the next paragraph. Regular nodes will be rewarded for acting as infrastructure in two ways:

1. Transaction fees from lightning transactions: These fees can be set arbitrarily high (or, more likely, low) by the regular node itself. Since lightning networks choose the 'path of least resistance' between two parties wishing to exchange value, an equilibrium of reasonable transaction fees is ensured. In other words, if a regular node sets its transaction fees too high, it will not be used as middleman for lightning transactions, not earning any profit at all. On the other hand, a lower bound for transaction fees is also guaranteed, mandated by the costs of running the node

(e.g. networking costs and electricity). Note how, since a regular node is expected to run minimal hardware configuration, electricity costs and ecological impact are multiple orders of magnitude lower than they are for comparable POW based approaches - with the added benefit of unmatchably low transaction fees.

2. Shares of the block rewards are obtained from the supernodes the regular node is connected to. The amount of those shares may be specified by the supernodes themselves. Similarly to the equilibrium of transaction fees, an equilibrium of block share amounts will settle, as regular nodes will be most likely to connect to the supernodes rewarding the highest share amounts. The importance of being conected to as many regular nodes as possible will be elaborated in the next section.

6.4 Entitled regular nodes

Entitled regular nodes are regular nodes with the additional right to be elected as a supernode. We implement this security measure against parties trying to set up malicious subnetworks within the cross-lightning network. Entitled regular nodes will be selected from regular nodes with the best track record holding at least 10000 AXC. Their absolute number is limited to 70.

6.5 Supernodes

A **supernode** is a physical device which, in addition to acting as a regular node, must verify the integrity of new transactions within the AtoX blockchain. The number of supernodes in the cross-lightning network will be limited to 35. A supernode gets rewarded for its work similarly to regular nodes:

1. Via transaction fees, just like regular nodes and entitled regular nodes.

2. Via block rewards. A supernode proposes the next snapshot of the public AtoX ledger (i.e. it proposes the next block to be appended to the AtoX blockchain). If the block gets accepted by the other supernodes, it will be written to the ledger and the generating supernode will be rewarded in the form of AXC coins. The supernode shares this reward with the regular nodes connected to it. The probability for creating the next block is given by the percentual amount of the cross-lightning network the supernode manages by taking into account all regular nodes and their processed transactions that supernode is connected to.

7 Block rewards

The block reward comes from two sources.

1. A fixed amount per block. This brings new coins into circulation.

2. The transaction fees in AXC coins contained in the processed cross-lightning transactions. This encourages supernodes to prioritize transactions with higher transaction fees in a natural way.

Note that while our 'replacement' for the classical harshly criticized POW mining vastly differs from the original model, the block reward system does not as it has already been well tested, well working and shown to achieve desirable results. This approach also implies that transaction fees paid in AXC will be distributed among transaction processing nodes.

7.1 RPCA

Many cryptocurrencies use a **proof of work** or **POW** consensus mechanism. This approach artificially increases the computing power necessary to generate

a new block by constraining the set of allowed values of block header hashes. POW wastes horrendous amounts of power (see e.g. [9] and fig. 1 this can be visualised with data from [10]). The usual alternative, a **proof of stake POS** mechanism; however, it has been criticised for two reasons. First, voting on a particular version of a proof of stake blockchain requires no resources and therefore has no opportunity cost. This means rational miners should simply mine on every competing branch they see, so as to maximize the amount of mining returns they get. Second, there is a problem of 'weak subjectivity.' This is the notion that a node that comes online for the first time will have to ask a trusted source what the hash of the valid chain is. This completely undermines the trustless nature of blockchains, something many view as the 'killer app' of blockchain technology. All proof of stake blockchains have this issue.

Our approach is, thus designed to be similar to an **RPCA** consensus mechanism. It's not considered a proof of work or a proof of state, but instead it is centered around a "voting" mechanism among trusted nodes on a network. RPCA is applied every few seconds by all nodes, in order to maintain the correctness and agreement of the network. Once consensus is reached, the current ledger is considered "closed" and becomes the last-closed ledger. Assuming that the consensus algorithm is successful, and that there is no fork in the network, the last-closed ledger maintained by all nodes in the network will be identical. This means that constant mining is not necessary, and RPCA is by far the most energy-efficient method of achieving transaction confirmations, more so than proof of power or proof of stake.

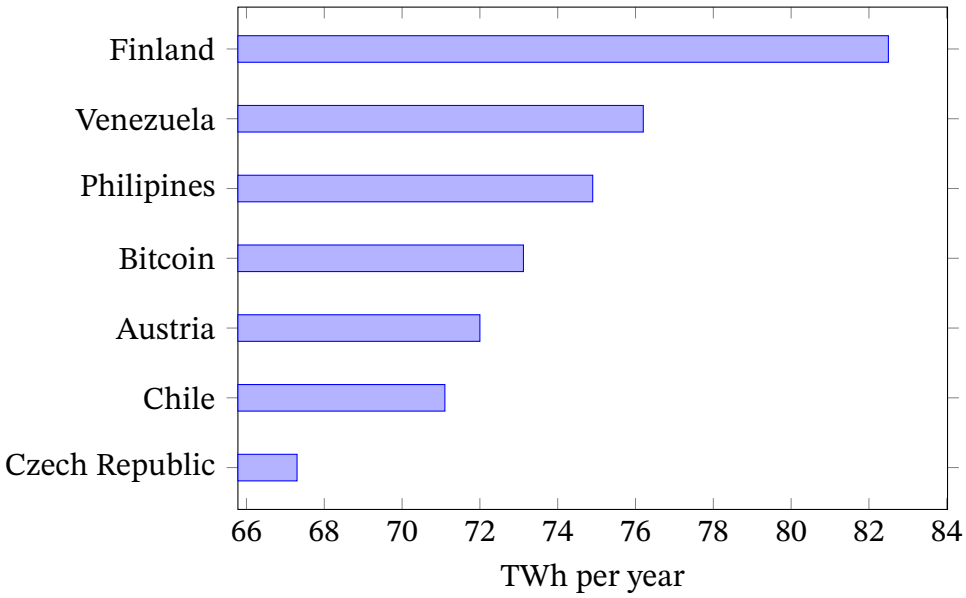


Figure 1: Estimated Bitcoin energy consumption in 2018.

Part II

Information for investors

This part of the paper provides information addressed at potential investors and individuals considering to set up AtoX Nodes.

8 Distribution of AXC

Although sometimes critizised as 'impure', the AtoX blockchain implements a larger-than-usual initial block reward amounting to 10 percent of the total amount of AXC to be created. This approach was chosen to quickly distribute AXC among as many parties as possible. In other words, a significant amount of individuals will be able to use AXC from the first block on. The absolute

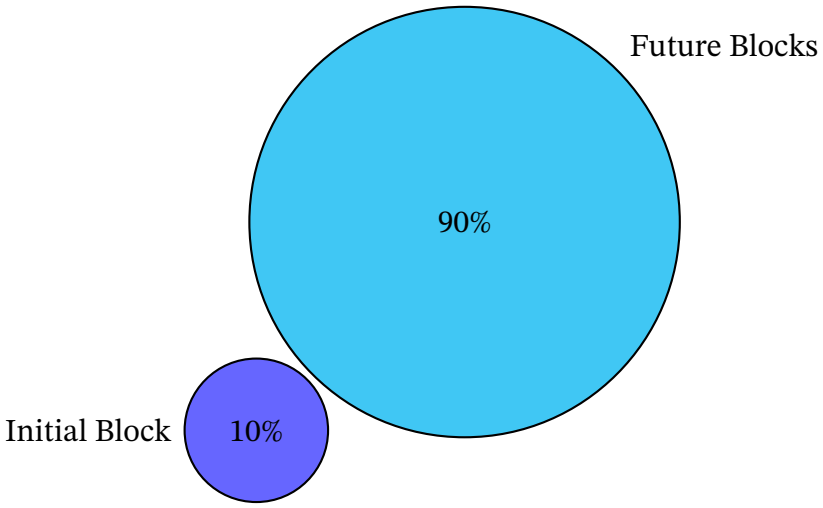


Figure 2: First block reward in relation to the rest of block rewards.

amount of AXC is hard-capped to 2×10^{11}. The initial block reward will be split as shown in fig. 3. Investors are able to invest into the initial AtoX node

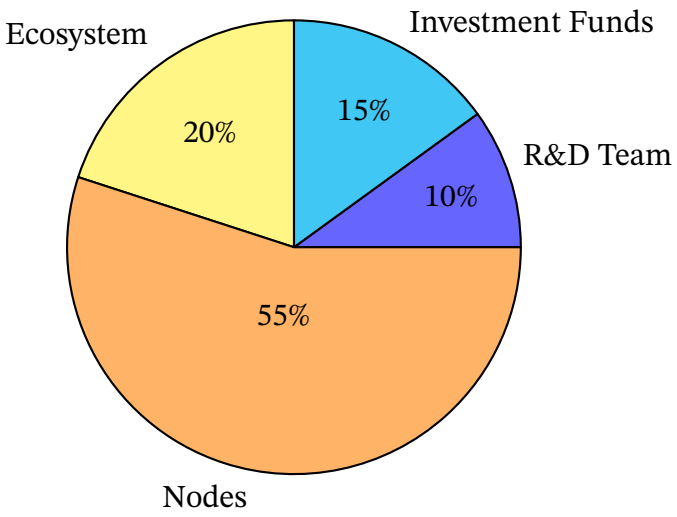


Figure 3: Distribution of the first block reward.

infrastructure amounting to 55% of the initial block reward. The initial block reward cannot be spent for 24 months to protect investors and the creators of the AtoX blockchain equally. The daily return on investments r, given an amount of AXC c, is set as

$$r(c) \coloneqq c \cdot d(c),$$

where d is defined as

$$d(c) \coloneqq 2c \times 10^{-9} + \begin{cases} 0 & \text{if } c < 2.5 \times 10^7, \\ 0.2 \times 10^{-2} & \text{if } 2.5 \times 10^7 \leq c < 5 \times 10^7, \\ 0.225 \times 10^{-2} & \text{if } 5 \times 10^7 \leq c < 1 \times 10^8, \\ 0.25 \times 10^{-2} & \text{else.} \end{cases}$$

Daily returns will decrease by 5% per month from the 11th month after the initial investment and will stop entirely after 2 years. Figure 4 summarizes the baseline annual return $c + r(c) \cdot 365$ (linear scaling, since only frozen AXC generate returns) for initial investments above 5×10^5 AXC. Additionally, the annual return on the initial investment increases by 0.5% (max 15%) per referred

customer of the AtoX Swap multiwallet, and by 1% (max 15%) per 1 Million AXC invested by referred customers. Absolute rewards in the form of 5% of first transaction AXC fees paid by referred customers, as well as 99 AXC for referred customers with account values of over 100$ are implemented. Table 1 summarizes the reward system.

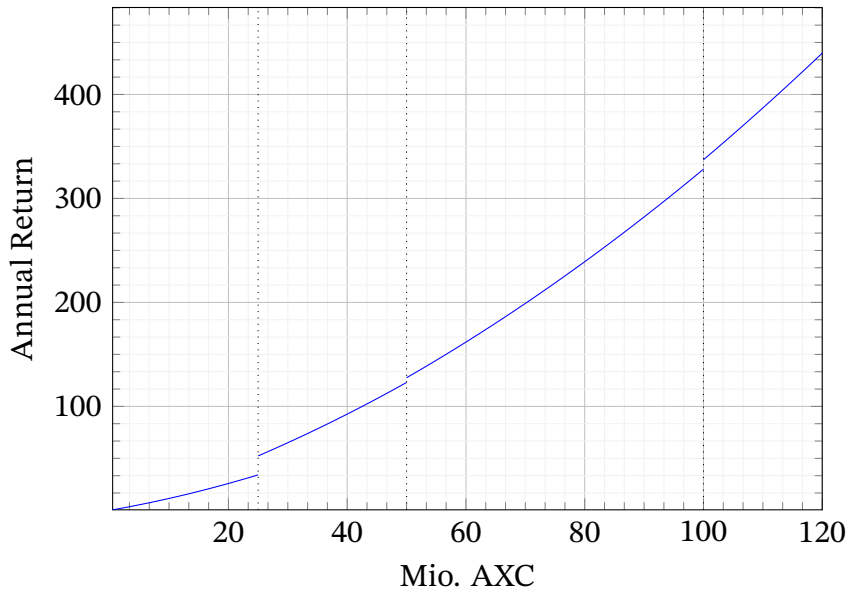


Figure 4: Baseline annual return on initial investments of at least 5×10^5 AXC. Referral rewards and dampening excluded.

AXC issue price at $0.02		
AXC in Mio.	Bonus AXC in Mio	**Daily** return
100	15	0.25%
50	5	0.225%
25	1.25	0.2%
0.5-25	0	0%
+ 0.002% **daily** return per 0.5 Mio. AXC invested		
+ 0.5% **annual** return per customer referral, max. 15%		
+ 1% **annual** return per 1 Mio. AXC invested by ref. customer, max. 15%		
+ 5% **one-time** reward of first transaction fees paid by ref. customer		
+ 99 AXC **one-time** per ref. customers with acc. value of over 100$		

Table 1: The AXC reward system.

9 Market Trends

Below, we analyze various market trends and developments.

9.1 Decrease in Bitcoin's dominance

Shortly after the initiation of the Bitcoin blockchain in 2009, the phrase 'cryptocurrency' was synonymous with Bitcoin. After the initial success of Bitcoin, Altcoins (a term for all cryptocurrencies except Bitcoin) emerged. However, their market capitalization remained negligible in comparison to Bitcoin. Ripple and Ethereum changed this pattern: The blockchain community noticed how different cryptocurrencies, specialized to specific tasks such as payments, smart contracts, ICOs, securities, utility tokens, and many more could be built. With this development of crypto markets, Bitcoin's dominance began to decrease while and Altcoins became increasingly important in terms of market

capitalization. Cryptocurrencies benefit from this development. Today, users expect fast and secure trades between large amounts of value from Cryptocurrency exchanges.

9.2 Growth of Altcoin marketcap

Altcoin market capitalization exceeded the 250 Billion Dollar mark in mid 2018. With the emergence of regularizations of the cryptocurrency market, traditional asset managers will be able to invest in this market as well, so the trend of rising market capitalization is expected to continue [11]. Chris McCann compares this adoption to the early days of the Internet [12]:

> *Even though we've seen a huge increase for number of users of cryptocurrencies, tokens, and DApps—we are still in year 1994 if we compare the trajectory to the growth of the internet.*

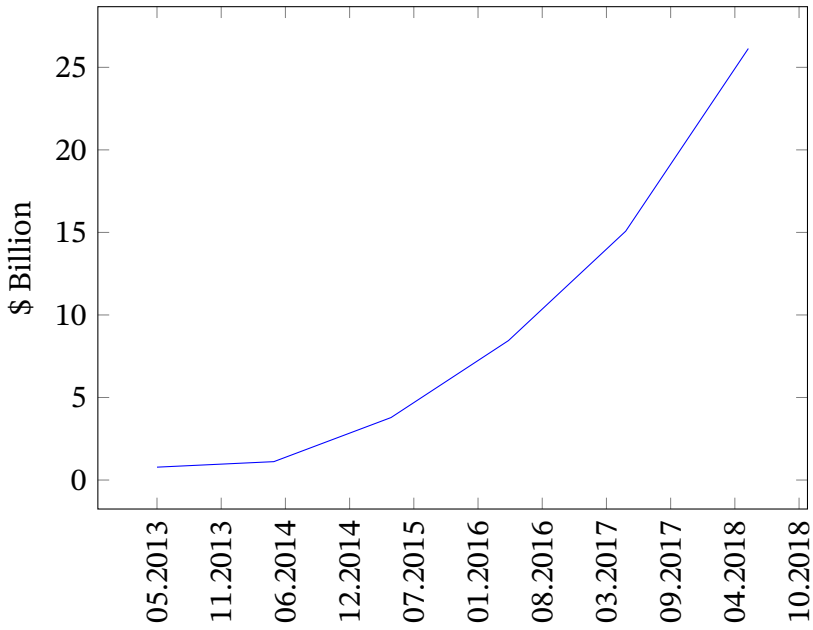


Figure 5: Total market capitalization of Altcoins over time.

9.3 Lightning network growth

Since its initiation, the number of nodes in the bitcoin lightning network grew substantially. With an increasing number of channels and capacities (in the form of frozen assets), it became possible to route large amounts of value through the lightning network. Ethereum's Plasma operates in a very similar fashion (and was even developed by the same team). Lightning networks and second layer solutions are predestined for micro payments, as they are able to process small transactions highly efficiently without imposing pressure on the main blockchain. See fig. 6 for a visualization of node growth and fig. 7 for a visualization of lightning channel growth. Data taken from the lightning network itself.

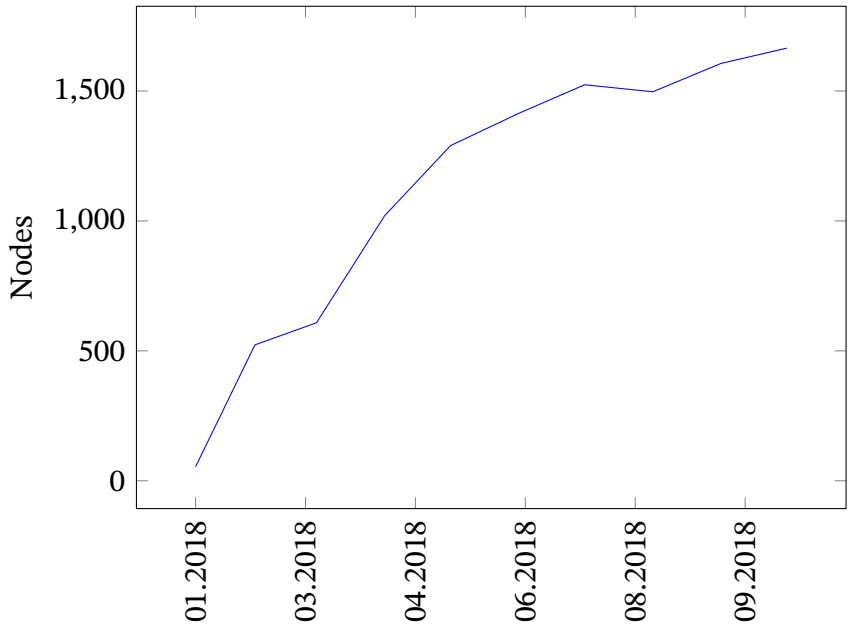


Figure 6: Number of nodes in the lightning network over time.

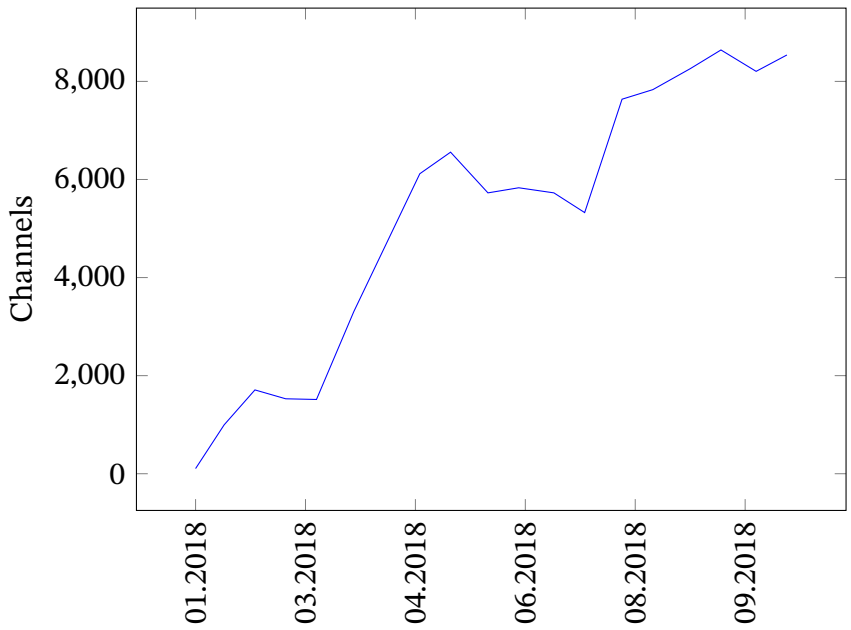


Figure 7: Number of Bitcoin lightning channels over time.

9.4 Growth of daily trading volume

With increasing global market capitalization and a growing number of altcoins, the daily trading volume on cryptocurrency exchanges is continually rising. On volatile days, trading volumes within 24 hours have exceeded $22 Billion in mid-2018.

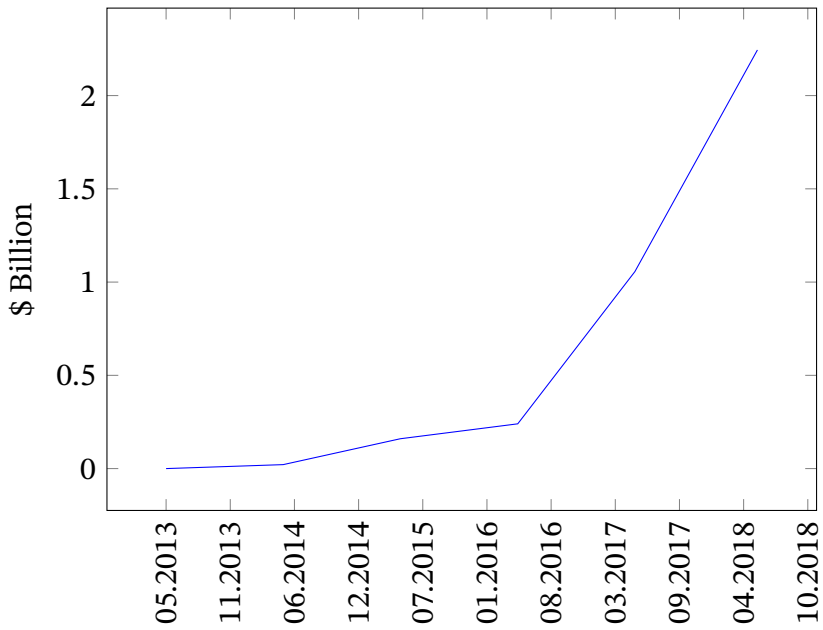


Figure 8: Daily cryptocurrency trading volume over time.

10 Hacks

This section concerns itself with methods, incidents and counter measures for hacks of cryptocurrency exchanges. To this end it will examine the most common hacking strategies before compiling an extensive list of documented hacks in the market. All items on the list are annotated with reliable news sources and all public information that could be gathered on the underlying security fault is compiled. This will lead to the formulation of specific systematic precautions an exchange can implement in an effort to prevent hacks.

10.1 Hacking Methods

Contrary to popular belief, the overwhelming majority of hacking attacks come in the form of social engineering. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information

that may be used for fraudulent purposes. The list of exchange hacks provided below will demonstrate that bypassing security measures is often achieved by these types of hacking and rarely requires actual breaking of encryption. Some of the more prevalent forms of social engineering hacks are:

Phone / Email Hijacking; Often with the use of personal information retrieved from social media, hackers impersonate their target and obtain a new SIM-Card from their victim's phone company or reset their victim's email password. This grants them access to all types of accounts and information, among which might be data on the cryptocurrency exchange where the target is working.

Phishing; Being by far the most common form of obtaining other people's accounts, many people are guarded against these attacks. Nevertheless this technique was used successfully to steal $9.5 Million from the exchange Cryptsy in July 2014 (see below). Phishing often asks people to log in to their account on a legit looking website in order to obtain login data. With the ubiquity of phishing sites and emails it is only a question of time until someone falls for the trick in an inattentive moment.

Malware; $5.2 Million were lost in January 2015 when multiple Bitstamp employees were tricked into downloading malicious software onto their work pc. This technique also exploits the target's interests to get them to download the malware

Preventing social engineering hacks; Very few databases worldwide remain unencrypted. Because it is highly improbable to ever break such an encryption, attacking these databases must concentrate on obtaining the private

key or password used to decrypt the database. Thus most exchange "hacks" can only happen because of bad information security protocols. Often the password of the encrypted database holding all private keys for an exchange's customers lies with a few key employees, who can then be targeted with low effort social engineering attacks. Not only are these kinds of data breaches very common in centralized systems but that is also where they cause the greatest damage.

Conclusively, cryptocurrencies are seldom "hacked", but their core protocol or their consensus mechanism can be compromised. This is almost always the result of a poorly designed consensus protocol and a very centralized system, in which human errors cause grievous damage.

As can be deduced from the circumstances of the hacks listed below and in fig. 9 client-side wallets and a decentralised system of private keys, storing assets in offline cold wallets and multi signature authentication are the most important counter measures for preventing theft.

10.2 Timeline of Exchange Hacks

Jun. 2011 **Mt. Gox, $8.75 Million;** The largest and most important crypto exchange of the early days also fell victim to the first known cryptocurrency exchange hack, which – it must be assumed – was due to its sub-standard security measures. At the time Japan-based Mt. Gox did not use any type of version control software. This meant that any programmer could accidentally undo all of a colleague's work, if they happened to be coding on the same file. Only shortly before the hack had the bitcoin exchange introduced a test environment. Therefore previous software changes had been pushed out to the exchange customers in an untested state. [13]

Oct. 2011 **Bitcoin7, $50.000;** Bitcoin7 – back then the third-largest BTC/USD exchange in the world – became the target of a Russian hacker group. On October 5th the website posted a message to its users stating, "The attack itself took action not only against the bitcoin7.com server but also against other websites and servers which were part of the same network. Eventually the hackers managed to breach into the network which subsequently led to a major breach into the bitcoin7.com website." Wherever the original breach happened, it gave them access to the site's hot wallets. Shortly after the hack Bitcoin7 closed its doors forever. [14]

Mar. 2012 **Bitcoinica, $228.000;** Bitcoinica was one of the most prominent victims of an attack exploiting a webhost called Linode. After initially stating a loss of 10.000 BTC, Bitcoinica's CEO Zhou Tong admitted to Ars Technica that actually 43,554 coins were lost, all of which had been stored in unencrypted hot wallets on Linode's servers. [15]

May 2012 **Bitcoinica, $87.000;** 10 weeks after the first attack Bitcoinica was again relieved of a significant sum. This time not only the bitcoins but also Bitcoinica's user database was compromised. Names, email addresses, passwords and other sensitive data were stolen although they had been stored on separate servers at a separate data centre with a different encryption regimen. [16]

Jul. 2012 **Bitcoinica, $300.000;** A third robbery saw Bitcoinica lose a significant amount of Bitcoin yet again. Rumours of the hack being an inside job however, could never be ascertained. [17]

Sept. 2012 **Bitfloor, $250.000;** The New York headquartered Bitfloor was the fourth largest exchange dealing in US dollars up until September 2012. In the attack hackers were able to gain access to an unencrypted backup of the exchange's wallet keys. This backup was created when Bitfloor's founder Roman Shtylman made a manual upgrade and put the data into an unencrypted partition on his disk. The compromised wallet keys were then used to empty Bitfloor's extensive hot wallets. [18]

May 2013 **Vircurex, $160.000;** A human error led to the theft of 1454 BTC, 225.263 TRC and 23.400 LTC, when according to Vircurex's May 2013 report the attacker acquired login credentials to their VPS control account with the hosting service provider and then successfully inquired after a root password reset of all servers. [19]

Jun. 2013 **Picostocks, $130.000;** On June 10 th a spokesman for Picostocks revealed on the bitcointalk.org forums that multiple accounts had been operated with the same password, allowing hackers to gain access to the exchange's wallets. [20]

Nov. 2013 **Picostocks, $3 Million;** A much larger sum was stolen from Picostocks in November of the same year. Because some of the wallets that were hacked were cold wallets and therefore inaccessible via the internet, the hack may have been an inside job. [21]

Feb. 2014 **Mt. Gox, $460 Million;** The second biggest crypto exchange hack of all time was, because of the comparatively small cryptocurrency market, the one with the biggest impact. The company admitted to a loss of $460 Million [22] after a leaked "crisis strategy draft" revealed that hackers had been leeching the company for years using one and the same bug. In the Aftermath sources from within the company reported the used source code to be "a mess" [23]. It seemed security measures hadn't been ramped up sufficiently since the June 2011 hack.

Mar. 2014 **Cryptorush, $570.000;** When BlackCoin released a new fork of their blockchain, it produced a bug that enabled owners of BlackCoin to cash out a larger sum than they actually possessed. A copy of the official statement is preserved in the bitcointalk.org forums. [24]

Mar. 2014 **Poloniex, $64.000;** A similar bug, that used the placing of transactions at the same instant in order to withdraw more than is stored in the respective wallet, was used to steal from Poloniex. [25]

Mar. 2014 **Flexcoin, $600.000;** After an attack on the cryptocurrency storage provider all of their hot wallets were emptied. How the attackers gained access to Flexcoin's system is unclear. [26]

Jul. 2014 **Cryptsy, $9,5 Million;** News of this extensive hack was only made public when the company declared bankruptcy two years later. After initially blaming technical issues Cryptsy allegedly became the target of Phishing attacks in the run up to its insolvency and was forced to suspend trading. [27]

Aug. 2014 **BTER, $1,65 Million;** Even though BTER managed to cut their losses by negotiating a partial return of the stolen coins, the hack would go down as another avoidable loss as a developer claimed the fault lay entirely with the exchange itself. [28]

Oct. 2014 **Mintpal, $1,3 Million;** The circumstances of Mintpal's hack as well as their subsequent demise are still unclear. The suspicion of it being an inside job arose when Ryan Kennedy, who was brought before a court in the UK for fraud and money laundering in 2017, acquired the exchange following the hack. [29]

Jan. 2015 **796Exchange, $230.000;** Not even the move of migrating servers to a highly secured cloud site could save the largest exchange at the time in terms of volume from being attacked successfully. After exploiting a weakness in the system the hackers were able to trick the customer service department so that they sent Bitcoins to the wrong wallet. 796Exchange's President Nelson Yu told cointelegraph.com that "precisely speaking, the wallet system is not affected at all in this event. The theft happened during the transaction of the fund." [30]

Jan. 2015 **Bitstamp, $5,2 Million;** The 2015 Bitstamp heist is a prime example of sophisticated phishing attacks. Multiple employees were targeted and tricked into downloading malware using information on personal interests. This way the attackers gained access to two servers containing the passphrase to Bitstamp's hot wallet. [31]

Feb. 2015 **BTER, $1,75 Million;** The second time BTER got hacked was significant in that the target of the attack were their cold wallets. How they managed to do that remains a mystery. [32]

Apr. 2016 **Shapeshift, $230.000;** Shapeshift's hack was one of the few that could be traced back to an employee of the company. Having robbed the exchange of $130.000 they then sold sensitive information to a hacker, who is believed to have engineered a second theft of $100.000. [33]

May 2016 **Gatecoin, $2,14 Million;** This hack represented a noteworthy twist on a tried and tested strategy. The attackers seemingly altered the system so that it stored deposit transfers in the hot wallet, instead of the cold wallet as intended, thus increasing the amount that was stolen from it later. [34]

Aug. 2016 **Bitfinex, $77 Million;** Using a multi-signature wallet system by BitGo, Bitfinex was reckoned by many to be extremely secure. Nevertheless the hackers must have managed to get hold of private wallet keys as well as the key to the API of BitGO, leaving many questions as to the nature and procedure of the hack to this day. [35]

Feb. 2017 **Bithump, $1 Million;** Hackers managed to get their hands on personal information on more than 30.000 of Bithump's customers. The data breach was the result of one of the company's employees private pc being hacked. The information was then used to make scam calls in order to steal the users' authentication codes. [36]

Apr. 2017 **Youbit, $5,3 Million;** Then known as Yapizon the South Korean exchange had four of their hot wallets compromised and emptied. The stolen amount equalled 36% of the company's total funds. [37]

Dec. 2017 **Youbit, "17% of total assets" [38];** The second robbery at Youbit forced the exchange to declare bankruptcy. Both attacks were linked to neighbouring country North Korea by the state's spy agency but these claims could not be verified. [39]

Jan. 2018 **Coincheck, $500 Million;** Coincheck became an easy target of this massive heist due to insufficient security practices. Not only did the exchange store it's customers assets in hot wallets but it also did not secure those wallets with industry-standard multi-signature authenticators. [40]

Feb. 2018 **Bitgrail, $187 Million;** Little is known about the hack that Italian Bitgrail filed with authorities in February. According to the exchange, not even the precise date of the loss could be determined. Naturally, allegations of CEO Francesco Firano having staged the theft himself rose but nothing could be proved. Firano tried to shift the blame to the developers behind the Nano token blockchain that BitGrail used. [41]

Jun. 2018 **Coinrail, $40 Million;** Coinrail is another exchange that had to close its doors after being hacked. Even though 70% of the company's assets were stored in cold wallets, the attackers made away with $40 Million. [42] The incident marks the third time a South Korean exchange was hacked within a few months, signalling the concentration of cryptocurrency exchange hacks in Asia.

Sept. 2018 **Zaif, $60 Million;** Japan-based Zaif was caught off guard when hackers stole $60 Million from their hot wallets. The Company could only be kept alive by partnering up with Fisco, who covered $44,5 Million of the stolen amount for a major share in the exchange's ownership. [43]

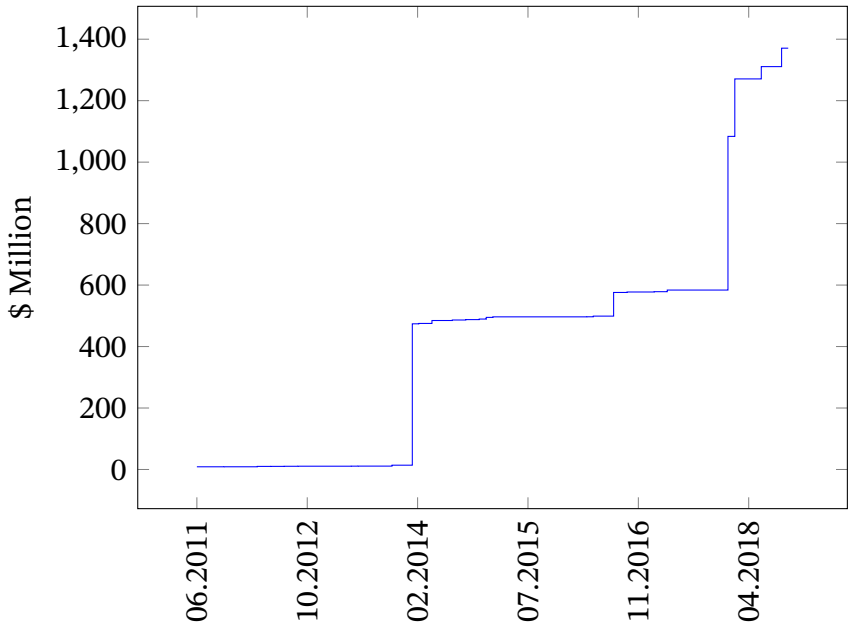


Figure 9: Total volume of funds lost through cryptocurrency exchange hacks.

Conclusion Some interesting observations can be made about these hacks:

1. The majority of successful attacks on cryptocurrency exchanges happened to companies based in Asia.

2. The majority of the hacks mentioned above targeted centrally administrated hot wallets.

3. Many of the hacks listed happened due to a human error, meaning data was stored unencrypted, updates were pushed without quality control,

impersonations were not uncovered or employees became the target of phishing.

Truly decentralising a cryptocurrency exchange by using client-side wallets and multi-signature authentication on private keys drastically reduces the probability that such hacks are successful. Aside from that it also makes it much harder for a company's employee to divert funds from within.

References

[1] Noel Tiernan. *Alt chains and atomic transfers*. 2013. URL: https://bitcointalk.org/index.php?topic=193281.0.

[2] Jamie Redman. *Segregated Witness (SegWit) to Activate Within 24 Hours: How Bitcoin Will Change*. 2017. URL: https://news.bitcoin.com/segregated-witness-has-officially-activated-on-the-bitcoin-network/.

[3] Joseph Poon and Thaddeus Dryja. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. 2016. URL: https://lightning.network/lightning-network-paper.pdf.

[4] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf.

[5] Juan Benet. *IPFS - Content Addressed, Versioned, P2P File System*. 2015. URL: https://github.com/ipfs/papers/blob/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf.

[6] *FIPS PUB 186-4*. 2013. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[7] Daniel R. L. Brown. *SEC 2: Recommended Elliptic Curve Domain Parameters*. 2010. URL: http://www.secg.org/sec2-v2.pdf.

[8] *BOLT 3: Bitcoin Transaction and Script Formats*. 2018. URL: https://github.com/lightningnetwork/lightning-rfc.

[9] Ellen Hughes-Cromwick. *Cryptocurrency Energy Consumption*. 2018. URL: http://energy.umich.edu/sites/default/files/umei_weekly_09_19_17_cryptocurrency_energy_consumption.pdf.

[10] URL: https://digiconomist.net/bitcoin-energy-consumption.

[11] Mike Novogratz. *Cryptocurrency market cap will hit 800 billion in 12 months*. 2018. URL: https://www.ccn.com/cryptocurrency-market-cap-will-hit-800-billion-in-12-months-novogratz/.

[12] Chris McCann. *Graphs that show just how early the cryptocurrency market is*. 2018. URL: https://medium.com/@mccannatron/12-graphs-that-show-just-how-early-the-cryptocurrency-market-is-653a4b8b2720.

[13] Robert Mcmillan. *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*. 2014. URL: https://www.wired.com/2014/03/bitcoin-exchange/.

[14] Kyt Dotson. *Bitcoin7 Hacked, Funds Recovery Requires Sensitive Personal Information*. 2011. URL: https://siliconangle.com/2011/10/07/bitcoin7-hacked-funds-recovery-requires-sensitive-personal-information/.

[15] Dan Goodin. *Bitcoins worth $228,000 stolen from customers of hacked Webhost*. 2012. URL: https://arstechnica.com/information-technology/2012/03/bitcoins-worth-228000-stolen-from-customers-of-hacked-webhost/.

[16] Dan Goodin. *Bitcoins worth $87,000 plundered in brazen server breach*. 2012. URL: https://arstechnica.com/uncategorized/2012/05/bitcoins-worth-87000-plundered/.

[17] Vitalik Buterin. *The July 13 Bitcoinica Investigation and Sound Justice*. 2012. URL: https://bitcoinmagazine.com/articles/the-july-13-bitcoinica-investigation-and-sound-justice-1343490976/.

[18] Vitalik Buterin. *Bitfloor Hacked, $250,000 Missing*. 2012. URL: https://bitcoinmagazine.com/articles/bitfloor-hacked-250000-missing-1346821046/#sources.

[19] Vircurex. *May 2013 Report*. 2013. URL: https://vircurex.com/Reports/2013-05.pdf.

[20] Brian Patrick Eha. *How one scrappy Startup survived the Early Bitcoin Wars*. 2017. URL: https://www.wired.com/2017/05/one-scrappy-startup-survived-early-bitcoin-wars/.

[21] Brian Patrick Eha. *How Money got Free. Bitcoin and the Fight for the Future of Finance*. 2017. URL: https://books.google.hu/books?id=w6CVDQAAQBAJ&pg=PT88&lpg=PT88&dq=picostocks+hack&source=bl&ots=Sq0cnJ9DS5&sig=WHDEZRZ0bLB-2JC18X14kVeE5kw&hl=en&sa=X&ved=0ahUKEwj_mv7-v93bAhVQaFAKHU2QAEw4ChDoAQg7MAQ#v=onepage&q=picostocks%20hack&f=false.

[22] Robert Mcmillan. *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*. 2014. URL: https://www.wired.com/2014/03/bitcoin-exchange/.

[23] Robert Mcmillan. *Bitcoin Exchange Mt. Gox goes Offline amid Allegations of $350 Million Hack*. 2014. URL: https://www.wired.com/2014/02/bitcoins-mt-gox-implodes-2/.

[24] URL: https://www.wired.com/2014/02/bitcoins-mt-gox-implodes-2/.

[25] Pete Rizzo. *Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack*. 2014. URL: https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/.

[26] Pete Rizzo. *Bitcoin Bank Flexcoin to Close After $600k Bitcoin Theft*. 2014. URL: https://www.coindesk.com/bitcoin-bank-flexcoin-close-600000-bitcoin-theft/.

[27] Stan Higgins. *Cryptsy Threatens Bankruptcy, Claims Millions Lost in Bitcoin Heist*. 2016. URL: https://www.coindesk.com/cryptsy-bankruptcy-millions-bitcoin-stolen/.

[28] Pete Rizzo. *Hackers Steal $1.65 Million in NXT from BTER Exchange*. 2014. URL: https://www.coindesk.com/bter-nxt-bitcoin-exchange-hack/.

[29] Stan Higgins. *Former Dogecoin Exchange CEO Faces Fraud Charges*. 2017. URL: https://www.coindesk.com/former-dogecoin-exchange-ceo-faces-fraud-charges-uk/.

[30] William Suberg. *Chinese Exchange Gets 'Goxed' for 1,000 Bitcoins*. 2015. URL: https://cointelegraph.com/news/chinese-exchange-suffers-1000-btc-loss-in-uncertain-service-compromise.

[31] Stan Higgins. *Details of $5 Million Bitstamp Hack Revealed*. 2015. URL: https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/.

[32] Gola Yashu. *Chinese Bitcoin Exchange Bter Hacked; HitBTC Also Offline*. 2015. URL: https://www.newsbtc.com/2015/02/15/chinese-bitcoin-exchange-bter-hacked-hitbtc-also-offlinechinese-bitcoin-exchange-bter-hacked-hitbtc-also-offline/.

[33] Stan Higgins. *ShapeShift Lost $230k in String of Thefts, Report Finds*. 2016. URL: https://www.coindesk.com/digital-currency-exchange-shapeshift-says-lost-230k-3-separate-hacks/.

[34] Stan Higgins. *Gatecoin Claims $2 Million in Bitcoins and Ethers Lost in Security Breach*. 2016. URL: https://www.coindesk.com/gatecoin-2-million-bitcoin-ether-security-breach/.

[35] Christoph Bergmann. *Das Nachspiel des Bitfinex-Hacks: Was jetzt passiert – und wie solche Hacks in Zukunft zu verhindern sind*. 2016. URL: https://bitcoinblog.de/2016/08/05/das-nachspiel-des-bitfinex-hacks-was-jetzt-passiert-und-wie-solche-hacks-in-zukunft-zu-verhindern-sind/.

[36] BBC News. *Hackers steal Bitcoin funds from Bithumb exchange traders*. 2017. URL: https://www.bbc.com/news/technology-40506609.

[37] Jamie Redman. *Hacked South Korean Bitcoin Exchange Yapizon Offers IOUs*. 2017. URL: https://news.bitcoin.com/hacked-korean-bitcoin-exchange-yapizon-offers-ious/.

[38] Stan Higgins. *Bitcoin Exchange Youbit to Declare Bankruptcy After Hack*. 2017. URL: https://www.coindesk.com/south-korean-bitcoin-exchange-declare-bankruptcy-hack/.

[39] Joyce Lee. *South Korean cryptocurrency exchange to file for bankruptcy after hacking*. 2017. URL: https://www.reuters.com/article/us-bitcoin-exchange-southkorea/south-korean-cryptocurrency-exchange-to-file-for-bankruptcy-after-hacking-idUSKBN1ED0NJ.

[40] Fortune. *How to Steal $500 Million in Cryptocurrency*. 2018. URL: http://fortune.com/2018/01/31/coincheck-hack-how/.

[41] Cointelegraph. *Interview with BitGrail's Francesco Firano*. 2018. URL: https://cointelegraph.com/news/its-impossible-to-refund-the-stolen-amount-interview-with-bitgrails-francesco-firano.

[42] Wolfie Zhao. *Coinrail Exchange Hacked, Loses Possibly $40 Million in Cryptos*. 2018. URL: https://www.coindesk.com/coinrail-exchange-hacked-loses-possibly-40-million-in-cryptos/.

[43] Wolfie Zhao. *Crypto Exchange Zaif Hacked In $60 Million Bitcoin Theft*. 2018. URL: https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft/.