General Terms of Service relating to the services provided on the websites http://ethpool.org, http://ethermine.org, http://etc.ethermine.org and http://zcash.flypool.org as well as Terms of Service to the open-source software "QtMiner"

Version 1.0

§ 1 General Principles; Scope of Application

1.1 The following General Terms of Service ("GTS") apply to any use of the mining pool services ("Services") offered over the websites ("Websites") mentioned above concerning the mining of the cryptocurrencies "Ethereum", "Ethereum Classic" and "Zcash". The service provider offering these Services is bitfly e.U. (Commercial Register: Handelsgericht Wien, FN 461382 d) ("SP").

1.2 By accessing and using the Services, you confirm that you have read these GTS and accept and agree to be bound by its provisions. Any factual participation in the Services will constitute such acceptance. If you do not agree to abide by these GTS, you are not allowed to use the Services.

1.3 To access the Services, you enter your specific address associated with your wallet. The websites http://ethpool.org, http://ethermine.org, http://etc.ethermine.org refer to Ethereum respectively Ethereum Classic mining pool services and require an Ethereum or Ethereum Classic address. The service offered via http://zcash.flypool.org refers to a Zcash mining pool requiring a wallet supporting Zcash. In order to use the Services, a mining software working with the operating system on your computer is necessary. Download links are available directly on the Websites.

1.4 In order to use the Services as defined below and operated via the Websites you must be at least sixteen (16) years old. By using the Services, you confirm to have reached the age of sixteen (16).

§ 2 Definitions

2.1 **Blocks** & **Transactions**: Transaction data is permanently recorded in files called blocks. They can be thought of as the individual pages of a city recorder's recordbook (where changes to title to real estate are recorded) or a stock transaction ledger. Blocks are organized into a

linear sequence over time ("**Miner**" or "**Worker**") also known as the block chain). New transactions are constantly being processed by Miners (into new blocks which are added to the end of the chain and can never be changed or removed once accepted by the network. Each block contains, among other things, a record of some or all recent transactions, and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle – the answer to which is unique to each block. New blocks cannot be submitted to the network without the correct answer – the process of "mining" is essentially the process of competing to be the next to find the answer that "solves" the current block. The mathematical problem in each block is extremely difficult to solve, but once a valid solution is found, it is very easy for the rest of the network to confirm that the solution is correct. There are multiple valid solutions for any given block – only one of the solutions needs to be found for the block to be solved. Because there is a reward of brand new cryptocurrency units for solving each block, every block also contains a record of which address is entitled to receive the reward. Transactions are broadcast to the network by the sender, and all peers trying to solve blocks collect the transaction records and add them to the block they are working to solve. Miners get incentive to include transactions in their blocks because of attached transaction fees. The difficulty of the mathematical problem is automatically adjusted by the network, such that it targets a goal of solving an average of (X) blocks per time interval (details are specified in the respective consensus rules of a cryptocurrency). The network comes to a consensus and automatically increases (or decreases) the difficulty of generating blocks. Because each block contains a reference to the prior block, the collection of all blocks in existence can be said to form a chain. However, it's possible for the chain to have temporary splits – for example, if two Miners arrive at two different valid solutions for the same block at the same time, unbeknownst to one another. The peer-to-peer network is designed to resolve these splits within a short period of time, so that only one branch of the chain survives. The client accepts the "longest" chain of blocks as valid. The "length" of the entire block chain refers to the chain with the most combined difficulty, not the one with the most blocks. [Source: https://en.bitcoin.it/wiki/Block]

2.2 **Uncles** are orphaned blocks that contribute to the security of the main chain, but are not considered the canonical "truth" for that particular chain height. They only exist in Ethereum-based cryptocurrencies. For more information on Ethereums uncle mechanism please review the relevant section of the Ethereum wiki under https://github.com/ethereum/wiki/wiki/Design-Rationale - uncle-incentivization. [Source: http://ethereum.stackexchange.com/questions/34/what-is-an-uncle-ommer-block]

2.3 **Block chain** is a decentralized and continually updated list of transactions occurring across a certain peer-to-peer network. Blocks of transactions are validated and linked together by specific methods of cryptography. Manipulating individual transaction records is hardly possible in this context. A blockchain provides a wide range of functionality. Besides establishing cryptocurrency and payment infrastructures, it can be used, for instance, to digitally sign documents (proving identity) or create verifiable records of business processes

2.4 **Mining** is the process of adding transaction records to a cryptocurrencies public ledger of past transactions. This ledger of past transactions is called the block chain (see above 2.3) as it is a chain of blocks. The block chain serves to confirm transactions to the rest of the network as having taken place. Cryptocurrency nodes use the block chain to distinguish legitimate transactions from attempts to re-spend coins that have already been spent elsewhere. Mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by Miners remains steady. Individual blocks must contain a proof of work to be considered valid. This proof of work is verified by other nodes each time they receive a block. Ethereum uses the "ethash" proof-of-work function while Zcash uses the "equihash" algorithm. The primary purpose of mining is to allow nodes to reach a secure, tamper-resistant consensus. Mining is also the mechanism used to introduce new units of cryptocurrency into the system: Miners are paid any transaction fees as well as a "subsidy" of newly created coins. These both serve the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system. Mining is so called because it resembles the mining of other commodities: it requires exertion and it slowly makes new currency available at a rate that resembles the rate at which commodities like gold are mined from the ground. [Source: https://en.bitcoin.it/wiki/Mining] To ensure mining can be carried out reasonably, certain hardware demands are to be fulfilled; mining entails a high level of power consumption. The process of mining is conducted using specialised software available for different operating systems. Each cryptocurrency defines a unique mining reward scheme. For more information on the rewarding scheme employed by the Ethereum cryptocurrency please consult the Ethereum Yellow Paper under https://github.com/ethereum/yellowpaper; for more information on the Zcash rewarding scheme please consult the Zcash protocol specifications under https://github.com/zcash/zips/blob/master/protocol/protocol.pdf.

2.5 **Mining pools** pursue the objective to solve blocks more quickly and split the rewards equally. Participants of a mining pool presenting a valid proof of work are awarded a "share". A share is

a hash, smaller than a specified difficulty, but generally without value as only the hash smaller than the target value solving a block and determined by difficulty is of importance. Mining pools are available in a range of forms and arrangements as well as for different types of cryptocurrency. Depending on the mining pool, various payout schemes may be applied, whereby those of relevance will be outlined under § 4.

2.6 A **Share** is awarded by the mining pool to the clients who present a valid proof of work of the same type as the proof of work that is used for creating blocks, but of lesser difficulty, so that it requires less time on average to generate. [Source: https://en.bitcoin.it/wiki/Pooled_mining]

2.7 **Wallet** is the term to describe the digital environment to access and spend cryptocurrency. In an untechnical thinking, the units are "stored" within. A secure private key with a corresponding public key is necessary to sign and verify transactions. Wallets are associated with a specific address ("**Address**") and exist in various forms, particularly desktop, mobile, web and hardware wallets.

2.8 **Ethereum** is an open-source project establishing a decentralised platform running applications exactly as programmed. Downtime, censorship, fraud and third party interference are not possible according to the developers. Using a customized blockchain able to move values, Ethereum has an enormously wide application area and provides numerous options for developers. The platform facilitates the realization of so called smart contracts, allowing, for example, the automatic negotiation or enforcement of contracts. **Ether**, as the actual cryptocurrency, is a necessary element for operating Ethereum (payment for requested operations). It is also traded on cryptocurrency exchanges. **Ethereum Classic** is a split from the existing cryptocurrency Ethereum and Etherium Classic offer the same features. Both blockchains act individually.

2.9 **Zcash** ("**ZEC**") is a decentralised and open-source cryptocurrency with increased confidentiality. Despite payments are – as usual in connection with cryptocurrencies – published on a blockchain, the sender, recipient and amount of transactions are only visible to those people with the corresponding "view key" as these "shielded" transactions are specifically encrypted. In using advanced cryptographic technology, transactions can be verified without revealing additional information.

§ 3 Liability

3.1 Nothing in these GTS shall limit any liability for fraud or fraudulent misrepresentation as well as intentional or grossly negligent infliction of damage by the SP.

3.2 The SP is continually implementing security standards complying with the latest state-of-the-art technology. All operated servers located in the EU-28 and North America are distributed-denial-of-service (DDOS) protected to ensure an incessant availability of the Services and a payout process without unwanted interruptions. The Services are also designed to pay out rewards as soon as possible in order to keep the pool balance low.

3.3 Despite such protective mechanisms, the SP cannot fully guarantee that the Websites will never be subject to hacker attacks or similar problems. Therefore, the SP shall not be obliged to compensate any losses due to stolen pool balance or temporary unavailability of the Services. The SP explicitly reserves the right to shut down services from time to time for maintenance reasons.

3.4 Furthermore, the SP shall not be liable for any damages of your hardware (computer and its components) or software (operating system, programs, stored data etc.) occurring while using the Services. The intensity of the mining tasks is highly demanding; hardware components may – exceptionally – be destroyed completely. As the hardware setup of each Worker is individually compiled, you must assess (and bear) the risk associated with such high electrical load by yourself.

3.5 Attacks on the system may also cause data loss. As far as sensitive data is collected (see § 5), the SP shall not be held responsible for any loss that cannot be reduced to security issues or other culpability by the SP.

3.6 Ethereum, Ethereum Classic and Zcash are highly experimental crypto software. Damages or loss of cryptocurrency units arising from software errors therefore remain possible. As the SP has no influence on the underlying software, he shall not in any case be exposed to claims relating to such errors.

§ 4 Terms of Payment

4.1 As mining is an intensive task for the hardware of your computer (CPU, GPU), the process can cause high costs for electricity. The SP shall not be responsible for any such costs. The Services are conducted at the sole discretion of the user in type, extent and frequency. All expenses arising are to be borne by the Worker.

4.2 Depending on the offer of each website, payout schemes may differ:

a) http://ethpool.org is a predictable Ethereum solo mining pool and implements a solo mining payout scheme. Each submitted share will increase the credits of the Miner who submitted the share by the fixed share difficulty of the pool. The Miner who accumulated the most credits will receive the reward of the next block that has been mined by the pool and his credits will be reset to his current credits minus the credits of the runner up Miner. "Uncles" are distributed in a similar way only that the credits of the Miner receiving the uncle reward will not be reset.

b) http://ethermine.org is an Ethereum mining pool using the traditional Pay-Per-Last-N-Shares ("**PPLNS**") payout scheme. This reward system is round based, whereby one round has an arbitrary number (N) of minutes. When a block has been found by the pool, the block reward is distributed according to the number and difficulty of the shares submitted during the last hour. Payout takes place immediately after the minimum payout amount of 1 "Ether" has been reached. However, the payout threshold is customizable (minimum 0,1 "Ether", maximum 10 "Ether").

c) http://etc.ethermine.org is an Ethereum Classic mining pool using the traditional PPLNS payout scheme. The payout scheme is working exactly in the same way as explained under b) above. Payout takes place immediately after the customizable minimum payout amount has been reached.

d) http://zcash.flypool.org is a Zcash mining pool using the traditional PPLNS payout scheme. The payout scheme is working exactly in the same way as explained under b) above. Payout takes place immediately after the minimum payout amount of 0,01 ZEC has been reached. However, the payout threshold is customizable (minimum 0,001 ZEC, maximum 10 ZEC).

4.3 The pool fee to be collected by the SP amounts to a uniform 1% calculated from the total mining rewards as defined by the cryptocurrency consensus protocol.

4.4 Network transaction fees of the pool payout transactions are paid by the SP.

§ 5 Privacy Policy

5.1 The Websites are designed as anonymous mining pools. The collection of personal data is strictly limited.

5.2 By accessing the Websites, the external IP address of your computer and http specific information (request, referrer and user agent) will be logged for statistical purposes. By using the Services (mining on the pools), the external IP address of your computer will be logged for verification purposes as well as to allow you to change specific settings (indication of email address, modification of minimum payout amount). Such data may potentially link to personally identifiable information.

5.3 Indicating your email address is no requirement to use the Services. However, you may leave such address in order to get notified if, for example, the Services are temporarily unavailable or the mining pools are experiencing technical problems. Such data will not be shared with third parties as outlined below or used for any other purpose apart from providing relevant information concerning the Services or these GTS.

5.4 The SP uses services of Twitter Inc., 1355 Market St, Suite 900, San Francisco, CA 94103, USA ("**Twitter**") on the Websites in order to provide important information by embedding his official Twitter account "etherchain_org". The timeline is integrated as list template and allows the Workers to directly share or like tweets on Twitter. By accessing the Websites, your browser will instantly communicate with the servers of Twitter in the USA. Thereby, certain data will be transferred and stored. If you are not logged in to Twitter or do not have a Twitter account, the information solely refers to your IP address and the fact that the Websites have been visited. If you are logged in to Twitter, this information can be associated with your account and thus your person. If you do not want Twitter to allocate such collected data to your account, you must log out of your profile before visiting the Websites. When using the liking/sharing function information will be transmitted as well and furthermore visible on Twitter. For advice or information regarding the purpose and scope of data collection, further

processing and use of data by Twitter as well as your specific rights and adjustable settings for privacy protection you may visit https://twitter.com/privacy?lang=en to review the privacy policy of Twitter. However, as an alternative, you can force your browser not to load the Twitter timeline by installing add-ons, for example, the script blocker "NoScript" available under http://noscript.net/.

5.5 Servers are located in Europe (EU-28), Asia and North America. If you do not want any data to be transferred outside of the European Union, please take it into account when selecting the respective server.

5.6 None of the information transmitted will be shared with third parties. However, you need to download and install third party software on your computer in order to use the Services and mine cryptocurrency. The SP has no influence on any data collected by these third parties. Hence, it is recommended to review available terms and conditions and privacy policies of such third parties carefully as well.

5.7 The mining software "QtMiner" is an exception as it is developed and provided by the SP. The software is available for Windows as well as Linux distribution Ubuntu and increases transparency due to its open-source nature. It does not gather any personal data. These GTS apply accordingly.

§ 6 Severability Clause

In the event that any provision or any part of any provision set forth in these GTS shall be void or unenforceable for any reason whatsoever, then such provision shall be stricken and of no force and effect. However, unless such stricken provision goes to the essence of the consideration negotiated by the contracting parties, the remaining provisions of these GTS shall continue in full force and effect, and to the extent required, shall be modified to preserve their validity.

§ 7 Further Contract Terms

7.1 So called botnets are strictly prohibited from participating in the mining pools. The term refers to computers used for mining, although their actual owners are unaware of it. Your computer may fall victim to a botnet due to insufficient security measures. It is hence recommended to

pay utmost attention to adequate protection. The SP generally reserves the right to exclude Workers from using the Service without prior notice.

7.2 The SP may change these GTS if necessary. Your continued use of the Services will signify your acceptance to any adjustment of these terms. The fact that the text respectively content has been changed will be visibly announced on the Websites. You should read these GTS again on a regular basis.

7.3 These GTS are exclusively governed by and construed in accordance with Austrian law.

7.4 Disputes shall be submitted exclusively to the competent courts of Austria, as far as a choice of law is permitted.