Equibit: A Peer-to-Peer Electronic Equity System

Brent Kievit-Kylar
brent.k@equibit.org
Cognitive Science Program
Indiana University, Bloomington IN
USA

Chris Horlacher
chris.h@equibit.org
Chartered Accountant
Toronto, ON
Canada

Marc Godard
marc.g@equibit.org
Computer Programmer
Toronto, ON
Canada

equibit.org

Abstract: The raising of capital via private, over-the-counter (OTC) markets represents a significant part of economic activity currently underserved by modern technological innovation. In addition, recent events have revealed problems of transparency, inviting public criticism and scrutiny from regulatory authorities. A peer-to-peer platform facilitating the creation and exchange of private shares represents a shift in the OTC market towards more efficient, transparent operations as well as greater accessibility to the investing public and issuing corporations. The bitcoin infrastructure solves the problem of transaction processing but the fungibility of its units pose a challenge in identifying the issuers and holders of specific equities. Furthermore, as the issuers are in a constant state of flux the benefits of a decentralized network are lost if a central manager is required to cancel equities from companies that no longer exist. We propose a solution to these problems using digital signatures, based on the Bitcoin protocol.

1. Introduction

Private shares represent one of the largest classes of equity investments, typically controlled by brokerages, underwriters, central depositories and stock transfer agents. Despite its size, the OTC market is opaque and market actors must rely on these industry insiders to raise capital, conduct trades, and accurately manage their shareholder registers. Extensive documentation is required in order to ensure that purchased units are authentic. Furthermore, issuers or their agents have to maintain a register of investor's identities and addresses in order to distribute earnings and collect votes on investor resolutions. This requires issuers to collect extensive information on their investors and incur significant costs in order to issue and transfer private shares, distribute earnings and poll their investors.

What is needed is an electronic equity system allowing private issuers to create, disseminate and maintain equity across a broad base of investors without the need for onerous recordkeeping. To move away from central authority based systems, we must embrace distributed trust. The movement toward

distributed trust systems has been building for years, growing out of the social movement facilitated by a connected world.[1],[2] Its advantages include increased flexibility, lack of single point failure, openness and cost.

These social trust systems have recently been making waves in the domain of economics with the rise to prominence of digital currencies. Systems like Bitcoin provide a distributed trust system for value exchange.[3] These cryptocurrencies are designed around a public ledger protected by cryptographic primitives that allow individuals to move value from one user to another securely, insofar as value cannot be double spent, nor given if it is not owned.

The same features that allow the blockchain in Bitcoin to be an effective monetary representation, can also easily handle the equity dissemination process and maintain a register of investors. With additional modifications it could also be made to allow for the creation of uniquely identifiable private shares within the blockchain itself, as well as distribute earnings to and collect votes from the relevant investors.

The following paper describes what changes must be made to the basic protocol to enable it to be used as a transfer vessel for equity instead of a pure digital currency. We describe the cost, trust, and flexibility benefits of this new system as well as presenting an example implementation based on the bitcoin code base that is free and open.

2. Equity Creation and Issuance

When a network node discovers new equibits the units contain an issuer field signifying that the unit is presently in a null state. This null state is the equivalent of a blank stock certificate, which would then be signed and sealed by an offering corporation and delivered to the investor. The Equibit system digitally models these same operations. Often this blank stock in itself has very little value but as we will discuss further, there is a limited amount of these null units in the system. These new equibits enter the market and may be traded from one user to another as any other equibit and will likely carry some nominal value due to their usefulness in becoming issuer signed in the future.

At some point this equibit will be transferred to a user in the network that has the need to create and issue private shares of their own. If the new user signs the issuer field, they overwrite the null value and thus give their authorization that these units are now a representation of equity in their particular business. At that point they may then transfer the equibit to another user or hold on to it.

Unlike traditional cryptocurrency, the value of an individual equibit comes from the issuer field and the presumed value that user provides. Thus, not all equibits are equal. Also, the real-life identity of the issuers becomes an important factor in the value of the equibit, as compared to the relative anonymity desired by most cryptocurrencies. Fortunately, the prominence of public key encryption algorithms already requires these entities to have the infrastructure to provably distribute public keys and identification. Thus, if a public key can be trusted to belong to a given entity, then that entity can prove to any user that a particular transaction was performed by them, because no other entity could have the relevant private key. While the identities of the issuers must be resolved, the purchasers can choose to maintain or not the same level of anonymity available to traditional bitcoin users.[4]

The status of all equibits in the system is a matter of public record due to the very nature of the blockchain. Therefore, it will be easy for market participants to take note of the sum total of equibits a particular issuer has signed, how many have left the originating address, as well as how many are still

retained by the issuer for future offerings. This is important information for investors as they desire knowledge of what potential dilution of their investment they could experience in the future. They would also immediately know when an existing issuer authorizes new units by adding their signature to them.

Verifying the authenticity of units received is also an important part of the system. This can be accomplished by tracing the chain of transactions of the equibit units held at a particular address back to the address they originated at. If the signatures match then the unit is authentic and should be accepted at its market value. If the signatures do not match then the unit is a forgery and should be immediately returned to its null state to avoid contaminating the Equibit network. Notice that equibits do not fall out of the system but may always be re-used.

It should be noted that under the proposed system, share splits, share dividends or other actions corporations have traditionally undertaken in order to uniformly increase the number of shares in the market, becomes obsolete. As equibits, like bitcoins, are divisible to infinitesimal amounts there is no longer any need to reduce the per-unit value of a company's shares by employing such methods. Therefore there is never any risk to the liquidity of any particular equibit and ownership can be as widely distributed as possible due to the ability to own fractional equibits.

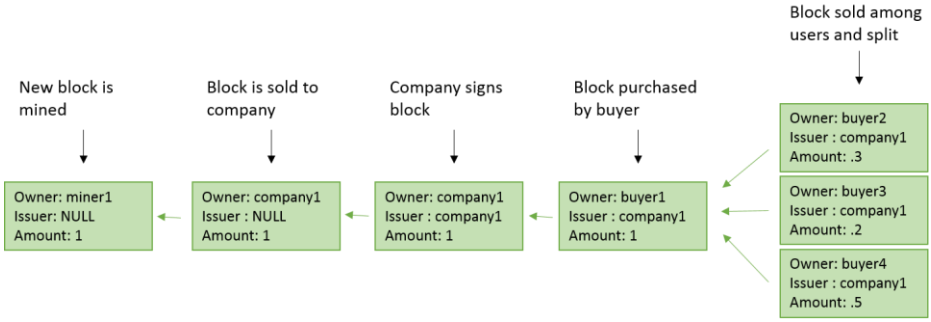

Figure 1.
Example of a mined equibit being created, signed and transferred.

3. Portfolio Addresses

All altcoins operate using their own blockchain and unique set of public and private keys. This poses a challenge to the Equibit system because it must operate on at least two blockchains; the Equibit chain for stock transactions, and Bitcoin (or other monetary altcoins) for monetary transactions such as dividends.

Equibit is thus the first multi-coin blockchain application. Efficient management of the inputs and outputs from each chain then becomes of paramount importance for the entire system to function and maintain a positive user experience. The challenge arises in knowing what bitcoin (or other monetary cryptocurrency) address to send dividends to, while only knowing the equibit addresses holding equity from a particular issuer.

To create the associations between addresses a user may add a payment block to the blockchain to specify the Bitcoin address that dividends will be paid out to. This payment block may be a general payment (referencing null), or it may be a specific payment (referencing a particular signing incident). Multiple payment blocks may be added by a user in the event that they want to specify different addresses for different issuers. When deciding where to send a payment, the company should first look for the

newest block that references their particular stock offering. If none is found, then they should look for the newest block that references null. If no block is found, then they are not obliged to pay out to this particular user.

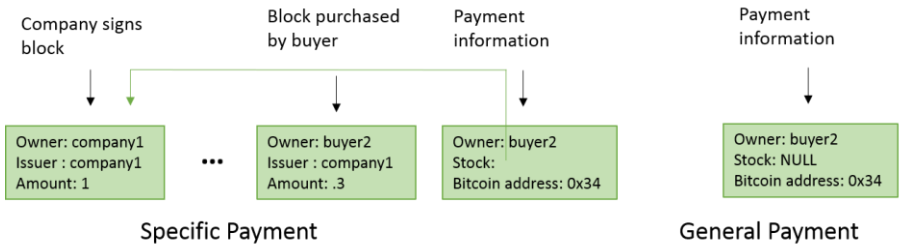

Figure 2.
A user specifying payment address for bitcoin dividends.

4. Transaction Fees

Transaction fees in this system will function in the same way as Bitcoin, with participating nodes receiving fractional equibits. These equibits may be signed or unsigned and thus the process of operating a miner becomes more lucrative because they have the opportunity to receive units that may carry relatively high values as compared to bitcoins or null-state equibits. As with Bitcoin, a larger transaction fee will encourage more miners and faster processing of transactions thus incentivising users to pay proportional to their need.

5. Distributing Earnings

In order to distribute earnings issuers will select the date and time of record which the system will use to determine who all the investors are at that given date. An amount of bitcoins (BTC) will also be specified as the gross amount of the dividend. After confirming the date and amounts the system will allocate the gross dividend across the relative share of issued units held at each address and initiate bitcoin transfers to dividend receiving address specified by each one. A transaction-like element may be added to the block chain to indicate that this operation has occurred although this is not required.

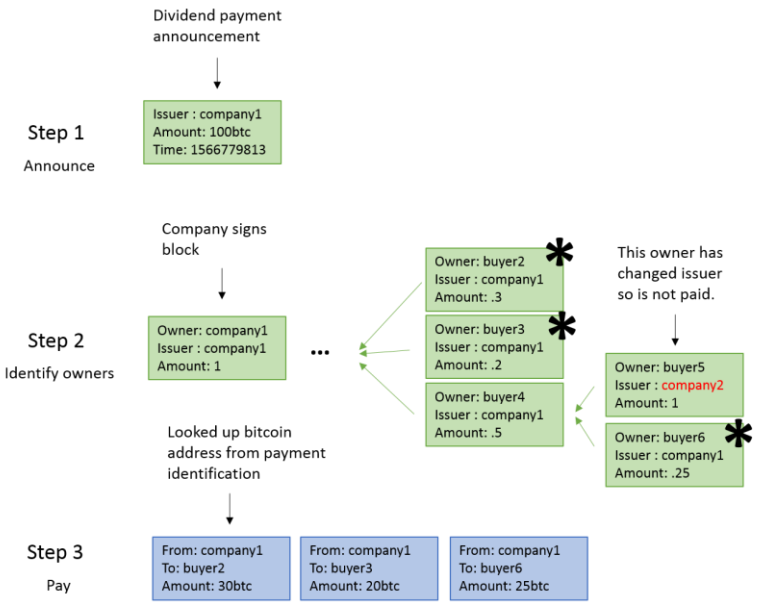

Figure 3.
Dividends being paid out to in bitcoin.

6. Polling Investors

Polls work just like dividends, but with the added step that addresses receiving the poll request are expected to send a response within a specified time frame. Issuers will create a transaction-like element representing the poll, which will specify an opening and closing date and time, the question to be answered, as well as the possible answers. These could be a simple yes or no, or multiple choices. This transaction will enter the block chain in the same way as any other transaction. The equibit software checks for all new poll transactions and will alert you if you control signed equibits from the same source.

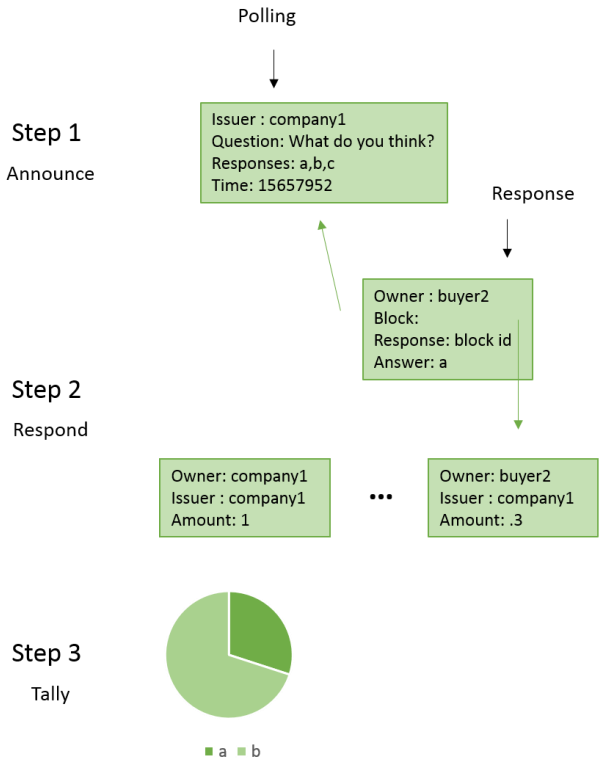

Figure 4.
How polling takes place in Equibit.

Votes are also represented by transaction-like element in which an individual selects their response to a vote block. Votes carry the same weight as each voter's proportion of the issued units. The system will weigh and tally the incoming votes to determine the overall investor consensus. Votes that are not cast by the poll closing date will be considered to have abstained from the process. The official tally will only include votes by users that owned the stock at the time the poll opened. This can be easily identified by all by checking transactions in the block chain to determine if a voter maintained control of the stock at the time in question. Votes of users who do not control stock at the time of opening are rejected by the system.

With this system, voter fraud is greatly mitigated. Secondly, the voters themselves have a greater level of assurance in the integrity of the voting process as votes are transparent, tallied automatically and effortlessly examinable by all the participants (see appendix for details on polling).

7. Attrition of Issued Units

Cancelling shares is a simple matter of the holder overwriting the issuer field with the system default, null value. This restores that unit back to its blank state and it can then be signed by a new issuer. We must allow anyone to be able to strip issuer's signatures and recycle the units they possess otherwise all of the blank units in Equibit will eventually be used up. We cannot count on individuals or companies to continually scrub the system of worthless units without the proper incentive.

By building in a system of natural attrition we create a supply/demand dynamic between the signed and unsigned units. This provides the mechanism through which the system will continually evolve with new issuers coming to market and terminated or declining business ventures being scrubbed from the system. As the maximum supply of blank units is fixed and determinable they will carry a certain value ascribed to them by incoming businesses wanting to issue equity. They will be in competition with the existing issuers who want to maintain their own equity base by providing value to their investors. Thus if an existing issuer's value drops below the value of an equivalent number of blank units they run the risk of their equity holders recycling the equity back to the more valuable blank units, which can be sold to new issuers. This also provides investors with a level of assurance that their investments will never go to zero, as they will always be able to recover the equivalent value of blank units.

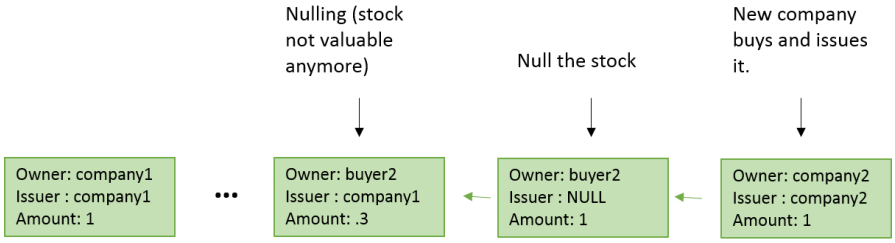

Figure 5.
A useless stock being nulled and signed by a new company.

8. Conclusion

Equibit solves a current OTC market need by replacing an antiquated, and expensive single trust system with a peer-to-peer network. It provides a great increase in openness and forces transparency on a system that is more and more popular among investors and issuing companies. Integrating seamlessly with the original Bitcoin protocol also allows Equibit to more easily gain traction with the community and can take advantage of existing infrastructure. Overall, we believe that Equibit will greatly advance how companies distribute equity and manage their ownership.

9. Extensions

There are many ways to extend the Equibit protocol now and even after its adoption. This is important to allow for changes such as integrating other digital currencies as the landscape of such currencies change. One such extension that we propose now as an example is a mechanism for paying for equibit with bitcoin. Say, person A, wants to sell their equibit to person B, for their bitcoin. To perform this transaction, one would usually need either a high level of trust between the two parties or a third party to act as an escrow agent. We propose instead, a protected transaction. In a protected transaction, the seller includes in the equibit transfer block, the seller bitcoin address, the buyer bitcoin address and the agreed upon amount of the transaction. This equibit is now considered in escrow and cannot be sold, cannot receive dividends, or vote, by either party. The equibit only changes state when one of two things happen. First: the bitcoin transfer is observed as stated in the bitcoin block chain (in which case, the receiver now owns the equibit). Second: the sender posts a retraction (in which case the equibit reverts to the sender). One problem with this transaction is synchronicity. If the bitcoin transaction has occurred and

the retraction posted, one must decide which one wins. While you could use a simple, first one in wins, this neglects the potential time lag between the two block chains (Bitcoin, and Equibit). To protect this, a sale of bitcoin wins over a retraction unless the bitcoin offering is more than 1 hour later than the retraction. Similarly, a retracted equibit is still considered in escrow for 1 hour after it is submitted.

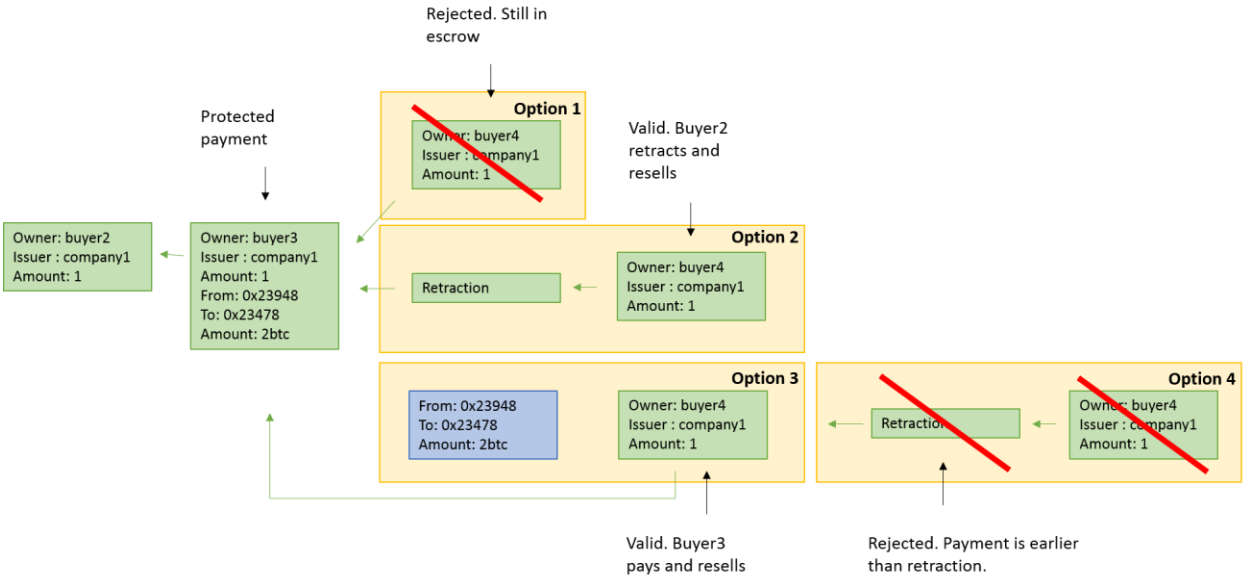

Figure 6.
Four possible outcomes of a protected transaction between Equibit and Bitcoin.

10. Appendix

We add three new transaction types to the Bitcoin system in order to deal with polling and dividends. These new transactions are incorporated into blocks in the same way that traditional exchange transactions are added but do not represent the exchange of equibit units.

A polling unit contains the following fields

id: A unique ID, similar to that in an exchange transaction.

fee: A tip that will increase the likelihood of this transaction being added.

from: A block from which the tip will be taken.

to: The same user. The quantity field here must be zero.

poll: The polling request. Must be in the following format:

"first question description","first possible answer","second possible answer" …

"second question description","first possible answer","second possible answer" …

...

due: Time in milliseconds since the epoch at which the poll closes.

To prevent clutter of the chain, if the poll field is too long, it can be rejected by the system. This can be defined as a sliding size requirement over time depending on the needs of the blockchain.

A response unit contains the following fields

id: A unique ID, similar to that in an exchange transaction.

fee: A tip that will increase the likelihood of this transaction being added.

from: A block from which the tip will be taken.

to: The same user. The quantity field here must be zero.

poll: The identifier of the poll that is being responded to.

response: Response to a particular poll

A response should only be accepted into the block-chain if it can be verified that the responder owns some stock in the polling company. This will prevent clutter of the chain. The response field must also match one of the possible polling options in the relevant polling block.

A dividend unit contains the following fields

id: A unique ID, similar to that in an exchange transaction.

fee: A tip that will increase the likelihood of this transaction being added.

from: A block from which the tip will be taken.

to: The same user. The quantity field here must be zero.

amount: The amount in bitcoin that will be distributed.

time: Time in milliseconds at which equity will be distributed (optional field).

A dividend unit is not required as a company may choose to send out equity as they desire. However, it is a courtesy to the system to include this block to indicate that such a transaction has occurred. The time field is optional although it may be set for a future date to indicate that the dividend will occur at a given time and potentially increase the current value of their stock. Note that there is nothing forcing a company to perform a shown dividend innate to the system, except for the potential loss in value of their stock and reputation as a company. Also checking that such a dividend has been performed requires a user to check that the company has indeed performed transfers to the given Bitcoin addresses.

References

[1] Abdul-Rahman, A., & Hailes, S. (1998, January). A distributed trust model. In *Proceedings of the 1997 workshop on New security paradigms* (pp. 48-60). ACM.

[2] Dou, W., Wang, H. M., Jia, Y., & Zou, P. (2004). A recommendation-based peer-to-peer trust model. *Journal of software*, *15*(4), 571-583.

[3] S. Nakamoto, (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org/bitcoin.pdf

[4] Reid, F., & Harrigan, M. (2011, October). An analysis of anonymity in the bitcoin system. In *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)* (pp. 1318-1326). IEEE.