Decentralized share issuing and distribution

In this document I describe how a decentralized share issuing and distribution system should work and why it is important to have one. This is supposed to be a non-technical introduction into the subject. All the technical details like which cryptographic algorithms to use and protocol specifications are left out and are non-important at this point. Although, some familiarity with Bitcoin ideas and concepts is required to understand this document.

Sections of this document are:

1. What's wrong with how companies are funded now?
2. A proposed idea: how a decentralized share distribution is going to work?
3. Terms to be used to describe the system.
4. Practical applications of the proposed protocol.
5. Possible shortcomings and busting some myths.

1. What's wrong with how companies are funded now?

Before we even start discussing this subject, I should probably note that a clear distinction between public and private companies exists purely within the governmental framework of law. From the standpoint of view of company shareholders there is no clear line: it simply gets more complicated to control the company which has more people as shareholders. It is a government that draws a clear line when a company should start to consider itself public.

That said, ultimately, it is a government that sets the rules for companies to distribute their shares and then also rules to distribute information that may affect those shares' prices and, thus, shareholders' interests. The problem is, that these rules are very often ineffective (insider trading happens all the time), navigating through these rules requires a lot of time, money and knowledge for both the company and its shareholders.

Another major problem is that it is rather difficult to invest in a company as a minor shareholder. Especially if this company is not a publicly traded one. At a minimum you'd have to hire a lawyer and go through all the paperwork before you can safely invest your money. Needless to say, that if the proposed investment is negligibly smaller than the amount spent on all the legal procedures people won't invest. Thus, a governmental legal system denies access to capital for startups whose only chance to get funded is by many small investors. And, of course, it denies investment opportunities to those who are not willing to invest enough to cover the legal costs.

Finally, it is very difficult for companies to set various rules for its investors. Companies do have some freedom - for instance they have a choice to pay or not pay dividends - but in many cases that freedom is very limited and does not allow them to do certain things that might be beneficial (although possibly more risky) to both the company and its shareholders. Ultimately, it's not the question of what rules to have (which is the answer a government tries to answer), but rather who's to decide on the rules. The proposition here is to shift the decision making to the parties involved into each particular deal.

Thus, goals for any kind of replacement for this system should be the following things:

1. Make it cheaper for people to invest.
2. Open more opportunities for companies to be funded.
3. Provide cheaper way of litigation conflicts either through purely technical

means or through a private mediator.
4. Allow more freedom in setting various rules of investment.

2. A proposed idea: how a decentralized share distribution is going to work?

Let's start with what we already have - Bitcoin - and step by step we'll change parts of the protocol so that it suits share distribution.

In Bitcoin, we only have one type of units - bitcoins themselves. There are no different kinds of bitcoins and the price of each one unit is exactly the same at any time. This is contrary to a system in which we need shares that are attributed to various entities. So the solution is to simply have as many different types of units as needed. By *type of units* I basically mean some name for all the shares of one particular company. A new *type of units* can be created by anyone at any time and the creation of a *type* can be seen as an act of incorporation. Only you don't pay anything at all for this procedure and you don't have to notify any kind of authority. The very fact of the creation of a new *type* is automatically broadcasted to all nodes in the system.

After the creation of a new type of units one creates units themselves. It is the owner of the type who ultimately decides how many units to issue. In general, the exact number should be irrelevant (of course, a number may not be more than a corresponding data type can store), so whether it's 1,000 or 1,000,000 would in no way affect the initial price of a single unit, which is going to be zero until the first purchase. After the initial issuance of shares there shall be no more additional issuance in order to prevent share dilution.

Now as the units are created they may be transferred to other parties. The act of transferring should be very similar to Bitcoin transactions, which means that it is

not a protocol's concern whether those shares were paid for or given away for free. The price of a single unit itself is determined outside of the distributed system on stock exchanges or in individual deals. It may be possible, however, to condition the execution of deals on external events like Bitcoin transactions and such.

In Bitcoin, as soon as units arrive and transactions are confirmed, the money are yours and you are free to do whatever you want with them. With shares it should be slightly less so: types of units may have certain *rules* which may affect how future shareholders can distribute their shares. Those rules are created by the initial owners of a particular type of units and may be amended later (if those rules themselves allow amendment). Of course, as well as other factors, these rules will be reflected in and will affect the price of each unit of this type. For example, a rule may exist for this type of units that no initial shareholder can sell most of his shares all in one day without the approval of the 70% of already transferred shares.

The rule system allows for various combination of powers to exists for various entities. Those rules are set before a single share is issued and all shareholders buying shares implicitly and voluntarily agree to those rules. This is contrary to the existing legal system where most of the rules are set by a single authority. Even more important is that the enforcement of those rules lies in the technical implementation of the protocol and thus they cannot be changed through procedures not agreed upon beforehand.

Rules, as created by the issuers of shares, are accepted by the entity (and, obviously, its founders) voluntarily. Thus, in stark contrast to a current legal system, they are seen not as a burden, but rather as a means of attracting capital.

Various types of rules that may be useful are discussed in the *"Practical applications of the proposed protocol"* section of this document.

The proposed system allows for gradual growth and investment cycles not constrained by the rules set to any particular kind of entity by a single authority. Let's say a company needs $10,000 and issues 100 shares, half of which the

founder wants to keep to himself. He then has an option of selling 50 shares to one single major investor or to 50 minor investors at as little as $200 each - all at the same processing cost - minor investors need not engage in costly legal procedures to secure their shares, as they are simply transferred to the now shareholders and they own them just like people own bitcoins.

A question may be raised, who guarantees a shareholder really owns a part of a company? In the existing legal framework it is the government who does this. The paperwork a government has to review in order to determine whether someone owns a share is ideologically no different from the blockchain of transactions we see in Bitcoin or the one that may be used in the proposed system. What's different is the cost of enforcing of what's written on a piece of paper (or in bits) and the reliability of the enforcement. In the case of the proposed system, many rules can be enforced without any human being reviewing and interpreting them. Other rules may be enforced by the agreed upon mediator. In any case, it is ultimately the trust - not the rules - that is required for a company to obtain any investment. From the standpoint of view of the minor investor who invests $200, it is irrelevant whether a government can or cannot enforce an entity to pay his fair share in the future. What's important is the probability of him getting his share, which depends on many factors, among which reputation and trust as well as purely technical constraints play a major role.

All that said, the proposed system indeed achieves the goals stated in the first section of the document:

1. It makes it cheaper for people to invest **by eliminating unnecessary legal costs.**
2. It opens more opportunities for companies to be funded **by the same token as (1)**
3. It provides a cheaper way of mitigating conflicts **through hardwired rules** or through a private mediator.
4. Allows more freedom for the company to set its own rules suitable for the type of operations it has.

3. Terms to be used to describe the system

Before we start with examples, I would like to agree upon a set of simple terms to be used:

- A ***type of unit*** or simply a *type* indicates which entity (company) this share belongs to. One may think of a type as a Class and share as an Object in OOP. As in OOP, it would probably be useful to have some kind of inheritance where different types of units may all belong to a single entity.

- A ***unit* or a *share*** represents the actual instance that gives its owner the right to claim something from the entity this share is attributed to.

- A ***rule*** is a programmed constraint that all units of a particular type know about and follow. Thus, when a new type is created, all its rules are created as well. Rules may be amended in the future but only by the procedures determined by the rules themselves. It would probably be reasonable to have a default set of rules applied to all newly created types unless others are specified.

- A ***type of rule*** is a feature of the protocol that allows for creation of various rules. For example, we may have a *type of rule* that requires a number of shareholders to allow initial shareholders to sell their shares. The actual *rule* implemented for this *type of rule* may sound something like “70% of other shareholders must approve the sale of more than 30% of shares from an initial shareholder in a single day”.

- A ***transfer*** is like a transaction in Bitcoin. You can transfer units from one address to another, thus changing their owner.

4. Practical applications of the proposed protocol

Practical applications are mostly a matter of implemented *rules*. In this section I will give a few ambiguous examples of *rules* from which *types of rules* can be derived later. This is not a specification of types of rules, which is to be created when implementing a protocol.

- An entity may wish to appear loyal to its potential shareholders by creating a rule which makes it impossible to transfer more than 30% of shares from initial address (founder) to another in a single day without the agreement of 70% of other units (in this case, I say *agreement of units*, because I would like to emphasize the difference from saying *70% of shareholders* - as it would be very easy to create an infinite amount of addresses each holding an infinitesimal share). This rule may ensure there are less options for insider trading. By settings various values for this rule, a company may find just the right combination to attract the maximum and the right kind of capital.

- A founder may set a rule by which shares when offered for sale should first be offered to a particular address at the same or lower price. This, obviously, requires external verification of value which can be performed by plugging in to other protocols, like Bitcoin.

- A rule may be created that prohibits any kind of rule amendment unless 99% of shares agree upon it.

- A rule may state to which degree a single share is divisible. Together with the number of actual units issued, this may be a good instrument in controlling the number of shareholders a company may have and, thus, controlling the balance of power between entity owners. It may also affect other rules dramatically as in the example where 70% of shareholders have a

voice: the less shareholders an entity can have, the less incentive it creates for a single shareholder to create many addresses for himself, pretending to be minor shareholders, and that way shift the balance of power.

[to be extended]

5. Possible shortcomings and busting some myths

[not yet written]