Peer-to-Peer Asset Issuance and Transactions with Confidence Chains

by BlueMeanie(a Pseudonym)
josh.josh421@gmail.com
www.altchain.org

May 14th, 2013

Abstract:

Bitcoin's popularity has grown exponentially in recent years as a new form of digital money that transcends geography and national governments. This paper describes a system for 1) **Asset Issuance** meaning the creation of digital property 2) and **Asset Transactions** meaning the exchange and trade of that property. Many of it's internal structures are derived from Bitcoin technology, thus many innovations in the Bitcoin world carry over to this platform. It is truly Peer-To-Peer, meaning there is no central server required. A very high level of transaction integrity and security can be achieved. It has several advantages over Bitcoin, namely speed of transactions and no need for 'mining'. The system is suitable for a wide range of applications, it is powerful enough to do high volume securities trading, secure enough to trade precious metals, and simple enough for Community Currency implementations. In this paper we will describe the core algorithm of **Confidence Chains**, in other proposals we will offer more details regarding asset issuance and related features.

1. A Few Notes on the Theory of Money

Money is, at it's essence, a tool for groups to interact with each other on a quantitative basis when social values are unstated, unclear, or unresolved. According to free market theory, the market is no less than a machine that generates social values by the very determination of winners and losers. Here we put the notion of wealth in the abstract, as a system of merit. Marxist/Socialist ideas could be seen as a revolt against this determination, a seizure of social values that directly opposes the determinations of the marketplace. We state these points because **Confidence Chains** recognizes the fact that money and authority cannot be divorced. Ultimately there *must* be a relationship between the digital asset and real world asset, thus some party(and this party may be organized in a very complex way) must ultimately back that value. Bitcoin *attempts* to model economic worth in a seemingly new way through the notion of 'proof of work'[1]. At Bitcoin's outset, the real world relationship to computing power was not so obvious. Today's world of mining pools and ASIC hardware manufacture display this relationship quite plainly. How this economic model plays out in the long term is not fully known. What is needed by the greater world of finance is a tool to allow for the peer-to-peer exchange of ANY asset. These Assets must be easy to identify(credible), have strict issuance qualities(impossible to covertly inflate, deflate or to alienate from public contract), and be readily communicable(tradable, movable, etc.). With these basic features, many useful applications can be developed(see below).

2. Confidence Chains

Here we introduce a new concept: **Confidence Chains**. This structure inherits many aspects from Bitcoin: transactions, blocks, and a hash timestamp. We revisit Satoshi Nakamoto's notion of 'trusted party'[5]. For our target users, the concept of a trusted party is implied in our financial arrangement[3]. We have, in all our use cases, an issuing party and asset owners necessarily have a relationship with this party. Confidence Chains offers, however, a very flexible way to define this trust relationship that is suitable for a wide range of applications. It also offers a very high degree of **irreversibility**, that does not necessarily depend on the direct authority of one party. It has similar anonymity and security characteristics to Bitcoin.

Like Bitcoin, the system is composed of a set of nodes in a peer-to-peer network arrangement. Each new transaction is published to all other nodes[6]. Periodically these transactions are packaged into blocks that are hashed to the current head of the block chain, cryptographically signed, and then broadcast to the entire network. Each node maintains a model of all transactions in the currency and most importantly attempts to work off the **most confident** block chain available to it. This confidence is determined by a simple algorithm(explained below). A key characteristic of this algorithm is such that *the more identities which approve the chain the higher the total confidence*. In addition, the chain(like Bitcoin) offers cryptographic *unidirectional temporality*. This linear aspect makes it difficult to reconstruct the chain and prevents problematic transactions(such as the double spend situation). It establishes *irreversability* because for any one individual node to create a false chain of higher confidence, and perhaps disrupt the network, they would need to re-poll each identity to reauthorize each block in the chain. Each particular identity would have no rationale to do that, unless of course they colluded to corrupt the currency. It is possible, in cases where high security is an absolute requirement(such as DGC schemes) to strictly prevent such an occurrence(at a cost of network node equality). In other scenarios where node equality is part of the social value system, security is attained by group interaction over time. Note that in this system, both configurations are supported with a common technology.

3. A Confidence Block

A Confidence Block is similar to the Block in Bitcoin, however it lacks the 'Proof Of Work' aspect(no *nonce* or requirement for SHA result). It is a set of transactions and a hash of the previous block. This block is then RSA signed by a participating **identity** in the network(not all nodes need identify themselves, full anonymity is supported). The chain is a linear linked list of RSA-signed transaction blocks. see: fig 1.

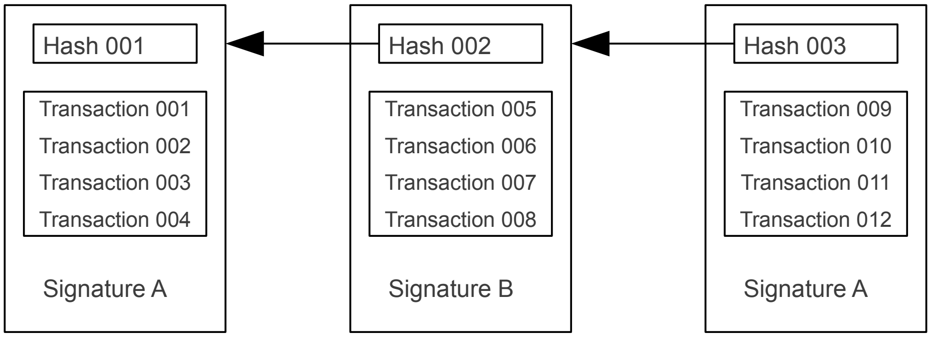

Figure 1

4. Confidence Algorithm

Each node in the network seeks to work off the most **confident** block chain available to it. It's important to understand that the algorithm is only a *recommendation*. Each node is free to adopt any metric it wishes to measure confidence, however choosing an idiosyncratic method will result only in disruption for the individual rather than the community(referred to as an *idiot node*). It may be possible, in some cases, for nodes to collude by publishing and promoting an alternative subversive chain, but in most scenarios this would be socially impossible(in some scenarios it may actually be invited). The most basic fundamental metric for confidence works as such:

i. Each **signed block** means that it and all blocks before it have been **approved** by the signing **identity**.

ii. Each block's **confidence value** is determined by the summated **identity weight** of each **identity** that **approved** it.

iii. The total **confidence** of the chain is computed by tallying the **confidence value** of all the blocks in the chain.

So in the action of the network, nodes keep on record all broadcasted transactions and signed blocks. If a particular node believes that it can create a *more confident* block chain by publishing a signed block, it does so[7]. If other credible identities accept this block as valid, then they in turn build their own subsequent signed blocks on top of it, creating a block chain of even higher confidence value. The action of the network continues this way creating a currency of higher and higher confidence. The confidence only **increases** over time, enforcing **irreversibility**. At any given point in the operation of the network, it becomes impossible for any single node to construct a chain of higher confidence with the information and cryptographic resources available to it individually, thus no single node can defraud others. The **confidence** of the chain becomes an **irreversible** function of the historical cryptographic interaction of one or more nodes.

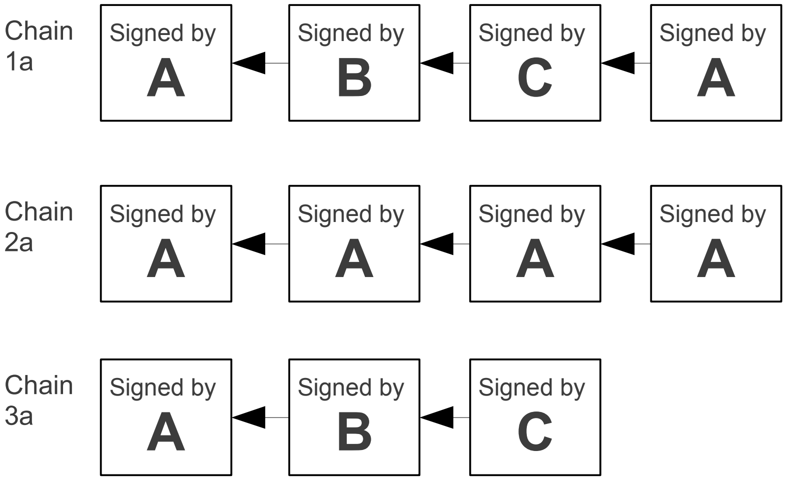

Figure 2

Figure 2 illustrates several sample **confidence chains**. In this case we have 3 different identities: A(weight 3), B(weight 2), and C(weight 1). Thus, the total Confidence Value for Chain 1a = (3+2+1) + (3+2+1) + (3+1) + (3) = 17. for Chain 2a = (3) + (3) + (3) + (3) = 12 and Chain 3a = (3+2+1) + (2+1) + (1) = 10. This demonstrates several features of the algorithm. For one the difference between chain 1a and 2a show the effect of diversity on the the chain(the more identities that participate in the chain the higher the confidence value). Secondly the difference between 1a and 3a show the effect of time(confidence value increases as time and chain length increase).

5. Incentives

What incentive does a node have to publish a signed block? This is an important consideration as it differs significantly to Bitcoin. First, the cost to compute a block is comparatively very low to that of Bitcoin. Similar incentives to Bitcoin may be offered by the issuer, but in most cases the resource costs to do so are relatively low, perhaps negligible. Other incentives may be designed. Secondly, in the majority of cases, participation in a trading community implies that the user has confidence in the future viability of that currency, thus active participation can be expected of that user. Our users motivations, tendencies, and p2p obligations differ significantly to that of Bitcoin. For many situations, the validating identities will be predetermined and fixed.

6. Identity Weight

By providing suggestions as to the **identity weight**(see algorithm above) the system may be fine tuned for different applications.

ex 1. Digital Gold Currency

In this case we have high dependence on a particular party for reimbursement(the DGC issuer), thus a very high weight is given to the issuance node, and other nodes begin with a very low weight. Ultimately, each of the owners and traders of the DGC need to eventually cash in their digital assets for gold with the issuer, thus at any given point of operation they look to work on a transaction chain with direct approval of the issuer(the notion of *fiat currency* is practically inapplicable here). This is our basic case and doesn't really offer strong P2P(it's similar to the kind of arrangement systems like Open Transactions offer). A more robust configuration is to coordinate two or more parties who are unlikely to collude, who are then given equally high **identity weight**. They in turn each validate the block chain. If any one party defects, falls out of favor, or is rendered inoperable, transactions continue unabated. For instance, each of the primary identities may be located in a different political region, thus adding to the overall confidence of the DGC issue's integrity.

ex 2. Securities Trading

One key problem with central authority model found in systems such as Open Transactions is the problem of 1) **transaction denial** or 2) **transaction prioritizing**. In the first case the central authority denies a client the ability to conduct transactions, this obviously has a negative effect on the ability to conduct commerce. In the second the central authority privileges one party over the other in order of precedence. In the case of high frequency trading, prioritizing could result in major gains or losses for particular parties according to the bias imposed. By distributing authority, this kind of bias becomes impossible, greatly adding to the credibility of the asset exchange.

ex 3. Community Currency

Community Currencies have unique characteristics in that some attempt to operate without the recognition of a central authority at all. Such an arrangement would be reflected in a more equitable **identity weight** arrangement where even casual members of a trade community would have the power to validate the transaction chain. Even more complex and innovative techniques could be used to derive **identity weight**, such as membership in a social network, possession of a digital asset in the system, or any other imaginable criteria. As long as there is a broad consensus(and this does exist in most Community Currency schema) then the possibility of exploit is extremely low.

7. Conclusion

We have outlined here the basic mechanism for a peer-to-peer system of asset issuance and transaction. The system has no requirement for central authority. Many interesting and valuable applications can be built on top of this basic system, to name a few:

1) a stock exchange similar to NYSE or NASDAQ or a commodities exchange similar to CME.

2) a 'voting shares' mechanism where rights(e.g. to a DNS record) are automatically determined by percentage stake in a tradable asset.

3) markets for complex assets(e.g. Credit derivatives allowing for a real and complete open source decentralized credit system).

In addition this system offers a high degree of familiarity to Bitcoin developers, making many technologies easy to adapt or implement. For instance we can easily determine feasibility of strong anonymity in Confidence Chains by refactoring the concepts from Zerocoin[2]. The technology is not subject to many problems encountered in Bitcoin. It's very easy to upgrade or modify the transaction formats according to need as there is no master block chain and no backward compatibility issues. Overall this technology offers a clear value to the financial world and those software developers concerned with implementing decentralized money systems.

8. References & Footnotes:

[1] S. Nakamoto, “Bitcoin: a Peer-to-Peer Electronic Cash System”

[2] Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin, “Zerocoin: Anonymous Distributed E-Cash from Bitcoin”

[3] in our system however trust may be distributed to many parties

[4] from [1]:

> The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

[5] for instance you cannot extract the Issuer from a Digital Gold Currency scheme. Ultimately the owners of the digital asset **must** be able to exchange them for real gold.

[6] partial network visibility is not a serious problem for the system

[7] there may be other cases where a node might sign a block, but in this is the common one.

With special thanks to Maria.