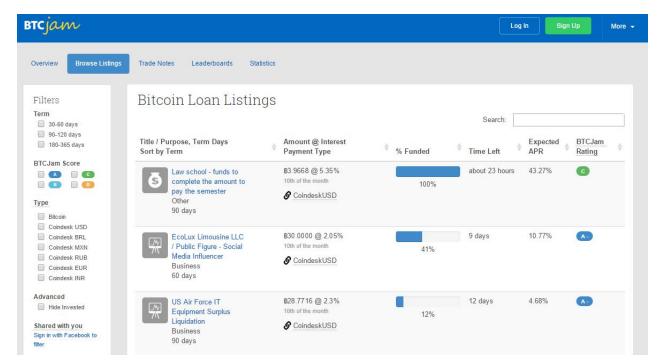
Loans and Financial Instruments in the Bitcoin Marketplace

Trisha Hajela and Merlin Zhang May 3rd, 2015 As the popularity of Bitcoin is growing, we thought it would be interesting to look into the current state of Bitcoin lending. The market for Bitcoin lending is expanding steadily, with new platforms emerging rapidly. Our project aims to examine the current state of Bitcoin lending, propose changes to the current system, and analyze the application of the Credit Default Swap as a solution to keeping Bitcoin lending anonymous.

CURRENT STATE OF BITCOIN LENDING

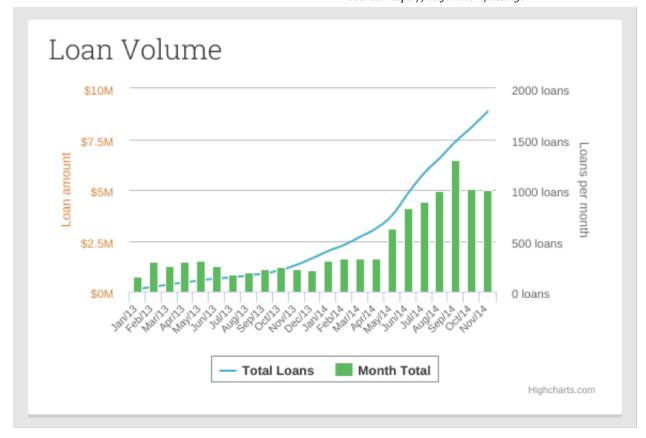
Bitcoin lending has many differences and similarities to common currency lending. Bitcoin lending is more universal than common currency lending because Bitcoin is a universal currency, which means that there is less overhead because there is no need to convert between different countries' currencies. The major differences between Bitcoin lending and common currency lending is that there is no real concept of standardized credit scores with Bitcoin lending. Because of this, Bitcoin lending has higher default rates due to higher rates charged to borrowers when the loan is repaid. Bitcoin lending is fairly new, in contrast to the more established common currency lending. Both forms of lending involve interest rates, intermediaries, and platforms. We will explore these aspects further by first introducing the major Bitcoin Lending Platforms.

There are three major Bitcoin Lending Platforms that facilitate lending among Bitcoin holders. The first, and most popular, is BTCJam. BTCJam is the largest p2p lending platform for Bitcoin. To use BTCJam, a borrower makes an account with their information and then lists their loan. This platform does not preserve anonymity, and in order to use this service the borrower must sign up with a valid email address and name. One feature that distinguishes BTCJam over other platforms is that the platform allows you to sell off a portion of your loan on the platform, without any need for a third party system.



Interface of BTCJam

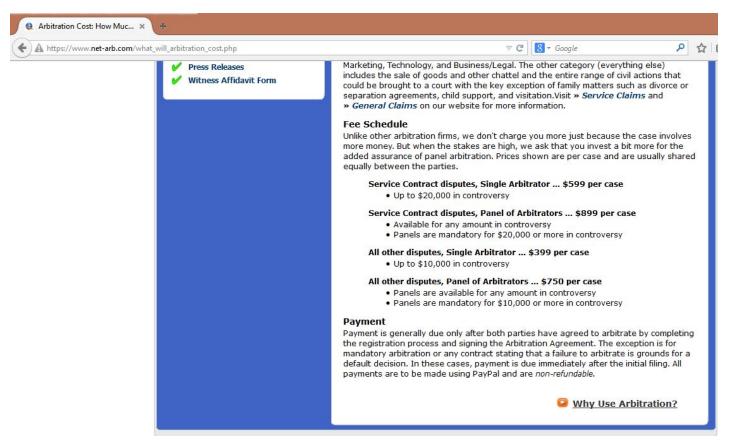
Source: https://btcjam.com/listings



Graph of loans between 2013-2014 on BTCJam

Source: http://www.lendacademy.com/introduction-marketplace-lending-bitcoin-part-2/

BTCJam uses a third party service called net-arb for loan collection. Although net-arb is a third party service that handles arbitration, it is very rare that BTCJam loan collection will actually happen through this service. The reason for this is that the costs involved with the overall process are relatively high and depend on geography, which may make it impractical for a lender to follow through. We believe that using net-arb is not the best way to handle loan collection because of the cost factors, and we will elaborate later on what we propose to be a better loan collection and accountability system.

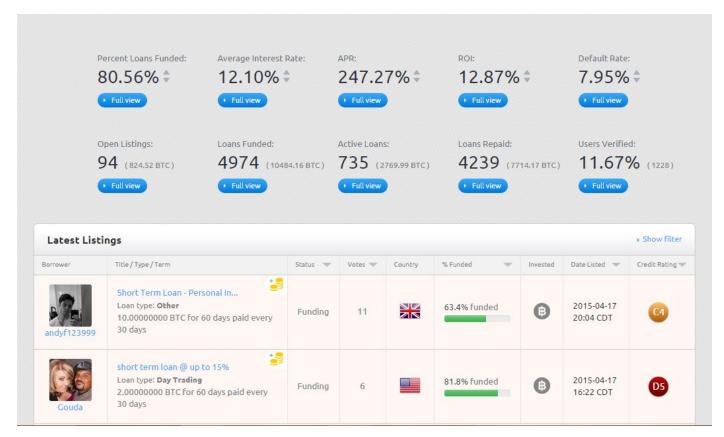


Fee breakdown for using net-arb

Source: https://www.net-arb.com/what will arbitration cost.php

BitLendingClub, the second largest Bitcoin lending platform, also does not preserve anonymity because of the signup features similar to BTCJam. BitLendingClub is quite different from most lending platforms in that it fosters a reverse auctioning system, where the borrower defines the amount of the loan and the interest rate which is then fulfilled by investors. BitLendingClub also features an amortization schedule and implements a pseudo-credit score feature named the "reputation" of the borrower. Borrowers with less than 100 reputation cannot automatically withdraw the coin that they borrow; they must have a legitimate reason and go through a manual process to do so. BitLendingClub does research and discloses suspicious activity about borrowers to investors regarding suspected multiple

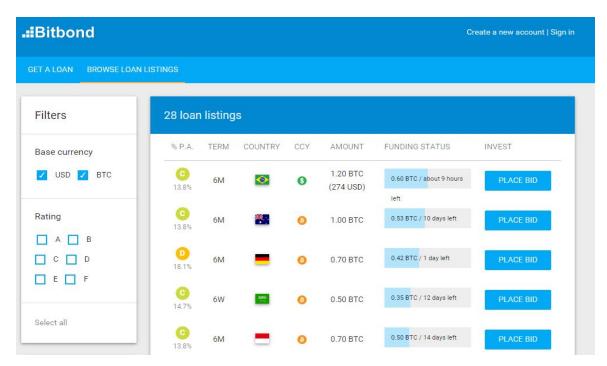
accounts and IP addresses. For loan collection, BitLendingClub releases the personal information of the borrowers to the lenders so that the lenders can pursue legal action against them. As with BTCJam, the loan-collection rate under this system is virtually zero. The reason for this is similar to BTCJam, in which the cost of loan collection (lawyers, transportation, time) exceeds the amount of the loan which makes it impractical.



Interface of BitLendingClub

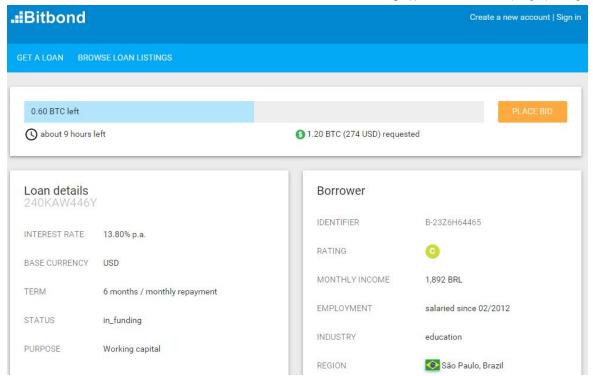
Source: https://bitlendingclub.com/

Bitbond is the last largest peer to peer platform for Bitcoin lending. What distinguishes Bitbond from the other platforms is that tries to preserve anonymity by identifying borrowers and lenders with a combination of numbers and letters that comprise the identification string. Bitbond has the lowest origination fees (~0.5-1%), which are fees that are paid to the intermediary for processing and handling. Bitbond also offers long-term loans that range from 3-5 years, a feature not available with the other platforms. For loan collection, Bitbond releases the personal information of the borrower to the lender and also sells the claim to a collection agency. To reiterate again, this system of loan collection rarely works because the incentive for lenders to follow through with collection is small.



Interface of Bitbond

Source: https://www.bitbond.com/buyer/listings



A loan listing, with blind identifiers

Source: https://www.bitbond.com/buyer/listings

One significant aspect of common currency loans that hasn't been integrated in Bitcoin is a real concept of standardized credit scores. Credit scores have been slightly integrated through reputation scores and letter-grades assigned to a particular borrower, but these are very dependent on the platform and are not uniform across platforms. We think that it could be possible for credit scores to be integrated into Bitcoin addresses, but we believe that this would severely impact the decentralized nature of Bitcoin. Credit scores are calculated by credit bureaus that differ across country lines. Since Bitcoin is a universal currency, it will be difficult to integrate a credit score standard that will work across country lines. Furthermore, credit scores are computed by a relatively secret algorithm (if the algorithm was public, people would be able to cheat the system). Integrating an algorithm that only a few authorities know about would severely hinder the decentralized nature of Bitcoin. We instead will propose a system where loan-repayment will be an incentive for borrowers, in the hopes of minimizing the high-default rate with Bitcoin loans that exists today.

IMPLEMENTATION OF FINANCIAL INSTRUMENTS INTO THE BITCOIN MARKETPLACE

Bitcoin, as a decentralized peer to peer cryptocurrency, theoretically cannot be regulated. Its decentralized nature juxtaposes with the more centralized financial systems that catalyzed its initial conception and eventual creation, so the introduction of financial markets and lending systems in Bitcoin introduces a number of conundrums and poses several challenges.

Financial markets require a degree of liquidity. For example, stock markets require matching of sellers and buyers, leading to centralization. Matching borrowers and lenders in the Bitcoin market is a challenge due to Bitcoin's decentralization and the lack of regulation and enforcement of repaying loans. Consequently, the very notion of financial markets is at odds with the Bitcoin market.

The degree of anonymity that Bitcoin provides certainly has appeal. That same anonymity, however, introduces a glaring problem in the establishment of lending markets. Without accountability, no individual has clear economic incentive to repay loans.

We propose a solution to help users maintain anonymity while providing a platform for lenders and borrowers. In order to do so, our proposition involves a centralized intermediary that matches borrowers and lenders. Although doing so seems to undermine Bitcoin's peer to peer, decentralized nature, a centralized intermediary, the intermediary provides a service and should be treated as such, more so than as a centralized authority. The service will thus charge a small fee for its usage that will only apply to lenders, who would be using the service in hopes of generating a profit. Charging such a fee to borrowers would be pointless because borrowers could simply increase the value of a requested loan, thus shifting the service fee to lenders. Additionally, borrowers are less likely to have existing capital to use such a service in the first place.

In order to maintain anonymity, every user who creates an account will be provided with a randomized account number to shield their Bitcoin wallet to protect their identity. This is similar to the strategy explored by BitBond. Borrowers will have their user accounts display the amount they wish to borrow, and lenders will be able to search for users wishing to borrow. Lenders are provided a choice as to whom they wish to lend based on personal averseness to risk.

The intermediary will have a bitcoin wallet that accepts loans from lenders. These loans are then transferred by the intermediary to borrowers. With sufficient traffic, even with all transactions recorded, it would be extremely difficult to map borrowers to lenders, especially if the period of time made between transactions between parties was randomized to a degree. Such a system would guarantee a high degree of anonymity. Additionally, should borrowers display suspicious behavior, or should lenders wish to retract their loans, the intermediary will have the ability to halt loans.

In order to tackle the issue of defaults, we propose a tiered credit rating system for different groups of users and their rates of defaults. This way, interest rates on loans can be charged accordingly, and borrowers are incentivized not to default if they wish to request future loans. In the case of default, users with a low enough credit score will have their Bitcoin wallet's address revealed publicly, thus eliminating (to an extent) their anonymity, especially since transactions are made available on the blockchain. For those with mid-level credit ratings who default, their address will be revealed solely to the lender.

Lender

		Payment	Default
Borrower	Payment	-I, I	0, -F
	Default	L-R-A, R-L+A	0, -F

I = interest

L = face value of loan

R = amount repaid

A = value of anonymity

F = service fee

We provide two simple models loosely based on game theory to analyze incentives involving transactions between borrowers and lenders.

For a loan, a lender can either choose to make a payment (provide a loan) or default (provide no loan). A borrower can either make a payment (repay a loan) or default (fail to repay a loan). If lenders provide no loans, their only cost is the small service fee paid to the intermediary, while the borrower loses nothing.

On the other hand, if a lender provides a loan, two cases arise. The borrower can repay in full in addition to interest. Thus, the borrower will have a net loss of -I, the amount repaid in interest, while the lender will gain I, the return on investment. In the case that a borrower defaults, the borrower will walk away with the face value of the loan minus whatever repayments they have made, which can be anywhere in the interval of [o, L), but with the potential of losing anonymity. Since transactions are all recorded on the blockchain, there is a cost to losing anonymity, particularly if the lender decides to pursue legal action. Although geography acts as an obstacle in loan collection, default remains a risky move on behalf of the

borrower because the location of the lender is unknown. Thus, the borrower will only default if the risks and costs associated with loss of anonymity do not exceed L-R. Meanwhile, the borrower loses R-L+A, the amount recuperated minus the face value of the loan plus some limited knowledge of the user's identity.

In order to reduce risk for lenders, we also propose a modified version of a credit default swap. In a regular credit default swap, two parties engage in normal loan agreements. The lender has the option of purchasing a credit default swap from a third party. The third party receives a portion of the interest paid on the loan from the lender as long as the borrower does not default. In the case of default (before an agreed upon date specified between the lender and third party), the third party will pay some fixed value to the lender (usually the face value of the initial loan).

Our version of a credit default swap involves the intermediary taking over the role of the third party. Should a lender choose to purchase a CDS, the intermediary will keep a percentage of interest payments made by the borrower. In the case of a default, the intermediary will pay an amount to the lender and purchaser of the CDS; however, this will not be the full face value of a loan. Instead, it will be (L-R)^{1+d^2} where d is one minus the default rate associated with the borrowers credit rating. Thus, the payment from the CDS will be greater if the credit rating of the borrower is lower, which will incentivize lenders to lend to more risky borrowers to generate a larger user base. In order to minimize risk for the intermediary, however, the interest rate on repayments for riskier borrowers will be significantly higher.

In the case of a CDS purchase, the risk of loss from default is shifted from the lender to the intermediary.

Intermediary

		Payment	Default
Borrower	Payment	-I, p*I +F -C	-I, p*I +F
	Default	L-R-A, -(L-R) ^{1+d^2} +F	L-R-A, -(L-R) ^{1+d^2} +F

C = cost of precaution

d = 1-risk percentage risk of default associated with a borrower's credit rating

p = percentage of interest on loan agreed in CDS sale by the intermediary and lender

In the above case, a CDS is involved. The game is the same for the borrower, but the other party is the intermediary rather than the lender. The intermediary has two choices: take precaution against default (payment) or take no precaution (default). Payment and default for the intermediary involves a simple difference of C, cost of precaution. If the borrower does not default, then the intermediary receives a percentage of the total interest paid plus the fee paid by the lender. In the case that the borrower defaults, the borrower walks away with L-R, the face value of the loan minus the amount repaid, but must assume the risks and cost of loss of anonymity. The intermediary, assuming it took sufficient precautions against default, will be able to cover the cost of precaution, and will pay the CDS buyer the previously agreed amount while keeping a fee (of course, there exists potential to retrieve an amount greater than C by the intermediary to further cushion its losses). In case the intermediary does not take precaution, the same outcome is guaranteed, but without potential for further recuperating any losses. It follows that the intermediary will only invest in taking precaution if there appears to be sufficient risk of default on part of the borrower.

CONCLUSION

Bitcoin, as a fairly revolutionary form of currency, may present challenges, but it also introduces a range of opportunities. The key to dealing with a decentralized cryptocurrency clearly relies on approaches that deviate from those traditional ones that are concretely established. Despite its birth following and in response to a financial crisis, the Bitcoin market

lends significant potential to financial instruments. While fiat currencies are successful because of their backing in the macro, Bitcoin and future cryptocurrencies derive future prospects directly from the demands and needs of individuals. But the two need not be mutually exclusive. Centralized currencies rely on the aggregate actions and motivations of individuals. Perhaps Bitcoin, as a decentralized currency, can benefit from the order and concentration of economic power brought about by financial groups and services.

REFERENCES

- 1. http://www.lendacademy.com/introduction-marketplace-lending-bitcoin-part-1/
- 2. http://www.lendacademy.com/introduction-marketplace-lending-bitcoin-part-2/
 - 3. https://bitcointalk.org/index.php?topic=828622.0
 - 4. http://www.net-arb.com/
 - 5. https://btcjam.com/
 - 6. https://www.bitbond.com/
 - 7. https://bitlendingclub.com/