Early Community Draft Version 0.2 - Subject to Change

Bloom Protocol

Decentralized credit scoring powered by Ethereum and IPFS

Bloom is a protocol for assessing credit risk through federated attestation-based identity verification and the creation of a network of peer-to-peer and organizational creditworthiness vouching ("credit staking")

Jesse Leimgruber, Alain Meier, John Backus

September 24, 2017

Table of Contents

1. Abstract

Background

In 2015, the US Congress declared credit scoring to be a monopoly controlled by just one organization, FICO[1]. FICO provides credit scoring for more than **90%** of top US lenders[2]. FICO's credit scoring system leaves over 26 million Americans "credit invisible" and an additional **19 million unscorable**[3].

Globally, the situation is even worse. **38%** of the world's population does not have a bank account[4]. **3 billion people** are unable to obtain a credit card and **91%** of residents in developing nations experience difficulty receiving debt financing from traditional financial institutions. Traditional credit bureaus require borrowers to take on debt before obtaining a credit score, leaving millions of potentially creditworthy individuals unscorable by the current credit system.

Credit scoring is similarly siloed around the world, further exacerbating these issues. Credit scoring providers can not operate globally, meaning that when a borrower moves to a new country, they must rebuild their credit scores from scratch as their score does not follow them. Since identity verification is also centralized, applying for a loan requires users to expose all of their personal information, putting individuals at increased risk of experiencing identity theft. Credit losses due to identity theft exceed **$21 billion** each year.

Overview

In this whitepaper, we introduce a global, decentralized credit protocol, Bloom. Bloom addresses these existing limitations in lending by moving credit scoring and risk assessment to the blockchain.

Bloom is a standardized, programmable ecosystem to facilitate on-demand, secure, and global access to credit services. Bloom presents a novel approach to credit risk assessment allowing both traditional fiat lenders and digital asset lenders to issue compliant loans on the blockchain while increasing competition to lower fees and improve borrower experience at every layer of the credit issuance process.

The Bloom protocol presents solutions to the following problems:

1. **Cross-Border Credit Scoring:** Credit histories are not portable across countries, forcing individuals to re-establish their credit track records from scratch when they relocate.
2. **Backward-Looking Creditworthiness Assessment:** Credit systems rely on historical debt repayment information and therefore cannot easily accommodate users who are new to credit. This is especially prevalent among minorities, the underbanked, and the youth[5].

3. **Lenders Have Limited Ability to Expand and Offer Loans Globally:** Borrowers in markets with less developed financial and regulatory infrastructure struggle to access credit as lenders have limited identity and scoring data to base credit decisions.
4. **High Risk of Identity Theft:** Borrowers must expose all of their personal information when applying for a loan - the same info an attacker can use to open new lines of credit.
5. **Uncompetitive Credit Scoring Ecosystem:** Credit data is centralized. In most markets, a single provider scores credit, resulting in an uncompetitive ecosystem for evaluating credit risk. FICO was checked on 90% of all U.S. Loans[2].

Protocol Components

There are three main systems which comprise the Bloom protocol:

1. **BloomID (Identity Attestation):** BloomID creates a global secure identity, allowing lenders to offer compliant loans globally, without forcing borrowers to expose personal information.
2. **BloomIQ (Credit Registry):** BloomIQ is a system for reporting and tracking current and historical debt obligations that are tied to a user's BloomID.
3. **BloomScore (Credit Scoring):** The BloomScore is a metric of consumers' creditworthiness. This decentralized score is similar to FICO or VantageScore score, but with updated models.

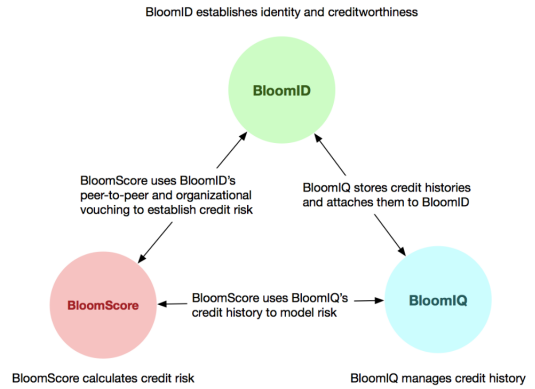
The Bloom protocol improves the current credit ecosystem by creating a globally portable and inclusive credit profile, reducing the need for traditional banking infrastructure and opaque, proprietary credit scores. This means both traditional fiat lenders and digital asset lenders will be able to also securely serve the 3 billion people who currently cannot obtain a bank account or credit score.

Bloom decentralizes the credit industry while lowering rates and increasing security. Bloom makes it easy for lenders to transition to the blockchain by offering a new, compliant way for them to access new markets.

2. Bloom Protocol Overview

The Bloom protocol facilitates the broadening and efficient operation of the credit market by allowing both fiat and digital asset lenders to extend credit to individuals and institutions operating in markets with underdeveloped or immature credit infrastructure, national identities or banking systems, without taking on additional risk.

The Bloom protocol provides solutions to enable any lender authorized by a borrower to safely and securely issue credit to that borrower. There are three components of the Bloom protocol:



BloomID, Attestation-Based Identity and Creditworthiness

BloomID lets users establish a global, federated identity with independent third parties who publicly vouch for their identity information, legal status and creditworthiness. These third parties can be friends, family or peers who vouch for a user's identity and/or creditworthiness ("peer-to-peer staking") or organizations who earn revenue by evaluating a user's credentials ("organizational staking").

Organizational stakers can either inherit trust from their existing reputation (such as existing credit bureaus and identity companies who publicly announce which attestation contracts they control) or by establishing a track record of successful identity attestations on the network.

BloomScore, A Decentralized Credit Score on the Blockchain

BloomScore is a dynamic indicator of an individual's likelihood to pay debts that adapts to the maturity of a user's credit history (or lack thereof). By splitting a user's credit scoring mechanism into three phases that each take into account different data points with varying weights, BloomScore can produce a score that is conducive to building credit from the ground up while helping creditors differentiate the credit risk of consumers in markets and communities with sparse data.

BloomScore initially relies on peer-to-peer credit stakes from BloomID as a means of bootstrapping trust and eventually transitions to primarily using the user's own spending habits and credit activity as a proxy for creditworthiness. Organizational stakers with an established presence can vouch for users with strong credit under the current system allowing them to transition their existing history and reputation to the Bloom network.

BloomIQ, A Registry for Reporting and Tracking Historical Credit

BloomIQ is a system for reporting and tracking current and historical debt obligations that are tied to a user's BloomID. BloomIQ's tracking mechanism puts the user in control, requiring each instance of payment data release to a 3rd party to be authorized by the user. One of the primary goals of BloomIQ is to allow a user to import existing credit history to this decentralized system, reducing the need for credit-established users to build up their credit quickly.

3. BloomID (Identity Attestation and Credit Vouching)

The foundation of a decentralized credit system is a securely established and verified identity. In order to prevent against common network attacks (such as Sybil attacks), each participant's identity must

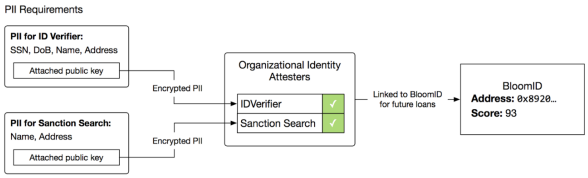
be adequately established with a high cost of attempting to create new, false identities that appear authentic.

BloomID is the Bloom protocol's method of both establishing reliable identity as well as forming the basis of creditworthiness for users who are newly entering the Bloom network. BloomID allows organizations who store information about individual identities to attest to the identity of a Bloom user and mark that information on the blockchain for future re-use.

In addition, a user's friends, family and peers can help an individual bootstrap creditworthiness by vouching for their ability to act responsibly with credit. During this credit vouching process, a user's peers can also attest to various identifying traits such an individual's name or date of birth to help secure the network and provide further proof of identity for the user.

Organizational Identity Attestation

Private companies like credit bureaus and governments currently hold the majority of identity data that exists in the world. These organizations play a critical role in helping onboard users onto the BloomID system by attesting to the authenticity of user-submitted data.



In a loan contract, the lenders detail the identity attesters whom they trust and would require to attest to the potential customer so that they can fulfill the loan within their risk parameters. These external attesters can then agree to verify the identity information and provide their public keys in response along with a description of the data they need in order to complete their attestation, such as "name", "date of birth", and "address". The user then attaches their identity information encrypted for each identity attester respectively using their public keys. The attesters evaluate the information returned to them by the user and publish on the blockchain whether it has satisfied their requirements.

Reusable Identity Verification

By publishing all historical identity attestations on the blockchain, organizations can help take part in building a reusable identity that builds up trust over time rather than having to be re-evaluated for every transaction with a new lender. This can not only save money across the network of lenders, but it can also help significantly reduce on-boarding time by reducing duplicate work by anti-fraud and compliance teams across lending organizations.

Example Organizational Identity Attestations

There are many kinds of identity attesters that can be supported by BloomID. Below is a non-exhaustive list of potential attestation types:

1. **Electronic ID Verification:** Verification of an identity data by cross-checking supplied information with a multitude of public records, private records and governments from around the world.
2. **Documentary Verification:** Verification of an identity document like a passport or a driver's license and whether the image of the person on the document matches the user submitting the scan of the document.
3. **Social Verification:** Verifying the identity information of users via social networks like Facebook and analyzing their friend graph to help reduce fraud.
4. **Sanction Screening:** Ensuring that a user is not on one of the many global sanction programs operated by various governments around the world.
5. **Politically Exposed Persons:** Ensuring that a user is not considered to be a politically exposed person (someone with a promi-

nent political function who is at high risk of potential bribery or corruption involvement).

Peer-to-Peer Attestation and Vouching

In the Bloom protocol, "peer-to-peer staking" is a mechanism for representing real-world relationships between individuals with the goal of establishing both an indicator of creditworthiness and authenticity of identity. Evidence suggests that an individual's creditworthiness can be reliably determined by the people who would vouch for their creditworthiness[6]. This concept of vouching would not be a specific statement about a credit event such as "Bob vouches that Alice is likely to repay a $10,000 loan", but rather a general statement that Bob trusts Alice's judgement to not apply for more credit than she can afford.

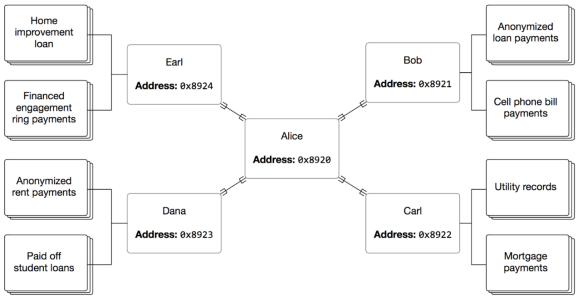
Conceptually, this is not dissimilar to Google's PageRank algorithm, at the core of which is the assumption that if a webpage has a high count of quality inbound links, then the webpage must be important.

Enabling users to vouch for ("stake") other people they personally know, and whom they expect to be financially responsible has several benefits:

1. Facilitates access to credit for new users
2. Increases permanence in credit scoring and ensuring appropriate weighting of long-term and short-term spending and payment habits, e.g. by avoiding users creating new accounts to reset their score
3. Enhances resilience to fraud through the Bloom network

Revealing Creditworthiness Through Relationships

By establishing bilateral stakes with trusted colleagues, friends and family, users reveal the type of financial network they are a part of. If a user does not have a rich credit history of their own, the financial history of their peers can be used as a heuristic and indicator for what patterns their own repayment behavior can reasonably be expected to follow[7]. FICO, by comparison, considers individuals who lack a credit history as "credit invisible". The purely retrospective approach by definition renders FICO (inter alia) unable to evaluate a new customer.



For example, if Alice stakes four of her peers who have all paid off their student loans and pay their rent on time, then a lender can take more of a risk on Alice because she is likely to behave similarly to her peers. Likewise, if Frank stakes several friends when he joins the Bloom network and these friends end up making late payments and / or defaulting on loans, then a lender can mitigate their risk in dealing with Frank by requiring a higher interest rate or requesting collateral.

In staking acquaintances who ultimately fail to meet obligations towards their creditors, Frank has compromised his own creditworthiness. Similarly, Frank's acquaintances have imposed a cost on him by failing to adequately meet their financial obligations. The network effect created by this system extends beyond enhancing accountability between creditors and debtors, but adds an additional element of accountability amongst real-world social groups.

If Frank realizes that most of his peers are unlikely to behave financially responsibly, he might be more conservative with the number of peer-to-peer stakes he establishes. Staking a small number of peers might be done to deliberately hide the fact that the user does not know many people who are financially responsible, but this reduced participation in the

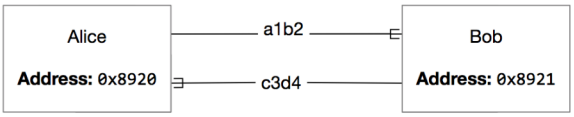
peer-to-peer staking network will be factored into the assessment of Frank's own creditworthiness.

These varying behaviors that produce a different number of stakes can be used as a heuristic for creditworthiness. A user who is part of a network of financially responsible participants should be able to quickly accrue bilateral stakes. Each of the users they stake is also likely to have more stakes of their own that have been acquired quickly. The expectation is that members of a riskier social grouping are more likely to add stakes slowly and be in a more sparsely connected network.

Identity Attestation and Furthering Permanence of Metrics

If a user has a low BloomScore and has difficulty obtaining credit, they will likely be tempted to abandon their BloomID and create a new one. Bilateral staking imposes a cost on such behavior, making it more detrimental for a user to abandon their BloomID than to simply accept their current BloomScore.

When Alice and Bob stake each other, the Bloom app can prompt each user to confirm the other user's birthday. Then, each user's stake can include a hash composed of a secret generated by the staking user and the birthday of the user they are staking. This creates an identifier unique to the staker and stakee that should remain the same if the recipient signs up for a new account with the same birthday. In turn, we can enforce that the user's birthday be the same across accounts by requiring that the signup birthday be provided as part of an attestation for a loan.



A user could try to stake an entirely different set of people with their new account, but this would require significantly more work and the user's incentive for their first account would have been to establish as many quality stakes as possible to improve their own creditworthiness. This leaves the user with the options of staking users they staked with their first account, staking peers they did not want to stake with their first account, or staking significantly fewer people with their new account. If the user stakes peers they chose not to stake with their first account, or stakes significantly fewer people, their new account will have a harder time getting access to credit as well. If the user chooses to stake even a subset of the same users that they staked with their first account, the network will be able to identify that several peer-to-peer stakes are showing up with the same attached secrets and flag the account as a duplicate.

This system acts as a valuable heuristic to ensure that fewer users will increase their perceived creditworthiness by abandoning their BloomID and moving to a new one, thereby enhancing the permanence of the BloomScore.

Securing the Bloom Network

An attacker could create hundreds of fake BloomIDs and have these fake accounts all stake each other. The attacker could then setup her own fake loan organization and have the fake accounts pretend to take out and pay off loans. This process could effectively produce BloomIDs that appear authentic with good financial history that the attack could then use to defraud real loan originators.

The Bloom network will bootstrap the network by marking a small number of users and organizations as "trusted" network participants. These participants will be manually vetted by the Bloom team. Loans, attestations, and risk assessments involving trusted participants during the bootstrapping phase will mark certain participants as authentic Bloom users. Trusted users will be instructed to only stake people they know and are willing to vouch for, so they are unlikely to stake the fake users created by our attacker. Likewise, unless the attacker is willing to create and maintain a real loan company, the real users are unlikely to interact with the fake loan companies.

Networks of real users should contain marked participants from the bootstrapping phase. The attacker's network will seem unusually disconnected from the rest of the network. If the attacker is successfully engaged in a loan scam with one of her fake users, it will taint the scores of many users in the attacker's network. An unusually disconnected network of users with financially responsible users that suddenly start scamming loan companies will be identifiable quickly before it can cause a meaningful amount of damage to the network. Peer staking doesn't solve fraud, but it dramatically increases the cost of abuse within the Bloom network.

4. BloomIQ (Credit Registry)

BloomIQ is a system for reporting and tracking current and historical debt obligations that are tied to a user's BloomID. BloomIQ is designed to bring the wealth of pre-existing and comprehensive credit history to the blockchain while maintaining privacy for the user by introducing a user approval-based system of information dissemination, offering a marked improvement over current systems. Data about an individual's ability to pay past debts remains an important part of determining credit risk, and BloomIQ enables this functionality to be decentralized and reusable.

For example, when issuing a loan to Alice, a lender can see Alice's:

1. Reliability score (a metric gauging a user's individual credit repayment history success)
2. Peer score (a metric to determine the average reliability score of the peers of the user)
3. Number of loans taken out in the past on the Bloom network
4. Past identity attestations performed

Unless Alice has taken out a loan from this company before, they cannot see:

1. Alice's past loan information (total loaned, payment amounts, etc)
2. Her peer's transaction history
3. Identifying information about Alice (name, address, etc)

If Alice has enough past loans and still has a very high BloomScore then the loan company could opt to issue the loan without further checks. If the loan provider wants more information though, they can set a requirement on the loan that a risk assessment of their choosing ("RiskCo") needs to stake the loan in order for the contract to release funds to Alice.

When RiskCo's stake is added as a requirement to the loan, RiskCo can

1. Ask for access to Alice's existing payment history
2. Add a requirement to the contract for a data provider ("DataCo") to provide payment data that isn't available on the blockchain (for example, utility bill payments)

If DataCo needs information about Alice's identity to lookup data then it would add a PII requirement stating that it needs Alice to share certain identifying information so it can perform a lookup via its alternative data sources.

Alice has final say over all requests. She can choose not to provide PII or payment information if she doesn't want to disclose it and it will simply terminate the contract without cost to any parties involved. If Alice wants to accept the requests, she can take the requested information (PII or payment history), encrypt it using the requesting party's public key, write it to IPFS, and attach the IPFS name to loan.

Payment Data Format

When DataCo shares payment information for a user, they are expected to share data in the following format:

```
struct PaymentEntry {
  date: Integer
  amount: Integer
}

struct RepaymentLog {
  nonce:    Integer
  Summary:  String
  schedule: Array<PaymentEntry>
  payments: Array<PaymentEntry>
}
```

Consider the following data:

```
{
  nonce:    489376254,
  summary:  "Cell phone bill payments
   for 2017",
  schedule: [
    { date: 1483228800, amount: 100 },
    { date: 1485936000, amount: 100 }
  ],
  payments: [
    { date: 1483228800, amount: 100 },
    { date: 1484438400, amount: 20  },
    { date: 1485936000, amount: 100 }
  ]
}
```

This represents an agreement that requires a payment of 100 on January 1st 2017 and February 1st 2017. The payments section indicates three payments on January 1st, January 15th, and February 1st. All past payment information is written to IPFS and a reference is stored on the user's BloomID. The summary should be displayed to Alice when asking her to confirm the payment information.

When a loan is paid off or the recipient defaults, the loan provider is expected to consolidate the loan information down to this format and attach it to the recipient's BloomID.

Tamper-Proofing Reported Data

When DataCo reports information to the loan contract, they share the IPFS uri of the encrypted information and the address of the intended recipient:

```
report(address _recipient, bytes
 _ipfsUri) {
   // ....
}
```

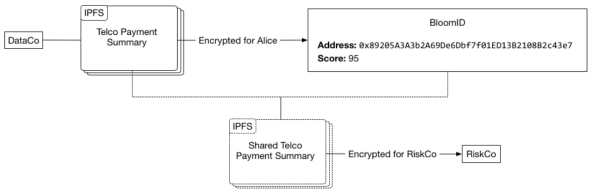
The recipient can interface with the contract to share the data with other collaborators:

```
shareReport(
  bytes _originalIpfsUri,
  address _recipient,
  bytes _ipfsUri
      ) {
   // ....
}
```

When an organization accesses a shared resource from contract, it can lookup the original IPFS resource to check that the original signature matches. The nonce helps deter against attackers generating different plausible JSON until one matches the signature. A shareReport will be rejected by the contract if the sender and _originalIpfsUri don't match an existing report. The loan recipient is never allowed to issue an original report to their own loan.

Fair Credit Reporting by Default

Bloom's privacy model puts loan recipients at the center of all transactions involving their private information and credit history. Users can review the information before sharing it with the company performing a risk assessment. In the event that information is incorrect, the user can work with the data vendor to amend their records using the same methods available today. This workflow promotes proactive correction of information before it impacts a user's BloomScore. Sharing data with the risk assessment company authorizes them to update the user's reliability score. Unlike traditional credit systems, users can catch mistakes before they impact their creditworthiness.



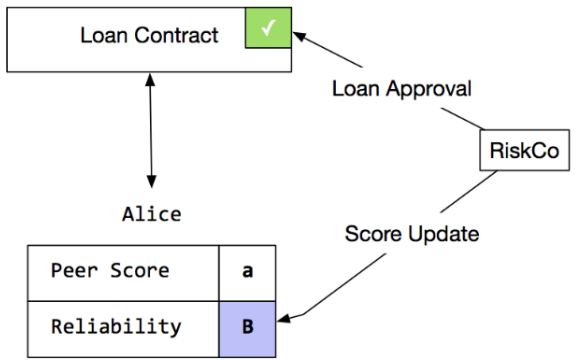
When a loan has matured, the loan provider is expected to consolidate the loan payment schedule down to the previously mentioned format, publish it to IPFS encrypted for the recipient, and attach it to the recipient's BloomID.

Risk Evaluation and Reliability Scores

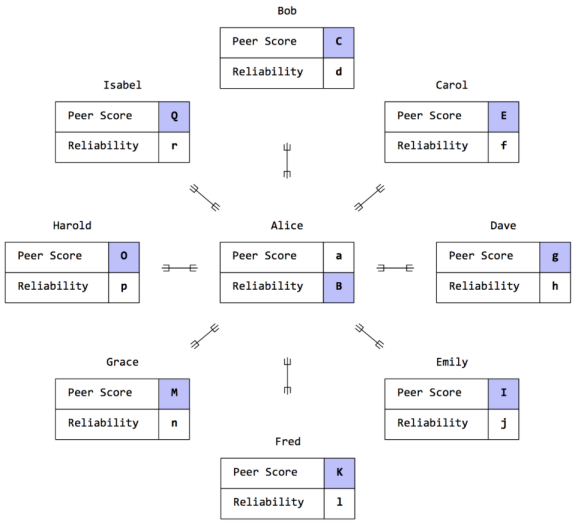
Once RiskCo has received all of the payment information required in order to assess Alice's creditworthiness, RiskCo is required to:

1. Update Alice's reliability score to reflect any new payment information attached to her BloomID
2. Approve or reject the loan

RiskCo does not have to make their decision for the loan solely based on the BloomScore, but they are required to update the BloomScore using the formula agreed upon by the network.



Alice's updated reliability also triggers updates to the peer scores of the users she has staked.



6. BloomScore (Credit Scoring)

The goal of the Bloom network is to securely expose anonymized information about financial networks and historical payments so both lenders and borrowers benefit. The Bloom network will compute a BloomScore for each user that evaluates their creditworthiness.

We can think of a Bloom user as being in one of three phases of account maturity as she enters the Bloom network:

1. The user has just recently signed up and has only staked other users, none of whom are financially active yet on the network
2. The user's peers are financially active
3. The user has taken out loans or otherwise has financial information available in the Bloom network

Bloom users in each phase are able to improve their creditworthiness. Each phase corresponds to more knowledge about the user and raises the ceiling for how high the user's credit score can be before the user ascends to the next phase.

The initial Bloom release computes a simple score based on past debt obligations and payment history. As the network grows with time we expect to increase the sophistication of the score based on what usage best predicts outcomes. Proposed improvements will be vetted and voted on by the participants in the ecosystem in response to how real-world use of the protocol unfolds.

The initial Bloom score will be between 0 and 100, inclusive. Phases one and two will be capped at 20 and 50, respectively. Each phase is scored differently in order to optimally fit the information available.

Users will start with a score of 10. New users will then stand out from users who have defaulted or scammed and therefore have a score closer to zero.

Scoring Phase 1

Users who have not staked any users with financial activity will be scored on the number of stakes they have established and how long it took them to establish those stakes. Individuals from more financially responsible social networks should be able to find more people they can stake, so they should have a higher number of stakes, and they should be established closer to the user's signup date.

New users should be able to quickly get to a score of 20 if they add eight or more stakes in a week or less. Fewer numbers or longer time to acquire stakes should reduce the number the user can reach. The target number of users required to get a perfect 20 will be lower as the Bloom network is starting off.

Calculating Reliability Scores

A reliability score is a prediction of whether a user is likely to pay back a future loan on time given their past financial activity. Bloom will start with a reliability score that takes into account:

- Total amount paid vs. total amount owed
- Longest repayment history on file
- Average payment total per month
- Number of past loans
- Total amount paid across all reported information

In order to make a prediction from these indicators, we will calculate a multivariate logistic regression. The indicators above would be represented as a vector $x = (x_1, x_2, x_3, x_4, x_5)$. Each indicator will also have a corresponding weight such that our logit is:

$$g(x) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + ... + \beta_5 x_5$$

and our regression is expressed by

$$R(u) = \frac{e^{g(u)}}{1 + e^{g(u)}}$$

where β_0 is an offset, β_i is the weight for the x_i indicator, and u is a user on the network. For the sake of having a simple implementation, each indicator will be bucketed into a discrete category. For example, "total amount paid across all reported information" will initially be included by taking $round(log(total))$ to reduce the variable down to a bucketing by order of magnitude.

The transformation of continuous indicators into discrete values requires adding dummy variables for each indicator. So, for example, if x_n has m discrete outcomes then the actual calculation of $\beta_n x_n$ would be

$$\sum_{i=0}^{m-1} \beta_{n,i} d_{n,i}$$

where each $d_{n,i}$ is a dummy variable for x_n and $\beta_{n,i}$ is the corresponding weight.

The final calculated score will be scaled up so that it is between 0 and 100. The weights, indicators, and indicator categories will be subject to a vote on the Bloom network.

Scoring Phase 2

The peer score for a user will be the average BloomScore of each peer the user has staked, capped at a maximum of 50. In the equation below, s is the number of peers the user has staked.

$$min(50, \sum_{i=0}^{s} \frac{R(u_i)}{s})$$

Scoring Phase 3

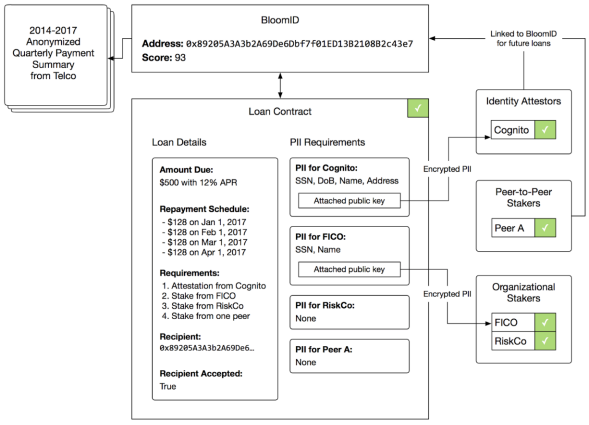
In the final phase of account maturity, the user has her own financial activity as well as financially active peers. Their BloomScore is now uncapped and the weight of each payment they make weighted equally to the BloomScore of one of their stakes. In the equation P and T still correspond to "paid" and "total owed" but instead of $P(u)$ we write, for example, P_2 to mean the second payment the user has ever paid.

$$\sum_{i=0}^{s} \frac{R(u_i)}{s+n} + \sum_{j=0}^{n} \frac{P_n/T_n}{s+n}$$

7. The Loan Risk Assessment Lifecycle

Putting these concepts together, below is a simplified example of the full risk assessment lifecycle including one identity attester and three credit stakers.

This example illustrates how one would port a traditional fiat-based lending lifecycle to the blockchain, but in less developed markets, the required attesters and credit stakers could be customized to fit the demographic that is being evaluated.



1. Loan originator creates contract detailing the amount of the loan, the repayment schedule, and the requirements of the risk assessment
2. User reviews and agrees to the contract
3. External attesters and stakers agree to verify identity and creditworthiness based on loan originator's set of desired attesters and stakers
4. Organizations update contracts with personally identifiable information (PII) requirements that they need to fulfill attestations such as "name", "address", "date of birth"
5. User attaches encrypted details for each attester and staker to their BloomID contract using the public keys of the respective parties
6. Identity verifier attests to the user's provided data
7. RiskCo pays alternative data provider (Telco) for anonymized transaction history
8. RiskCo uses additional payment history information to decide whether to stake user
9. Requirements all met. Borrower can withdraw credited funds

8. Bloom Token (BLT)

The Bloom Token (BLT) is both the currency and scoring enhancement mechanism of the Bloom network. The Bloom token allows organizations to participate in evaluating user identities and creditworthiness. It also serves as the proposal and voting

token to guide the evolution of the Bloom credit scoring system.

Network Currency

In the current credit infrastructure, it is common for lenders to pay identity verification and credit risk assessment companies for their services. Similarly, identity attesters and risk assessors on the Bloom network will be able to set prices and receive payment for their services in BLT.

Distributed Scoring Enhancements

One of the primary functions of BLT is to serve as a proposal mechanism for instituting changes to the BloomScore phases and algorithms. This proposal mechanism allows Bloom to maintain a credit scoring system that evolves according to the needs of its users. As identity and risk attesters provide their services to lenders, they will accrue an amount of BLT roughly proportional to their benefit created within the ecosystem. This in turn will allow lenders, identity attesters, and risk assessors to propose and vote on the changes they would like to see happen at a credit scoring level. Our decentralized scoring enhancement system will be handled using Aragon.

Accrediting Attesters

Lenders and organizations within the Bloom network can have their customers' payment histories reflected in an individual's BloomScore. This is similar to how credit bureaus work with private companies both big and small to form reporting relationships where nonpayment for loans is reflected on an individual's credit report. To handle this in a decentralized environment, payment history providers and lenders will need to submit proposals to the ecosystem regarding why they are trustworthy, what their business does, and why their data should be included in BloomScores.

This will take an approach similar to the AdChain Registry wherein BLT is paid by organizations applying to be included in the BloomScore and users who vote on that organization's inclusion receive a reward funded by the application fee.

Voting users will be required to review applications submitted by these organizations for legitimacy to determine if they should be included in the BloomScore by completing activities such as reviewing the applicant's website, researching the directors and other controlling parties, and reviewing the applicant's proposed means of contributing to the network.

Bloom Invitation System

While the network is in its infancy without a wide array of identity attesters, lenders, and risk attesters, it is more susceptible to attack. In order to account for this in the bootstrapping days of the network, Bloom will have an invitation system in which BLT users will be required to put a fractional amount of BLT up as collateral for users who they invite. This is not collateral to ensure that invited users do not default on loans in one-off instances but rather collateral to serve as protection against a mass-scale network of malicious accounts.

Requiring some BLT to be put up as collateral for an invite adds a negligible amount of friction for signing up and inviting friends. The small amount of BLT required to create an account builds up a meaningful amount of capital if an attacker wants to create a network of malicious accounts. If members of this network end up committing exit scams, then this upfront cost is mostly sacrificed, making exit scams via large fake networks more expensive even during the bootstrapping phase of the network.

Any BLT collateralized in the invitation system will be returned to the sending users after one year.

This invitation system will also serve as a way of concentrating launches of the network within different communities around the world. The Bloom system relies heavily on network effects and thus the invitation system will help Bloom overcome the activation energy that would otherwise be prohibitive in a fully organic and potentially sparse network spread.

9. Roadmap

The Bloom protocol will be developed in 6 major phases:

Phase 1: Bloom Invitation System and Voting
Phase 1 will allow for users to use BLT to invite their friends and colleagues to seed the initial network securely. Users with BLT will be able to vote on early development-related proposals for the future of the network.

Phase 2: Bloom Identity Matching (BloomID)
Phase 2 will deploy an application allowing users to verify their identity and get matched with their BloomID. During this phase, users will be able to confirm identity information as well as add additional information which will be reflected in their score.

Phase 3: Credit Staking (Precursor to BloomScore)
Peer to Peer staking modules will be built first, followed by organizational staking.

Phase 4: Creditworthiness Assessment (BloomScore)
Phase 4 will allow users to check their score, as well as open up a developer ecosystem for additional decentralized lenders to check a given user's BloomScore, providing sufficient privileges are granted from the loan recipient.

Phase 5: Bloom Credit Protocol Launch + BloomCard
Once the risk assessment and scoring protocol is complete, Bloom will launch the BloomCard. The BloomCard will serve as the first full credit card on the blockchain, offering credit services to the nearly three billion individuals who are currently not able to participate in the global credit ecosystem.

Phase 6: Democratized Autonomous Credit Infrastructure
BLT flows through the network. Lenders, data attestation providers, and borrowers all own Bloom Token and their amount acquired will correlate to their influence on the network. As a result, there is an even distribution of BLT relative to a given player's influence in the ecosystem. Assigning the ability to propose and vote on scoring-level improvements and accrediting actors within the network to these tokens creates a fair and democratized setup. This is further described below.

Governance of the scoring protocol will be gradually turned over to BLT holders, granting them determination over:

- Which organizations will be able to update and provide information to a BloomScore
- The weights and factors considered in the BloomScore
- Development and scoring protocol updates

10. BloomCard

To help expedite the adoption of the protocol, Bloom is launching the BloomCard. BloomCard is a blockchain credit card built on the Bloom protocol. BloomCard is intended to serve as a model for all future credit providers and simultaneously allow the Bloom protocol to be deployed and developed in a live environment.

Overview

BloomCard is the first project based on Bloom credit infrastructure, launched alongside the Bloom protocol. The intention is not for Bloom to become a large-scale credit provider. Instead, BloomCard is an example that sets a precedent for other lenders.

Anyone whose application is supported by their BloomScore will be able to obtain a BloomCard, whether they have a FICO score and an established

traditional credit history, or live in a market that currently lacks credit services.

BloomCard is differentiated from any other traditional unsecured consumer credit provider on the market by allowing global access to credit, including in underdeveloped markets. BloomCard is fully compliant with all relevant regulatory standards and can be freely used in the United States. BloomCard will provide users with the best-available spot exchange rate from BTC & ETH to USD without any mark-up.

A user may obtain a BloomCard, but instead opt to use it as a debit card. Users will be able to deposit coins into their BloomCard wallet, allowing them to use their card as a debit card. Card holders may then opt to make their coins available to be lent out to other BloomCard users. These loaned-out deposits would generate interest income, allowing a card user's balance to increase.

This interest income opportunity would attract additional users of BloomCard and provide a new economic sector within a decentralized P2P model.

The BloomCard will be the first credit card built entirely on the blockchain. It is also more powerful than any other crypto card on the market — it has no foreign exchange transaction fees, it enables consumers to spend Bitcoin and Ethereum in the United States. Unlike a traditional debit or credit card, purchases on BloomCard contribute to your BloomScore. BloomScore measures your purchasing power, frequency of purchases, and payment consistency to build your credit.

Peer-to-Peer Lending

We anticipate additional services being built by other providers. One example is a peer-to-peer lending system.

For example: Funds lent through BloomCard will not be on a peer to peer lending system. However, given the decentralized and compliant nature of the Bloom protocol, one could envision a world where credit funds are lent through other users.

Those users of BloomCard who have opted to make their funds available to be loaned to other users and who are earning interest on their deposits would not be required to sacrifice liquidity. Their deposits would always remain liquid, even when they've been lent out. The interest earned on the deposits would vary depending on market rates and conditions as well as the available pool of liquidity.

With BloomScore and BloomCard, borrowers would have an alternative avenue to obtaining loans. Rather than having to turn exclusively to centralized credit institutions, they can turn to users on the blockchain for funds. The distribution of risk across a wide user base will allow borrowers to achieve lower interest rates on borrowings, as well as facilitate instant access to liquidity, while at the same time allowing lenders to diversify their credit exposure and mitigate their own risk.

Early applications of this principle are already live, for example, Poloniex is a successful centralized digital asset exchange, which also offers a lending platform. Their margin trading allows exchange users to earn interest by lending their cryptocurrency to margin traders. BloomScore would enable similar exchanges, but these could be decentralized on the blockchain rather than centralized within a single exchange or company.

Providing this capability to everyday users through a simple to use, but decentralized (P2P) exchange is the focus of the BloomCard and the BloomScore.

11. Team

Founding Team

Jesse Leimgruber
Jesse studied computer science at Stanford University. Jesse is an advisor to The Alchemist Accelerator, a Thiel Fellow, and a mentor at the European Innovation Academy. He's served as a guest lecturer at Stanford University, The University of Southern California, DePaul, among others. Prior to Bloom,

Jesse founded enterprise analytics software, NeoReach. NeoReach provides analytics for Fortune 500 brands including Microsoft, Citrix, Walmart, among others.

Ryan Faber
Ryan Faber developed a behavioral recognition methodology designed to leverage online psychographic data for user acquisition. Using his research, Ryan launched Flatiron Collective. Flatiron now manages over $100M annually in digital marketing spend. His developments in user acquisition have allowed him to become a 3x Webby Award winner and his methodology has been attributed to the exponential growth of numerous billion dollar brands.

Alain Meier
Alain Meier studied computer science at Stanford University and served as a research scientist for Stanford Bitcoin Group. Founded by 21 CEO, Balaji S. Srinivasan, The Stanford Bitcoin Group is Stanford University's blockchain research organization. Alain developed a number of open source cryptography projects including CryptoNote.me, an open-source service allowing users to send encrypted, single-view messages in seconds. Following his work at Stanford, Alain is serving as the CEO of compliance and identity verification company, Cognito (formerly BlockScore).

John Backus
John is a founding research scientist at Stanford Bitcoin Group and studied computer science at Stanford University. He is a Thiel Fellow and cofounder and CTO of identity verification company, Cognito. John is an expert at identity infrastructure, previously engineering data preprocessing algorithms for large-scale entity extraction for deterministic and probabilistic record linkage. This is currently implemented into Cognito's core identity resolution and record linkage infrastructure, now processing identity and compliance for tens of millions of cryptocurrency users globally.

Advisors

Meg Nakumura, CEO of Shift Payments
Shift developed the Shift Card, a VISA debit card that currently allows Coinbase users in select states and territories in the U.S. to spend bitcoin anywhere VISA is accepted.

Joseph Urgo, Co-Founder at District0x, CIO at Sourcerers Capital
Joe is the co-founder of District0x, an Ethereum dApp decentralizing the world's marketplaces. Prior to this, Joseph founded Sourcerers.io, a consultancy supporting leading Ethereum-based projects. Joe previously spent three years as an Operations Manager for Coinbase. Prior to Coinbase, he was a derivatives trader for Three Arrows Capital, an international hedge fund based in Singapore.

David Raphael
David Raphael is the CEO of Infinity Media, a digital agency specializing in conversion rate optimization. He studied at the University of Chicago and has spent the last six years sharpening the product-marketing funnels for companies like Artsy, FanDuel and Wag!

Special Thanks

A very special thank you to the people who helped to review this whitepaper:

- Spiros Zarkalis
- Stelios Manolopoulos
- Devon Zuegel
- Daniel Maren
- Brian Sorel
- PJ Leimgruber
- Shannon Wu
- Joe Urgo
- ray-jones

References

[1] https://royce.house.gov/uploadedfiles/credit_score_competition_act.pdf

[2] http://www.myfico.com/credit-education/how-lenders-use-fico-scores/

[3] https://www.consumerfinance.gov/about-us/newsroom/cfpb-report-finds-26-million-consumers-are-credit-invisible/

[4] http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf#page=3

[5] http://www.perc.net/wp-content/uploads/2013/09/web_layout-you-score.pdf

[6] http://pubsonline.informs.org/doi/abs/10.1287/mnsc.1120.1560

[7] http://pubsonline.informs.org/doi/abs/10.1287/mnsc.2015.2181