Unique Identifiers for Online Marketplace Lending using the Blockchain

A Whitepaper proposing Planetary Unique Financial Instrument Numbers (PUFIN)

We propose a worldwide open-source identification system for the online marketplace lending asset class using blockchain technology. This unique identifier is intended for use in any application in the trading and administration of online loans or more generally any financial instrument. By fostering interoperability at this critical junction in the burgeoning online marketplace lending industry, we seek an expansive future as online marketplace lending matures into a bonafide asset class within the financial services industry. Rather than an incessant narrowing of possibilities, we seek to lay a foundation for new platforms, protocols, and standards.

The securities industry still uses legacy numbering systems developed as far back as the 1960s, when manual trading and administration of securities was the order the day. The advent of blockchain technology and online marketplace lending provides a unique opportunity to harness modern capabilities instead of backfilling to legacy approaches with proprietary models.

As a pilot program, we plan to introduce *Planetary Unique Financial Instrument Number* (PUFIN), an open-source system in which anyone can freely generate a unique 34-digit address and associate it with evidence of a financial instrument, such as cryptographic proof of a prospectus, offering document or other similar local identifier. To mitigate actions by bad actors, an optional cryptographic signature in each transaction record may serve as a way to add credibility to a record.

See **www.pufin.org** for the latest updates.

August 2016

Authors:
Michael F. Mazier
mikem@lendingcalc.com

Ben McMillan
ben@lendingcalc.com

Lendingcalc.com is a startup providing productivity tools for portfolio managers investing in online marketplace lending

Our goals in this project are:

1. ***Single global version of the truth*:** An unambiguous global ID is one step in helping to standardize and merge loan-level data across multiple *online marketplace lenders* (also known as "origination platforms").
2. ***Open-source*:** We embrace collaborative participation on a structural issue that affects and benefits all market participants. Open-source also increases the chances of collaboration among competing commercial interests.
3. ***Low cost*:** We wish to avoid the legacy situation in the U.S. where S&P currently collects ongoing annual licensing fees of $10,000 to hundreds of thousands of dollars from financial institutions for storing CUSIP codes in internal databases.[1] We think global IDs can be created at a net cost of fractions of a penny and accessed for free. Data costs are a drag on innovation.
4. ***The need for speed*:** We want to match the speed of online loan approvals. Initializing a new global ID on a blockchain may take minutes to confirm and then fractions of a second to access.
5. ***Reduce pain of merging data from multiple sources:*** Avoid having another Rosetta Stone-like cross-reference table that many firms manage locally to help merge data from multiple sources.
6. ***No central point of trust or failure*:** Competing commercial interests may result in competing numbering systems that attempt to lock users into different commercial ecosystems. Quite simply, we believe a global ID should be like a boring but efficient utility company. Vendors then compete by providing complementary data enriching and ancillary services.
7. ***Scalable*:** Identify every loan and financial instrument in the world. Develop a plan to ID a number of financial instruments as large as the number of atoms on planet Earth ~ 10^{50}.
8. ***Security*:** Use cryptographic tools and game-theory strategies to defend against inevitable attacks while preserving the integrity of the system.
9. ***Decentralized core foundation*:** Anyone can create a global ID for any financial instrument. We are inspired by blockchain consensus strategies.
10. ***Start a debate*:** We hope blockchain enthusiasts, technologists, market participants, and lawyers will chime in. If arrows are slung our way, we'll at least check off goal number 10 as done.

[1] Finops Report, http://finops.co/investments/us-sec-will-it-finally-address-cusip-fees/

Background on Security Identifiers

Behind every stock or bond is a unique identifier. Like a serial number stamped on the back of a flat screen TV, unique identifiers foster a meeting of the minds between buyer and seller. Identifiers form part of an audit trail. Many identifier systems grew independently and organically to solve specific local problems before sprawling into conflict with other systems. Exhibit 1, The long history of security identifiers, shows a timeline of a few major identifier systems. In the United States, the vast majority of tradable securities settle via the industry-owned Deposit Trust and Clearing Corporation (DTCC), which uses CUSIP codes as security identifiers. Globally, ISIN is a widely used identifier, which is derived from national numbering systems and follows standards set by international organizations. Additionally, stocks and bonds may have other identifier codes issued by local clearinghouses, agencies or commercial interests. For example, bonds have proprietary RIC codes on Reuters' systems, which do not talk with Bloomberg's systems. The exact same security may have different codes to indicate different closing prices on exchanges in New York, London, and Tokyo.

CUSIP first appeared in 1964, when manual trading and paper administration was the order of the day order the day

Proprietary Identifier– Taking the example of CUSIP in the U.S.A

For a new CUSIP: Fill out an application, pay $168 and wait for one or two business days. Or pay 50% extra for express turnaround in one hour. [6] *Fees vary, depending on asset class.*

To use CUSIP in your database: pay $10,000 to as much as hundreds of thousands of dollars in annual licensing fees.[7]

Most loans do not have ISIN or CUSIP codes, nor are they classified as a "security" for purposes of U.S. federal securities law.[2] Accordingly, we use the broader term "financial instrument." No central exchange for loans exists. Instead, market participants have developed a patchwork of processes for transferring ownership of certain loans, particularly syndicated loans and mortgages. Typically, the process entails both buyer and seller going back to a loan originator who transfers ownership for a fee. One vendor, Orchard Platform, has announced plans to create a secondary market for online marketplace loans.[3] As loan documents stand now, online loan originators would need to be a party to such a secondary market or exchange. If history is to repeat itself, each new party that somehow touches a loan may patch up another layer of loan identifiers.

[2] Proskauer Rose LLP, http://www.proskauer.com/files/uploads/broker-dealer/Syndicated-Loans-as-Securities.pdf (accessed May 25, 2016)
[3] Crowdfundinside.com, www.crowdfundinsider.com/2016/04/83816-orchard-will-launch-electronic-trading-platform-for-marketplace-lending-assets/
[6] S&P's CUSIP Global Services, https://www.cusip.com/pdf/2016FeesforCUSIPAssignment.pdf and https://www.cusip.com/cusip/request-an-identifier.htm
[7] Bond Dealers of America, "Request for Commission action re CUSIP identifiers", letter to the SEC, http://www.bdamerica.org/wp-content/uploads/2010/12/CUSIP-SEC-Letter-FINAL-IAA-GFOA-BDA-111010.pdf

Mapping identifiers helps to reduce some trade errors

Many financial organizations maintain internal databases to cross-reference different types of identifiers, e.g., RIC, BBID, CUSIP, ISIN, SEDOL, and pool numbers to name a few. Again, for good measure, firms often add their own overlay layer of IDs. Morgan Stanley's fixed income division (FID), for instance, created "fidId" as in internal ID. When in doubt just add another layer of identifiers. It's hard to say just how many trade errors have a root cause in faulty identifiers. Some IDs such as CUSIP encode a meaning into a subset of its digits, such as a number that identifies the issuer. This works well until merger and acquisition activity deprecates such meaning for the life of the security. Now humans who find meaning within such IDs may be misled. In many cases, in accordance with regulatory rules, the cost of trade errors must be borne by the investment advisor, not the investor. Regardless, trade errors are a cost of doing business for an investment advisor - a cost that is ultimately and indirectly borne by investors. Many asset management firms pay "Errors and Omissions" insurance, typically costing around $10,000 to $15,000 per $1million of coverage. [4]

In summary, the main pain points with traditional IDs:

1. Cost to get or use them
2. Time to get them
3. IDs are usually only locally unique
4. Pain to merge data from multiple sources.
5. Proprietary restrictions and license fees

Online Marketplace Lending today

Online Marketplace Lenders assign their own loan identifiers to loans they originate. An investor or service provider wishing to compare loans from multiple lenders may be tempted to create another overlay set of locally unique IDs. We believe truly globally unique IDs are a first step in standardizing data sets. A recent white paper by the US Treasury indicated that industry respondents "strongly supported and agreed on the need for greater transparency" and "suggested areas for greater

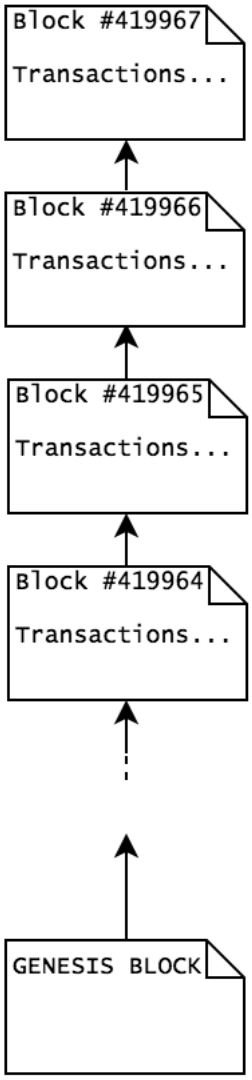
[4] Smart Business, http://www.sbnonline.com/article/what-emerging-managers-need-to-know-about-hedge-fund-management-liability-insurance/

transparency include pricing terms for borrowers and standardized loan-level data for investors." [5]

We believe Online Marketplace Lending is at a critical juncture, especially after the May 2016 events surrounding Lending Club CEO's departure, which shook investor confidence across the marketplace as a whole. We believe the silver lining is greater transparency as Lending Club and the market as a whole take more of a "trust but verify" approach to investing in loans and in connecting data from multiple sources as part of a push towards increasing transparency.

Bitcoin/U.S. Dollar exchange rate

When it comes to lack of a global ID, this stage in the grown of Online Marketplace Lending mirrors the challenges faced by the securities industry during the 1960s, when CUSIP was first developed. But today we believe the blockchain provides an opportunity to start a new approach from scratch. First, we provide an overview of Blockchain then propose one solution.



Bitcoin Blockchain

A brief overview of the Bitcoin Blockchain

Blockchain is conceptually a singular global database or ledger, but physically comprises an append-only log of transactions distributed and shared across a network of nodes. A distributed database is nothing new. The innovation of the bitcoin blockchain is:

1. *No central authority* – a consensus algorithm automatically updates transactions.
2. *Solve the "double spend problem"* – A bitcoin is a long string of numbers. Attempts to double spend the same bitcoin should fail.

A debit, a credit, and verification by the crowd

Under the hood, new transactions – such as "Alice sends one bitcoin to Bob" – are broadcast to the entire network of nodes. Conceptually, the transaction begins as an alleged debit to Alice and credit to Bob on a ledger. The crowd verifies transactions to make them permanent. The three steps of debit, credit, and final verification may be referred to as *triple entry accounting*.

In bitcoin, the crowd that performs verification are certain nodes, called miners, which crunch numbers and may earn

[5] U.S. Department of the Treasury, https://www.treasury.gov/connect/blog/Documents/Opportunities_and_Challenges_in_Online_Marketplace_Lending_white_paper.pdf

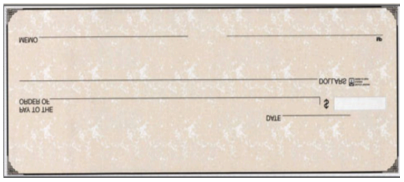
bitcoin rewards. Miners gather individual transactions and package them into a block. Miners also perform a series of checks such as preventing "double spending" by assuring that new bitcoin transactions are composed of previously unspent bitcoin transactions.

Miners then enter into a competitor to become the leader that will append the next block to the blockchain. In bitcoin, the leader of each round is determined by the fastest miner to solve a computation problem. The winner collects transaction fees and brand new minted bitcoins, which is how the bitcoin money supply grows in a predictable way. Once a block is successfully written and verified by other miner nodes, the next round of competition begins. In bitcoin, a new block is created approximately every 10 minutes.

For more details, we suggest Andreas Antonopoulos' book, *Mastering Bitcoin*. We understand a new edition is coming out soon. In the current edition, the first 3 chapters are non-technical. The rest dives into details showing snippets of code for the technical reader.

The salient points about Bitcoin for this paper:

- ***The blockchain is conceptually singular but physically distributed*.**
- ***Bitcoin transactions are stored forever and anyone can do it***.
- ***Bitcoin got the memo*:** Just as old-fashioned banking paper checks have a blank memo field, Bitcoin transaction messages have an analogous empty field that can be used any purpose. This empty Bitcoin field (OP_RETURN) is where third-party applications embed immutable data onto the blockchain. This data is ignored by bitcoin protocols. Now IDs are forever.



Bitcoin transactions have an OP_RETURN field analogous to the blank memo field in a check

The job of an identifier organization

The first step in creating a global ID or any ID for that matter is having *evidence of a financial instrument*. In the centralized case, for example, S&P's CUSIP Global Services collects *evidence of a financial instrument,* which they review before issuing a new CUSIP. The functions of an ID issuer include:

- Validate – assure the existence of a financial instrument.
- Preserve – maintain and manage database of IDs

- Ownership – maintain intellectual property rights

S&P's CUSIP Global Services validation process guarantees a one-to-one match between their assigned CUSIP code and a true financial instrument. In a decentralized approach, we let anyone create a Global ID, which will inevitably result in IDs pointing to spam. That's OK if we handle it.

Design considerations for creating IDs on the blockchain:

- Permissioned addition – If we use cryptographic signatures to assign permission for others to add ID, we are back to having a central authority control, which defeats our purposes. No need for a blockchain to exists if central authority returns.
- Permission-less and anonymous – anyone can add a Global ID, and we'll never know who he or she is. This encourages the global community to add records, but it invites hackers, spammers, and whatever else the cat dragged in.
- Permission-less with a cryptographic signature – Anyone can add a Global ID, but they may want to prove their credibility in the future. Hence IDs from this signature would be credible.

The building blocks of PUFIN - Planetary Unique Financial Instrument Identifier

We seek to create a unique secure link between a loan and a global ID. To do so, we use the following top-level building blocks.

- *Blockchain infrastructure* – We are using Bitcoin in our model. At this point in July 2016, Bitcoin is the largest and, we believe, most secure blockchain. As of July 9, 2016, Bitcoin (BTC) has a market cap of $10.3 billion (total bitcoins times the dollar value of one bitcoin). Ethereum is a promising alternative that we shall research. We suspect that Hyperledger's closed design would not fit with the goals of this particular use case. Someday, it may make sense to generate IDs from bitcoin and copy them to Hyperledger's more insulated blockchain.

- *Evidence of a financial instrument* – PUFIN links to evidence such as, from strongest to weakest:

1. a prospectus, loan or offering document filed with a regulatory body such as the SEC;
2. private documents, not filed with a regulatory body;
3. any widely known public financial instrument identifier;
4. a local identifier, such as a local loan number a loan originator;
5. an identifier created by a third-party.

- *Data encoding tool* – We don't store actual prospectuses' local IDs on the blockchain. Instead, we store an encoded version of the file - a *cryptographic hash* on the blockchain. We borrow ideas from proofofexistence.com.

- *ID creator client application on top of Bitcoin Blockchain* – This thin app is what anyone can use to generate a new PUFIN.

- *ID reader client application on top of Bitcoin Blockchain:* This slow reader traverses the entire bitcoin blockchain to find IDs by using a rule set to filter for relevant bitcoin transactions.

- *ID lookup table outside of Bitcoin Blockchain:* In practice, it may take too long to lookup IDs directly from the bitcoin blockchain. So an index of all IDs is created and stored outside the blockchain – this also listens to new transactions to update itself in real-time. Data not on the bitcoin blockchain can live on a distributed system such as Interplanetary File System (ipfs.io).

Challenges and some possible answers:

- **Privacy issues on the open blockchain:** Laws governing data privacy, which vary by geographic jurisdiction, raise challenges for decentralized systems. The terms "personal information" and "personally identifiable information" have specific legal meanings in the UK and US. How do we safeguard personally identifiable information (PII)? This is a concern because of the immutable nature of a write-only blockchain. In China, the names of defaulting individuals may lawfully be published. Europe shows more information than in the US.

Many senior financial executives see an un-permissioned blockchain as a deal breaker. Blockchain is an "append-only data store."

- **Bad Actor**: A hacker or malicious actor or disgruntled employee may someday release a trove of private information about consumer loans and may seek to link them onto a blockchain. We need to mitigate that possibility in our design. The blockchain itself stores only IDs. The bad database would exist outside the blockchain.
- **Intellectual Property:** Needs to be considered and balanced with commercial interests. We believe open-source and governance by an industry association or consortia of the underlying framework would best produce wider acceptance while allowing for proprietary vendor solutions on top, such as data enrichment solutions that ride on top of the open standards.

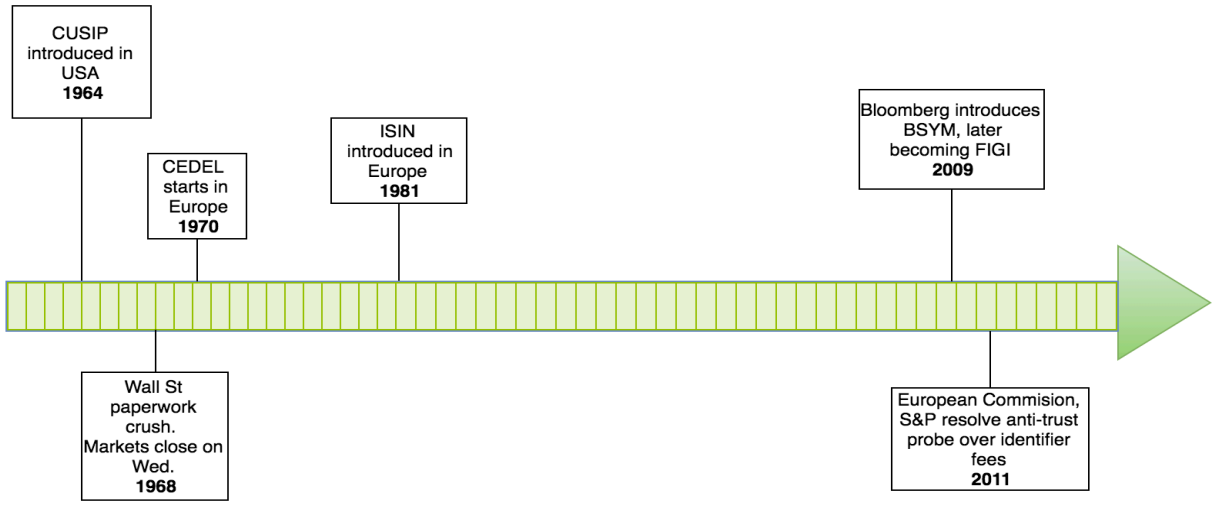


Exhibit 1. The long history of security identifiers

	CUSIP Global Services	PUFIN	Blockchain 3rd Party service provider
Validate	Makes sure that new CUSIP points to a qualifying security	none	Validates link between ID and financial instrument
Preserve	Private servers	Immutable Blockchain	
Ownership	Proprietary; Charges fees to create (~$168), and license to use (~$10K to $100K)	Open-source license	3rd party would own data enhancement or reference data

Exhibit 2. Tradition and Blockchain ID service.

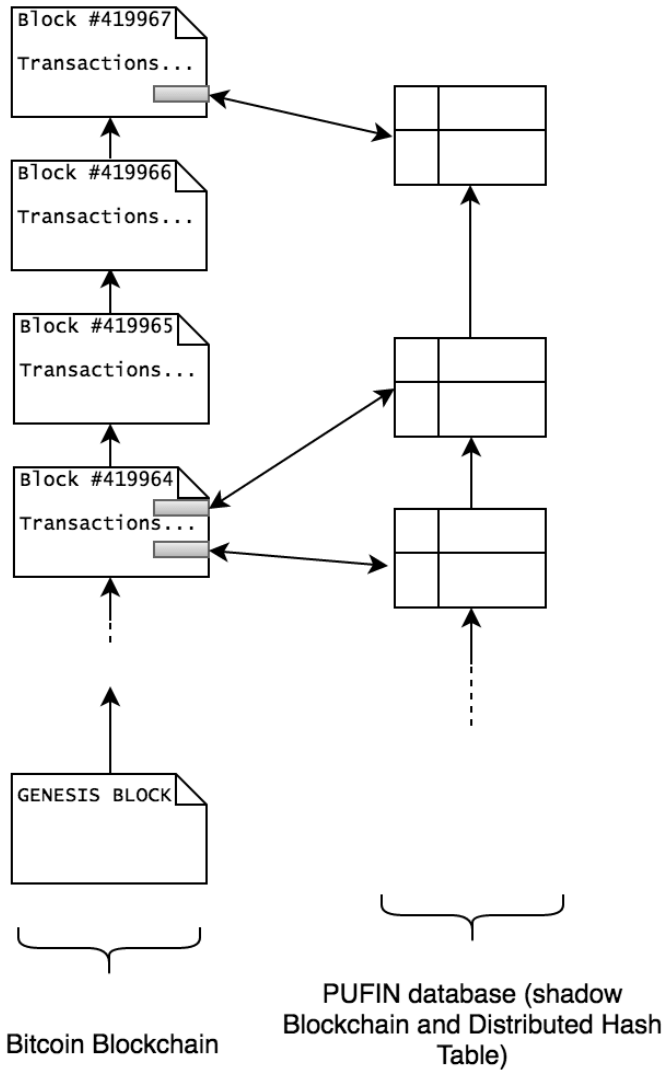


Exhibit 3. Bitcoin Block Chain plus PUFIN database

`Psdjeivnoi4rnriei55sdvmS4m9m323em23`

Exhibit 4. Example of a PUFIN