2018

Pre Authorized Debit Solidity Smart Contract

CED CAPSTONE PROJECT

SHIV BATH, BRADLEY TAGUIBAO

Contents

Problem Statement

Pre-authorized debits (PADs) are an extremely convenient way to pay bills and make other payments automatically. Instead of a consumer sending payments to a provider of services, a company withdraws funds from the consumer's bank account. It's a useful way to pay bills like mortgage, utilities, donations and insurance premiums. The consumer, aka the payor, has to provide permission to the service provider, aka the payee, to withdraw funds from the payor's bank account. The benefit to the payor is that bill payments are performed automatically, avoiding missed payments, and amounts deducted can be variable as determined by the payee company based on consumed services, e.g. monthly utility bills can vary.

Various evolved processes attempt to make the transactions more seamless. However,

- PAD agreements between financial institutions, consumers and companies have to adhere to very strict guidelines as established by Payments Canada. In particular, PADs have to abide by Rule H1 of the Automated Clearing Settlement System (ACSS) Rules and Standards as maintained by Payments Canada. This is a 32 page detailed document which is largely to ensure integrity and protection of parties for an ongoing transaction between payor and payee.
- Businesses, payees, offering PADs must have letters of understanding with financial institutions.
- Businesses have to indemnify financial institutions.
- Businesses must ensure ongoing rules, as per Rule H1, are managed and enforced.
- For a consumer, the PAD set up process can take several days if not weeks. Typically there is a paper trail, containing signatures. The setup process is not immediate.
- The consumer, payor, has to provide personal account information to a payee. Bank details, including void copies of cheques, submitted to the payee are part of the process. The payee must then, in turn, present such details to financial institutions for PAD setup.
- Personal banking information belonging to a payor is released to utility companies, charity organizations, landlords and anyone accepting PAD agreements. The nature of shared sensitive information necessitates involvement of Payments Canada, financial institutions and strict observance of all Rule H1 rules.
- Once setup, a consumer cannot change the PAD details without going through another paper trail process. This can take several days without the ability to preempt an existing withdrawal agreement. Inadequate or excessive funds transfer scenarios require post-transfer corrective activity.
- There is no ability for a consumer, the payor, to view their set of PAD agreements.
- There is no ability for a payor of immediately terminating a PAD. The termination request has to be submitted and may take up to a month before PAD termination is finalized.

Solution Abstract

This solution describes the automated process of transferring funds from an end consumer to businesses as payment for the provision of services by the business to the consumer. The solution offers an alternative to the PAD process.

Definition

PAYOR: A person, business or organization being the originator of a PAD agreement and whose account is to be, or has been, debited with the amount of a PAD

PAYEE: A person, business or organization being whose account is to be, or has been, credited with the amount of a PAD.

The consumer, or payor, has the ability to select businesses, the payee, to whom he/she can provide authorizations for automated payments. Setup of an authorization is through a client side portal. The payor can select from a validated set of businesses, or payees, that have been accepted onto the platform. Only authenticated businesses are presented for PAD setup to mitigate fraud.

Each authorization is similar to the current PAD information provided by a consumer to prospective businesses except the information no longer needs to be disseminated to the business. When defining a PAD, the payor can:

- select a business for PAD agreement,
- define a periodic payment amount, if any, or permit amounts be set by payee,
- indicate the payment frequency,
- set a start date for PAD agreement commencement,
- set an expiry date or an indefinite expiry date for the authorization.

Multiple payment authorizations can be set up. The consumer has full control over which businesses are authorized, how often payments occur and can readily change or cancel an authorization from within the same client side portal.

Unlike PAD agreements today, there is no further need to communicate with the respective business for payment changes or cancellations and hope, or rely upon, the business and banking processes to achieve eventual desired outcome.

The system onboards businesses that are prepared to accept direct payor payments in lieu of requesting PADS from payors. The onboarding of a business authenticates a business as legitimate and leverages the blockchain to record a validated business available for payor selection.

The payor can control PAD setup, update of PADs and deletion of PADs. No personal banking information is shared between payor and payee. The effect is akin to a scheduled bill payment by a payor to a payee.

The payee can, however, view PAD setups assigned to itself. For those PADS with no fixed amount, and given payor authorization, the payee can assign variable amounts for payment. The payee can adjust payment amounts to be withdrawn from a payor account equivalent to its own billed or invoiced values on an ongoing basis.

Based on the effective payment date within a PAD, and the record of PAD agreement on the blockchain, a payment obligation from payor to payee is presentable as authentic to banks for funds transfer. This well-defined and immutable agreement on the blockchain can be considered an actionable financial transaction on the day of payment.

Why Blockchain

- Provides data integrity of digital data
- Provides identity authentication for each user of system
- Immutable transaction records
- Allows for exchange of value in a transparent manner
- Allows for an increased order of efficiency for business transactions
- Facilitates value exchange without compromising personal sensitive information
- High availability through a distributed peer-to-peer network
- Potential cost savings via third-party overhead reductions or elimination.

Solution

Scenario Use Cases

1. Onboarding of business to receive payments - payee

- Only businesses which have been successfully onboarded are visible to consumers from the front-end portal.
- A Payee must register onto system. The system interfacing to the smart contract code (bank server side code) will validate a business before adding into the smart contract and assigning an address.
- An onboarded business payee is one for which a unique address has been generated and logged into the smart contract.
- The smart contract maintains all unique business entities as an array of mapped addresses.
- Smart contract adds a new entity, generating a new unique address. The key will be the Unique Business Identifier (UBI) also known as the 9-digit Unified Business Identifier in the US, or the 9 digit Business Number (BN) as assigned by the Canada Revenue Agency. Companies without a BN or UBI will be unable to onboard.
- Only the mapped address for a company will be used and visible within the blockchain. The UBI or BN itself will never be published to the blockchain.
- Adding a business:
        - addNewPayee(string uniqueBusinessIdentfier) returns bool
    - The BN is passed to the smart contract to record the map to an address.
    - *Note from Solidity docs:*
        - Mappings can be seen as hash tables which are virtually initialized such that every possible key exists and is mapped to a value whose byte-representation is all zeros: a type's default value. The similarity ends here, though: The key data is not actually stored in a mapping, only its `keccak256` hash used to look up the value.
    - However, the map's key is the input string. This could conceivably be used to identify the business against blockchain transactions if a node examined the EVM memory space. The input string for the BN will be hashed or obfuscated before passing to the function addNewPayee(), even though it will be further hashed as a mapping key.

- Removing a business:
        - removePayee(string uniqueBusinessIdentfier) returns bool
    - The BN is passed as a hashed value.
    - The smart contract removes the payee on request. That is, removal always succeeds even if consumers have setup payment authorizations against that payee.
    - Any authorizations related to this payee are marked as no longer valid/applicable. The payee's list of authorized PADs is used by the interfacing server application for any payor change notification.

2. Onboarding of consumers - payor

- The end user from whom the payment will be deducted to pay a service provider.
- Consumers, or payors, onboard via proprietary UI, web or mobile applications. Typically we see this as a feature or provision with a bank’s online banking offering.
- Functions for consumer
  - A payor is onboarded when first creating a PAD agreement. Until a PAD agreement is required, or created, there is no record of the payor entity within the smart contract.

  - List available payees: `function payeeList()` returns array[address]
    - The backend server needs to retrieve the payee list from a call to the smart contract function `payeeList()` and translate the returned array of address values back to a human readable name of the payee.

  - Add new authorization for selected payee. Requires[1]
    - Payee identifier – the 20 byte Ethereum address pulled from the selection returned in `payeeList()` function.
    - Bank account from which debit will be made – this is not passed to the smart contract. It is part of the front-end bank setup, vis-à-vis a bill payment setup for source of funds.
    - Debit type – fixed amount, or variable to be payee defined with an upper limit

      ```
      enum DebitType {Fixed, MaximumLimited, Unlimited}
      ```

    - Debit frequency

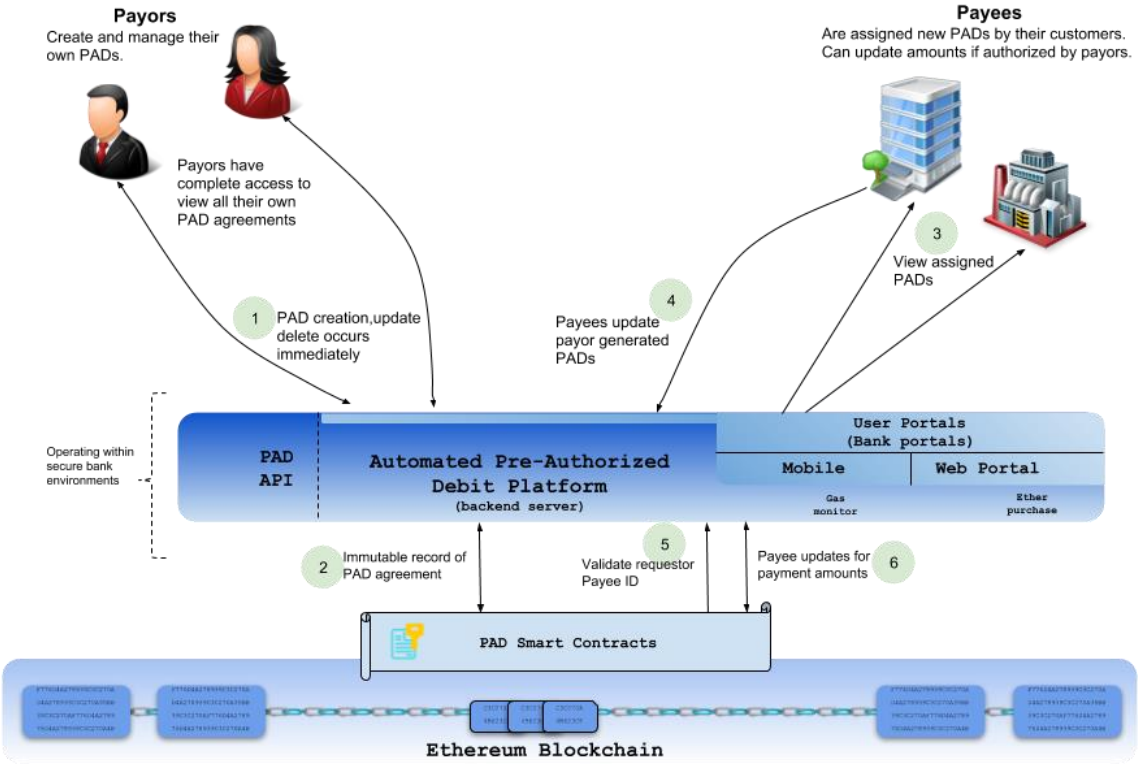
      ```
      enum DebitFrequencyType {Daily, Weekly, BiWeekly, Monthly, Annual, Sporadic}
      ```

    - Start date, End date or no expiry of PAD agreement

  - Change an existing authorization
  - Remove/delete an authorization. Payors can remove an authorization at any time. No need to engage target payee directly. Deletion are performed immediately, unlike current process which can take up to 30 days in some cases.
  - List current authorizations.

[1] See “Bank bill payment screens – online banking” page10 for examples.

Pre-Authorized Debit Setup Process



Payors
Create and manage their own PADs.
Payees
Are assigned new PADs by their customers. Can update amounts if authorized by payors.
Payors have complete access to view all their own PAD agreements
1
PAD creation,update delete occurs immediately
4
Payees update payor generated PADs
3
View assigned PADs
Operating within secure bank environments
PAD API
Automated Pre-Authorized Debit Platform (backend server)
User Portals (Bank portals)
Mobile
Web Portal
Gas monitor
Ether purchase
2
Immutable record of PAD agreement
5
Validate requestor Payee ID
Payee updates for payment amounts
6
PAD Smart Contracts
Ethereum Blockchain

Client side portal - APIs

Although the client side portal is imagined to be either web or mobile based UI through a proprietary app, the longer term preferred approach from a consumer viewpoint is likely integration within existing online banking applications.

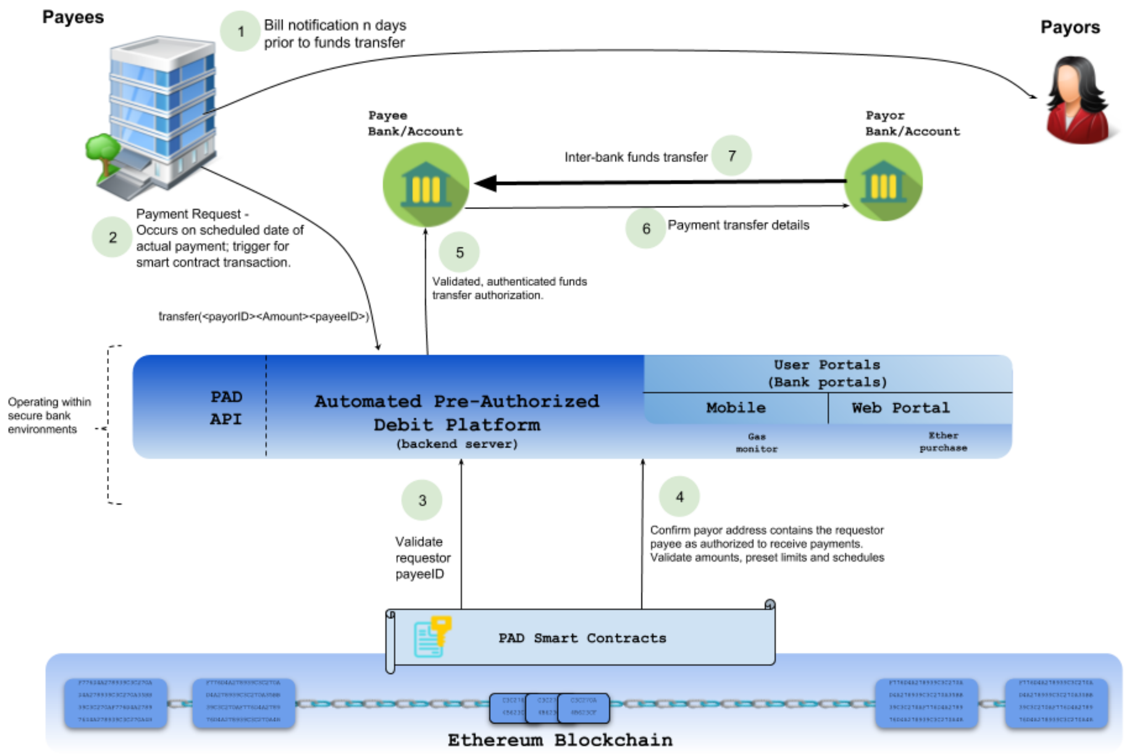
This platform can expose a set of **APIs** to allow for bank applications to integrate through current web or mobile apps and expand the feature offerings on their own platforms to include the facility for consumer managed payment authorizations. For the consumer this becomes seamless and the most logical container for payments setup. Most online banking portals contain almost all of the required elements for payments except a variable payment amount as dictated by the payee – hence the need for PAD agreements.

The API will be made available as open source code.

3. Pre Authorized Debit Payment Process

- Currently (v0.4.23) Solidity contracts do not have ability to schedule events or transactions at future dates. Contract execution is triggered by transactions. For PAD agreements the external trigger for a transaction to fulfill a PAD agreement will occur from a payee payment request.
- This request is either directly from the payee organization or the interfacing bank server system. The request results in a call to the processPreAuthorizedDebit() function. Transaction execution occurs on due date of the PAD agreement.
- The process of a debit payment from a contract view point as recorded within the smart contract is an acknowledgement of the parameters of an existing PAD and to permanently chronicle payment obligation of the payor to the payee timestamped to date of transaction.
- Once this occurs on each periodic day of a PAD stipulated agreement, the immutable agreement on the blockchain can be considered an actionable financial transaction on the day of payment.
- Any change by payor to the PAD will affect future payment obligations only.
- For funds transfer, a daily extract or view of such chronicled transactions are:
  a) messaged by payee to the payor/payee bank for payment if transaction is payee initiated, or,
  b) retrieved from smart contract by payor/payee bank directly if transaction is bank server side initiated.

Automated Pre-Authorized Debit Payment Process


Payees
1
Bill notification n days prior to funds transfer
Payors
Payee Bank/Account
Payor Bank/Account
Inter-bank funds transfer
7
6
Payment transfer details
2
Payment Request - Occurs on scheduled date of actual payment; trigger for smart contract transaction.
5
Validated, authenticated funds transfer authorization.
transfer(<payorID><Amount><payeeID>)
Operating within secure bank environments
PAD API
Automated Pre-Authorized Debit Platform (backend server)
User Portals (Bank portals)
Mobile
Web Portal
Gas monitor
Ether purchase
3
Validate requestor payeeID
4
Confirm payor address contains the requestor payee as authorized to receive payments. Validate amounts, preset limits and schedules
PAD Smart Contracts
Ethereum Blockchain

Appendix A

Benefits for a business to establish a PAD agreement.

- Pre-Authorized debits (PADs) are a powerful tool for businesses. They are sometimes called direct debit, pre-authorized chequing (PAC), pre-authorized withdrawals or pre-authorized payments (PAPs).
- PADs are typically used for recurring payments, like mortgages and utilities, membership dues, charitable donations, RSP investments, and insurance premiums.
- Personal PADs are automated recurring payments from the customers' bank accounts for the goods or services a business provides.
- Business PADs arrange payments for goods or services related to a business, for example, payments between franchisees and franchisors, distributors and suppliers, or dealers and manufacturers.
- Cash Management PADs transfer, consolidate or reposition funds between accounts held by the business or closely affiliated businesses at different financial institutions. For example, a parent company can use cash management PADs to draw funds from an account of its subsidiary.

FAQ for businesses setting up a consumer PAD process.

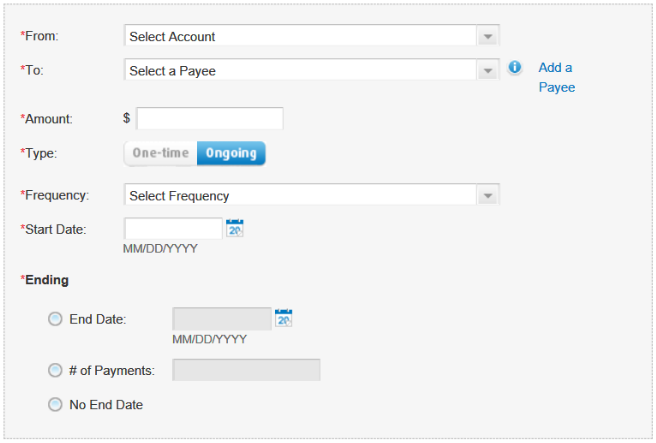
The current process contains many potential concerns and issues. The following is an extract from the Payments Canada site addressing common concerns around the PAD process from a business viewpoint.

Most of these issues are eliminated when the origin of payment setup and control is the consumer itself and not the business. In particular the business no longer needs to receive and be accountable for ensuring secure handling of consumer's bank information.

> - What if the customer's account information changes?
> - Can my customer cancel a payor's PAD agreement?
> - Can the amount of a PAD agreement be changed? Can we add extra charges? If a customer signs up for additional goods/services, can these fees be added to an existing agreement?
> - Do businesses outside of Canada need to follow Rule H1?
> - Is a one-time payment allowed? Do I need to have an agreement in place?
> - Can the amount of a PAD vary depending on how much the customer owes?
> - Do PADs have to occur at set intervals (e.g. monthly)?
> - Can I mask my customer's bank account information in my correspondence with them?
> - What happens if my business makes a mistake when taking money from an account?
> - If a customer doesn't have enough funds (NSF) in their account to cover a payment and it bounces, can I try again?
> - If a payment is returned because the customer doesn't have enough funds (NSF), does this cancel the agreement? Can I withdraw funds from the account at the next scheduled time?
> - Can I cancel an agreement for my customer?
> - Can my customer reverse a payment?
> - Can I charge my customers a fee for paying by PAD?
> - What can I do if a payment is returned for the reason "No agreement exists" when there is an agreement in place?
> - What if I sell or buy a company? Can the new owner continue the PADs?

Bank bill payment screens – online banking

Almost all functionaility for PAD definition is already provided on a typical bill payment screen. However, the amount field is a fixed value only, unable to vary month to month based on the billing needs of target business. Hence a PAD agreement must be setup with all its associated process. Through provision of a smart contract enabled connection to such a payment screen, or similar model, PAD setup and ownership is in the control of the consumer, the payor.



*From: Select Account

*To: Select a Payee — Add a Payee

*Amount: $

*Type: One-time | Ongoing

*Frequency: Select Frequency

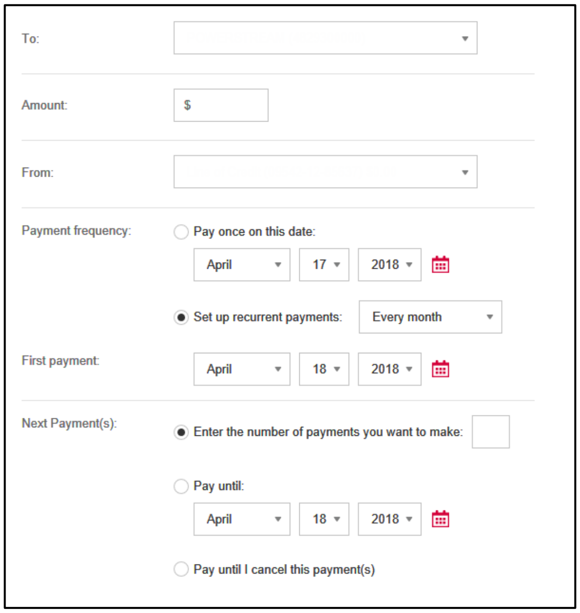
*Start Date: MM/DD/YYYY

*Ending

○ End Date: MM/DD/YYYY

○ # of Payments:

○ No End Date



To:

Amount: $

From:

Payment frequency: ○ Pay once on this date: April 17 2018

● Set up recurrent payments: Every month

First payment: April 18 2018

Next Payment(s): ● Enter the number of payments you want to make:

○ Pay until: April 18 2018

○ Pay until I cancel this payment(s)

References

- Payments Canada www.payments.ca
  - *Payments Canada is responsible for the clearing and settlement infrastructure and rules essential to meet the payment needs of consumers and business. It is delegated by the Canadian Government to provide Canada's national payment systems.*
- Payments Canada – Rule H1 – Pre Authorized Debits
- Telpay Incorporated – Electronic payment solutions for businesses http://telpay.ca
- Solidity documentation http://solidity.readthedocs.io

Credits

Various icons and images:

- http://www.icons-land.com Licence: Linkware
- http://awicons.com `"Icons by Lokas Software"` Licence: CC Attribution 4.0
- https://cibc.com - CIBC online banking
- https://www1.bmo.com – BMO Bank of Montreal online banking