Revisiting the Liquidity/Risk Trade-Off with Smart Contracts

Vincent Danos
CNRS, École Normale Supérieure, PSL, INRIA, Paris, France
vincent.danos@ens.fr

Jean Krivine
CNRS, Université de Paris, France
jean.krivine@irif.fr

Julien Prat
CNRS, École Polytechnique, Paris, France
Julien.Prat@ensae.fr

Abstract

Real-time financial settlements constrain traders to have the cash on hand before they can enter a trade [3]. This prevents short-selling and ultimately impedes liquidity. We propose a novel trading protocol which relaxes the cash constraint, and manages chains of deferred payments. Traders can buy without paying first, and can re-sell while still withholding payments. Trades naturally arrange in chains which contract when deals are closed and extend when new ones open. Default risk is handled by reversing trades.

In this short note we propose a class of novel financial instruments for zero-risk and zero-collateral intermediation. The central idea is that bilateral trades can be chained into *trade lines*. The ownership of an underlying asset becomes distributed among traders with positions in the trade line. The trading protocol determines who ends up owning that asset and the overall payoffs of the participants. Counterparty risk is avoided because the asset itself serves as a collateral for the entire chain of trades. The protocol can be readily implemented as a smart contract on a blockchain.

Additional examples, proofs, protocol variants, and game-theoretic properties related to the order-sensitivity of the games defined by trade lines can be found in the extended version of this note [1]. Therein, one can also find the definition and game-theoretic analysis of standard trade-lines with applications to trust-less zero-collateral intermediation.

2012 ACM Subject Classification Information systems → Online banking

Keywords and phrases Electronic trading, Smart contracts, Static analysis

Digital Object Identifier 10.4230/OASIcs.Tokenomics.2020.10

Category Short Paper

1 Bilateral contracts

A bilateral contract between traders u, v is a set of clauses describing their time-dependent payment and delivery obligations.

An *atomic clause* for x in $\{u, v\}$ is a triple (a, b) in $\mathbb{R}_+ \times \mathbb{R}$, where $a \geq 0$ is the *activation payment*, b the *passive effect*, and x is the *active trader*. The first component a specifies the amount x needs to pay to trigger the clause. The second component b is the payment which ensues, with the convention that $b \geq 0$ if x receives the payment.

A *constant clause* is a disjunction of atomic ones ie an element of $\mathcal{P}_{\text{fin}}(\mathbb{R}_+ \times \mathbb{R})$.

A *clause* is a finite piecewise-constant function from $\mathbb{Z}$ to $\mathcal{P}_{\text{fin}}(\mathbb{R}_+ \times \mathbb{R})$.

Time corresponds to block number in a blockchain implementation.

The *domain* of a clause is $|\Theta| = \{t \mid |\Theta(t)| > 0\}$.

We write $\mathcal{C} \subseteq \mathbb{Z} \to \mathcal{P}_{\text{fin}}(\mathbb{R}_+^2)$ for the set of clauses.

We say a clause Θ is: *deterministic*, if $|\Theta(t)| \leq 1$; *eventually defined* if $[M, +\infty) \subseteq |\Theta|$ for some M. We write $\mathcal{C}_0$, $\mathcal{C}_e \subset \mathcal{C}$ for the associated sets.

2nd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2020).
Editors: Emmanuelle Anceaume, Christophe Bisière, Matthieu Bouvard, Quentin Bramas, and Catherine Casamatta; Article No. 10; pp. 10:1–10:5

OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Clauses can be merged using two operations: $(\Theta + \Theta')(t) = \Theta(t) + \Theta'(t)$ where the sum on the right is taken pairwise $\{\theta_i\} + \{\theta'_j\} = \{\theta_i + \theta'_j\}$; and $(\Theta \vee \Theta')(t) = \Theta(t) \cup \Theta'(t)$.

The triple $(\mathcal{C}, \vee, +)$ is a commutative idempotent semi-ring, with sub-semi-ring the set of eventually defined clauses (but not the deterministic ones $\mathcal{C}_0$). The domain map is a semi-ring morphism from $(\mathcal{C}, \vee, +)$ to $(\mathcal{P}_{\text{fin}}(\mathbb{Z}), \cup, \cap)$.

A *bilateral contract* between u and v consists of a *backward clause* β for u, and a *forward clause* ϕ for v. One can depict a contract as a game (Fig. 1). The forward/backward distinction only makes sense when contracts are composed (see next Section).

A contract ϕ, β between u and v is said to be: *exclusive* if $|\phi| \cap |\beta| = \emptyset$; in an *$F$-state* (*$B$-state*) if active payments requested by ϕ (β) have been made by v (u); *idle* if neither in a B-state or an F-state; *eventually-F* (B) if ϕ (β) is eventually defined.

Notice that the game tree is not strictly speaking that of a sequential game [2]: the availability of moves to either player is context-dependent and so are the payoffs; and moves may (depending on the context) be available simultaneously to both players.

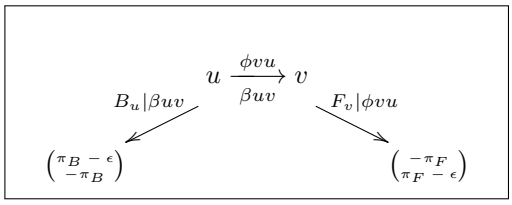

Figure 1 A contract as a game: ϵ is the constant cost of a move (gas); π_B (π_F) is the aggregated payoff to u (v); move B_u (F_v) is available in contexts where β (ϕ) holds.

A basic example is the *standard bilateral contract* with forward and backward clauses $\phi(t) = t < \Sigma \mapsto (a, 0)$, and $\beta(t) = t \geq \Delta \mapsto (0, p)$. This means that v may buy u's asset at price a at any time $t < \Sigma$; while u may cancel the deal at any time $t \geq \Delta$ and be paid a penalty p by v. One has $|\phi| = (-\infty, \Sigma)$, $|\beta| = [\Delta, +\infty)$. Hence this contract is: eventually-B; idle during the $[\Sigma, \Delta)$ interval if $\Sigma < \Delta$; and exclusive iff $\Sigma \leq \Delta$.

Absent the property of exclusivity, traders may move simultaneously. As a consequence, in a blockchain implementation, outcomes may depend on the order in which moves are ordered by the block-makers. A form of order-insensitivity can be achieved (see Supp. Inf. [1]).

2 Composite contracts

A *tradeline* is a non-empty list of composable contracts:

$$u_1 \xrightarrow[\beta_1]{\phi_1} u_2 \xrightarrow[\beta_2]{\phi_2} \cdots \quad u_{n-1} \xrightarrow[\beta_{n-1}]{\phi_{n-1}} u_n$$

u_1 is called the *origin* and u_n the *end* of the trade line. If $u_1 = u_n$, one says the trade line is *resolved*. If, in a given context, no contract is in an F- or a B-state, one says the trade line is *irreducible*; if every contract is in an F- or a B-state, one says the trade line is *connected*.

A trade line represents a game being played between the owners of its positions. We distinguish two types of moves.

Contractions are moves whereby the owner of an active position acquires an adjacent position. Below the active (acquired) position is in red (blue). Boundary cases where v is the end of the trade line (indicated by the symbol $v\,\cdot$) are shown on the right. Payments

consequent to clauses being triggered are left implicit.

$$u \xrightarrow[\beta]{\phi} v \xrightarrow[\beta']{\phi'} w \quad \overset{F_v}{\Longrightarrow}_{\phi} \quad v \xrightarrow[\beta\vee\beta']{\phi+\phi'} w \qquad u \xrightarrow[\beta]{\phi} v\cdot \quad \overset{F_v}{\Longrightarrow}_{\phi} \quad v\cdot$$

$$u \xrightarrow[\beta]{\phi} v \xrightarrow[\beta']{\phi'} w \quad \overset{B_u}{\Longrightarrow}_{\beta} \quad u \xrightarrow[\beta\vee\beta']{\phi+\phi'} w \qquad u \xrightarrow[\beta]{\phi} v\cdot \quad \overset{B_u}{\Longrightarrow}_{\beta} \quad u\cdot$$

If the trade line fully resolves under contraction, the owner of the last remaining position is now in full possession of the underlying asset.

The idea adding forward clauses is that the payment just made (or once promised) by v is transferred onto w's forward clause. The idea of taking the union of backward clauses is that u is carrying over his original cancellation condition in the new contract with w. Specifically, the new backward clause $\beta \vee \beta'$ which ties in u and w is implied by β. This means that the player triggering the B-move does not have to stop after the first contraction and *can sweep the entire trade line* if she wishes to, for as long as β holds.

Let γ, γ' be trade lines, and suppose γ contracts to γ' under the rules above. The following holds: (i) if γ is connected, so is γ'; (ii) if γ is exclusive, so is γ'; (iii) if all arcs in γ are eventually-B or -F, so are the ones in γ'.

We can return to the standard contracts and compute their reductions. With simplified and self-evident notations we get the following contraction rules:

$$u \xrightarrow[\Delta_1, p_1]{\Sigma_1, a_1} v \xrightarrow[\Delta_2, p_2]{\Sigma_2, a_2} w \quad \overset{B_u}{\Longrightarrow}_{v \to^{p_1} u} \quad u \xrightarrow[\Delta_1, p_1 \vee \Delta_2, p_2]{\min(\Sigma_1,\Sigma_2),\, a_1+a_2} w \qquad \textit{for } t \geq \Delta_1$$

$$u \xrightarrow[\Delta_1, p_1]{\Sigma_1, a_1} v \xrightarrow[\Delta_2, p_2]{\Sigma_2, a_2} w \quad \overset{F_v}{\Longrightarrow}_{v \to^{a_1} u} \quad v \xrightarrow[\Delta_1, p_1 \vee \Delta_2, p_2]{\min(\Sigma_1,\Sigma_2),\, a_1+a_2} w \qquad \textit{for } t < \Sigma_1$$

For $t \geq \max(\Delta_1, \Delta_2)$ the trader with the backward clause will pick the highest of p_1 or p_2.

2.1 Extension

We also need a move to grow a trade line. Any trader at the end u of the trade line can extend it using the sell rule $S_{uv}(\phi, \beta)$ and append a new contract with clauses ϕ, β, thereby adding a new position v to the game:

$$u\cdot \quad \overset{S_{uv}(\phi,\beta)}{\Longrightarrow} \quad u \xrightarrow[\beta]{\phi} v\cdot$$

If extensions were not constrained to happen the end of the trade line, the owner of the origin could introduce a new position u_0 left of it:

$$u_0 \xrightarrow[-\infty<t\mapsto(0,a)]{-} u_1 \longrightarrow \cdots \longrightarrow u_n$$

and sweep through the entire line by iterating B_{u_0} and collect an arbitrary fee a from everyone. We show below that our design choices prevent such catastrophic events.

3 Soundness of the trade game

We establish now an upper bound on the expenses incurred by playing the game.

The simplify the derivation we assume deterministic clauses. Let γ be a trade line, and let t be a time. We denote by $<$ the positional ordering in γ. For any position $i \in \gamma$ not at the end of γ, we denote by $\phi_i(t)$, $\beta_i(t)$ the clauses where i is in backward position.

Payoffs at fixed time are specified by pairs of real numbers: $\phi_i^1(t) \geq 0$ is the active payment i's Buyer makes to i to complete the deal; and $\phi_i^2(t)$ is the (possibly negative) passive payment from i to his Buyer which follows. When i's Buyer plays that forward move, i's payoff is therefore: $\phi_i^1(t) - \phi_i^2(t)$. We suppose henceforth that $\phi_i^1(t) \geq \phi_i^2(t)$, so that a forward move is always profitable to the passive player. This constraint is stable under contractions.

Likewise: $\beta_i^1(t) \geq 0$ is the active payment i needs to make to i's Buyer to cancel the deal; and $\beta_i^2(t)$ is the (possibly negative) passive payment from i's Buyer to i which follows. When i plays that backward move, i's payoff is therefore: $\beta_i^2(t) - \beta_i^1(t)$.

Fig. 2 summarises the situation. For F_v, B_v, v is the active trader; for B_u, F_w, v is passive

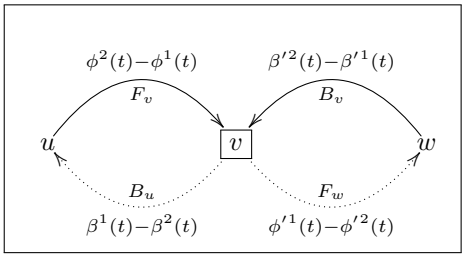

Figure 2 Contractions which change the balance of v together with the subsequent payoffs.

and evicted by the move. Accordingly, from v's viewpoint $\phi^2(t) - \phi^1(t)$, and $\beta'^2(t) - \beta'^1(t)$ are the active payoffs, and $\beta^1(t) - \beta^2(t)$, $\phi'^1(t) - \phi'^2(t)$ the passive ones.

We define the *leftward bounds* (leaving out positions where payoffs are undefined):

$$\begin{array}{lcll} \beta(v,t) & = & \max_{i<v}(\sup_{s\geq t}(\beta_i^2(s) - \beta_i^1(s))) & \textit{passive expense on a } B\textit{-move} \\ \phi(v,t) & = & \sum_{i<v} \sup_{s\geq t}(\phi_i^1(s) - \phi_i^2(s)) & \textit{active expense on an } F\textit{-move} \end{array}$$

The idea is that $\beta(v,t)$ is an upper bound for the expenses v may incur upon eviction by a B-move, whichever is the trace followed. Likewise, $\phi(v,t)$ is an upper bound for the price v will ever have to pay to acquire the underlying (by buying all left positions using a series of F-moves). Both quantities depend only on contracts left of v in γ.

We define also the *rightward bounds*:

$$\eta_v^B(t) \quad = \quad \sup_{s\geq t}(\beta_v^1(s) - \beta_v^2(s)) \qquad \textit{active expense on a } B\textit{-move}$$

The idea is that $\eta_v^B(t)$ upper bounds the active payment made by v on a B-move. This bound assumes no trader is fool enough to pick an option worse than his original backward clause. Here the control is local to v, because v's β clause self-propagates under reduction. Note that $\eta_v^B(t) \leq 0$ if v's backward clause always specifies a profit for v. There is no need to define a symmetric $\eta_v^F(t)$ to control for passive expenses on an F-move, as we have assumed above that F-moves are always profitable to the Seller.

▶ **Proposition 1** (max expenses)**.** *Let γ be a trade line, and v a position in γ. Along any trace starting from γ where v plays no extension, v's expenses are upper bounded by:*

$$\phi(v,t) + \beta(v,t) + N\eta_v^B(t)$$

with N the number of B_v moves played by v. If $\eta_v^B(t) \leq 0$, v's expenses are upper bounded by $\beta(v,t) + \phi(v,t)$.

To cope with traces where v extends the trade line, ie plays with moves of type $S_{vw}(\beta_k, \phi_k)$, one can readily adapt $\eta^B_v(t)$ to also maximise over such moves k:

$$\hat{\eta}^B_v(t) \quad = \quad \max_k \sup_{s \geq t}(\beta^1_k(s) - \beta^2_k(s))$$

If all these payments are Seller-positive, ie $\hat{\eta}^B_v(t) \leq 0$, we can forget this additional term.

One can also show that the evolution of a trade line cannot lead to a solution where a Seller receives less than the originally asked price for a forward as well as a backward move.

▶ **Proposition 2** (Monotonicity). *Let γ be a trade line, and v a position in γ: v's forward payoff (as Seller) is non-decreasing, and v's backward payment is invariant.*

Note that even if there are Buyers waiting to join, v's forward payoff may never happen. Suppose v faces a w who extends the tradeline with a *forward-dead* contract $S_{wx}(\mathbf{0}, \beta)$, and w never plays F_w. The only way out for v is to B-sweep the trade line entirely.

4 Aside on implementation

Trade lines and their evolution rules can be interpreted by a dedicated smart contract connected to an external custodial contract to define the ownership of the assets traded in the protocol. When the game starts, the owner of the asset transfers its property to an account of the custodial contract which is controlled by the interpreter contract.

To implement passive payments which are essential to the protocol, one could forward payment obligations to an external system managing the players' debts. Prop. 1 gives a solution for a trust-less implementation. Using the associated upper bounds, the contract can statically compute the amount of cash a trader needs to stake in, upon joining. By asking traders to fully *provision* potential expenses, one does not have to trust them to honour their debts. Depending on specific time-dependencies, provisions can be partially returned as time advances and provisions are re-evaluated. There is no such concern for active payments, as these are payments which players have to make to change the state of the game.

When the trade line finally resolves, it remains for the interpreter contract to ask the custodial contract to transfer the ownership of the asset to the owner of the one remaining position in the game (which implies that the owner is known to the custodial contract).

5 Conclusion

We have defined a consistent trade protocol to manage chains of reversible bilateral contracts. Its design derives entirely from a simple premise: the need for a theory of deferred payments which allows one to postpone payments, and resell an asset one has not paid for yet. To do this one has to keep somehow a memory of past transactions, and introduce mechanics to revert some, as the need may occur. This leads to a protocol where chains of transactions define the state of an open game; the evolution of which relies on the reversibility of the component games.

References

1 Vincent Danos, Jean Krivine, and Julien Prat. Reversible and composable financial contracts, 2019. URL: `http://www.di.ens.fr/~danos/tls.pdf`.

2 Drew Fudenberg and Jean Tirole. Game theory, 1991. *Cambridge, Massachusetts*, 393(12):80, 1991.

3 Mariana Khapko and Marius Zoican. How fast should trades settle? *Society for Financial Studies (SFS) Cavalcade*, 2017.