

LEXIFY INSIGHTS

YOUR TRUSTED LEGAL NEWSLETTER

ATOMIC SWAPTIONS: CRYPTO DERIVATIVES WITHOUT A TRUSTED THIRD PARTY

Technology & Digital Assets | 18/2026



LEXIFY
MORE THAN LAWYERS

i Introduction

Derivatives let crypto users hedge price risk, but trading them on centralized venues brings back the counterparty and custody risks that crypto set out to remove. This article walks through a research paper that builds option contracts settling directly between two parties and works through how these instruments interact with the EU financial regulation. The Paper is by James A. Liu, *Atomic Swaptions: Cryptocurrency Derivatives*, University of California, Irvine, arXiv no. 1807.08644, hereinafter the referred to it as the “**Paper**”.

Atomic Swaptions: Crypto Derivatives Without a Trusted Third Party

The idea

The idea is simple: use derivatives in crypto the way traditional finance already uses them. Derivatives are a good tool for hedging, especially when your costs sit in a different currency from your revenue.

Take a concrete case. Miners earn their revenue in crypto-assets but pay most of their expenses in other currencies, including stablecoins. A futures contract could cover that mismatch.

Why centralized venues don't solve it

There's a catch. If you trade these derivatives on a centralized exchange (“**CEX**”), you inherit the same risks crypto was meant to avoid, and sometimes worse ones given the regulatory position: counterparty risk, liquidity risk, custody risk. Most crypto derivatives today are booked offshore, which compounds the problem.

The Paper makes the point sharply. Derivatives are long-dated, so users have to leave their assets on the exchange for the entire life of the contract. Any margin the venue offers adds direct and indirect counterparty risk, and in a sharp market move the exchange itself can become insolvent.

What the Paper proposes

It shows that atomic swaps can limit the risks above. An atomic swap uses Hashed Time-Lock Contracts (“**HTLCs**”), a form of cryptographic escrow, with the blockchains themselves acting as the trusted third party. Put differently, you use cryptographic proof on one chain that a prerequisite payment happened on another.

There are two features that matter here. First, the chains don't need to be Turing-complete (like Ethereum), which makes the method more scalable. Second, the construction needs no oracle, so it removes a point of failure and the need to trust an external data provider. The Paper also describes how to route these contracts over the Lightning Network.

How an atomic swap works

An atomic swap solves a basic trust problem. If notorious Alice sends her coins to notorious Bob first, Bob can take them and walk away without sending his. The reverse is true if Bob goes first.

The fix is an HTLC on each chain. Alice creates a secret and locks her tokens in a contract that unlocks only if that secret is revealed within a set time. Bob does the same with his tokens, on a slightly shorter deadline. When Alice claims Bob's tokens, she reveals the secret, which lets Bob claim hers. If anything breaks, both parties recover their funds once the timelocks expire.

From a swap to an option

Now add the option. An option contract gives Alice the right, not the obligation, to swap 1 ACoin for 1 BCoin up to a set date (E), in exchange for a premium paid to Bob. If the price moves her way, she exercises and Bob must deliver; if not, she lets it expire.

The buyer holds the right to decide whether delivery happens, and the buyer pays the seller a premium. Alice's value is the choice between the two assets; Bob takes the premium and the obligation.

For the sake of completeness: a so-called "American option" can be exercised any time before expiry, a so-called "European option" only at maturity. This construction gives Alice early exercise, so it's American-style.

In traditional finance a "swaption" is an option to enter into an interest-rate swap. The Paper coins "*atomic swaption*" for something different: an atomic swap that exchanges a premium for the creation of an option.

Building the atomic swaption and brief note on put-call parity

The Paper's construction nests two atomic swaps. I'll keep this light on the cryptographic detail.

The first swap, the funding contract, pays Bob the premium and at the same time funds the second swap, which is the option itself. The second swap looks like a standard atomic swap, except its expiry is set far out (say, 1 year), which gives Alice the time to decide whether to exercise. In short, Alice pays a premium for the future right to swap.

For safety, the principal deposit transactions need both parties' signatures plus the secret, and they're pre-signed so neither side can change the terms on its own.

The capital problem, and margin

There's a downside, and it's the one every on-chain contract faces. Someone has to lock the full principal in the contract until exercise or expiry. In traditional markets you wouldn't post the whole amount up front; you'd post a small margin.

The Paper's answer is the margin contract. Instead of locking the full sum, Alice and Bob each post an agreed margin. Each signs transactions that force the other, if it wants to proceed, to deposit the full principal into the swaption. If a party doesn't, the counterparty keeps the margin as a penalty.

Bob, for example, has to complete his deposit by a deadline. If he misses it, Alice takes his margin without even revealing the secret, and she simply doesn't exercise. Alice's side is symmetric but on a shorter deadline: if she fails to fund, Bob keeps her margin and forfeits his own. The mechanism cuts the capital tied up at the start and gives both sides a reason to perform.

It is noteworthy that the Paper states that floating margin **can closely replicate a call or put payoff, and that a version of put-call parity then lets you build a futures contract**: a long futures position equals a long call plus a short put at the same strike and expiry.

The regulatory question

A genuinely peer-to-peer atomic swaption has no regulated person for EU financial law to attach to. The exposure appears the moment someone centralizes the arrangement.

Freedom of contract in private law comes first in most legal systems. Private parties can agree to swap one asset for another. As long as the essential elements of a contract are present (e.g., in civil law agreement, lawful cause, a determinate object, and any required form), a bilateral, off-market swaption

is valid. Its private nature doesn't make it unlawful or defective.

The financial regulatory question is narrower: does the arrangement fall inside an European Union's supervisory perimeter?

Directive 2014/65/EU ("**MiFID II**") lists financial instruments in Annex I, Section C. Point (4) covers options, futures and swaps relating to securities, currencies, interest rates or yields, financial indices, or other derivative instruments. An atomic swaption is, in form, an option (a contingent claim), and even a swap of a premium for an option. The problem may be the underlying: one crypto-asset against another. A crypto-asset isn't a currency in the legal sense, isn't a transferable security, and isn't any of the listed underlyings. So, the fit with Section C is real on the contract type but may be on some level contestable on the underlying. Where the underlying crypto-asset itself qualifies as a transferable security, the instrument reads more naturally as a Section C(4) derivative; where it doesn't, the classification could stay open.

This matters beyond MiFID, because Regulation (EU) 648/2012 ("**EMIR**") borrows the same definition. EMIR defines a derivative by reference to points (4) to (10) of MiFID's Section C, and an OTC derivative as one not executed on a regulated market. If the swaption is a Section C derivative, EMIR's obligations on counterparties can attach: clearing, reporting to a trade repository, and risk-mitigation for non-cleared OTC derivatives. But each of those runs against identifiable counterparties, and several turn on counterparty status and thresholds. Are two wallets running an HTLC protocol candidates for that machinery? Probably not.

Furthermore, is there a regulated person or activity? MiFID doesn't regulate instruments in the abstract.

It regulates persons, activities, namely financial services.

An "*investment firm*", in MiFID's words, is any legal person whose regular business is providing investment services to third parties or performing investment activities on a professional basis (Article 4(1)(1)). The investment services themselves (Annex I, Section A) all presuppose someone providing a service or running a system: receiving and transmitting orders, executing clients, dealing on own account, placing, or operating a multilateral or organised trading facility. A "*trading venue*" is a regulated market, an MTF or an OTF, and an MTF or OTF is a multilateral system operated by an investment firm or a market operator. A "*systematic internaliser*" is, again, an investment firm dealing on own account outside a venue.

Every one of these has a built-in subject. Remove the issuer, the operator and the intermediary, and there's no person on whom authorisation, conduct or organisational duties can rest. In fact, the Paper's whole point is that cryptography replaces the trusted third party. When the third party goes, the regulated person goes with it.

The Regulation (EU) 2017/1129 ("**Prospectus Regulation**") confirms the pattern from the issuance side. At certain conditions it requires a prospectus for an offer of securities to the public or admission to trading on a regulated market, and "*securities*" means transferable securities as defined in MiFID Article 4(1)(44). Someone may defend a position where a privately negotiated swaption (without possibility to transfer it to other third parties) may be neither a "transferable" security nor a public offer, so apparently someone could say that no prospectus duty arises, unless a centralised issuer packages and offers these contracts to the public.

That leaves the interpretation problem the draft raises. Should MiFID be read to catch decentralised instruments even though it contains no decentralisation exemption? MiFID's operative provisions all presuppose a regulated person, and a rule that governs "*the provision of investment services to third parties*" can't bite where there's no provider and no third party being served.

EU secondary law is read purposively and systematically, not only literally. On that method, the tension resolves in favour of substance. The regime targets the function, **an intermediated and organised market activity, rather than the bare existence of an instrument on a public ledger.** MiCAR points the same way in principle, since it leaves genuinely decentralised arrangements without an identifiable operator outside its issuer- and provider-based obligations. It would not be wise to lean on MiCAR's text here, but the functional logic may be considered consistent across the framework.

Conclusion

In conclusion, the two main questions can be: whether a crypto-to-crypto option is always a Section C(4) instrument when its underlying isn't itself a financial instrument, and whether two protocol counterparties could ever function as "*counterparties*" for EMIR reporting in practice.

Lexify as Your Consultant

Lexify continuously monitors regulatory developments and assists European and international companies within this sector, including digital-asset derivatives and decentralized finance, from instrument classification under MiFID II and EMIR to issuance and distribution questions under the Prospectus Regulation and MiCAR.

Contact

Connect with us

Thank you for taking the time to read our article. We hope you find it informative and engaging. If you have any questions, feedback, or would like to explore our services further, we're here to assist you.

Contact Information

For inquiries about our legal assistance, please contact:



Emanuele Gambula

+41 76 232 66 83
emanuele.gambula@lexify.io



Alberto Borri

+41 77 461 38 47
alberto.borri@lexify.io

Follow Us

Stay updated and connected with us on social media for the latest news, insights, and updates:

- **LinkedIn:** [Lexify](#)
- **X:** [Lexify](#)
- **YouTube:** [Lexify](#)

Explore More

Visit our website, register to our Newsletter at <https://www.lexify.io/> and never miss a legal insight!