dr laurence e. day / @functi0nZer0; ethcc6

Kanav My Money Back?: The Rise of “Counter-Exploits” and Court Interventions in DeFi

What We’re Talking About

Contract upgradeability being used as a counter-offensive weapon for exploits, and how we can or should react to it

Onchain: Platypus, Oasis/Jump
Offchain: Illinois SB1887 (*lmao*)

Contains one (1) diagram on how one type of upgradeability ‘works’, but slides are code free otherwise – we’re all tired

“I Am Altering The Deal…”

The difference between EOAs and smart contracts is that EOAs have no bytecode associated with them

At present a smart contract cannot easily change its bytecode (without disruption) after deployment.

But often, changing that bytecode is exactly what we want or need to do!

Altering It Further

Two scenarios are the most common –

a) A bug is spotted: needs fixing
b) Scheduled upgrade: needs patching

This talk introduces two more:

c) Recovery is possible: needs reacting
d) A court is involved: needs forcing

Impetus behind these changes is different!

Platypus Finance

Groundwork: AMM on Avalanche
– single sided liquidity, stable oriented

Introduced an overcollateralised stablecoin: deposit LP tokens, mint USP

Bug in Masterchef-like contract in the form of an `emergencyWithdraw` that let you pull out LP without paying off USP debt

Result: US$9.1mm stolen

Platypus Finance

PLATYPUS

Summary of attack:

- Flash loan stables
- Deposit flash loan to Platypus
- Deposit LP to Masterchef
- Max out USP borrow against LP
- Withdraw LP from Masterchef
- Withdraw flash loan from Platypus
- Swap USP for more stables via Platypus
- Repay flash loan (plus fee)

Platypus Finance

PLATYPUS

Attack was a comedy of errors:

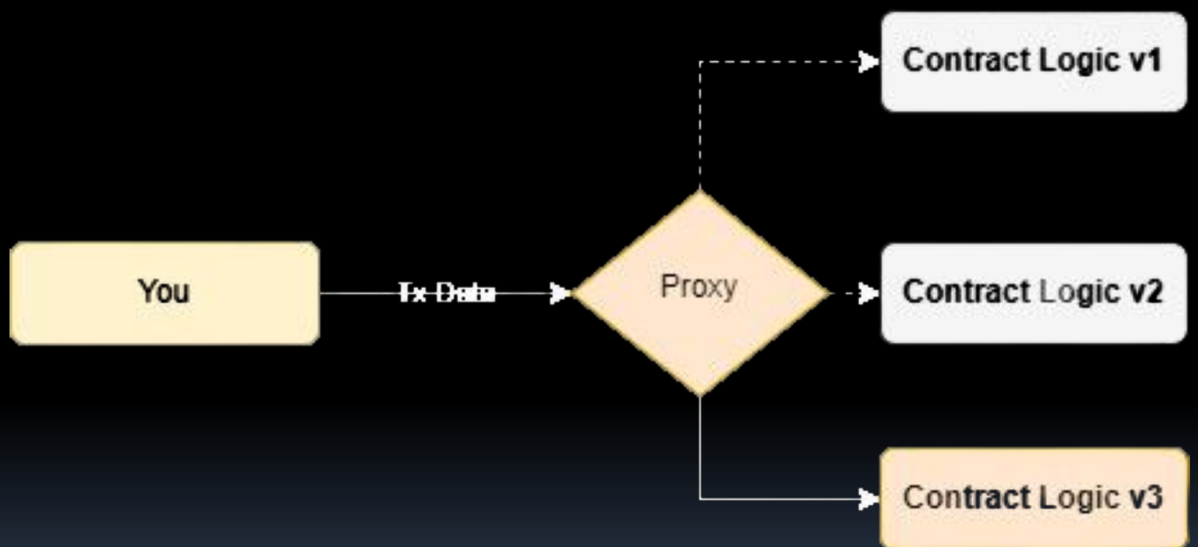
1) No transfer function out of exploit contract, funds trapped there

2) Second attempt sent US$380k to Aave

3) Flash loan function contained a callback with no access control – callback hardcoded USDC approval to a proxy

Interlude: Proxies 101

When a contract is proxy upgradeable, this is how a transaction flows:



Proxy contains a slot for a mutable address pointing at the current implementation (it self-maintains state via `DELEGATECALL`)

Platypus Finance

PLATYPUS

Counter-exploit was 'simple':

1) Upgrade proxy implementation to a new contract that can move tokens

2) Invoke the flash loan callback, forcing exploit contract to approve USDC

3) Seize the approved 2,403,762 USDC

Because Of The Implications

This was a slick partial recovery, but it brings up two consequences that are going to become increasingly important:

A) Developer teams have *always* had this power *if* using a proxy implementation

B) Given the above, what happens when a court of law demands a contract upgrade for some purpose or another?

Gifts From My Overlords

Today's talk is sponsored by Raid Shadow Legends, one of the biggest mobile role-playing games of 2019 and it's totally free! Currently almost 10 million users have joined Raid over the last six months, and it's one of the most impressive games in its class with detailed models, environments and smooth 60 frames per second animations! All the champions in the game can be customized with unique gear that changes your strategic buffs and abilities! The dungeon bosses have some ridiculous skills of their own and figuring out the pe[illegible]rty an[illegible]ateg[illegible] ov[illegible]hem's a lot of fun! Currently with ov[illegible]0[illegible]00 re[illegible]s, Ra[illegible]as almos[illegible] perfect score on the Play Store! Th[illegible]om[illegible]unity[illegible]growin[illegible]st[illegible] th[illegible]ighly anticipated new faction wars[illegible]are is no[illegible] l[illegible] you[illegible]igh[illegible]e[illegible]nd my squad out there in the arena! It's e[illegible]er t[illegible]ow[illegible]n e[illegible] w[illegible]rates program for new players you get a ne[illegible]dai[illegible]ogi[illegible]ew[illegible] fo[illegible]st 90 days that you play in the game! So what are you waiting for? Go to the video description, click on the special links and you'll get 50,000 silver and a free epic champion as part of the new player program to start your journey! Good luck and I'll see you there!

Jump × ~~Oasis~~ Summer

Wormhole bridge attack of February 2022 stole 120,000 ETH worth of collateral

Jump (market-maker) plugged the shortfall within 24 hours: valued at over US$320m

Funds moved around various protocols for the next year, eventually settling in Oasis vaults (automation-empowered leverage)

Jump × Oasis

Enabling a stop-loss trigger on an Oasis vault involves granting an approval to a contract (to buy collateral or take on debt)
Wormhole exploiter enabled such a trigger

That contract is proxy upgradable, owned by the Oasis multi-sig – see the pattern?

A whitehat group did, and reached out to Oasis with a proof of concept

Jump × Oasis

Presumably due to concerns about the legality of intervening, Oasis sought – and was granted – an injunction from the UK High Court [Oazo Apps is UK-based]

Read: Oasis requested legal permission to facilitate an 'exploit' of its own protocol

This isn't really a counter-exploit – *Wormhole* was attacked, this is a retrieval at an opportune moment from *elsewhere*

Jump × Oasis

Wallet X added to Oasis multi-sig, which deployed new contracts for the automation proxy (and others) that handed total control of attacker vaults over to them

X migrated all debt and collateral from vaults to a new one, restored proxy implementations, then had power removed

Jump sent $80m in DAI to X to pay off debt, and walked away with ≈124,000 ETH


"Aagh, call an ambulance!"
"But not for me"

What Precedent Was Set?

This was a *huge* win for Jump, but they couldn't have done it without:

- having a wallet added to the multisig, and
- three Oasis key-holders cosigning

This was a unique set of circumstances: and Oasis explicitly sought a legal mandate for it

What if Jump forced the matter in court?
What if Oasis didn't *want* to comply?

Legal Objection In Theory

There are some in crypto who balk at the idea of a protocol being forced to bend the knee to an imposition from a court

Your options in that case are quite limited:

- Be truly anonymous from the start
- Don’t use diamond proxy patterns
- Don’t use metamorphic contracts
- Renounce all ownership (very limiting!)

Legal Objection In Practice

Let's keep it 💯, if you're a doxxed entity and your local court demands you comply with a task in your power to perform, you're going to comply – you're very unlikely to spitefully burn access *after* an injunction

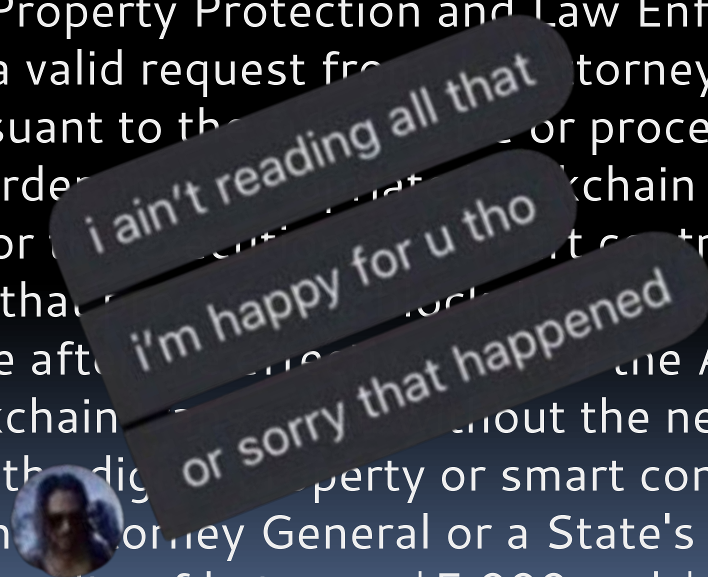
...assuming that the law you're being asked to comply with is sensible

So let's see how that's going

Illinois SB1887

Currently sitting in committee after a first reading in the Illinois Senate:

Creates the Digital Property Protection and Law Enforcement Act. Provides that upon a valid request fr [illegible] torney General or a State's Attorney, made pursuant to th [illegible] or procedural laws of the State, a court may orde [illegible] kchain transaction for digital property or for [illegible] tract. Provides that a blockchain network tha [illegible] saction originating in the State at any time aft [illegible] the Act shall process a court-ordered blockchain [illegible] hout the need for the private key associated with th [illegible] perty or smart contract. Provides that upon a petition by th [illegible] orney General or a State's Attorney, the court shall assess a civil penalty of between $5,000 and $10,000 for each day that the blockchain network fails to comply with the order.



Illinois SB1887

We can pretty much treat this bill as DOA, but this is the gist of it:

An Illinois court can demand that any blockchain that processes a transaction from IL must *hard-fork* to force a change (i.e. moving a balance, unwinding positions)

And 'the network' gets fined up to US$10k per day that it doesn't comply

Illinois SB1887

Some thoughts:

This was hard enough to do after the DAO incident with widespread consensus

Shifting native tokens (e.g. ETH) is already tricky difficulty–wise: for a DeFi protocol this is a Herculean task: determining the state root alone would kill a Victorian child

Illinois SB1887

Who's liable for that civil penalty? Illinois validators or miners? A foundation that stewards the chain (c.f. EF)?

It beggars reason to imagine a validator being held liable for a failure to fork if someone gets an injunction vs Yearn: even if all Americans comply (42%), not enough!

Chain would fail to finalise, inactivity leak

On Externalities

We don't get to ignore the elephant in the room – chain legitimacy is now partially bestowed by stablecoin redemption support

What happens if America is forced to cleave off from the rest of the network? Tether probably sticks with canonical chain, how about Circle? They're as American as it gets

To steelman Ethereum, *must* we introduce more stables at scale? Widen the 3pool?

Can *We* Do Better?

There are better efforts at producing legal thought regarding the obligations and responsibilities when it comes to granting legal personality to smart contracts, along with all the implications regarding upgrades:

- LexDAO/LeXpunK Army
- Coalition of Legal Automated Applications
- Stanford Journal: Blockchain Law & Policy
- and many, many others

Closing Thoughts

"We have involved ourselves in a colossal muddle, having blundered in the control of a delicate machine, the working of which we do not understand. The result is that our possibilities of wealth may run to waste for a time – perhaps for a long time."

–John Maynard Keynes,
The Great Slump of 1930