

# 5 年後還是新手

WordPress Plugin 開發大冒險

# The Levels - Agenda

- 故事背景

Background

- 新手村

Why, and how to start your own plugin?

- 打怪

Here comes the users

- 打大佬

Gutenberg, Modern Admin UI, Security



[About me](#)

# Background - Our plugin and products



LikeCoin

## [LikeCoin:](#)

blockchain for content creators and publishing

## [LikerLand:](#)

Writing NFTs and bookstore



Liker Land

## [Web3Press:](#)

Web3 plugin for WordPress users



# Introduction - Why make a plugin?

## Site owners:

- Enable and disable plugin easily
- Track the actual changes all in one place
- WordPress upgrade doesn't break your change

## Developer:

- Share your code and functionalities

## Business:

- Sell your product!

# Overview - How to make a plugin?

Plugin Handbook - 新手指南

<https://developer.wordpress.org/plugins/>

- Hooks
  - Change the post content on publish “content”
  - Add a Google Analytics in your site header “hook\_header”
- APIs
  - Post your post to <https://matters.town> as a draft
  - Send your url to Internet Archive for snapshot

# Overview - Code Setup

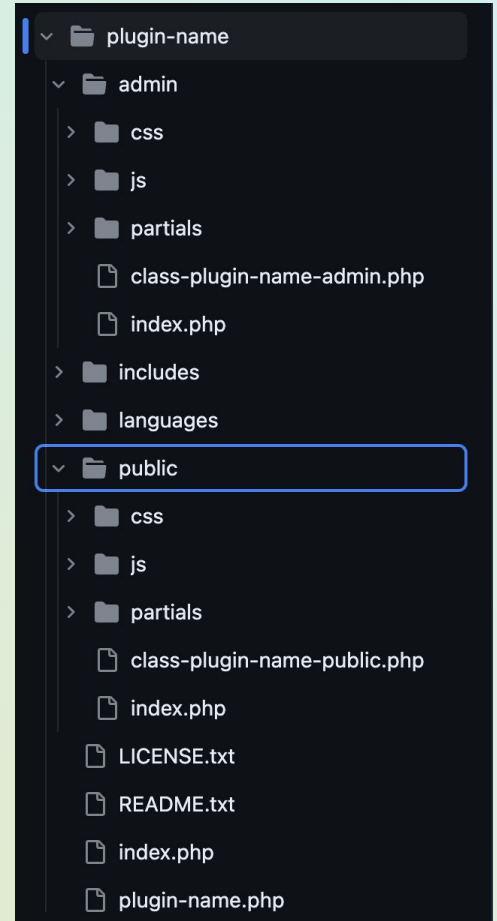
WordPress runs on:

Basic (oldschool) setup

- PHP - Pages, Logic, where hook happen
- Javascript - Browser interactions, update UI and calls API
- CSS - Style your UI

Protip: Start with a boiler plate

- [wp scaffold plugin](#)
- <https://github.com/devinvinson/WordPress-Plugin-Boilerplate>



# Overview - Code best practices

<https://developer.wordpress.org/plugins/plugin-basics/best-practices/>

e.g. WordPress PHP codes are all in one global namespace

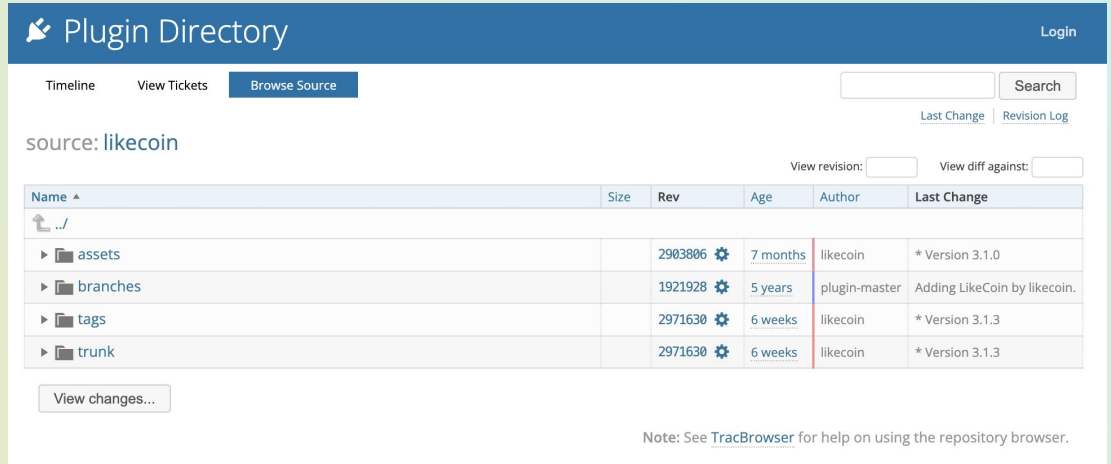
If you function has a 公廁名 then it will either overwrite someone else's stuff, or get overwritten.

Prefix your functions (likecoin\_foo) vs Objects (still has to be unique in class name)

# Overview - Done? Ship it!

- GPLv2 compatible
- Code must be human readable, or come with source map/source code
- [Plugin slug approved by wordpress.org](https://wordpress.org/plugins/likecoin/)
- Push version to SVN
- Profit!

You can always view code of any plugin on wordpress.org SVN



The screenshot shows the 'Plugin Directory' interface for the 'likecoin' plugin. It features a navigation bar with 'Timeline', 'View Tickets', and 'Browse Source' buttons. A search bar is present with a 'Search' button. Below the navigation, the source is identified as 'likecoin'. There are input fields for 'View revision:' and 'View diff against:'. A table lists the repository structure with columns for Name, Size, Rev, Age, Author, and Last Change. The table shows a directory structure with subfolders like 'assets', 'branches', 'tags', and 'trunk', each with associated revision numbers, ages, authors, and last change dates. A 'View changes...' button is located below the table. A note at the bottom right states: 'Note: See [TracBrowser](#) for help on using the repository browser.'

Name ^	Size	Rev	Age	Author	Last Change
↑ ../					
▶ assets		2903806 ⚙	7 months	likecoin	* Version 3.1.0
▶ branches		1921928 ⚙	5 years	plugin-master	Adding LikeCoin by likecoin.
▶ tags		2971630 ⚙	6 weeks	likecoin	* Version 3.1.3
▶ trunk		2971630 ⚙	6 weeks	likecoin	* Version 3.1.3



Now the true adventure begins

Hey I use PHP 5.2 and your  
site breaks

<https://github.com/likecoin/likecoin-wordpress/pull/28>

# Hey I use PHP (insert legacy version here)

- WordPress can run on PHP 5.2 - 8.0
- <https://make.wordpress.org/core/handbook/references/php-compatibility-and-wordpress-versions/>
- Newer syntax won't work on sites with newer PHP
- Dev: Always prefer older syntax
- Define minimum support PHP version in your plugin
- Site owner: Try to upgrade PHP!

```
// Before php 5.4  
$array = array(1,2,3);
```

```
// since php 5.4 , short syntax  
$array = [1,2,3];
```

WP Version	5.2	5.3	5.4	5.5	5.6	7.0	7.1	7.2	7.3	7.4
6.4	N	N	N	N	N	Y	Y	Y	Y	Y
6.3	N	N	N	N	N	Y	Y	Y	Y	Y
6.2	N	N	N	N	Y	Y	Y	Y	Y	Y
6.1	N	N	N	N	Y	Y	Y	Y	Y	Y
6.0	N	N	N	N	Y	Y	Y	Y	Y	Y

# Hey can it also be in Spanish

This one is from discord

income, either with likes or the sale of my content, however I don't know why where to start because my audience is Spanish and I see that the community is in English, if someone can help me I would appreciate it. Note the platform I am building on WordPress

# Hey can it also has a (insert language here) version?

Internationalization problem - i18n


Meet [translate.wordpress.org](https://translate.wordpress.org)

Projects / Plugins / Web3Press – Decentralize Publishing with Writing NFT

New to Translating WordPress? Read through our [Translator Handbook](#) to get started. [Hide](#)

Web3Press – Publish your posts as NFT and sell it right away; build your community in the Web3 way.

[WordPress.org Plugin Page](#)

 Web3Press – Decentralize Publishing with Writing NFT

Projects ▾

Locale	Development	Development Readme	Stable	Stable Readme	Waiting/Fuzzy
<a href="#">Chinese (Taiwan)</a>	61%	40%	61%	40%	0
<a href="#">Chinese (Hong Kong)</a>	61%	39%	61%	39%	59
<a href="#">Chinese (China)</a>	59%	32%	59%	32%	64
<a href="#">Japanese</a>	10%	7%	10%	7%	0
<a href="#">Korean</a>	8%	2%	8%	2%	0
<a href="#">Dutch</a>	4%	0%	4%	0%	0

# Meet translate.wordpress.org

Translation of Stable (latest release): Chinese (Taiwan)

[Translate Live](#) • [Locale Glossary](#)

Filter ↓ • Sort ↓ • [All \(219\)](#) • [Translated \(135\)](#) • [Untranslated \(84\)](#) • [Waiting \(0\)](#) • [Changes requested \(0\)](#) • [Fuzzy \(0\)](#) • [Warnings \(1\)](#)

← 1 ... 4 5 6 7 8 ... 15 →

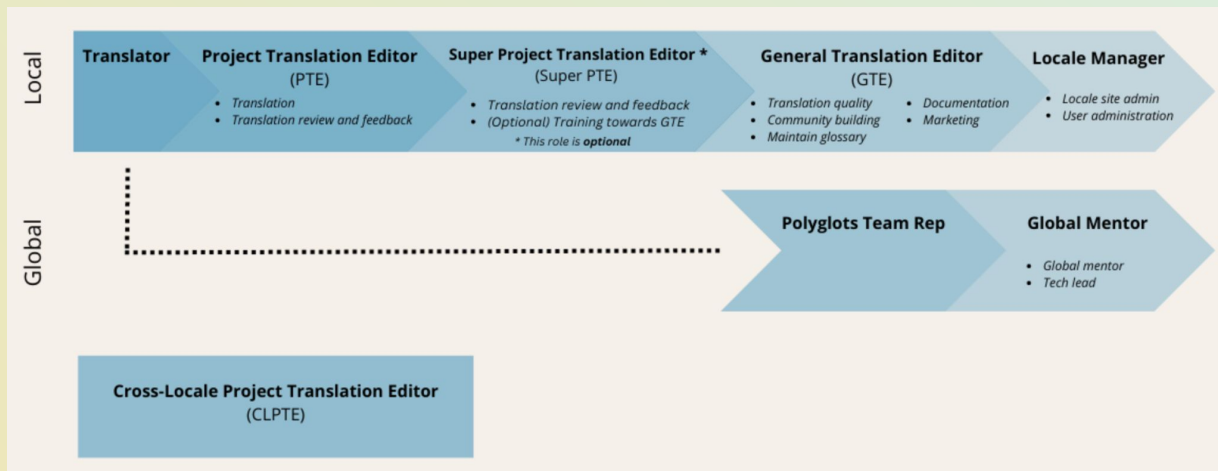
Original string	Translation	—
<a href="#">S3 Access Key</a>	<i>You <a href="#">have to log in</a> to add a translation.</i>	<a href="#">Details</a>
<a href="#">Internet Archive S3 Config</a>	<i>You <a href="#">have to log in</a> to add a translation.</i>	<a href="#">Details</a>
<a href="#">Auto publish post to Internet Archive</a>	自動備份到 Internet Archive	<a href="#">Details</a>
<a href="#">Auto archive</a>	自動備份	<a href="#">Details</a>
<a href="#">Internet Archive S3 API Key</a>	Internet Archive S3 API Key	<a href="#">Details</a>
An <a href="#">&lt;Register&gt;</a> is needed for auto publishing your post to <a href="#">Internet Archive</a> .	需要 <a href="#">&lt;Register&gt;</a> 以設定自動備份到 Internet Archive。	<a href="#">Details</a>
<a href="#">Internet Archive (archive.org)</a>	Internet Archive (archive.org)	<a href="#">Details</a>
<a href="#">&lt;InternetArchive&gt;</a> is a non-profit digital library offering free universal access to books, movies & music, as well as 624 billion archived web pages.	<a href="#">&lt;InternetArchive&gt;</a> 是一個非牟利的數碼典藏庫，免費提供書籍、影片、音樂、及 6,240 億個網頁備份給任何人仕瀏覽。	<a href="#">Details</a>
<a href="#">Connect to Matters</a>	<i>You <a href="#">have to log in</a> to add a translation.</i>	<a href="#">Details</a>
<a href="#">this guide</a>	此教學	<a href="#">Details</a>
Please refer to <a href="#">&lt;Help&gt;</a> for help on using this plugin	<i>You <a href="#">have to log in</a> to add a translation.</i>	<a href="#">Details</a>

Keys are the original string

Anyone can propose translation for any string and locale

# Polyglot team, i.e. You don't own your i18n!


- Making the plugin does not automatically makes you a approved translator
- Try get approved as PTE for your plugin, per locale basis



<https://make.wordpress.org/polyglots/handbook/plugin-theme-authors-guide/pte-request/>

# How You can help

- Help translate [WordPress Core](#)

<p>Chinese (China) 简体中文 zh_CN</p> <p> 1009</p> <p><a href="#">Contribute Translation</a></p>	<p>Chinese (Hong Kong) 香港中文 zh_HK</p> <p> 143</p> <p><a href="#">Contribute Translation</a></p>	<p>Chinese (Singapore) 中文 zh_SG</p> <p> 18</p> <p><a href="#">Contribute Translation</a></p>	<p>Chinese (Taiwan) 繁體中文 zh_TW</p> <p> 368</p> <p><a href="#">Contribute Translation</a></p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- Help translate any plugin you use/[like](#)



Web3Press – Decentralize Publishing with Writing  
NFT  
By LikeCoin

[Download](#)

這個外掛目前提供了 [繁體中文](#) 及 [简体中文版](#)。請協助改進本地化譯文品質。

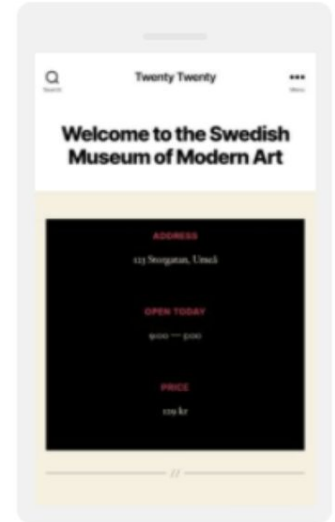


Q: Hey I use AMP, your  
iframe broken

<https://github.com/likecoin/likecoin-wordpress/pull/51>

# Hey I use AMP, ...

- Many sites enable AMP for SEO
- AMP plugin <https://wordpress.org/plugins/amp/>
- When AMP is active, not only style get simplified, e.g. [iframe get sandboxed](#)
- In our case, add attribute we need from <https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe#sandbox>
- In PHP, test for AMP mode using [is\\_amp\\_endpoint\(\)](#) / [amp\\_is\\_request\(\)](#)
- Always test the AMP version!



## **Twenty Twenty**

Our default theme for 2020 is designed to take full advantage of the flexibility of the block...

[Learn more](#)

Hey your stuff doesn't show  
properly in my theme

<https://github.com/likecoin/likecoin-wordpress/pull/88>

# Hey your stuff doesn't show properly in my theme

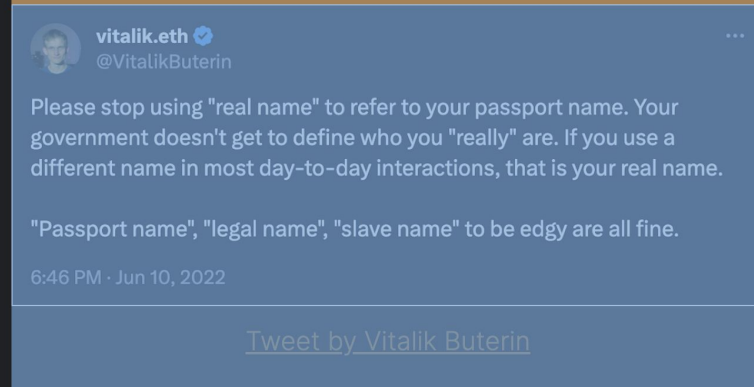
- Normally this one is very hard
- All the themes with different DOM and CSS => can't fit all
- Turns out just wrapping our iframe in `<figure>` does wonder
- This is due to blocks are mostly wrapped with `<p>` or `<figure>`, modern themes are designed to handle them properly

「真名」也是一樣，一般人透過這個詞表達的意思，其實應該稱為「法定名字」，即一個人在其所屬司法管轄區的數據庫中的名字。我們說「金庸」的「真名」是「查良鏞」，但金庸才是他為自己取的名字，最能代表這個人，關連著他的作品，承載著他的

有人會認為他在欺騙，只是在法律

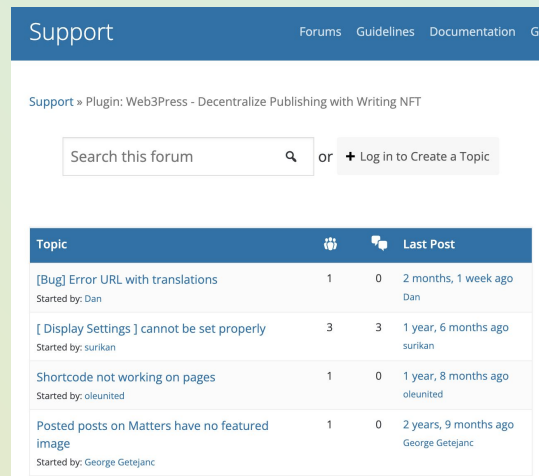
僅此而已。

figure.wp-block-image.aligncenter.size-large.has-custom-border 640 x 326.74er



- Hey I want to use shortcode!
- Hey your plugin throw JS error after upgrade!
- Hey.....

TL;DR today, plz buy DLC



Support Forums Guidelines Documentation Ge

Support » Plugin: Web3Press - Decentralize Publishing with Writing NFT

Search this forum  or [+ Log in to Create a Topic](#)

Topic			Last Post
[Bug] Error URL with translations Started by: Dan	1	0	2 months, 1 week ago Dan
[ Display Settings ] cannot be set properly Started by: surikan	3	3	1 year, 6 months ago surikan
Shortcode not working on pages Started by: oleunited	1	0	1 year, 8 months ago oleunited
Posted posts on Matters have no featured image Started by: George Gitejanc	1	0	2 years, 9 months ago George Gitejanc

Did we just mention blocks?

# The Bosses

# Gutenberg

Modern block editor



# Gutenberg

- [Block based editor](#)
- Full site editing
- Released as default in WordPress 5.0
- Now the old editor is a plugin called [“Classic Editor”](#)

## What does that mean for plugin?

- Editor sidebar support
- Block support

## Say Hello to Gutenberg, the WordPress Editor

Experience the flexibility that blocks allow, whether you're building your first site or write code for a living.

[Try Gutenberg today in WordPress](#)

*This page was built with blocks — pieces of content that you can move around. **Click around to explore them.***

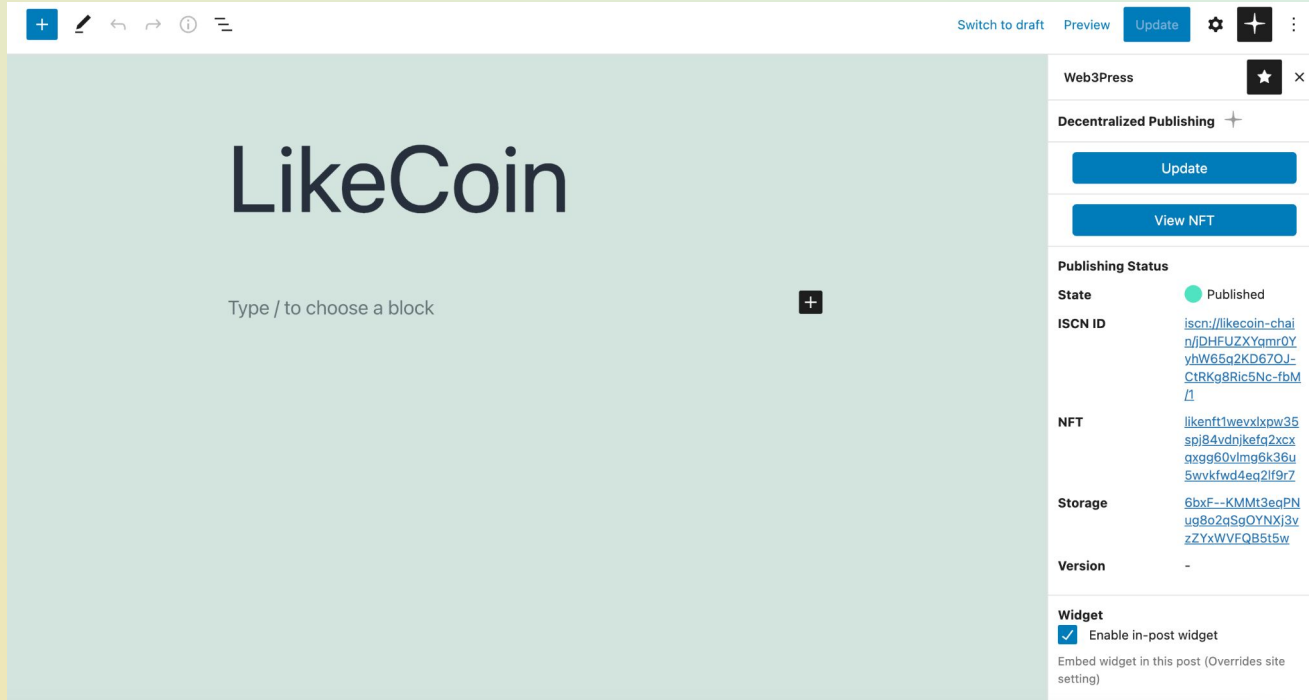
# Editor Sidebar - metabox is now outdated

The image shows a screenshot of the WordPress editor sidebar. The main content area is titled "LikeCoin" and has a permalink of "http://localhost:8080/?p=105". The sidebar contains several metaboxes:

- Publish:** Contains a "Preview Changes" button, status information (Status: Published [Edit](#)), visibility information (Visibility: Public [Edit](#)), and published date (Published on: May 12, 2023 at 16:03 [Edit](#)). It also has "Move to Trash" and "Update" buttons.
- Format:** A list of block formats with radio buttons: Standard (selected), Link, Aside, Gallery, Image, Quote, Status, Video, Audio, and Chat.
- Categories:** Shows "All Categories" and "Most Used" tabs.

At the bottom of the sidebar, there is a "Web3Press" metabox titled "LikeCoin button" with a checked checkbox "Embed LikeCoin button in this post".

# Editor Sidebar - metabox is now outdated



The image shows a screenshot of the WordPress editor interface. The main content area on the left displays the title "LikeCoin" and a prompt "Type / to choose a block" with a plus icon. The right sidebar contains a metabox for "Web3Press". At the top of the sidebar, there are navigation buttons: "Switch to draft", "Preview", "Update", a settings gear, a plus icon, and a close icon. The "Web3Press" metabox includes a star icon and a close icon. Below the title "Decentralized Publishing" is a plus icon, followed by an "Update" button and a "View NFT" button. The "Publishing Status" section shows the state as "Published" with a green dot. It lists three fields: "ISCN ID" with a long alphanumeric string and a link icon, "NFT" with another alphanumeric string and a link icon, and "Storage" with a third alphanumeric string and a link icon. The "Version" field is empty. At the bottom, the "Widget" section has a checked checkbox for "Enable in-post widget" and a note: "Embed widget in this post (Overrides site setting)".

Switch to draft Preview Update ⚙️ + ✕

Web3Press ☆ ✕

Decentralized Publishing +

Update

View NFT

**Publishing Status**

State ● Published

ISCN ID <iscn://likecoin-chain/DHFUZYgmrOYyhW65g2KD67OJ-CTRkG8Ric5Nc-fbM/>

NFT <likent1wevxlpw35spi84vdnjkefg2xcxqxgg60vimg6k36u5wvkwfwd4eg2lf9r7>

Storage <6bxF--KMMt3egPNug8o2gSgOYNXj3vzZYxWVFQB5t5w>

Version -

**Widget**

Enable in-post widget

Embed widget in this post (Overrides site setting)

# Editor Sidebar - metabox is now outdated

Metabox in its simplest form, is just extra fields in HTML `<form>`

- Submit post => Submit fields in metabox => Updates data with post

Sidebar is a complex web app

- On publish, Gutenberg does a XHR instead of refresh
- Your sidebar is expected to listen to events and does XHR too
- Maybe also multitab JavaScript based navigation, like a full blown SPA
- In fact it is a React SPA!

# Blocks - shortcode is now outdated

Remember shortcode [likecoin liker-id=ckxpress]?

How about a UI to list all shortcodes, configure their parameters, and maybe also a preview?

The image displays the WordPress Gutenberg editor interface. On the left, a search bar contains the text 'likecoin'. Below it, three block options are visible: 'Writing NFT Widget', 'Writing NFT Collect Button', and 'Writing NFT Widget (Mini)'. The 'Writing NFT Widget' option is selected. In the center, a preview of the 'Writing NFT Widget' block is shown. The preview features a green and red topographic map image, the text 'Writing NFT - Let&#039;s mint Writ...', a price of '\$0.5', and a 'Collect Now' button. Below the preview, there is a 'Like' button and the user name 'William Chong'. On the right, the 'Block' settings panel is open, showing the 'Writing NFT Widget' block with its description: 'Writing NFT widget with customizable size and style'. The 'Widget Settings' section is expanded, showing the 'COLLECT BUTTON TEXT' field with the value 'Collect Now'. The 'Advanced' section is also visible but collapsed.

# Blocks - shortcode is now outdated

- Add your own blocks for site
- [block.json](#) defines all the metadata
- edit.js and save.js defines different behaviour, in editor vs in actual post view
- Make variants for blocks that has common attributes

## Blocks

This plugin provides 2 blocks.



### Writing NFT Widget

Writing NFT widget with customizable size and style



### Writing NFT Collect Button


Writing NFT minimal collect button

<https://developer.wordpress.org/block-editor/>

## ▼ blocks

### ▼ nft-collect-button

`}` block.json

 index.asset.php


`#` index.css

`JS` index.js

`#` style-index.css

### ▼ nft-widget

`}` block.json

 index.asset.php

`#` index.css

`JS` index.js

`#` style-index.css

# Security!

How many CVE are from plugin instead of core?

# Why a plugin breach affect the whole site?

- WordPress code runs in a global space
- No effective isolation between plugins, or actually, everything
- Horrible in security sense

i.e.

You can write a [plugin to change any user/admin data](#)

You can write a plugin to change data used by other plugin

- Actually thats how plugin for plugins work

e.g. woocommerce, woocommerce plugins, woocommerce plugins pro version, which is a paid plugin for woocommerce plugin



# How can plugin developer prevent this?

- Sanitize all input and output

Why both? Don't trust any data to be safe

sanitize\_\*, escape\_\*

洗手洗手洗手

- Use WordPress provided function instead of PHP or writing your own

wp\_remote\_get()

- Wordpress coding standard linter warns all unsanitized output

<https://developer.wordpress.org/plugins/security/>

- sanitize\_email()
- sanitize\_file\_name()
- sanitize\_hex\_color()
- sanitize\_hex\_color\_no\_hash()
- sanitize\_html\_class()
- sanitize\_key()
- sanitize\_meta()
- sanitize\_mime\_type()
- sanitize\_option()
- sanitize\_sql\_orderby()
- sanitize\_term()
- sanitize\_term\_field()
- sanitize\_text\_field()
- sanitize\_textarea\_field()
- sanitize\_title()
- sanitize\_title\_for\_query()
- sanitize\_title\_with\_dashes()
- sanitize\_user()
- sanitize\_url()
- wp\_kses()
- wp\_kses\_post()

# How can site owner prevent this?

## Disable unneeded plugin

- Disabling plugin disable many of its hook and API, reducing attack surfaces

## Uninstall unneeded plugin

- Plugin can hook on install, uninstall and upgrade

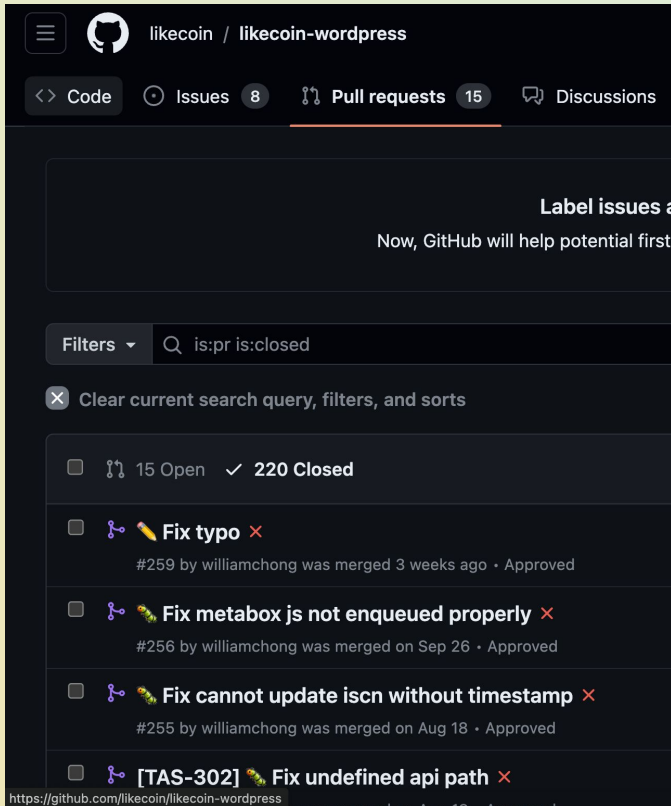
Try to understand what data and option are created by your plugin, and does it clean them up after uninstall?

- WordPress does not record these on install, devs can be lazy or don't even know they should clean up data

@wordpress/data

TL;DR today, plz buy DLC

# There's more...



Like 200 more things about

- Really silly APIs
- Subtle non-documented functions
- Stupid mistakes we made (mostly this)

... that I can talk about, but let's not dig too deep into this here.

# Hey it's Q&A

Now it's your chance to contribute content to this slide!

or checkout [GOTY version](#) of this slide