

HUMBERTO GREGORIO

SCAMCOINS

DEEP DIVE INTO CRYPTO RUG PULLS



No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

Disclaimer

The information contained in this book is for educational and informational purposes only. The content is provided “as is” and without warranties of any kind, either express or implied.

Not Financial Advice: The author is not a financial advisor. Nothing in this book constitutes financial, investment, tax, or professional advice. The cryptocurrency market is inherently high-risk, and you should always conduct your own thorough research (DYOR) and consult with a qualified professional before making any investment decisions. Any action you take upon the information in this book is strictly at your own risk.

Not Legal Advice: The author is not an attorney. The content of this book should not be construed as legal advice. The descriptions of illegal activities are for educational purposes to illustrate potential scams. For legal matters, please consult with a qualified legal professional.

Warning Against Illegal Activities: This book is intended as a tool for defense and prevention, not as a guide for committing illegal acts. The methods described herein, including but not limited to fraud, market manipulation, and theft, are serious crimes with severe legal consequences, including fines and imprisonment. The author and publisher do not endorse or condone any illegal activity.

Limitation of Liability: The author and publisher shall not be held liable for any financial losses, damages, or legal consequences incurred by any reader as a result of applying or misusing the information presented in this book. By reading this book, you agree that you are solely responsible for your own decisions and actions.

Table of contents

Table of contents	2
Warning and important notice from the author	9
A Love Letter to Technology, Written as a Hate Letter to Scams	11
Foreword from Mr. Patrick Schmitt	13
The Scammer’s Blueprint: From Idea to Exit	14
Introduction	18
 Chapter 1: Creating the Token	 19
1.1. What is a Cryptocurrency (Crypto)?	19
1.1.1. Key Aspects of Cryptocurrencies:.....	19
1.1.2. What do Memecoins Have to Do with Cryptocurrencies?.....	20
1.2. The Scammer’s Toolkit: Why Creating a Token is the First Act of Deception	21
1.3. What You Need to Create a Token	22
1.3.1. Smart Contract	22
1.3.2. The Token	22
1.3.3. Liquidity Pool	23
1.4. Creating the Token: The Low/No-Budget Method	25
1.4.1. Solana	25
1.4.2. Binance Smart Chain	26
1.4.3. The Alternatives: Where the Journey Can Also Lead	27
1.5. How Trading Works on Platforms like pump.fun, bonk.fun & Co.	29
1.5.1. Initial Provision of the Liquidity Pool via Bonding Curve	29
1.5.2. The Graduation Process: From Hype to Tradable Reality	30
1.6. PancakeSwap & Co.....	31
1.7. Creating Your Own Token: The High-Roller Method	32
1.7.1. Information Needed for Token Creation	32
1.7.2. Other Important Considerations.....	33
1.8. Activating and Scanning the Smart Contract	34
1.9. Possible Scam During Token Creation.....	35
1.9.1. Creating a Manipulated Facade.....	36
1.9.2. Psychological Lures	37
1.9.3. The Technical Traps in the Smart Contract	38
1.10. Checklist: Signs of a Token Manipulated from the Start .	40

Chapter 2: Setting the Stage	41	
2.1. The 20-Minute Promise: The Website as Bait	41	
2.1.1. Fake Partnerships and Endorsements	43	
2.1.2. Domain Forwarding: The Digital Bait and Switch.....	43	
2.1.3. The Interactive Trap: The „Claim Airdrop“ Button as an Attack Vector	44	
2.1.4. Fake Whitepapers and Sham Audits for Download.....	45	
2.2. The Echo Chamber of Hype: Telegram as a Temple of Manipulation	45	
2.2.1. The Public Telegram Group	46	
2.2.2. The Private Channel.....	46	
2.3. The Megaphone: The Art of Deception on X (Twitter).....	47	
2.3.1. Fake Community (Bot Armies).....	47	
2.3.2. Alpha Callers	48	
2.4. The “Burn” Myth: The Illusion of Artificial Scarcity	49	
2.5. Inflating the Number of Holders	51	
2.5.1. The Airdrop Bluff: Creating a Ghost Community.....	52	
2.5.2. Airdrop into a Honeypot	53	
2.6. Buying Holder Addresses	54	
2.7. The Roadmap to Nowhere ...	54	
2.7.1. Phase 1: Laying the Foundation (The Empty Promise of Legitimacy).....	55	
2.7.2. Phase 2: Expansion and Partnerships (The Credibility Fiction-Booster)	56	
2.7.3. Phase 3: Adoption and Innovation (The House of Cards of Ultimate Value)	56	
2.7.4. The Invention of the Phantom Team: Faces Without People, Names Without Honor.....	57	
2.8. The Seal of False Security: Bought Audits and Empty Promises	58	
Chapter 3: The Liquidity Pool	61	
3.1. What is a Liquidity Pool?	61	
3.2. Setting up a Liquidity Pool on a Blockchain	62	
3.2.1. What is Raydium?.....	62	
3.2.2. What is PancakeSwap?	63	
3.2.3. Alternatives on the Solana Blockchain.....	65	
3.3. The LP Scam of the Biggest Whales	65	
3.4. Neutralizing the Liquidity Lock	65	
3.4.1. Alternatives on Other Blockchains.....	67	
3.4.2. DEX Aggregators	67	

3.5. Why the Initial Liquidity Pool is a Key Metric.....	67	4.8. Checklist: Interpreting Key Metrics Correctly.....	81
3.5.1. Scenario 1: You're too stingy (Start with 0.1 SOL $\approx$ €20)	68	Chapter 5: Manipulating the Trade.....	82
3.5.2. Scenario 2: You play the game (Start with 1 SOL $\approx$ €200)	68	5.1. Inflating the Trading Volume	82
3.5.3. Scenario 3: You're serious about this (Start with 10 SOL $\approx$ €2,000).....	69	5.2. Wash trading.....	83
3.6. Liquidity with borrowed money	69	5.3. Pumping the Price	84
3.7. The Liquidity Pool Scam (Classic Hard Rug Pull)	69	5.4. Increasing the Number of Holders	85
3.8. Checklist: Checking the Liquidity Pool (LP)	72	5.4.1. The Airdrop Bluff 2.0: Digital Dusting	85
Chapter 4: Important metrics.....	73	5.4.2. Bought Holders: The Extras for Your Show.....	85
4.1. Market Cap	74	5.5. Bundle buys / sells	86
4.1.1. Market Cap on Raydium	74	5.6. Multiple Boosts.....	87
4.1.2. Market Cap on pump.fun.....	75	5.7. The Perfectly Staged Deception through Automation and the Combination of All Tools	88
4.2. 24h Volume.....	75	5.7.1. The Preparation: Assembling the Ensemble	89
4.3. Price 76		5.7.2. Act 1: The Staged Rush – The Illusion of Common Interest	89
4.4. Buy and Sell Volume (Candles).....	76	5.7.3. Act 2: The Strategic Pullback – Creating a Plausible Story.....	90
4.5. Price Movement in the Last 5 Minutes, 1 Hour, 6 Hours	77	5.7.4. Act 3: The Artificial Revival – The Illusion of Stability and Activity.....	91
4.6. Holder 78		5.7.5. Act 4: The Final Surge – The Bait is Set	91
4.7. Bubble Maps.....	79	5.7.6. Act 5: The Payout – The Curtain Falls	92
4.7.1. How Bubble Maps Work:.....	79		
4.7.2. What You Can Identify with Bubble Maps	79		

5.8.	Checklist: Recognizing Trading Manipulation.....	94
------	--	----

Chapter 6: Keeping the Scam Alive 96

6.1.	The Telegram Channel.....	97
6.1.1.	Telegram-Bot-Strategien.....	98
6.1.2.	Trading Bots.....	98
6.1.3.	Community Management Bots: The Professional Facade	100
6.1.4.	Engagement and Hype Bots: The Artificial Enthusiasm	101
6.1.5.	Censorship and Control Bots: The Iron Fist	101
6.1.6.	Trading & Analysis Bots: The Hype on the Chart.....	102
6.1.7.	Hiring Moderators.....	103
6.1.8.	How You Get Ripped Off by Other Telegram Channels	103
6.1.9.	Hiring Graphic Designers / Animators.....	105
6.2.	Playing the X / Twitter Game	106
6.2.1.	Buying X Influencers.....	106
6.2.2.	What are AMAs?	108
6.2.3.	Buying YouTubers	109
6.3.	Exposing a Fake Community	111

Chapter 7: The Psychology of the Gamble – Or Why You Might Be a Gambling Addict..... 112

7.1.	The Unfair Casino: Welcome to the Rigged Wild West.....	113
7.2.	The Neurochemical Basics: Your Brain on Memecoins .	114
7.2.1.	The Three-Act Play of Addiction in Your Brain:	114
7.2.2.	The Failing Brake System: The Prefrontal Cortex	115
7.3.	The Psychological Traps: The Weapons of the Meme-coin Casino	115
7.4.	The Systematic Manipulation: Why the House Always Wins	116
7.5.	The Addiction Risk is Real: The Alarming Facts	116
7.6.	An Unfair Game You Cannot Win	117
7.7.	Self-Test – Do I Have a Gambling Addiction?	119

Chapter 8: Your Shield in the Digital Wild West.....120

8.1.	Paranoia as a Virtue: The Investor's Essential Mindset.	120
8.1.1.	The Golden Rule: Trust No One, Verify Everything (Trust, but Verify)	120
8.1.2.	FOMO is Your Enemy: How to Replace Greed with Discipline	121
8.1.3.	Accept the Risk: Only Invest What You Are Prepared to Burn to Ashes.....	121

8.2. The Anatomy of the Audit: Your Due Diligence Checklist Before Every Click.....	121		
8.2.1. Deciphering the Code: The Smart Contract Under the Magnifying Glass.....	121	8.4.2. The Echo Chamber on Telegram: Are Critical Questions Allowed or Are You Immediately Banned?	124
8.2.2. The Hunt for the Honeygot: Tools for Checking Sellability (e.g., Honeygot.is)	122	8.4.3. The Website Analysis: Who is the Domain Owner (Whois Lookup)? Is the Content Copied from Other Projects?	124
8.2.3. Finding the Control Keys: Have “Mint Authority” and “Freeze Authority” Really Been Revoked?	122	8.5. The Seal of False Security: Verifying Audits and Phantom Teams	125
8.2.4. The Token Distribution (Tokenomics): Do 90% of the Tokens Belong to a Single Wallet?.....	122	8.5.1. The Audit Counter-Check: How to Verify on the Audit Firm’s Website if the Report is Real.	125
8.3. Follow the Money: Analysis of the Liquidity Pools (LP)	123	8.5.2. The Reverse Image Search: Are the “Team Photos” Just AI-Generated or from Stock Photo Sites?	125
8.3.1. Is the Liquidity Locked? Where and for How Long? (Check on Platforms like Team.Finance, Unicrypt)	123	8.6. The Investor’s Arsenal: Indispensable Online Tools	125
8.3.2. How Big is the Pool? A Small Liquidity is a Massive Red Flag.	123	8.6.1. Block Explorers (Solscan, Etherscan): Your Window to the Truth of the Blockchain.	125
8.3.3. Who are the Top Holders of the LP Tokens? Do They Belong to the Developers?.....	123	8.6.2. Charting Platforms (DEXTools, Dexscreener): More Than Just Following the Price.	126
8.4. Seeing Through the Facade: Social Media and Website Under Cross-Examination	124	8.6.3. Specialized Scanners (Honeygot-Checker, Token Sniffer): The Fast Hounds.	126
8.4.1. Unmasking the Bot Army: Tools for Analyzing X (Twitter) Followers and Engagement.	124	8.6.4. Community Analysis Tools: Measuring the Sentiment Behind the Hype.	126
		8.7. Securing the Fortress: Practical Wallet Hygiene	126

8.7.1.	The “Burner Wallet” Principle: Never Gamble with Your Main Wallet.....	126	9.3.	The Toothless Sheriff? The Hurdles of Law Enforcement	134
8.7.2.	The Power of Approvals: How to Check and Revoke Token Permissions (Revoke Cash).....	127	9.4.	What You Can Do (and What It Really Means)	135
8.7.3.	Phishing and “Wallet Drainer”: Never Click on Suspicious “Air-drop” Links.....	127	9.5.	The Most Painful Lesson... ..	135
			9.6.	Checklist: What to Do After a Scam.....	137
8.8.	Red Flags After the Purchase: When You Need to Pull the Plug.....	127	Chapter 10: The Anatomy of a “Green Flag”		
8.8.1.	The Team Goes Silent, the Telegram Chat is Restricted.....	128	10.1.	The Fundamental Question: Does the Team Have Something to Lose?	138
8.8.2.	The Roadmap Goals are Postponed Without Comment.....	128	10.2.	Green Flag #1: The Anti-Phantom Team – Real and Verifiable Identities	139
8.8.3.	Large Amounts of Tokens are Transferred from Developer Wallets to Exchanges.	128	10.3.	Green Flag #2: The Anti-Nowhere Utility – An Existing or Emerging Product.....	140
8.8.4.	Sudden Hype Without a Discernible Reason (the Prelude to the “Dump”).....	128	10.4.	Green Flag #3: The Anti-Dump Tokenomics – Long-Term Incentives	141
8.9.	Your 10-Point Survival Guide	129	10.5.	Green Flag #4: The Anti-Censorship Community – Open and Critical Dialogue	142
8.10.	The Final Pre-Investment Check.....	130	10.6.	The Big Picture Counts: A Single Green Flag is Not Enough	143
Chapter 9: The Scream into the Void – The Reality After the Fraud.....			132	10.7.	Checklist: The Anatomy of a „Green Flag“
9.1.	The Irreversible Truth of the Blockchain	133			144
9.2.	The Hunt for a Phantom	133			

Chapter 11: Online-Tools.....	146	Afterword: The Weapon in Your Hand	156
11.1. Selection of the Most Im- portant Tools	146	A Direct “Letter to a Would-Be Scammer”	158
11.1.1. TokenSniffer: Your First Line of Defense	146	A word about myself.....	161
11.1.2. DEXTools & GeckoTermi- nal: The Wall Street Termi- nals of Degens	148	Glossary	163
11.1.3. RugDoc: Your Communi- ty-Sourced Scam Radar	149		
11.1.4. BSCScan & Etherscan: Where All Secrets Are Recorded.....	150		
11.1.5. Debank & Revoke.cash: Wallet Safety Checkers.....	150		
11.1.6. Honeypot.is: The Trap Detector.....	151		
11.1.7. Wallet Tracking Tools (Nansen, Breadcrumbs, Arkham): Stalk Like a Sleuth	152		
11.2. Other Tools & Projects.....	153		

Warning and important notice from the author

Read this before you turn another page.

This book is a weapon for defense, not a manual for attack. It was written with a single, unequivocal intention: to protect potential investors from the systematic and ruthless scams in the memecoin market. It is a map of enemy territory, drawn so that you don't walk into the traps.

The detailed description of fraudulent methods from a perpetrator's perspective is a didactic tool. We are dissecting the anatomy of the crime so that you can recognize the disease before it infects you. Just as a medical student studies the workings of a virus to combat it, we study the methods of the scammer to neutralize them. Every technique described here serves exclusively for education and prevention.

Let me be perfectly clear:

- ➔ **This is not an encouragement for illegal activities.** The actions described in this book—including market manipulation, fraud, and theft—are serious crimes. Attempting to replicate these techniques will inevitably lead to severe legal consequences, including substantial fines and prison sentences. This book is a warning sign, not an invitation.
- ➔ **This is not financial or investment advice.** The cryptocurrency market, especially the memecoin sector, is extremely volatile and highly speculative. A total loss of invested capital is not just possible, but probable. The information presented here is for educational purposes and not a basis for investment decisions. Never make financial decisions without conducting your own thorough research (DYOR – Do Your Own Research) and, ideally, consulting a certified financial advisor.
- ➔ **No assumption of liability.** The author assumes no liability whatsoever for financial losses incurred by readers through investments in

cryptocurrencies. Likewise, any liability for the misuse of the information presented here to carry out illegal activities is expressly excluded. Anyone who uses this knowledge to harm others does so at their own sole responsibility and must face the full consequences of the law.

➔ **This knowledge is a shield.** Use it to protect yourself and others. Use it to make more informed decisions. Use it to contribute to education and to help drain the swamp where these scams thrive.

Anyone who reads this book and finds inspiration for their own criminal acts has not only misunderstood its fundamental message—they have twisted it into its opposite and are precisely the kind of person this book aims to warn the world about.

Let me state unequivocally at this point: I am not a lawyer. What you are reading is not legal guidance but a sober description of the playing field you are on. If you lose your money in one of the scams described here, there is generally no higher authority that will get it back for you.

The perpetrators are anonymous, the transactions are irreversible, and international law enforcement is often a toothless tiger when it comes to such offenses. The “Wild West” is not just a metaphor for the greed and hype, but also for the widespread absence of the sheriff. This is precisely why every single point in this book is so vital for survival. Do not count on someone to help you when it’s too late. Your only shield is your knowledge and your discipline. For legal action, always consult a specialized lawyer.

A Love Letter to Technology, Written as a Hate Letter to Scams

Welcome to the world's largest, unregulated casino: the memecoin market. A place where digital millionaires are born overnight and, a second later, thousands of portfolios are wiped out. A digital Colosseum where greed, hype, and anonymity are the gladiators, and your money is the bet.

But before we dive into this swamp of deception and manipulation, one distinction is of existential importance to me: This book is not an attack on blockchain technology. Quite the opposite.

I revere the blockchain. I consider it one of the most transformative inventions since the internet. The ability to create and transfer value in a decentralized, transparent, and intermediary-free way has the potential to revolutionize entire industries. The elegance of a well-written smart contract, the mathematical beauty of cryptography, and the vision behind serious projects aiming to solve real-world problems—I admire all of it deeply.

This admiration is not purely theoretical. As part of the team behind projects like Levolution, which creates a sustainable infrastructure for tokenization, and Gemcy.com, where we use scientific analysis to map real-world assets like jewelry and watches immutably on the blockchain, I witness the immense potential of this technology every day. I see how hard teams work to build transparent and fair systems.

And it is precisely from this reverence that I despise memecoins.

Memecoins are to the blockchain what spam emails are to the internet: the dirty, loud, and fraudulent abuse of a brilliant idea. They are the parasites that feed on the reputation of a revolutionary technology. They have nothing to do with innovation. They are empty shells, digital vehicles created for the sole purpose of transferring money from the uninformed to the unscrupulous through coordinated manipulation.

Therefore, this book will not discuss the incredible potential of Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs), or securing supply chains.

Instead, we will dissect the weapons forged from this technology to scam you. I will show you the anatomy of a scam, from the creation of a worthless token to the manipulation of social media channels, right up to the final act of theft. This is not a technical treatise. It is a survival guide for the digital Wild West and, simultaneously, an indictment of those who have turned the promise of a better future into a dirty game.

Consider it my attempt to isolate the poison so that the actual technology has a chance to grow healthily.

Yes, I know that reality is often painted in shades of gray. I know the stories of projects that started as a joke and developed an unpredictable momentum of their own. I know about the fine line between aggressive marketing and intentional deception, about failed experiments, and projects that collapse due to sheer incompetence.

This book deliberately draws a hard, black line.

Why? Because a beginner cannot navigate these gray areas. For the newcomer risking their savings, every gray area is a trap where they lose their money. Whether a project fails due to pure malice or naive incompetence—for the victim, the result is the same: a total loss.

That is why this book treats every project following the pattern described here as what it inevitably is for a novice: a potential scam. Don't see it as an oversimplification, but as a sharpening of focus on the deadliest danger in the field. This is not a guide for the experienced gambler, but a shield for the recruit stepping onto the battlefield for the first time.

The Scammer's Blueprint: From Idea to Exit

If you think scam tokens are tossed together by amateurs in hoodies, let me stop you right there. These aren't chaotic acts. These are precision-engineered, emotionally manipulative weapons. Every pump-and-dump that made you rage-sell your bags on a Sunday night followed a blueprint. A real roadmap. But not the kind you see plastered on a website next to some astronaut dog riding a rocket.

This chapter is your backstage pass to the rug pull opera. We're going to walk step-by-step through the scammer's timeline—how they launch, bait, hype, and disappear with your money faster than your cousin disappears when the dinner bill arrives.

Step 1: The "Idea" Phase — Make It Buzz, Not Make It Work

The scam begins not with code, but with a vibe. The token doesn't need a use case; it needs a narrative. It's a trendy combination of whatever is hot that week. AI? Slam it in. Real-world assets? Toss it in. A new dog breed? Inject that DNA. They'll mix buzzwords into a salad that sounds like: "Revolutionizing decentralized AI automation across multi-chain ecosystems via Layer 2 tokenomics."

It doesn't have to make sense. It just has to feel like you're missing out if you don't get in early. The name matters. It has to sizzle. If it doesn't sound like something a billionaire would ironically tweet, it gets tossed out.

Step 2: The Contract – Copy, Paste, Obfuscate

Why build from scratch when someone already rugged better than you ever could? The scammer grabs an open-source token contract from GitHub or uses a token generator on a cheap blockchain like Binance Smart Chain or Solana. They barely write code anymore; they use pre-made templates and click a few buttons.

But here's where the malice is baked in. Behind the "advanced features" toggle lies the dark arts:

- ➔ Hidden Mint Functions: Renamed to something harmless like `supplySync()` or `manualAdjust()`.
- ➔ Adjustable Taxes: A "marketing tax" that can be changed from 5% to 99% with a single transaction.
- ➔ Blacklist Triggers: The ability to prevent specific wallets (yours) from selling.
- ➔ Fake Renounced Ownership: The contract says ownership is renounced, but a proxy contract or hidden function still gives the developer full control.

They deploy this weaponized code in minutes, for less than the price of a pizza.

Step 3: The Hype Machine – Full Send, Full Fake

A token without hype is just a digital ghost town. So, scammers build a fake city. This is where they lean into their inner social media warlord:

- ➔ Spin up a Telegram group and fill it with 10,000 bots.
- ➔ Buy thousands of fake Twitter followers to create an illusion of popularity.

- ➔ Pay mid-tier influencers—the ones with an anime profile picture and a price list in their bio—to post bullish nonsense.
- ➔ Post fake partnership announcements with logos stolen from Google Images.
- ➔ Tease “upcoming CEX listings” that will never happen.

They talk about “roadmap 2.0” and mysterious VCs “in talks” without ever dropping a name. You, meanwhile, are aping in. Because it feels like everyone else is.

Step 4: The Controlled Pump and Exit

The stage is set. The actors are paid. Now the show begins. They add just enough liquidity to make the chart move and start the controlled pump with their own bots to simulate “demand.” The chart goes vertical. Your cousin, who just discovered crypto two weeks ago, messages you, “Bro, you gotta check this out.”

And just when it feels like the rocket is about to reach the moon, the developers press the red button. The exit comes in several flavors:

- ➔ Liquidity Removal (Hard Rug): They pull all the valuable currency (SOL, ETH, BNB) from the trading pool and vanish. The token’s value instantly drops to zero.
- ➔ Contract Lockdown (Honeypot): A hidden function is activated, and suddenly, you can no longer sell your tokens.
- ➔ Soft Rug: They just stop posting. Stop responding. The project is ghosted, and the chart slowly bleeds to death.

Funds are moved to mixers. Wallets go dark. The Telegram group gets deleted mid-sentence, like a Thanos snap. And just like that, it's over.

This isn't magic. It's a formula. And it works over and over again. Now that you know the blueprint, we'll dive deeper into each part in the following chapters. You now know: the game is rigged. Unless you learn how to see the cards.

Introduction

The altcoin market booms in cycles. Every year in late summer and early autumn, the so-called “altcoin season” begins, promising immense profits.

If you’re thinking about investing in a so-called memecoin, or—even crazier—creating one yourself, this book is for you. You might be surprised to learn that you are being scammed at literally every turn. You cannot protect yourself from it. No matter what metrics you think you can use to make a balanced decision—they have probably already been manipulated.

To expose all these machinations and show you where you’re being lied to and cheated, I will guide you from the creator’s point of view.

Before we enter the scammer’s workshop, we must draw a line as sharp as a razor blade. This book is not about memecoins that start as a joke or a social experiment and become a phenomenon through the unpredictable momentum of a community—think of the forefathers like Dogecoin. Such projects may often lack fundamental value and end in financial disaster, but their creation was not necessarily driven by an initial intent to steal. They are the result of viral madness, an uncontrollable digital bonfire.

This book, however, is an autopsy of a premeditated crime. We dissect those tokens that were designed as weapons from the very beginning. Their creators follow a cold, calculated script with only one goal: to transfer your money from your wallet to theirs. The “community hype” here is not an organic development but a paid performance. The “roadmap” is not a vision but a lie to buy time. And the “launch” is not the start of a project but the beginning of the countdown to the final theft.

So, we are not distinguishing between “good” and “bad” memecoins. This book is your guide to recognizing the latter before the trap snaps shut.

Chapter 1:

Creating the Token

1.1. What is a Cryptocurrency (Crypto)?

Cryptocurrency is a form of digital or virtual money that is secured by cryptography. This makes counterfeiting or double-spending nearly impossible. Unlike traditional currencies, which are issued and controlled by central banks, cryptocurrencies are based on decentralized networks, typically blockchain technology. The blockchain is a distributed, public ledger that stores all transactions in a chain of blocks that are cryptographically linked together. Every transaction is transparent and immutable.

There are various blockchain ecosystems with specific token standards: Ethereum (ERC-20), Solana (SPL), and Binance Smart Chain – BSC (BEP-20).

1.1.1. Key Aspects of Cryptocurrencies:

- **Decentralization:** No central authority (like a government or bank) controls the cryptocurrency.
- **Cryptography:** Uses advanced encryption to secure transactions and control the creation of new units.
- **Blockchain:** The underlying technology that serves as a tamper-proof and transparent transaction ledger.
- **Volatility:** Cryptocurrencies are known for their extreme price fluctuations.

1.1.2. What do Memecoins Have to Do with Cryptocurrencies?

Memecoins are a special type of cryptocurrency that originated from internet memes, jokes, or social media hypes. They belong to the broader category of cryptocurrencies but differ in their origin story and often in their intended utility.

Memecoins use the same technology—on both Solana and Binance. The majority of scam coins, rug pulls, and hypes are realized on these chains.

Connection and Differences:

- ➔ **Basis:** Technically, memecoins are based on the same blockchain technology as other cryptocurrencies (e.g., Ethereum, Solana). They are digital tokens managed by smart contracts.
- ➔ **Lack of Intrinsic Value/Utility:** Unlike many “serious” crypto projects that aim to solve real-world problems, develop decentralized applications (DeFi, NFTs), or create new infrastructure, memecoins often have no fundamental utility or a compelling technical foundation. Their value is derived almost exclusively from hype, community engagement, and speculation.
 - **Community-Driven:** Their success heavily depends on viral spread and the support of an online community, which is often humorous or ironic.
 - **Extreme Volatility:** Memecoins are notorious for their extreme volatility. They can achieve immense gains in a very short time but can fall to nearly zero just as quickly.
 - **Risk of Fraud:** As described in this book, many memecoins are designed as scams from the outset (rug pulls, honeypots), as their easy creation and hype factor make them ideal targets for unscrupulous actors.

In summary, memecoins are a subcategory of cryptocurrencies that, while using the underlying technology, are primarily distinguished from

project-specific cryptocurrencies by their speculative and hype-driven nature. They are the “fun” element (or often the “danger” element) in the world of digital currencies.

1.2. The Scammer’s Toolkit: Why Creating a Token is the First Act of Deception

Before I show you how easy it is to create your own token, we need to clarify one thing: the act of creation is not the moment something new is made. It is the moment the weapon is loaded. Every click and every setting I am about to describe is, for a scammer, merely the precise preparation for theft. I am showing you the script that is being written behind the scenes long before the first investor spends a single cent.

What you are about to learn is how I can create a perfect illusion of legitimacy with minimal effort. With a cool logo, a website I can click together in twenty minutes, and a few social media profiles, I build a facade that gives inexperienced investors the impression of a promising project. Each of the following steps serves only to make this backdrop as convincing as possible.

The actual goal I am pursuing almost always culminates in one of two scenarios, which I will break down for you in the smallest detail later: the classic memecoin or the lightning-fast rug pull. (A ‘rug pull’ is a scam where the developers of a project drain all the liquidity from the trading pool, causing the token’s value to instantly drop to zero, leaving investors with worthless holdings. The name comes from the idiom ‘to pull the rug out from under someone’s feet.’) In both cases, it’s all about creating hype, collecting your money, and then disappearing.

This whole spectacle is supported by an invisible army of bots, which I will also unmask. They artificially drive up prices and fake a community on social media that never actually existed.

The foundation for all of this? Complete anonymity. It is the breeding ground on which these scams thrive. It allows me to vanish without a trace and repeat the game the next day under a new name.

So, understand this: when I now show you how a token is created, I am not giving you a guide to riches. I am giving you a front-row seat to the theater of fraud. You are learning the scammer's tools not to use them, but to recognize them. Every technical parameter you learn is a potential vulnerability for you as an investor and a weapon in the hands of the person who wants to scam you.

1.3. What You Need to Create a Token

Before we dive into the creation, let's briefly cover the basics so you understand what you're actually building.

1.3.1. Smart Contract

The foundation of every token is the so-called smart contract. Think of it as a computer program or a digital contract stored on the blockchain. This code is the brain and the rulebook of your coin: it defines how many tokens exist, who owns them, and what can be done with them. Once a smart contract is on the blockchain, it cannot be changed and automatically executes actions when predefined conditions are met. This is especially true for contracts created with online tools. However, skilled developers can program a smart contract to be modified or stopped later.

1.3.2. The Token

The token itself is the product of this smart contract; it is essentially a digital unit of value that runs on an existing blockchain (e.g., Solana). For this token to be traded at all, it needs liquidity.

1.3.3. Liquidity Pool

This is where the liquidity pool comes in. It's essentially a large pot of digital assets locked in another smart contract. Instead of directly matching buyers and sellers, users trade against this pool. When someone wants to buy your new token, they put another currency (e.g., SOL) into the pool and receive your tokens from the pool in return. This exchange is managed by an algorithm, a so-called Automated Market Maker (AMM), which automatically adjusts the price based on the ratio of the two tokens in the pool. More on this in the following chapters.

What was once reserved for skilled development teams is now a matter of minutes. Depending on your budget, you can create a coin in two ways: a low-budget or no-budget version (teaser: it's a waste of time) and a high-cost version with more potential for upside and downside, and much more effort.

If you're more "serious" (lol), you essentially need only three things, in addition to a Twitter account and a Telegram channel:

- ➔ **A Crypto Wallet:** You need a compatible wallet (e.g., MetaMask or Phantom) connected to the blockchain supported by platforms like pump.fun (usually Solana). This wallet must contain a small amount of the blockchain's native cryptocurrency (e.g., SOL for Solana) to cover transaction fees (gas fees) for creation and later interactions.
- ➔ **An Idea for Your Coin:** This could be a funny name, a reference to a current trend, an animal theme, or something entirely original. Meme-coins thrive on their community and the "meme factor," so a catchy and memorable idea is important.
- ➔ **An Image/Logo:** An appealing or humorous image that represents your coin is crucial to attract attention and differentiate it from others.
- ➔ **Optional**
 - **An X Account:** Essential for promotion and community

management.,

- **A Telegram Group:** To provide a direct communication platform for your community.
- **A Website:** A simple but informative website to provide basic information about your coin and build trust. Don't make it too complicated; a website with your logo and links to your token is sufficient. Register a domain and, for example, use Canva to create a simple page with links to the profiles.

Attention: You can never change the name, ticker, texts, logo, and links again!

1.4. Creating the Token: The Low/No-Budget Method

Forget the image of the brilliant programmer spending nights writing revolutionary code. Today, creating a crypto token—your weapon—is as easy as ordering a pizza. There are entire ecosystems designed to make this process as simple and cheap as possible for you. They are the digital counterfeit presses that allow anyone to produce worthless shells and sell them as the next big thing.

Two battlegrounds dominate this scene: Solana and the Binance Smart Chain (BSC).

1.4.1. Solana

The Solana ecosystem has become the preferred breeding ground for fast-paced hypes, driven by a platform that has perfected the process: **Pump.fun**.

➔ The Process:

The path to your own token here is absurdly simple. You don't need programming skills or significant starting capital. You connect your Solana wallet (e.g., Phantom), fill out a simple form with a name, ticker, and an image, and pay a tiny fee in SOL. Seconds later, your coin is born.

➔ The Trap: The Bonding Curve.

The actual mechanism is the so-called “bonding curve.” Instead of you having to immediately create a real liquidity pool on a decentralized exchange (DEX) like Raydium, trading initially takes place within the closed ecosystem of Pump.fun. The price is determined by an algorithm: every purchase drives it up, every sale lowers it. For you as a scammer, this is a dream. You don't have to risk your own money to provide liquidity. The hype finances itself and creates an illusion of massive growth even before the token is traded on an open market.

GET THE FULL VERSION

www.scamcoins.xyz