



Roll Your Own 24 Word Bitcoin Seed Phrase Offline

with D++

Presentation by Keysa
simplestbitcoinedu.com

WHY ROLL YOUR OWN SEED?



- ♦ **Strong Entropy:** It safeguards against weak entropy that could potentially be exploited in the future.
- ♦ **Trust Minimized:** It ensures robust entropy, eliminating the need to trust the RNG (Random Number Generator).
- ♦ **Enhanced Security:** Generating your seed offline reduces reliance on hardware or software wallets that could be compromised.
- ♦ **Control:** You maintain complete ownership of your private keys, eliminating any risk of a third-party having knowledge of your key.
- ♦ **Privacy:** No digital footprint is created.
- ♦ **Educational Value:** It deepens your understanding of Bitcoin's cryptography.

MATERIALS NEEDED

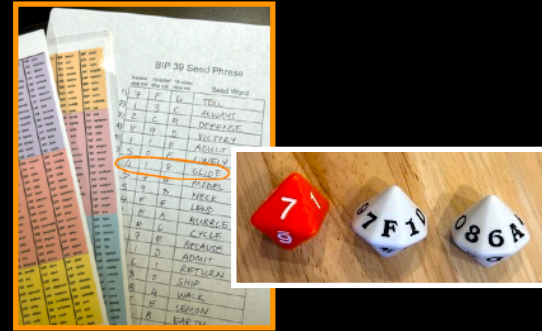
Visit: entropy.page/dice

- ◆ Dice: x1 Octal (8-sided) die
x2 Hex (16-sided) dice



- ◆ BIP39 Worksheet (included)
- ◆ BIP39 Word List (included)
- ◆ Signing Device: Cold Card, Seed Signer, Jade or Passport
(Needed to calculate the checksum/24th word offline)
- ◆ Pen
- ◆ Cup to roll the dice in
- ◆ Hard, flat surface, in a room free of all electronics

IMPORTANT NOTES:



- ◆ Read through this whole guide before you start.
- ◆ I highly recommend doing a complete practice run, carefully following all the instructions.
- ◆ When you are ready to do it 'for real', be sure to follow all the instructions on the following page to ensure maximum security.

PREPARATION



- ◆ Make sure you're in a room without any **electronics (aside from the signing device) and draw the shades** so no one can see in.
- ◆ Switch on the lights if needed.
- ◆ Since you are doing the proof-of-work to roll your own seed, **you want to maximize security and privacy** while doing so.
- ◆ Let anyone else in the house know that **you need to be undisturbed** for an hour, ideally locking the door to prevent anyone accidentally coming in with a phone on.
- ◆ Ensure you have a **hard surface for rolling the dice**—an empty box with a flat bottom can be helpful.
- ◆ Check that you **have all the materials ready and with you** in the room.



- ♦ Use a cup to shake the three dice.
- ♦ Throw them down on the table or in the box.



- ♦ Carefully place them in a row, **with the octal one on the left side.**
- ♦ The order of the next two doesn't matter.
- ♦ Don't worry if they roll to a different number as you place them.





BIP 39 Seed Phrase

	8-sided dice roll	16-sided dice roll	16-sided dice roll	Seed Word
1)	7	F	6	
2)				
3)				
4)				
5)				
6)				
7)				
8)				
9)				
10)				
11)				
12)				
13)				
14)				
15)				
16)				
17)				
18)				
19)				
20)				
21)				
22)				
23)				
24)	8 sided dice roll:			Checksum

- ♦ Write the numbers and letters shown on the dice in the boxes on Line 1 of the BIP 39 Seed Phrase Worksheet.
- ♦ Make sure your writing is **legible!**

BIP 39 Seed Phrase

	8-sided dice roll	16-sided dice roll	16-sided dice roll	Seed Word
1)	7	F	6	
2)				
3)				
4)				
5)				
6)				
7)				
8)				
9)				

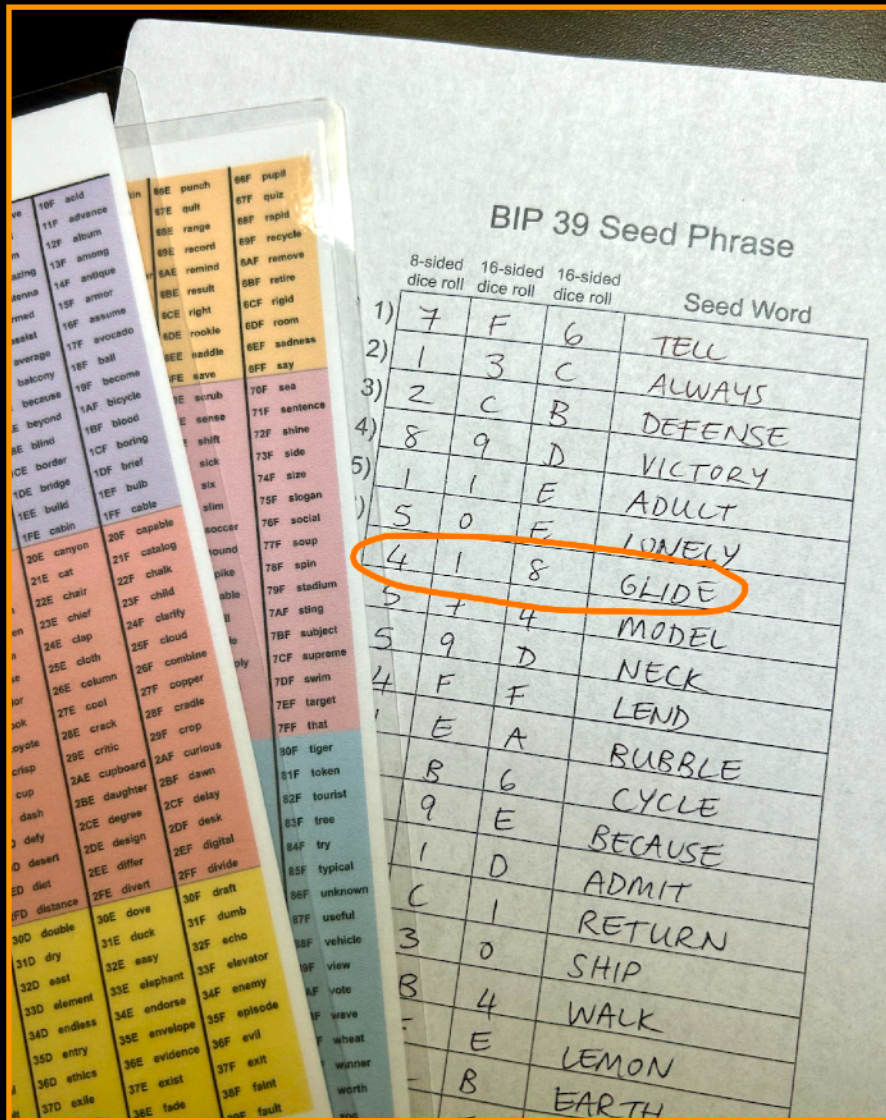
20)	4	4	F	
21)	2	7	5	
22)	0	B	3	
23)	8	1	A	
				Checksum
24)	8 sided dice roll:	4		



- ♦ Continue the process until you get to the 24th word (the checksum).
- ♦ Roll only the octal die one time, and enter the number in the box on the left.

- ◆ Take a look at the **BIP 39 Dictionary**.
- ◆ Note how **each section is a different color**, depending on the first number.
- ◆ This will make it easier to find your words.





7 friend	3E8 fringe	3E9 frog
7 galaxy	3F8 gallery	3F9 game
genius	408 genre	409 gentle
glass	418 glide	419 glimpse
gossip	428 govern	429 gown
group	438 grow	439 grunt
happy	448 harbor	449 hard

- Using the word list, write the 23 words corresponding to each dice roll on the BIP 39 Seed Phrase Worksheet.
- Leave the 24th word blank for now.

23)	8	1	7	Checksum
24)	8 sided dice roll	4		

BIP 39 SEED PHRASE WORKSHEET

BIP 39 Seed Phrase

	8-sided dice roll	16-sided dice roll	16-sided dice roll	Seed Word
1)				
2)				
3)				
4)				
5)				
6)				
7)				
8)				
9)				
10)				
11)				
12)				
13)				
14)				
15)				
16)				
17)				
18)				
19)				
20)				
21)				
22)				
23)				

Checksum

24) 8 sided dice roll:

--	--

BIP 39 Dictionary

100	abandon	101	ability	102	able	103	about	104	above	105	absent	106	absorb	107	abstract	108	absurd	109	abuse	10A	access	10B	accident	10C	account	10D	accuse	10E	achieve	10F	acid
110	acoustic	111	acquire	112	across	113	act	114	action	115	actor	116	actress	117	actual	118	adapt	119	add	11A	addict	11B	address	11C	adjust	11D	admit	11E	adult	11F	advance
120	advice	121	aerobic	122	affair	123	afford	124	afraid	125	again	126	age	127	agent	128	agree	129	ahead	12A	aim	12B	air	12C	airport	12D	aisle	12E	alarm	12F	album
130	alcohol	131	alert	132	alien	133	all	134	alley	135	allow	136	almost	137	alone	138	alpha	139	already	13A	also	13B	alter	13C	always	13D	amateur	13E	amazing	13F	among
140	amount	141	amused	142	analyst	143	anchor	144	ancient	145	anger	146	angle	147	angry	148	animal	149	ankle	14A	announce	14B	annual	14C	another	14D	answer	14E	antenna	14F	antique
150	anxiety	151	any	152	apart	153	apology	154	appear	155	apple	156	approve	157	april	158	arch	159	arctic	15A	area	15B	arena	15C	argue	15D	arm	15E	armed	15F	armor
160	army	161	around	162	arrange	163	arrest	164	arrive	165	arrow	166	art	167	artefact	168	artist	169	artwork	16A	ask	16B	aspect	16C	assault	16D	asset	16E	assist	16F	assume
170	asthma	171	athlete	172	atom	173	attack	174	attend	175	attitude	176	attract	177	auction	178	audit	179	august	17A	aunt	17B	author	17C	auto	17D	autumn	17E	average	17F	avocado
180	avoid	181	awake	182	aware	183	away	184	awesome	185	awful	186	awkward	187	axis	188	baby	189	bachelor	18A	bacon	18B	badge	18C	bag	18D	balance	18E	balcony	18F	ball
190	bamboo	191	banana	192	banner	193	bar	194	barely	195	bargain	196	barrel	197	base	198	basic	199	basket	19A	battle	19B	beach	19C	bean	19D	beauty	19E	because	19F	become
1A0	beef	1A1	before	1A2	begin	1A3	behave	1A4	behind	1A5	believe	1A6	below	1A7	belt	1A8	bench	1A9	benefit	1AA	best	1AB	betray	1AC	better	1AD	between	1AE	beyond	1AF	bicycle
1B0	bid	1B1	bike	1B2	bind	1B3	biology	1B4	bird	1B5	birth	1B6	bitter	1B7	black	1B8	blade	1B9	blame	1BA	blanket	1BB	blast	1BC	bleak	1BD	bless	1BE	blind	1BF	blood
1C0	blossom	1C1	blouse	1C2	blue	1C3	blur	1C4	blush	1C5	board	1C6	boat	1C7	body	1C8	boil	1C9	bomb	1CA	bone	1CB	bonus	1CC	book	1CD	boost	1CE	border	1CF	boring
1D0	borrow	1D1	boss	1D2	bottom	1D3	bounce	1D4	box	1D5	boy	1D6	bracket	1D7	brain	1D8	brand	1D9	brass	1DA	brave	1DB	bread	1DC	breeze	1DD	brick	1DE	bridge	1DF	brief
1E0	bright	1E1	bring	1E2	brisk	1E3	broccoli	1E4	broken	1E5	bronze	1E6	broom	1E7	brother	1E8	brown	1E9	brush	1EA	bubble	1EB	buddy	1EC	budget	1ED	buffalo	1EE	build	1EF	bulb
1F0	bulk	1F1	bullet	1F2	bundle	1F3	bunker	1F4	burden	1F5	burger	1F6	burst	1F7	bus	1F8	business	1F9	busy	1FA	butter	1FB	buyer	1FC	buzz	1FD	cabbage	1FE	cabin	1FF	cable
200	cactus	201	cage	202	cake	203	call	204	calm	205	camera	206	camp	207	can	208	canal	209	cancel	20A	candy	20B	cannon	20C	canoe	20D	canvas	20E	canyon	20F	capable
210	capital	211	captain	212	car	213	carbon	214	card	215	cargo	216	carpet	217	carry	218	cart	219	case	21A	cash	21B	casino	21C	castle	21D	casual	21E	cat	21F	catalog
220	catch	221	category	222	cattle	223	caught	224	cause	225	caution	226	cave	227	ceiling	228	celery	229	cement	22A	census	22B	century	22C	cereal	22D	certain	22E	chair	22F	chalk
230	champion	231	change	232	chaos	233	chapter	234	charge	235	chase	236	chat	237	cheap	238	check	239	cheese	23A	chef	23B	cherry	23C	chest	23D	chicken	23E	chief	23F	child
240	chimney	241	choice	242	choose	243	chronic	244	chuckle	245	chunk	246	churn	247	cigar	248	cinnamon	249	circle	24A	citizen	24B	city	24C	civil	24D	claim	24E	clap	24F	clarify
250	claw	251	clay	252	clean	253	clerk	254	clever	255	click	256	client	257	cliff	258	climb	259	clinic	25A	clip	25B	clock	25C	clog	25D	close	25E	cloth	25F	cloud
260	clown	261	club	262	clump	263	cluster	264	clutch	265	coach	266	coast	267	coconut	268	code	269	coffee	26A	coil	26B	coin	26C	collect	26D	color	26E	column	26F	combine
270	come	271	comfort	272	comic	273	common	274	company	275	concert	276	conduct	277	confirm	278	congress	279	connect	27A	consider	27B	control	27C	convince	27D	cook	27E	cool	27F	copper
280	copy	281	coral	282	core	283	corn	284	correct	285	cost	286	cotton	287	couch	288	country	289	couple	28A	course	28B	cousin	28C	cover	28D	coyote	28E	crack	28F	cradle
290	craft	291	cram	292	crane	293	crash	294	crater	295	crawl	296	crazy	297	cream	298	credit	299	creek	29A	crew	29B	cricket	29C	crime	29D	crisp	29E	critic	29F	crop
2A0	cross	2A1	crouch	2A2	crowd	2A3	crucial	2A4	cruel	2A5	cruise	2A6	crumble	2A7	crunch	2A8	crush	2A9	cry	2AA	crystal	2AB	cube	2AC	culture	2AD	cup	2AE	cupboard	2AF	curious
2B0	current	2B1	curtain	2B2	curve	2B3	cushion	2B4	custom	2B5	cute	2B6	cycle	2B7	dad	2B8	damage	2B9	damp	2BA	dance	2BB	danger	2BC	daring	2BD	dash	2BE	daughter	2BF	dawn
2C0	day	2C1	deal	2C2	debate	2C3	debris	2C4	decade	2C5	december	2C6	decide	2C7	decline	2C8	decorate	2C9	decrease	2CA	deer	2CB	defense	2CC	define	2CD	defy	2CE	degree	2CF	delay
2D0	deliver	2D1	demand	2D2	demise	2D3	denial	2D4	dentist	2D5	deny	2D6	depart	2D7	depend	2D8	deposit	2D9	depth	2DA	deputy	2DB	derive	2DC	describe	2DD	desert	2DE	design	2DF	desk
2E0	despair	2E1	destroy	2E2	detail	2E3	detect	2E4	develop	2E5	device	2E6	devote	2E7	diagram	2E8	dial	2E9	diamond	2EA	diary	2EB	dice	2EC	diesel	2ED	diet	2EE	differ	2EF	digital
2F0	dignity	2F1	dilemma	2F2	dinner	2F3	dinosaur	2F4	direct	2F5	dirt	2F6	disagree	2F7	discover	2F8	disease	2F9	dish	2FA	dismiss	2FB	disorder	2FC	display	2FD	distance	2FE	divert	2FF	divide
300	divorce	301	dizzy	302	doctor	303	document	304	dog	305	doll	306	dolphin	307	domain	308	donate	309	donkey	30A	donor	30B	door	30C	dose	30D	double	30E	dove	30F	draft
310	dragon	311	drama	312	drastic	313	draw	314	dream	315	dress	316	drift	317	drill	318	drink	319	drip	31A	drive	31B	drop	31C	drum	31D	dry	31E	duck	31F	dumb
320	dune	321	during	322	dust	323	dutch	324	duty	325	dwarf	326	dynamic	327	eager	328	eagle	329	early	32A	earn	32B	earth	32C	easily	32D	east	32E	easy	32F	echo
330	ecology	331	economy	332	edge	333	edit	334	educate	335	effort	336	egg	337	eight	338	either	339	elbow	33A	elder	33B	electric	33C	elegant	33D	element	33E	elephant	33F	elevator
340	elite	341	else	342	embark	343	embody	344	embrace	345	emerge	346	emotion	347	employ	348	empower	349	empty	34A	enable	34B	enact	34C	end	34D	endless	34E	endorse	34F	enemy
350	energy	351	enforce	352	engage	353	engine	354	enhance	355	enjoy	356	enlist	357	enough	358	enrich	359	enroll	35A	ensure	35B	enter	35C	entire	35D	entry	35E	envelope	35F	episode
360	equal	361	equip	362	era	363	erase	364	erode	365	erosion	366	error	367	erupt	368	escape	369	essay	36A	essence	36B	estate	36C	eternal	36D	ethics	36E	evidence	36F	evil
370	evoke	371	evolve	372	exact	373	example	374	excess	375	exchange	376	excite	377	exclude	378	excuse	379	execute	37A	exercise	37B	exhaust	37C	exhibit	37D	exile	37E	exist	37F	exit
380	exotic	381	expand	382	expect	383	expire	384	explain	385	expose	386	express	387	extend	388	extra	389	eye	38A	eyebrow	38B	fabric	38C	face	38D	faculty	38E	fade	38F	faint

BIP 39 DICTIONARY cont.

390	faith	391	fall	392	FALSE	393	fame	394	family	395	famous	396	fan	397	fancy	398	fantasy	399	farm	39A	fashion	39B	fat	39C	fatal	39D	father	39E	fatigue	39F	fault
3A0	favorite	3A1	feature	3A2	february	3A3	federal	3A4	fee	3A5	feed	3A6	feel	3A7	female	3A8	fence	3A9	festival	3AA	fetch	3AB	fever	3AC	few	3AD	fiber	3AE	fiction	3AF	field
3B0	figure	3B1	file	3B2	film	3B3	filter	3B4	final	3B5	find	3B6	fine	3B7	finger	3B8	finish	3B9	fire	3BA	firm	3BB	first	3BC	fiscal	3BD	fish	3BE	fit	3BF	fitness
3C0	fix	3C1	flag	3C2	flame	3C3	flash	3C4	flat	3C5	flavor	3C6	flee	3C7	flight	3C8	flip	3C9	float	3CA	flock	3CB	floor	3CC	flower	3CD	fluid	3CE	flush	3CF	fly
3D0	foam	3D1	focus	3D2	fog	3D3	foil	3D4	fold	3D5	follow	3D6	food	3D7	foot	3D8	force	3D9	forest	3DA	forget	3DB	fork	3DC	fortune	3DD	forum	3DE	forward	3DF	fossil
3E0	foster	3E1	found	3E2	fox	3E3	fragile	3E4	frame	3E5	frequent	3E6	fresh	3E7	friend	3E8	fringe	3E9	frog	3EA	front	3EB	frost	3EC	frown	3ED	frozen	3EE	fruit	3EF	fuel
3F0	fun	3F1	funny	3F2	furnace	3F3	fury	3F4	future	3F5	gadget	3F6	gain	3F7	galaxy	3F8	gallery	3F9	game	3FA	gap	3FB	garage	3FC	garbage	3FD	garden	3FE	garlic	3FF	garment
400	gas	401	gasp	402	gate	403	gather	404	gauge	405	gaze	406	general	407	genius	408	genre	409	gentle	40A	genuine	40B	gesture	40C	ghost	40D	giant	40E	gift	40F	giggle
410	ginger	411	giraffe	412	girl	413	give	414	glad	415	glance	416	glare	417	glass	418	glide	419	glimpse	41A	globe	41B	gloom	41C	glory	41D	glove	41E	glow	41F	glue
420	goat	421	goddess	422	gold	423	good	424	goose	425	gorilla	426	gospel	427	gossip	428	govern	429	gown	42A	grab	42B	grace	42C	grain	42D	grant	42E	grape	42F	grass
430	gravity	431	great	432	green	433	grid	434	grief	435	grit	436	grocery	437	group	438	grow	439	grunt	43A	guard	43B	guess	43C	guide	43D	guilt	43E	guitar	43F	gun
440	gym	441	habit	442	hair	443	half	444	hammer	445	hamster	446	hand	447	happy	448	harbor	449	hard	44A	harsh	44B	harvest	44C	hat	44D	have	44E	hawk	44F	hazard
450	head	451	health	452	heart	453	heavy	454	hedghehog	455	height	456	hello	457	helmet	458	help	459	hen	45A	hero	45B	hidden	45C	high	45D	hill	45E	hint	45F	hip
460	hire	461	history	462	hobby	463	hockey	464	hold	465	hole	466	holiday	467	hollow	468	home	469	honey	46A	hood	46B	hope	46C	horn	46D	horror	46E	horse	46F	hospital
470	host	471	hotel	472	hour	473	hover	474	hub	475	huge	476	human	477	humble	478	humor	479	hundred	47A	hungry	47B	hunt	47C	hurdle	47D	hurry	47E	hurt	47F	husband
480	hybrid	481	ice	482	icon	483	idea	484	identify	485	idle	486	ignore	487	ill	488	illegal	489	illness	48A	image	48B	imitate	48C	immense	48D	immune	48E	impact	48F	impose
490	improve	491	impulse	492	inch	493	include	494	income	495	increase	496	index	497	indicate	498	indoor	499	industry	49A	infant	49B	inflict	49C	inform	49D	inhale	49E	inherit	49F	initial
4A0	inject	4A1	injury	4A2	inmate	4A3	inner	4A4	innocent	4A5	input	4A6	inquiry	4A7	insane	4A8	insect	4A9	inside	4AA	inspire	4AB	install	4AC	intact	4AD	interest	4AE	into	4AF	invest
4B0	invite	4B1	involve	4B2	iron	4B3	island	4B4	isolate	4B5	issue	4B6	item	4B7	ivory	4B8	jacket	4B9	jaguar	4BA	jar	4BB	jazz	4BC	jealous	4BD	jeans	4BE	jelly	4BF	jewel
4C0	job	4C1	join	4C2	joke	4C3	journey	4C4	joy	4C5	judge	4C6	juice	4C7	jump	4C8	jungle	4C9	junior	4CA	junk	4CB	just	4CC	kangaroo	4CD	keen	4CE	keep	4CF	ketchup
4D0	key	4D1	kick	4D2	kid	4D3	kidney	4D4	kind	4D5	kingdom	4D6	kiss	4D7	kit	4D8	kitchen	4D9	kite	4DA	kitten	4DB	kiwi	4DC	knee	4DD	knife	4DE	knock	4DF	know
4E0	lab	4E1	label	4E2	labor	4E3	ladder	4E4	lady	4E5	lake	4E6	lamp	4E7	language	4E8	laptop	4E9	large	4EA	later	4EB	latin	4EC	laugh	4ED	laundry	4EE	lava	4EF	law
4F0	lawn	4F1	lawsuit	4F2	layer	4F3	lazy	4F4	leader	4F5	leaf	4F6	learn	4F7	leave	4F8	lecture	4F9	left	4FA	leg	4FB	legal	4FC	legend	4FD	leisure	4FE	lemon	4FF	lend
500	length	501	lens	502	leopard	503	lesson	504	letter	505	level	506	liar	507	liberty	508	library	509	license	50A	life	50B	lift	50C	light	50D	like	50E	limb	50F	limit
510	link	511	lion	512	liquid	513	list	514	little	515	live	516	lizard	517	load	518	loan	519	lobster	51A	local	51B	lock	51C	logic	51D	lonely	51E	long	51F	loop
520	lottery	521	loud	522	lounge	523	love	524	loyal	525	lucky	526	luggage	527	lumber	528	lunar	529	lunch	52A	luxury	52B	lyrics	52C	machine	52D	mad	52E	magic	52F	magnet
530	maid	531	mail	532	main	533	major	534	make	535	mammal	536	man	537	manage	538	mandate	539	mango	53A	mansion	53B	manual	53C	maple	53D	marble	53E	march	53F	margin
540	marine	541	market	542	marriage	543	mask	544	mass	545	master	546	match	547	material	548	math	549	matrix	54A	matter	54B	maximum	54C	maze	54D	meadow	54E	mean	54F	measure
550	meat	551	mechanic	552	medal	553	media	554	melody	555	melt	556	member	557	memory	558	mention	559	menu	55A	mercy	55B	merge	55C	merit	55D	merry	55E	mesh	55F	message
560	metal	561	method	562	middle	563	midnight	564	milk	565	million	566	mimic	567	mind	568	minimum	569	minor	56A	minute	56B	miracle	56C	mirror	56D	misery	56E	miss	56F	mistake
570	mix	571	mixed	572	mixture	573	mobile	574	model	575	modify	576	mom	577	moment	578	monitor	579	monkey	57A	monster	57B	month	57C	moon	57D	moral	57E	more	57F	morning
580	mosquito	581	mother	582	motion	583	motor	584	mountain	585	mouse	586	move	587	movie	588	much	589	muffin	58A	mule	58B	multiply	58C	muscle	58D	museum	58E	mushroom	58F	music
590	must	591	mutual	592	myself	593	mystery	594	myth	595	naive	596	name	597	napkin	598	narrow	599	nasty	59A	nation	59B	nature	59C	near	59D	neck	59E	need	59F	negative
5A0	neglect	5A1	neither	5A2	nephew	5A3	nerve	5A4	nest	5A5	net	5A6	network	5A7	neutral	5A8	never	5A9	news	5AA	next	5AB	nice	5AC	night	5AD	noble	5AE	noise	5AF	nominee
5B0	noodle	5B1	normal	5B2	north	5B3	nose	5B4	notable	5B5	note	5B6	nothing	5B7	notice	5B8	novel	5B9	now	5BA	nuclear	5BB	number	5BC	nurse	5BD	nut	5BE	oak	5BF	obey
5C0	object	5C1	oblige	5C2	obscure	5C3	observe	5C4	obtain	5C5	obvious	5C6	occur	5C7	ocean	5C8	october	5C9	odor	5CA	off	5CB	offer	5CC	office	5CD	often	5CE	oil	5CF	okay
5D0	old	5D1	olive	5D2	olympic	5D3	omit	5D4	once	5D5	one	5D6	onion	5D7	online	5D8	only	5D9	open	5DA	opera	5DB	opinion	5DC	oppose	5DD	option	5DE	orange	5DF	orbit
5E0	orchard	5E1	order	5E2	ordinary	5E3	organ	5E4	orient	5E5	original	5E6	orphan	5E7	ostrich	5E8	other	5E9	outdoor	5EA	outer	5EB	output	5EC	outside	5ED	oval	5EE	oven	5EF	over
5F0	own	5F1	owner	5F2	oxygen	5F3	oyster	5F4	ozone	5F5	pact	5F6	paddle	5F7	page	5F8	pair	5F9	palace	5FA	palm	5FB	panda	5FC	panel	5FD	panic	5FE	panther	5FF	paper
600	parade	601	parent	602	park	603	parrot	604	party	605	pass	606	patch	607	path	608	patient	609	patrol	60A	pattern	60B	pause	60C	pave	60D	payment	60E	peace	60F	peanut
610	pear	611	peasant	612	pelican	613	pen	614	penalty	615	pencil	616	people	617	pepper	618	perfect	619	permit	61A	person	61B	pet	61C	phone	61D	photo	61E	phrase	61F	physical
620	piano	621	picnic	622	picture	623	piece	624	pig	625	pigeon	626	pill	627	pilot	628	pink	629	pioneer	62A	pipe	62B	pistol	62C	pitch	62D	pizza	62E	place	62F	planet
630	plastic	631	plate	632	play	633	please	634	pledge	635	pluck	636	plug	637	plunge	638	poem	639	poet	63A	point	63B	polar	63C	pole	63D	police	63E	pond	63F	pony
640	pool	641	popular	642	portion	643	position	644	possible	645	post	646	potato	647	pottery	648	poverty	649	powder	64A	power	64B	practice	64C	praise	64D	predict	64E	prefer	64F	prepare

BIP 39 DICTIONARY cont.

650	present	651	pretty	652	prevent	653	price	654	pride	655	primary	656	print	657	priority	658	prison	659	private	65A	prize	65B	problem	65C	process	65D	produce	65E	profit	65F	program
660	project	661	promote	662	proof	663	property	664	prosper	665	protect	666	proud	667	provide	668	public	669	pudding	66A	pull	66B	pulp	66C	pulse	66D	pumpkin	66E	punch	66F	pupil
670	puppy	671	purchase	672	purity	673	purpose	674	purse	675	push	676	put	677	puzzle	678	pyramid	679	quality	67A	quantum	67B	quarter	67C	question	67D	quick	67E	quit	67F	quiz
680	quote	681	rabbit	682	raccoon	683	race	684	rack	685	radar	686	radio	687	rail	688	rain	689	raise	68A	rally	68B	ramp	68C	ranch	68D	random	68E	range	68F	rapid
690	rare	691	rate	692	rather	693	raven	694	raw	695	razor	696	ready	697	real	698	reason	699	rebel	69A	rebuild	69B	recall	69C	receive	69D	recipe	69E	record	69F	recycle
6A0	reduce	6A1	reflect	6A2	reform	6A3	refuse	6A4	region	6A5	regret	6A6	regular	6A7	reject	6A8	relax	6A9	release	6AA	relief	6AB	rely	6AC	remain	6AD	remember	6AE	remind	6AF	remove
6B0	render	6B1	renew	6B2	rent	6B3	reopen	6B4	repair	6B5	repeat	6B6	replace	6B7	report	6B8	require	6B9	rescue	6BA	resemble	6BB	resist	6BC	resource	6BD	response	6BE	result	6BF	retire
6C0	retreat	6C1	return	6C2	reunion	6C3	reveal	6C4	review	6C5	reward	6C6	rhythm	6C7	rib	6C8	ribbon	6C9	rice	6CA	rich	6CB	ride	6CC	ridge	6CD	rifle	6CE	right	6CF	rigid
6D0	ring	6D1	riot	6D2	ripple	6D3	risk	6D4	ritual	6D5	rival	6D6	river	6D7	road	6D8	roast	6D9	robot	6DA	robust	6DB	rocket	6DC	romance	6DD	roof	6DE	rookie	6DF	room
6E0	rose	6E1	rotate	6E2	rough	6E3	round	6E4	route	6E5	royal	6E6	rubber	6E7	rude	6E8	rug	6E9	rule	6EA	run	6EB	runway	6EC	rural	6ED	sad	6EE	saddle	6EF	sadness
6F0	safe	6F1	sail	6F2	salad	6F3	salmon	6F4	salon	6F5	salt	6F6	salute	6F7	same	6F8	sample	6F9	sand	6FA	satisfy	6FB	satoshi	6FC	sauce	6FD	sausage	6FE	save	6FF	say
700	scale	701	scan	702	scare	703	scatter	704	scene	705	scheme	706	school	707	science	708	scissors	709	scorpion	70A	scout	70B	scrap	70C	screen	70D	script	70E	scrub	70F	sea
710	search	711	season	712	seat	713	second	714	secret	715	section	716	security	717	seed	718	seek	719	segment	71A	select	71B	sell	71C	seminar	71D	senior	71E	sense	71F	sentence
720	series	721	service	722	session	723	settle	724	setup	725	seven	726	shadow	727	shaft	728	shallow	729	share	72A	shed	72B	shell	72C	sheriff	72D	shield	72E	shift	72F	shine
730	ship	731	shiver	732	shock	733	shoe	734	shoot	735	shop	736	short	737	shoulder	738	shove	739	shrimp	73A	shrug	73B	shuffle	73C	shy	73D	sibling	73E	sick	73F	side
740	siege	741	sight	742	sign	743	silent	744	silk	745	silly	746	silver	747	similar	748	simple	749	since	74A	sing	74B	siren	74C	sister	74D	situate	74E	six	74F	size
750	skate	751	sketch	752	ski	753	skill	754	skin	755	skirt	756	skull	757	slab	758	slam	759	sleep	75A	slender	75B	slice	75C	slide	75D	slight	75E	slim	75F	slogan
760	slot	761	slow	762	slush	763	small	764	smart	765	smile	766	smoke	767	smooth	768	snack	769	snake	76A	snap	76B	sniff	76C	snow	76D	soap	76E	soccer	76F	social
770	sock	771	soda	772	soft	773	solar	774	soldier	775	solid	776	solution	777	solve	778	someone	779	song	77A	soon	77B	sorry	77C	sort	77D	soul	77E	sound	77F	soup
780	source	781	south	782	space	783	spare	784	spatial	785	spawn	786	speak	787	special	788	speed	789	spell	78A	spend	78B	sphere	78C	spice	78D	spider	78E	spike	78F	spin
790	spirit	791	split	792	spoil	793	sponsor	794	spoon	795	sport	796	spot	797	spray	798	spread	799	spring	79A	spy	79B	square	79C	squeeze	79D	squirrel	79E	stable	79F	stadium
7A0	staff	7A1	stage	7A2	stairs	7A3	stamp	7A4	stand	7A5	start	7A6	state	7A7	stay	7A8	steak	7A9	steel	7AA	stem	7AB	step	7AC	stereo	7AD	stick	7AE	still	7AF	sting
7B0	stock	7B1	stomach	7B2	stone	7B3	stool	7B4	story	7B5	stove	7B6	strategy	7B7	street	7B8	strike	7B9	strong	7BA	struggle	7BB	student	7BC	stuff	7BD	stumble	7BE	style	7BF	subject
7C0	submit	7C1	subway	7C2	success	7C3	such	7C4	sudden	7C5	suffer	7C6	sugar	7C7	suggest	7C8	suit	7C9	summer	7CA	sun	7CB	sunny	7CC	sunset	7CD	super	7CE	supply	7CF	supreme
7D0	sure	7D1	surface	7D2	surge	7D3	surprise	7D4	surround	7D5	survey	7D6	suspect	7D7	sustain	7D8	swallow	7D9	swamp	7DA	swap	7DB	swarm	7DC	swear	7DD	sweet	7DE	swift	7DF	swim
7E0	swing	7E1	switch	7E2	sword	7E3	symbol	7E4	symptom	7E5	syrup	7E6	system	7E7	table	7E8	tackle	7E9	tag	7EA	tail	7EB	talent	7EC	talk	7ED	tank	7EE	tape	7EF	target
7F0	task	7F1	taste	7F2	tattoo	7F3	taxi	7F4	teach	7F5	team	7F6	tell	7F7	ten	7F8	tenant	7F9	tennis	7FA	tent	7FB	term	7FC	test	7FD	text	7FE	thank	7FF	that
800	theme	801	then	802	theory	803	there	804	they	805	thing	806	this	807	thought	808	three	809	thrive	80A	throw	80B	thumb	80C	thunder	80D	ticket	80E	tide	80F	tiger
810	tilt	811	timber	812	time	813	tiny	814	tip	815	tired	816	tissue	817	title	818	toast	819	tobacco	81A	today	81B	toddler	81C	toe	81D	together	81E	toilet	81F	token
820	tomato	821	tomorrow	822	tone	823	tongue	824	tonight	825	tool	826	tooth	827	top	828	topic	829	topple	82A	torch	82B	tornado	82C	tortoise	82D	toss	82E	total	82F	tourist
830	toward	831	tower	832	town	833	toy	834	track	835	trade	836	traffic	837	tragic	838	train	839	transfer	83A	trap	83B	trash	83C	travel	83D	tray	83E	treat	83F	tree
840	trend	841	trial	842	tribe	843	trick	844	trigger	845	trim	846	trip	847	trophy	848	trouble	849	truck	84A	TRUE	84B	truly	84C	trumpet	84D	trust	84E	truth	84F	try
850	tube	851	tuition	852	tumble	853	tuna	854	tunnel	855	turkey	856	turn	857	turtle	858	twelve	859	twenty	85A	twice	85B	twin	85C	twist	85D	two	85E	type	85F	typical
860	ugly	861	umbrella	862	unable	863	unaware	864	uncle	865	uncover	866	under	867	undo	868	unfair	869	unfold	86A	unhappy	86B	uniform	86C	unique	86D	unit	86E	universe	86F	unknown
870	unlock	871	until	872	unusual	873	unveil	874	update	875	upgrade	876	uphold	877	upon	878	upper	879	upset	87A	urban	87B	urge	87C	usage	87D	use	87E	used	87F	useful
880	useless	881	usual	882	utility	883	vacant	884	vacuum	885	vague	886	valid	887	valley	888	valve	889	van	88A	vanish	88B	vapor	88C	various	88D	vast	88E	vault	88F	vehicle
890	velvet	891	vendor	892	venture	893	venue	894	verb	895	verify	896	version	897	very	898	vessel	899	veteran	89A	viable	89B	vibrant	89C	vicious	89D	victory	89E	video	89F	view
8A0	village	8A1	vintage	8A2	violin	8A3	virtual	8A4	virus	8A5	visa	8A6	visit	8A7	visual	8A8	vital	8A9	vidid	8AA	vocal	8AB	voice	8AC	void	8AD	volcano	8AE	volume	8AF	vote
8B0	voyage	8B1	wage	8B2	wagon	8B3	wait	8B4	walk	8B5	wall	8B6	walnut	8B7	want	8B8	warfare	8B9	warm	8BA	warrior	8BB	wash	8BC	wasp	8BD	waste	8BE	water	8BF	wave
8C0	way	8C1	wealth	8C2	weapon	8C3	wear	8C4	weasel	8C5	weather	8C6	web	8C7	wedding	8C8	weekend	8C9	weird	8CA	welcome	8CB	west	8CC	wet	8CD	whale	8CE	what	8CF	wheat
8D0	wheel	8D1	when	8D2	where	8D3	whip	8D4	whisper	8D5	wide	8D6	width	8D7	wife	8D8	wild	8D9	will	8DA	win	8DB	window	8DC	wine	8DD	wing	8DE	wink	8DF	winner
8E0	winter	8E1	wire	8E2	wisdom	8E3	wise	8E4	wish	8E5	witness	8E6	wolf	8E7	woman	8E8	wonder	8E9	wood	8EA	wool	8EB	word	8EC	work	8ED	world	8EE	worry	8EF	worth
8F0	wrap	8F1	wreck	8F2	wrestle	8F3	wrist	8F4	write	8F5	wrong	8F6	yard	8F7	year	8F8	yellow	8F9	you	8FA	young	8FB	youth	8FC	zebra	8FD	zero	8FE	zone	8FF	zoo

CALCULATE THE 24th WORD CHECKSUM

Instructions follow for **calculating the final word** of your Seed Phrase using each of the following signing devices:

Cold Card



Seed Signer



Foundation Passport



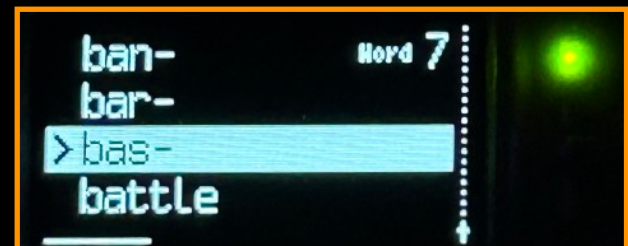
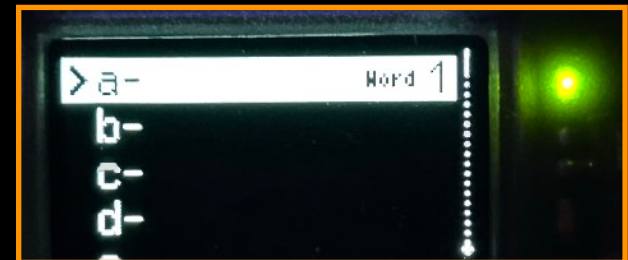
Blockstream Jade



Note: There will be some differences in the process on each device.

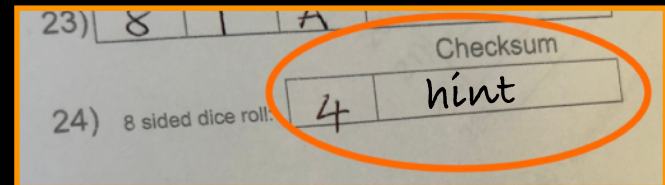
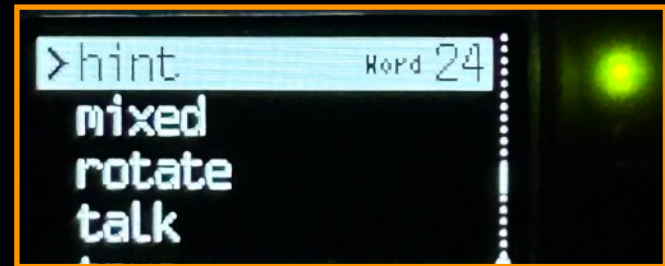
>>>>>>>>>>>>>>> COLD CARD <<<<<<<<<<<<<<<

- ◆ Set up your Cold Card with a secure pin code.
- ◆ Select > **Import Existing**
- ◆ Select > **24 Words**
- ◆ Enter the 23 words from the worksheet.



>>>>>>>>>>> COLD CARD <<<<<<<<<<<<

- ◆ After entering 23 words, 8 options will be shown for the 24th word.
- ◆ Write down the one corresponding to the number you rolled for line 24
- ◆ For this example, 'hint' was the fourth word.
- ◆ Add this last word to your Worksheet on Line 24.



>>>>>>>>>>>>> COLD CARD <<<<<<<<<<<<<<

- ◆ Once you have selected the 24th word, you will want to **view your seed words** to confirm you entered them correctly.
- ◆ Select:
 - > **Advanced/Tools**
 - > **Danger Zone**
 - > **Seed Functions**
 - > **View Seed Words**
 - > **Accept** and check your words are correct.



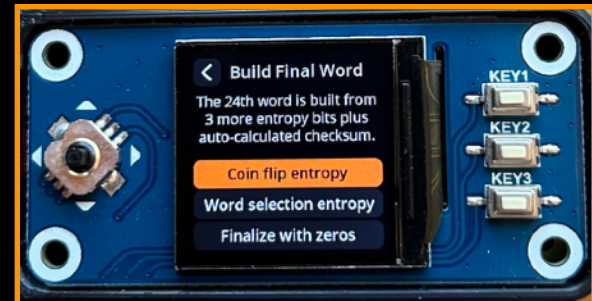
>>>>>>>>>>>>>>>>SEED SIGNER<<<<<<<<<<<<<<<<<

- ◆ Power on your Seed Signer.
- ◆ Select > Tools
- ◆ Select > Calc 12th/24th word
- ◆ Select > 24 words



>>>>>>>>>>>>>SEED SIGNER<<<<<<<<<<<<<

- ◆ Enter your 23 words
- ◆ Once these are entered, the Build Final Word screen will appear.
- ◆ Select a method to calculate the checksum.
- ◆ For this tutorial, we'll use 'Coin flip entropy'.
- ◆ Flip a coin 3 times and enter the results.



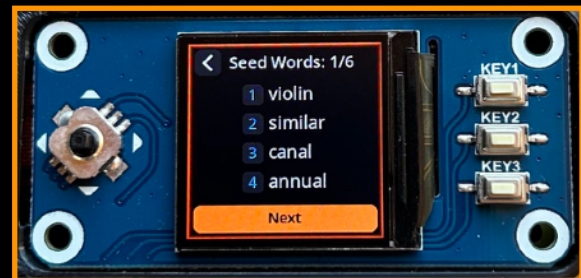
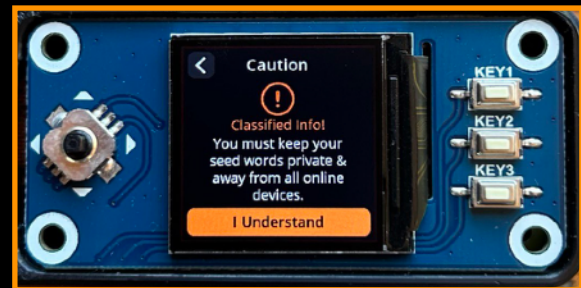
>>>>>>>>>>>>>>>>SEED SIGNER<<<<<<<<<<<<<<<<

- ◆ When the final word is calculated, write it on Line 24 of your Worksheet
- ◆ Click Next > Load Seed.
- ◆ Note down the Fingerprint and click Done.
- ◆ Since Seed Signer is stateless, it will forget your seed when powered off.
- ◆ When you re-enter your seed in the future, you can confirm it is correct by checking the fingerprint matches.



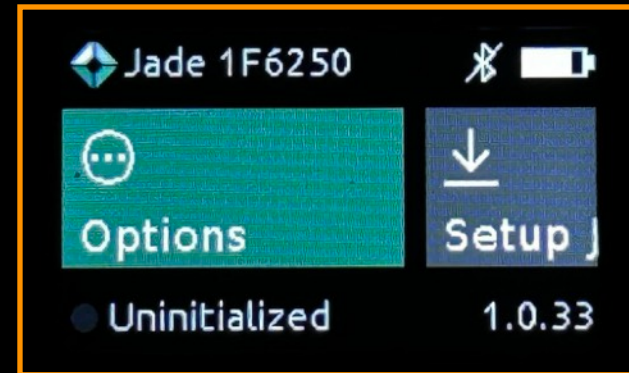
>>>>>>>>>>SEED SIGNER<<<<<<<<<<<

- ◆ Time to confirm you entered your seed word correctly.
- ◆ Select > Backup Seed
- ◆ Select > View Seed Words
- ◆ Select > I Understand
- ◆ Go through and check the words against your Worksheet.



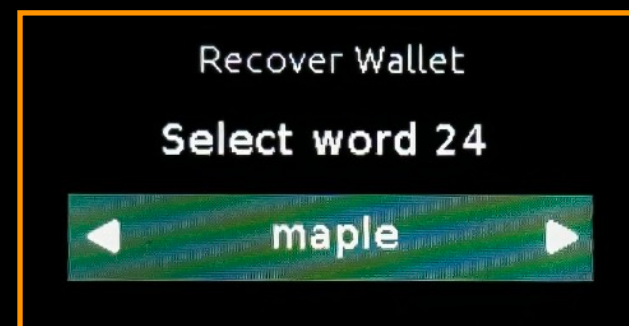
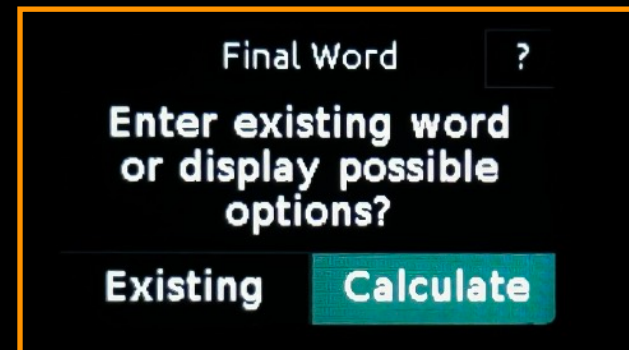
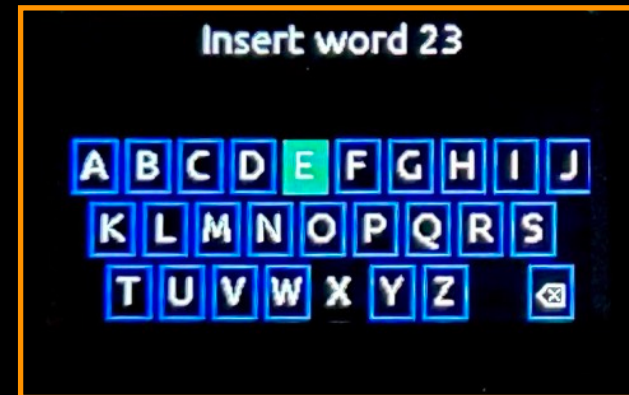
>>>>>>>>BLOCKSTREAM JADE<<<<<<<<<

- ◆ Power on your Jade.
- ◆ Select > Options
- ◆ Select > Temporary
Signer
- ◆ Select > 24 words



>>>>>>>>BLOCKSTREAM JADE<<<<<<<<<

- ◆ Enter the 23 words from your Worksheet.
- ◆ Select > **Calculate** for the Final 24th Word
- ◆ **Scroll L/R** to select the word that matches the number you entered on Line 24.
- ◆ **Note:** Any of the 8 words offered will work as the checksum (24th word).



>>>>>>>>BLOCKSTREAM JADE<<<<<<<<<

- ♦ Select > **No** for Export
- ♦ Select > **QR** for Connection to return to the **Home Screen**.
- ♦ Note down the **Master Fingerprint** shown in the bottom right corner.
- ♦ Power off the device.
- ♦ Power it on and **repeat the whole process**.
- ♦ Check the master fingerprint matches the one you wrote down, to verify your seed phrase.

Export recovery phrase
as a CompactSeedQR?

No

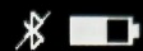
Yes

Select Connection

USB

QR

Jade 1F6250



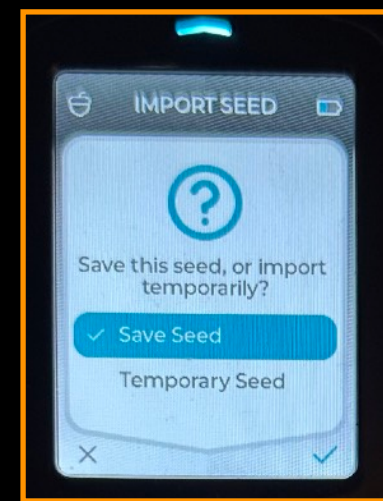
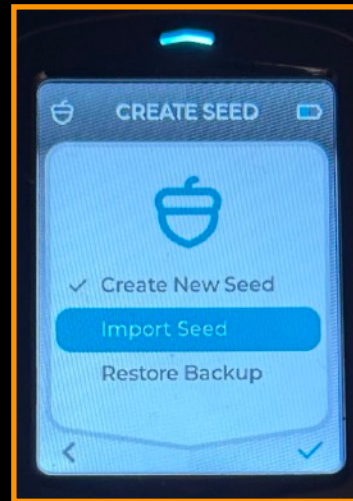
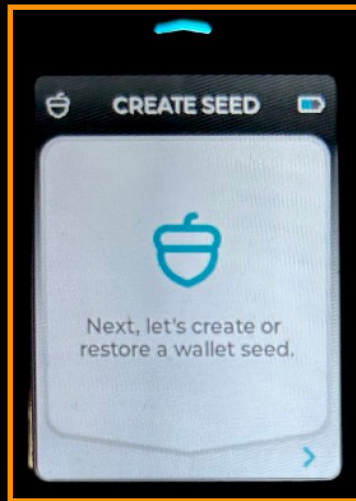
Options

Sessio

Active

408DAB5D

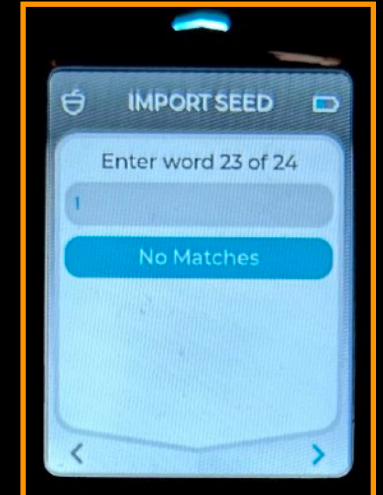
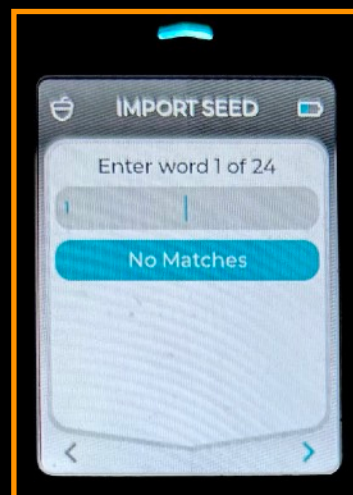
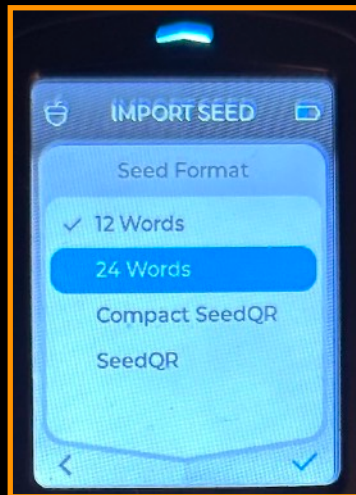
>>>>>>>FOUNDATION PASSPORT<<<<<<<<



◆ Power on your device

◆ Select > **Import Seed**

◆ Select > **Save Seed or Temporary Seed ***

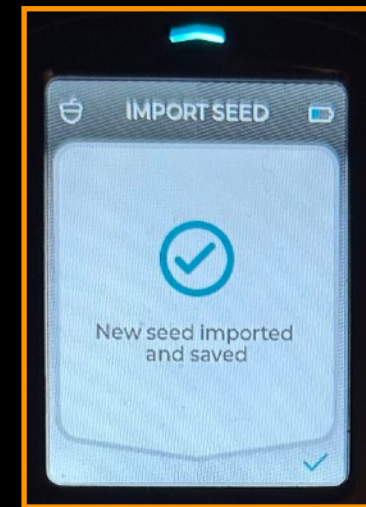
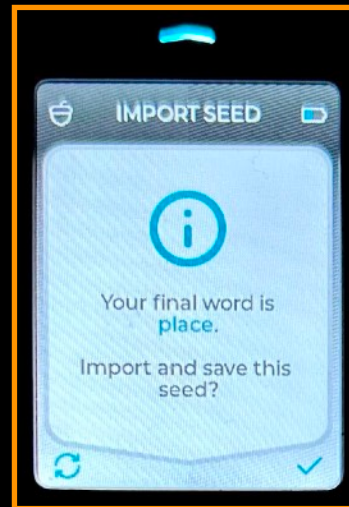
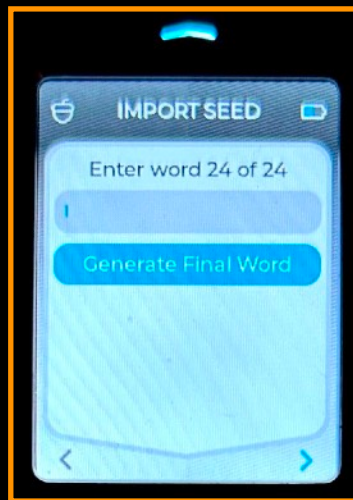


◆ Select > **24 words**

◆ Enter the 23 words from your Worksheet

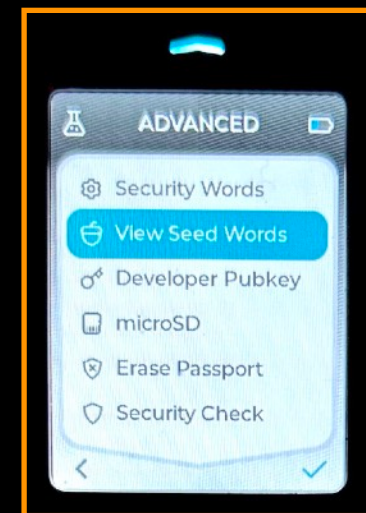
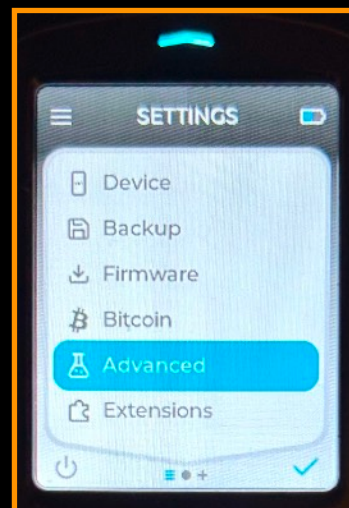
* Select **Temporary Seed** if you already have a seed in your Passport & just want to calculate a checksum for a new seed.

>>>>>>>FOUNDATION PASSPORT<<<<<<<<



◆ Select > Generate Final Word

◆ Select > Import and Save Seed



◆ Backup to MicroSD

◆ Settings > Advanced

◆ Select > View Seed Words & verify they are correct.

And that's it!

CONGRATULATIONS



You just rolled your own Seed Phrase offline!

IMMEDIATE NEXT STEPS:

- ◆ Make a copy so you have two backups.
- ◆ Put clear packing tape over each one.
- ◆ SECURELY HIDE EACH COPY SEPARATELY!

FINALLY:

- ◆ Buy 2 metal plates and stamp your seed in them for ultimate durability & protection from the elements. Hide separately and securely!



Read: blog.lopp.net/a-treatise-on-bitcoin-seed-backup-device-design/

REMEMBER:



- ♦ In bitcoin, possession is 10/10ths of the law!
- ♦ Whoever has your Seed Phrase has access to your bitcoin!
- ♦ Secure it very very well!
- ♦ As always > Don't Trust, **Verify** > DYOR **Do Your Own Research**

FURTHER RESOURCES:



- ♦ learnmeabitcoin.com/technical/keys/hd-wallets/mnemonic-seed/ by **Greg Walker**
- ♦ dplusplus.me/master by **D++**
- ♦ iancoleman.io/bip39/ by **Ian Coleman**
- ♦ blog.lopp.net/a-treatise-on-bitcoin-seed-backup-device-design/ by **Jameson Lopp**

Follow us on Nostr > primal.net/d++
> primal.net/keysa

WHY DOES ONE OCTAL & TWO HEX DICE CREATE A SEED WORD?



- ♦ A bitcoin Private Key contains **256 bits** of entropy.
- ♦ Each word in a Seed Phrase is **11 bits**.
- ♦ An **octal die** offers **3 bits of entropy**, since 8 is 2 to the power of 3, as in $2 \times 2 \times 2 = 8$
- ♦ A **hex die** offer **4 bits of entropy**, since 16 is 2 to the power of 4, as in $2 \times 2 \times 2 \times 2 = 16$.
- ♦ So one octal + two hex dice throws is:

 $3 \text{ bits} + 4 \text{ bits} + 4 \text{ bits} = 11 \text{ bits of entropy} = \text{One Seed Word.}$