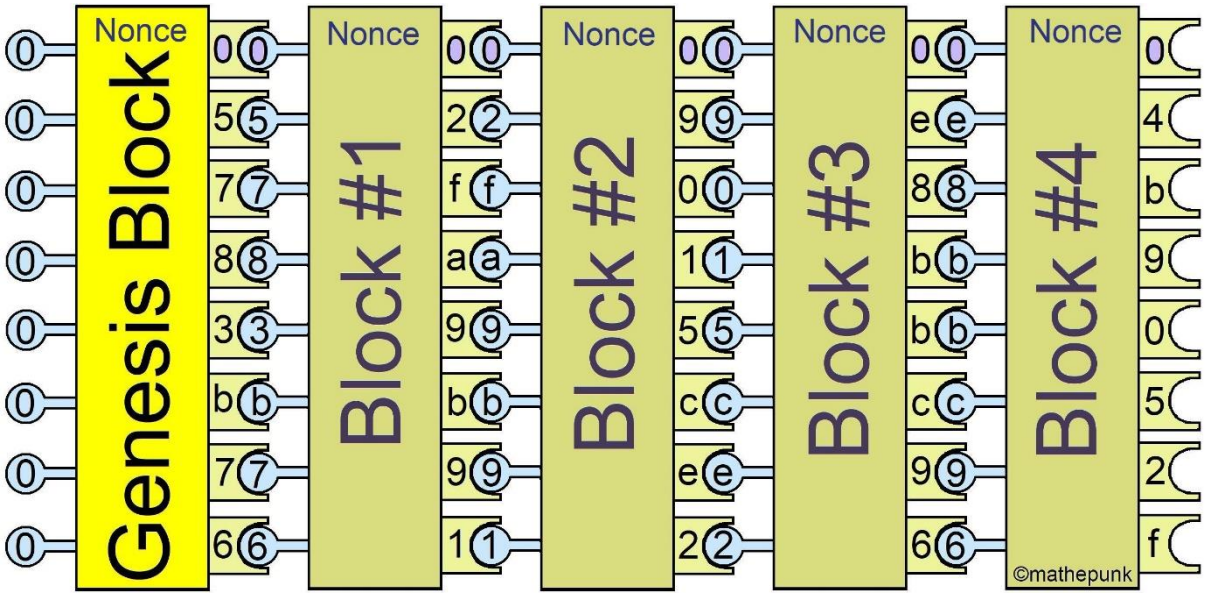
Blockchain

https://youtu.be/cOFAlfjSvxU

Name: ..... Vorname: .....

Wert von k: .....



Unterlagen auf https://mathepauker.com/Blockchain/Uebungen1.pdf

Hashfunktionen

Hashfunktionen sind dadurch gekennzeichnet, dass sie für einen alphanumerischen Input einen "Funktionswert" mit genau definierter Länge ergeben. Wie verwenden hier die SHA256 (National Institute of Standards and Technology). Eine von einer Hashfunktion geforderte Eigenschaft ist, dass sie "chaotisch" reagiert, d.h. geringfügig unterschiedliche Eingaben sollen völlig unterschiedliche Hashwerte erzeugen. Dazu die erste Übung.

©2020 mathepunk

Übung 1 (SHA 256):

https://www.mathepauker.com/Blockchain/hash.html

Nonce A (horizontal): .....

Nonce B (vertikal): .....

hex. Ziffer	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.
horizontal																
vertikal																

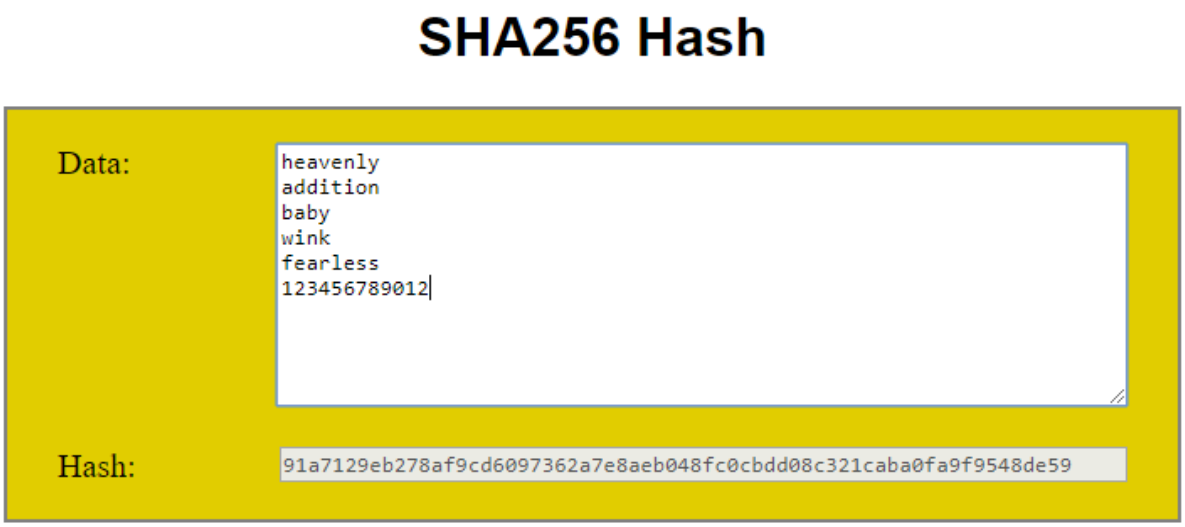
vertikal

f																
e																
d																
c																
b																
a																
9																
8																
7																
6																
5																
4																
3																
2																
1																
0																
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

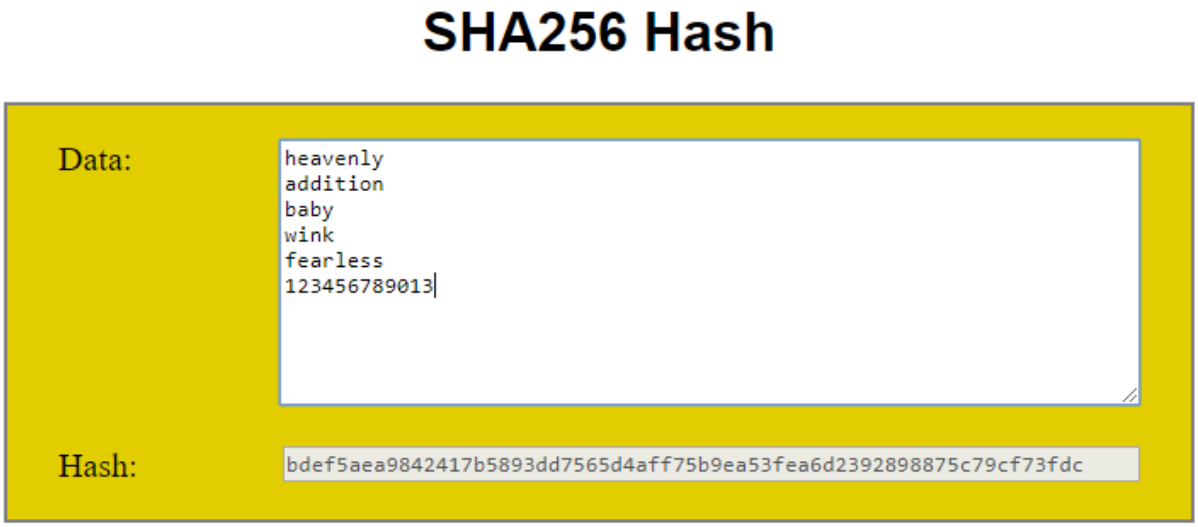
horizontal

©2020 mathepunk

Erstelle im "Fenster" für SHA256 (https://www.mathepauker.com/Blockchain/hash.html) eine Liste von fünf englischen Zufallswörtern aus der Tabelle im Anhang beginnend mit dem k-ten Wort in der Tabelle. Der Liste soll am Schluss eine zwölfstellige Nonce angehängt werden, z.B. für k = 86



Verwende für k den Wert, der auf der ersten Seite dieses Dokuments notiert ist. Notiere die ersten 16 hexadezimalen Ziffern des angezeigten Hashwerts (horizontal). Beim obigen Beispiel erhält man dafür 91a7129eb278af9c. Ändere danach eine Ziffer der Nonce und notiere die ersten hexadezimalen Ziffern des neuen Hashwerts. Im obigen Beispiel wurde die letzte hexadezimale Ziffer geändert. Auf dem Bildschirm hat man dann folgendes Bild:

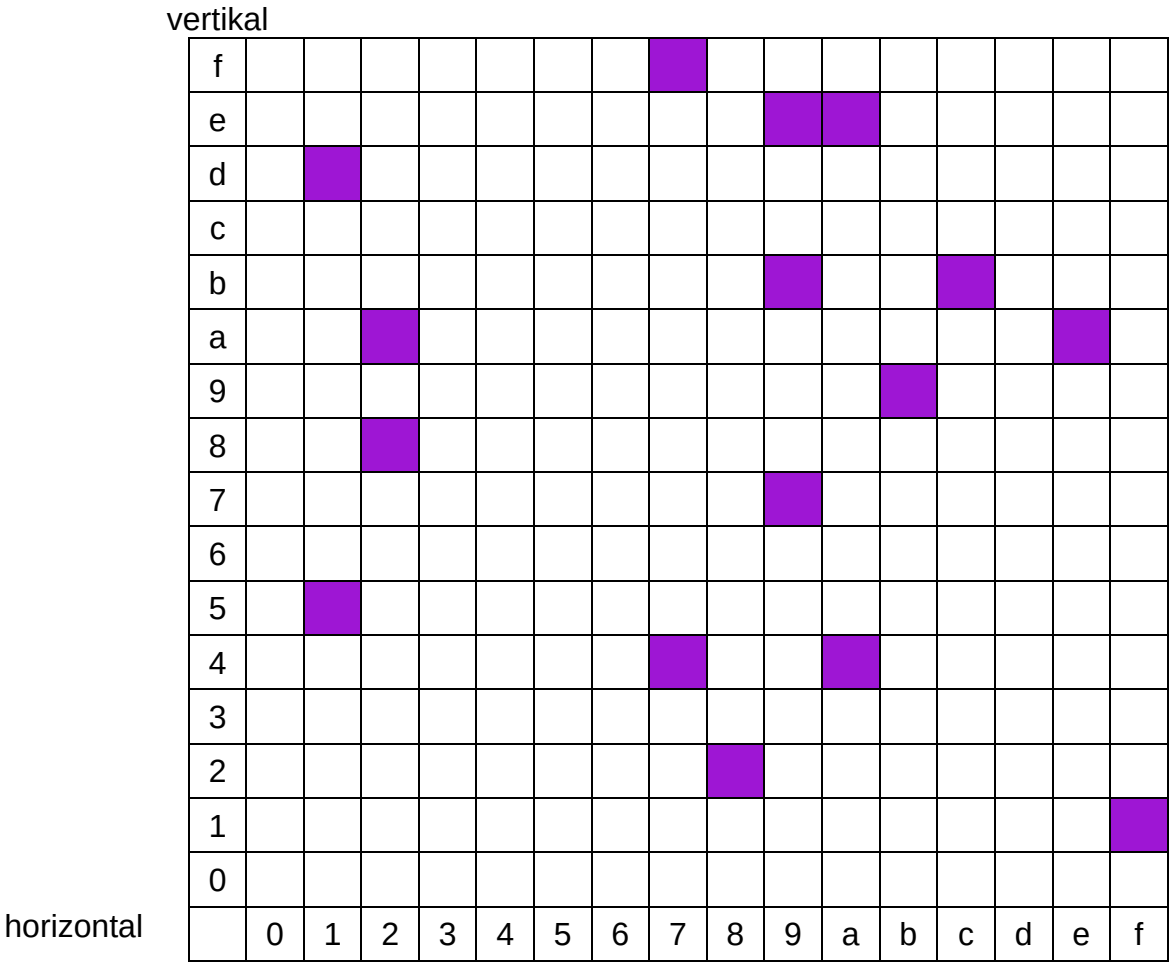


©2020 mathepunk

Die ersten 16 hexadezimalen Ziffern des Hashwerts des Blocks sind bdef5aea9842417b. Man erhält folgende Tabelle:

hex. Ziffer	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.
horizontal	9	1	a	7	1	2	9	e	b	2	7	8	a	f	9	c
vertikal	b	d	e	f	5	a	e	a	9	8	4	2	4	1	7	b

Aus obiger Tabelle kann folgende Grafik erstellt werden:



Aus der Verteilung der Markierungen ist ersichtlich, dass die ersten 16 hexadezimalen Ziffern des Hashwerts durch eine kleine Veränderung im Input in scheinbar willkürlicher Weise verändert werden. Darum geht es bei der Übung 1.

©2020 mathepunk

Übung 2 (Die Nonce):

https://www.mathepauker.com/Blockchain/blockchain.html

Gehe auf obige Website. Schreibe im Genesis Block (in der Data Box) deinen Namen (ohne Eingabetaste am Schluss!) und setze die Nonce gleich 0. Wähle den Schwierigkeitsgrad (Difficulty) 1. Ausgehend von 0 erhöhe den Wert der Nonce um 1. Notiere dabei in untenstehender Tabelle jeden Wert der Nonce bei welchem der Hashwert des Genesis Blocks mindestens eine Anfangsnull aufweist. Beim Schwierigkeitsgrad 0 wird der Genesis Block "grün aufleuchten" wenn der Hashwert mindestens eine Anfangsnull aufweist.

Name:						
Nonce: Liste von Werten für welche der Hashwert des Genesis Blocks mindestens eine Anfangsnull aufweist	1.	2.	3.	4.	5.	6.

Finde auf diese Weise sechs ersten Werte für die Nonce für "geschürfte Blöcke" (Schwierigkeitsgrad = 1, d.h. eine Anfangsnull).

Erhöhe den Schwierigkeitsgrad (Difficulty) auf 4 und drücke den "Mine-Knopf" des Genesis Blocks und notiere unten die Nonce für Schwierigkeitsgrad = 4.

Eine Nonce für vier Anfangsnullen: .....

Übung 3 (Schürfen):

https://www.mathepauker.com/Blockchain/blockchain.html

Gehe auf obige Website. Schreibe in die fünf Blöcke die fünf in Übung 1 verwendeten Worte aus der Tabelle von Zufallswörtern. (In jeden Block ein Wort, ohne Eingabetaste am Schluss). Setze zunächst den Schwierigkeitsgrad auf 1 (mindestens eine Anfangsnull beim Hashwert in hexadezimaler Darstellung). Beschreibe eine effiziente Vorgehensweise beim Schürfen der ganzen Blockchain mit fünf Blöcken.

Optimales Vorgehen beim Schürfen der gesamten Blockchain:

©2020 mathepunk

Notiere in untenstehender Tabelle die Werte der Nonce der geschürften Blöcke (für Schwierigkeitsgrad 1) in der Blockchain bestehend aus fünf geschürften Blöcken. Wiederhole danach die ganze Prozedur für höhere Schwierigkeitsgrade von 2 bis 5 und notiere in gleicher Weise die Werte der Nonce der fünf Blöcke der Blockchain für die höheren Schwierigkeitsgrade bis die Tabelle vollständig ausgefüllt ist. Berechne ausserdem den Mittelwert und die Standardabweichung der Nonce der fünf Blöcke für die verschiedenen Schwierigkeitsgrade (auf eine Stelle nach dem Dezimalpunkt). Für die Berechnung der Standardabweichung (Streuung) kannst du einen Online-Statistikrechner verwenden, z.B. unter

https://www.zinsen-berechnen.de/statistik-rechner.php

Schwie-rigkeits-grad	**Block**					**Mittel-wert**	**Stabw**
	Genesis	**#1**	**#2**	**#3**	**#4**		
1							
2							
3							
4							
5							

Erkläre und begründe welchen Mittelwert und welche Standardabweichung der Nonce man für den Schwierigkeitsgrad 6 erwarten würde. (Nur richtig mit Begründung!)

Geschätzter Mittelwert der Nonce für Schwierigkeitsgrad 6:

Begründung:

Geschätzte Stabw der Nonce für Schwierigkeitsgrad 6:

Begründung:

©2020 mathepunk

Übung 4 (Distributed Ledger):

https://www.mathepauker.com/Blockchain/blockchain.html

Gehe auf obige Website. Rekonstruiere die Blockchain von Übung 3 für Schwierigkeitsgrad 4. Ersetze in Block#2 den ersten Buchstaben des Worts aus der Liste von Zufallswörtern durch den entsprechenden Grossbuchstaben und beantworte zwei Fragen wie folgt:

4.1. Welche Blöcke der Blockchain sind nach der Manipulation an Block#2 nicht mehr geschürft (grün markiert)?
4.2. Wenn die Blockchain durch Schürfen von Blöcken rekonstruiert werden soll, in welcher Reihenfolge sollten die nicht geschürften Blöcke (rot) geschürft werden?

Notiere die ersten acht hexadezimalen Ziffern der ursprünglichen Hashwerte aller Blöcke der Blockchain in untenstehender Tabelle. Notiere alsdann die Hashwerte aller Blöcke der Blockchain nach der Manipulation von Block#2 in untenstehender Tabelle. Schürfe alle ungeschürften Blöcke der Blockchain und notiere die Hashwerte aller Blöcke der Blockchain nach der "Reparatur" ("neu geschürft") in untenstehender Tabelle.

Block	**Acht hexadezimale Anfangsziffern der Hashwerte**		
	Ursprüngliche Blockchain	**Manipulierte Blockchain**	**Neu geschürfte Blockchain**
Genesis			
#1			
#2			
#3			
#4			

©2020 mathepunk

Beantworte folgende Frage:

4.3. Wie könnte man einen einzelnen Block einer Blockchain so manipulieren, dass die Manipulation aus den Hashwerten der Blöcke der Blockchain nicht erkennbar wäre?

©2020 mathepunk

Anhang

Englische Zufallswörter (k)

1	soap	41	habitual	81	closed	121	seat	161	tooth
2	continue	42	blow	82	jittery	122	post	162	flight
3	industrious	43	front	83	elderly	123	end	163	perpetual
4	pollution	44	dark	84	sincere	124	smelly	164	shop
5	breakable	45	houses	85	cemetery	125	nose	165	hammer
6	breakable	46	party	86	heavenly	126	thick	166	argument
7	pizzas	47	view	87	addition	127	moan	167	impolite
8	heartbreaking	48	amuck	88	baby	128	shock	168	puzzled
9	women	49	overflow	89	wink	129	square	169	pushy
10	substance	50	hypnotic	90	fearless	130	irritate	170	animal
11	remarkable	51	title	91	hole	131	quick	171	rabbits
12	invincible	52	scissors	92	reflect	132	exercise	172	slap
13	evanescent	53	lace	93	amount	133	mend	173	far
14	quack	54	legs	94	quarter	134	zephyr	174	pan
15	outstanding	55	whip	95	rejoice	135	lyrical	175	fireman
16	observant	56	zinc	96	airport	136	enter	176	stretch
17	far-flung	57	punish	97	muddle	137	wide	177	train
18	familiar	58	massive	98	small	138	channel	178	funny
19	elegant	59	thin	99	secret	139	alert	179	quiet
20	adjustment	60	drum	100	roasted	140	sparkling	180	tree
21	troubled	61	treat	101	terrific	141	gainful	181	fallacious
22	mellow	62	pot	102	rude	142	current	182	fence
23	whispering	63	saw	103	lame	143	crime	183	penitent
24	possessive	64	queue	104	able	144	happen	184	last
25	imminent	65	inject	105	quizzical	145	tip	185	well-to-do
26	quarrelsome	66	plucky	106	languid	146	close	186	name
27	eggs	67	start	107	ski	147	exchange	187	rich
28	jagged	68	slip	108	calculator	148	earth	188	unlock
29	committee	69	smart	109	crooked	149	decisive	189	reduce
30	present	70	copy	110	promise	150	grape	190	loving
31	guard	71	mine	111	swim	151	governor	191	frequent
32	uttermost	72	clean	112	dance	152	hanging	192	wrist
33	giraffe	73	tramp	113	eye	153	fluttering	193	hideous
34	belligerent	74	mint	114	guarded	154	glossy	194	vegetable
35	harmonious	75	spill	115	separate	155	bustling	195	twig
36	stupendous	76	hour	116	tedious	156	greasy	196	crook
37	development	77	milk	117	pig	157	volleyball	197	allow
38	damaged	78	practise	118	rat	158	entertain	198	powder
39	office	79	chance	119	scene	159	leather	199	train
40	fancy	80	anxious	120	trade	160	blush	200	drain

©2020 mathepunk

Notizen:

YouTube Videos

Datenstruktur einer Blockchain
(Blockchain für Dummies)
https://youtu.be/fFiI7xnY0u0

Was ist die "Nonce" in Blockchain
(Blockchain für Dummies)
https://youtu.be/AQwwxDw2pVo

Unterlagen zur Übung: https://www.mathepauker.com/Blockchain/Uebungen1.pdf

©2020 mathepunk