Mein Bitcoin-Nachlassplan

Allgemeine Informationen

Liebe Erben

Ich schreibe diesen Brief, um euch zu informieren, dass ich digitale Assets wie zum Beispiel den Bitcoin besitze. Dieses volldigitale Geld wird von keiner Bank oder sonstigen Dritten verwahrt oder verwaltet – wer Bitcoins besitzt, betreibt sozusagen seine eigene Bank. Falls ich eines Tages nicht mehr unter euch weile oder selber keinen Zugriff auf die kryptografischen Vermögenswerte mehr habe, möchte ich sichergehen, dass ihr darauf zugreifen könnt. Bitte lest diesen Brief vollständig und aufmerksam durch. Er sagt euch, welche Möglichkeiten ihr nun habt und was ihr jeweils tun müsst.

Wenn ich nicht mehr persönlich verfügbar sein sollte, um euch zu helfen, ihr aber trotzdem Hilfe braucht oder Fragen habt, schlage ich euch folgende(n) vertrauenswürdige(n) Kontakt(e) vor:

Kontakt 1 (Name, Firma, Tel-Nummer, E-Mail, Webseite):

Satoshi Nakamoto, 855-835-5324, hello@satoshi.com, bitcoin.org

Kontakt 2 (Name, Firma, Tel-Nummer, E-Mail, Webseite):

Ich vertraue diesen Kontakten, unabhängig davon, ob sie über ihre Rolle in meinem Nachlassplan wissen oder nicht. Natürlich könnt ihr euch auch an jemand anderen wenden, wenn ihr wollt. Bitte beachtet aber, dass diese Personen integer sind und sich mit der Materie auskennen. Im Gegensatz zu Transaktionen bei einer gewöhnlichen Bank lassen sich Transfers in der Bitcoinwelt oft nicht mehr rückgängig machen. Das heißt, dass sämtliche Überweisungen korrekt ausgeführt werden müssen, da sonst das Geld für immer verloren sein kann.

Ich möchte euch einige technische Begriffe erläutern, denen ihr auf den folgenden Seiten immer wieder begegnen werdet:

- **Kryptowährungen:** digitale Assets auch Coins oder Tokens genannt. Ein Beispiel ist Bitcoin
- **Wallet:** eine digitale Brieftasche, welche die Zugänge (Schlüssel) zu den Bitcoins verwahrt
- **Hardware-Wallet:** ein physisches Gerät, welches Wallets beinhaltet und Bitcoins verwaltet, vergleichbar mit einem speziellen USB-Stick
- **Software-Wallet:** eine App auf dem Smartphone oder Computer, welche Bitcoins verwaltet
- **Seed-Phrase:** Als Hauptpasswort ist sie wichtig für den Zugang zu den Wallets. Sie besteht aus 12 bis 24 Wörtern. Damit lasst sich das Wallet wiederherstellen, falls man alle Zugänge zu den Wallets verloren hat
- **Passphrase:** ein Zusatzpasswort für Wallets
- **2FA(ktoren)-Authentifizierung:** Verfahren, bei dem zwei Geheiminformationen (Faktoren) eingeben werden müssen, um Zugang zu erlangen. Beim ersten Faktor handelt es sich um das in der Regel auswendiggelernte Passwort oder eine PIN. Der zweite Faktor, eine zeitlich begrenzte Sicherheitsnummer, wird meistens von einer App auf dem Smartphone erzeugt. Die Zwei-Faktoren-Authentifizierung wird beispielsweise bei Online-Börsen verwendet
- **Exchanges:** Online-Börsen, auf dene man Bitcoins kaufen oder verkaufen kann

Geht mit den Wallets, Passwörtern, Pass- und Seed-Phrasen äußerst vorsichtig um. Gemeinsam sind sie euer Schlüssel zu meinen Bitcoins. Gelangen jedoch Unbefugte in den Besitz der Daten, können sie alles stehlen.

Diesen Brief habe ich mit dem Hilfstool von http://www.marcsteiner.tech/ erstellt. Dort findet ihr gebündelt weiterführende und vertiefende Informationen. Weitere Inhalte und Ressourcen findet ihr im Internet. Achtet auch hier auf die Vertrauenswürdigkeit der Informationsquellen.

Schnellübersicht

Die folgende Übersichtstabelle enthält alle wichtigen Zugangsdaten. Nochmals: Haltet diese Informationen streng geheim! Wie ihr mit ihnen umgeht, erfahrt ihr im weiteren Verlauf dieses Briefes. Falls dann noch Fragen bestehen, solltet ihr die oben angegebene Vertrauensperson kontaktieren.

Wallet	Benutzername	PIN oder Passwort	Passphrase oder 2FA	Wallet zu finden	Backup des Wallets
HW Wallet #1 - BitBox02	-	123456	NotCraighWright	Safe Bank of Satoshi,Nakamoto-Street, Japan	Safe zu Hause
SW Wallet Computer #1	-	Password123	-	Apple iMac	Safe zu Hause
SW Wallet Smartphone #1	-	7890	-	iPhone XYZ	-
Exchange Bitstamp	ToTheMoon	Password5678	-	-	-

Hardware-Wallet

Ich verwende folgende Hardware-Wallets, um meine Bitcoins zu verwahren. Diese Geräte können zwar an öffentliche oder virenverseuchte Computer angeschlossen werden, du solltest aber trotzdem schauen, dass du sie nur in einer privaten Umgebung nutzt. Die folgenden Informationen solltet ihr allerdings streng geheim halten.

Hardware-Wallet #1

Gerätetyp: **BitBox02**

Website für Zugriffssoftware oder Infos: https://shiftcrypto.ch/

Wo befindet sich das Gerät: Safe Bank of Satoshi,Nakamoto-Street, Japan

Wallet-PIN: 1234

Optionaler Sicherheitscode (Passphrase): NotCraigWright

(Optional) Wo befinden sich die Backup Wörter (Seed-Phrase): Safe zu Hause

Seed-Phrase Wörter:

1 race	7	13	19
2 medal	8	14	20
3 ...	9	15	21
4 ...	10	16	22
5	11	17	23
6	12	18	24 ...

Ihr braucht die offizielle Software des Herstellers, um auf das Hardware-Wallet zuzugreifen. Den entsprechenden Link zu der Software findet ihr oben. Für den Zugriff auf das Guthaben benötigt ihr das richtige Gerät, die Wallet-PIN sowie eventuell eine Passphrase. Diese Informationen sind alle oben angegeben.

Wenn ihr das Gerät oder die PIN nicht findet, das Gerät beschädigt oder zerstört ist: keine Panik. Beschafft euch einfach das gleiche Gerät **neu auf der offiziellen Webseite des Herstellers**. Mithilfe der Backup-Wörter (Seed-Phrase) könnt ihr die Wallets auf dem neuen Gerät wiederherstellen und auf die Gelder zugreifen.

Software-Wallets auf meinem Computer oder Smartphone

Für bestimmte Kryptowährungen benutze ich eigenständige Wallets, die auf meinem Computer oder Smartphone gespeichert sind. Dies sind normale Apps, wie ihr auch andere auf den Geräten habt. Falls der Computer oder das Smartphone defekt ist oder ein anderes Problem auftritt, könnt ihr die Software-Wallet-Apps auf anderen Geräten frisch installieren und die Wallets mithilfe der Backup-Wörter (Seed-Phrase) wiederherstellen.

Folgende Software-Wallets (App) nutze ich auf dem Computer

Computer-Marke: Apple iMac

Benutzername: FakeToshi

Passwort: 12345

Wallet #1

Wallet-Name: Wasabi

Wallet für Kryptowährung: Bitcoin

Wallet-Passwort: Password123

Optionaler Sicherheitscode (Passphrase): -

(Optional) Wo befinden sich die Backup Wörter (Seed-Phrase): Safe zu Hause

Seed-Phrase Wörter:

1 infant	7	13	19
2 meat	8	14	20
3 ...	9	15	21
4 ...	10	16	22
5	11	17	23
6	12	18	24 ...

Folgende Software-Wallets (App) nutze ich auf dem Smartphone:

Smartphone-Marke: iPhone XYZ

Login PIN: 12345

Wichtiger Hinweis: Wichtiger Hinweis: Man kann parallel zu biometrischen Sperrmechanismen, wie Fingerabdruckscan, den Pin eingeben, um das Gerät zu entsperren.

Wallet #1

Wallet-Name: GreenWallet

Wallet für Kryptowährung: Bitcoin

Wallet-Passwort: 7890

Optionaler Sicherheitscode (Passphrase): -

(Optional) Wo befinden sich die Backup Wörter (Seed-Phrase): -

Seed-Phrase Wörter:

1 can	7	13	19
2 day	8	14	20
3 humor	9	15	21
4 ...	10	16	22
5 ...	11	17	23
6	12	18	24 ...

Online-Exchanges (Börsen)

Ich benutze Online-Exchanges, also elektronische Börsen, um mit Bitcoins zu handeln. Möglicherweise befinden sich dort noch Bargeld und weitere Krypto-Assets neben dem Bitcoin. Ihr solltet diese Vermögenswerte in absehbarer Zeit von der Börse entfernen, da die meisten Börsen nicht sicher vor Hackerangriffen sind.

Um online auf meine Börsenkonten zuzugreifen, benötigt ihr meinen Benutzernamen, mein Passwort und einen temporären 2FA-Sicherheitscode. Dieser Code wird auf der entsprechenden App auf meinem Smartphone generiert.

Auf diesem Gerät findest du meine App für den temporären 2FA-Sicherheitscode:

Smartphone-Marke: iPhone XYZ

Login PIN: 12345

Name der 2FA-App: Google Authenticator

Passwort: -

Folgende Börsen nutze ich:

Account #1

Exchange: Bitstamp

Offizielle Website: https://www.bitstamp.net/

Benutzername: ToTheMoon

Passwort: Password5678

Optionaler 2FA-Sicherheitscode aktiviert (Ja/Nein): JA

Passwortmanager-App

Ich verwende die folgende App auf meinem Smartphone und/oder Computer, um wichtige Daten zu sichern.

Smartphone-Marke: iPhoneXYZ

Login PIN: 12345

Name der Passwort-Manager-App: 1Password

Passwort: DasIstMeinSuperKrassesPasswort!!!

Daten digital gespeichert

Ich habe meine Zugangsdaten und andere Informationen digital gespeichert und verschlüsselt. Um darauf zuzugreifen, braucht ihr folgende Informationen. Auch hier gilt: Wenn ihr allein nicht weiterkommt, fragt meine Vertrauensperson um Rat.

Speichermedium (Art, Name oder Typ): SD-Karte, Marke Kingston, Schwarz

Wo befindet sich das Speichermedium: Safe Zu Hause

Verwendetes Verschlüsselungsprogramm: VeryCrypt

Entschlüsselungspasswort: NiemandKannDiesesPasswortKnacken!!

Multisignatur-Wallet

Ich habe Wallets mit einer Multisignatur erstellt. Das bedeutet, dass immer eine bestimmte Anzahl von Personen zusammenkommen muss, um die Wallets zu öffnen und Transaktionen zu genehmigen.

Minimale Anzahl der Schlüssel, die gebraucht wird (z. B. 2 von 3): 2 von 3

Verwendetes Multisig-Wallet (Marke, Typ): Electrum Desktop Wallet

Dein persönlicher Teilschlüssel (Seed-Phrase deiner Wallet):

1 able	7	13	19
2 kiwi	8	14	20
3 ...	9	15	21
4 ...	10	16	22
5	11	17	23
6	12	18	24 ...

Personen mit weiteren Teilschlüsseln (Name, Adresse, E-Mail, Telefonnummer, XPUB)

Person 1: Craig Wright, Im Busch 21, Sidney, Australien, fake@satoshi.com, 855-835-5325

Person 1 (XPUB dessen Wallet): xpub6CU....

Person 2: Satoshi Nakamoto, thereal@satoshi.com, bitcoin.org, 123-456-789

Person 2 (XPUB dessen Wallet): xpubonZ....

Person 3: _____

Person 3 (XPUB dessen Wallet): _____

Person 4: _____

Person 4 (XPUB dessen Wallet): _____

Shamir's Secret Sharing Scheme

Ich nutzte einen speziellen Sicherheitsmechanismus, der sich Shamir's Secret Sharing Scheme (SSSS) nennt. Mit dessen Hilfe habe ich die Zugangsdaten auf mehrere Personen aufgeteilt. Das heißt, dass jede Person nur ein Teilstück (secret) der Zugangsdaten besitzt und eine bestimmte Anzahl von Personen zusammenkommen muss, um die Zugangsdaten zu rekonstruieren und Zugriff zu erlangen.

Minimale Anzahl Teilgeheimnisse (Secrets), die gebraucht wird (z.B. 2 von 3):2 von 3

Name des verwendeten Tools für die Entschlüsselung:SLIP-0039 fähiges Hardware Wallet (Trezor T)

Welche Daten wurden mit SSSS verschlüsselt (z.B. Seed-Phrase oder Verschlüsselungspasswort):Seed-Phrase HW Wallet XY

Das ist dein persönliches Teilgeheimnis (Secret):

Mein verwendetes Hardware Wallet (siehe oben) unterstützt Shamir's Secret Sharing Scheme (Standard: SLIP-0039). Dein Teilgeheimnis (Secret) sind folgende Worte:

1 adult	7	13	19
2 bulb	8	14	20 ...
3 ...	9	15	21
4 ...	10	16	22
5	11	17	23
6	12	18	24

Personen mit einem weiteren Teilgeheimnis (Secret) (Name, Adresse, E-Mail, Telefonnummer)

Person 1: Craig Wright, Im Busch 21, Sidney, Australien, fake@satoshi.com, 855-835-5325

Person 2: Satoshi Nakamoto, thereal@satoshi.com, bitcoin.org, 123-456-789

Person 3: _____

Person 4: _____

Poor Man's Shamir's Secret Sharing Scheme

Ich nutzte einen speziellen Sicherheitsmechanismus, der sich Shamir's Secret Sharing Scheme (SSSS) nennt. Anstelle einer Software habe ich die Papiervariante gewählt, die als „Poor Man's Shamir's Secret Sharing Scheme" bekannt ist. Die Seed-Phrase, die ihr für die Wiederherstellung des Wallets braucht, wurde dreigeteilt, wobei zwei Karten zusammen jeweils die kompletten 24 Wörter ergeben. Hier ist dein Teil der Seed-Phrase.

LISTE A

Wort 1	above			Wort 17	off
Wort 2	about	Wort 10	hole		
		Wort 11	crazy	Wort 19	minor
Wort 4	bunker			Wort 20	earn
Wort 5	buzz	Wort 13	nose		
		Wort 14	net	Wort 22	lio
Wort 7	coin			Wort 23	cat
Wort 8	color	Wort 16	calm		

LISTE B

Wort 1		Wort 9			
		Wort 10		Wort 18	
Wort 3				Wort 19	
Wort 4		Wort 12			
		Wort 13		Wort 21	
Wort 6				Wort 22	
Wort 7		Wort 15			
		Wort 16		Wort 24	

LISTE C

		Wort 9		Wort 17	
Wort 2				Wort 18	
Wort 3		Wort 11			
		Wort 12		Wort 20	
Wort 5				Wort 21	
Wort 6		Wort 14			
		Wort 15		Wort 23	
Wort 8				Wort 24	

Personen mit einem weiteren Teilgeheimnis (Secret) (Name, Adresse, E-Mail, Telefonnummer)

Person 1: Craig Wright, Im Busch 21, Sidney, Australien, fake@satoshi.com, 855-835-5325

Person 2: Satoshi Nakamoto, thereal@satoshi.com, bitcoin.org, 123-456-789

Liquidieren der Vermögenswerte

Um die kryptografischen Vermögenswerte in US-Dollar, Euro, Schweizer Franken oder andere Währungen zu wechseln, braucht ihr ein Konto bei einer Kryptobörse (Exchange). Am besten nutzt ihr die Börse, bei der ich bereits ein Konto habe. Dort könnt ihr die Bitcoins verkaufen und das Geld auf euer Konten übertragen.

Um Bitcoins an andere Personen zu übertragen, ohne sie zu liquidieren, muss jede Person ein eigenes Konto einrichten. Dies kann aus Sicherheitsgründen nicht von einem Testamentsvollstrecker, Treuhänder oder anderen Dritten durchgeführt werden. Wendet euch an den von mir angegebenen Kontakt, falls ihr Unterstützung braucht.

Auf den Blockchains kommt es immer wieder zu Spaltungen, sogenannten Forks. Dabei entstehen Assets, die man tatsächlich kostenlos mitbekommt. Weil sie aber nicht viel Wert haben, nennt man sie oftmals auch Airdrops oder Walhalla Coins. Informiert euch im Internet über mögliche Forks bei für euch relevanten Kryptowährungen, schaut auf den Exchanges oder direkt in den Wallets nach. Teilweise erscheinen sie auch automatisch, wenn der Hersteller entschieden hat, diese Assets zu unterstützen. Auch hier solltet ihr euch an die von mir angegebene Kontaktperson oder eine andere professionelle, vertrauenswürdige Organisation wenden, um Unterstützung zu erhalten.

Was ihr sonst noch wissen müsst

Hier weitere, optionale Infos von Hand eintragen wie zum Beispiel:

- Instruktionen, Schlüssel, Passwörter wie man an ein Schliessfach einer Bank herankommt
- ob es juristisch oder steuertechnisch etwas zu beachten gibt
- Hinweise zu gewissen vertrauenswürdigen Personen
- ob man weitere Kopien dieses Plans erstellt hat und wo man diese findet

Schau regelmässig, dass du in den Tresorraum der Bank kommst. Ich hatte schon Probleme.
Meine Kopien sind nicht nur im Banksafe sondern bei mir zu Hause im Safe.

Schlusswort

Ich hoffe, dass ich mit diesem Nachlassplan geholfen habe, einfacher an mein Erbe zu gelangen und wünsche viel Kraft und Erfolg in diesen schwierigen Zeiten. Macht etwas Gutes daraus und schaut nach vorne.

Dieser Brief wurde zuletzt am 31/08/2020 aktualisiert.

Unterschrift: _____