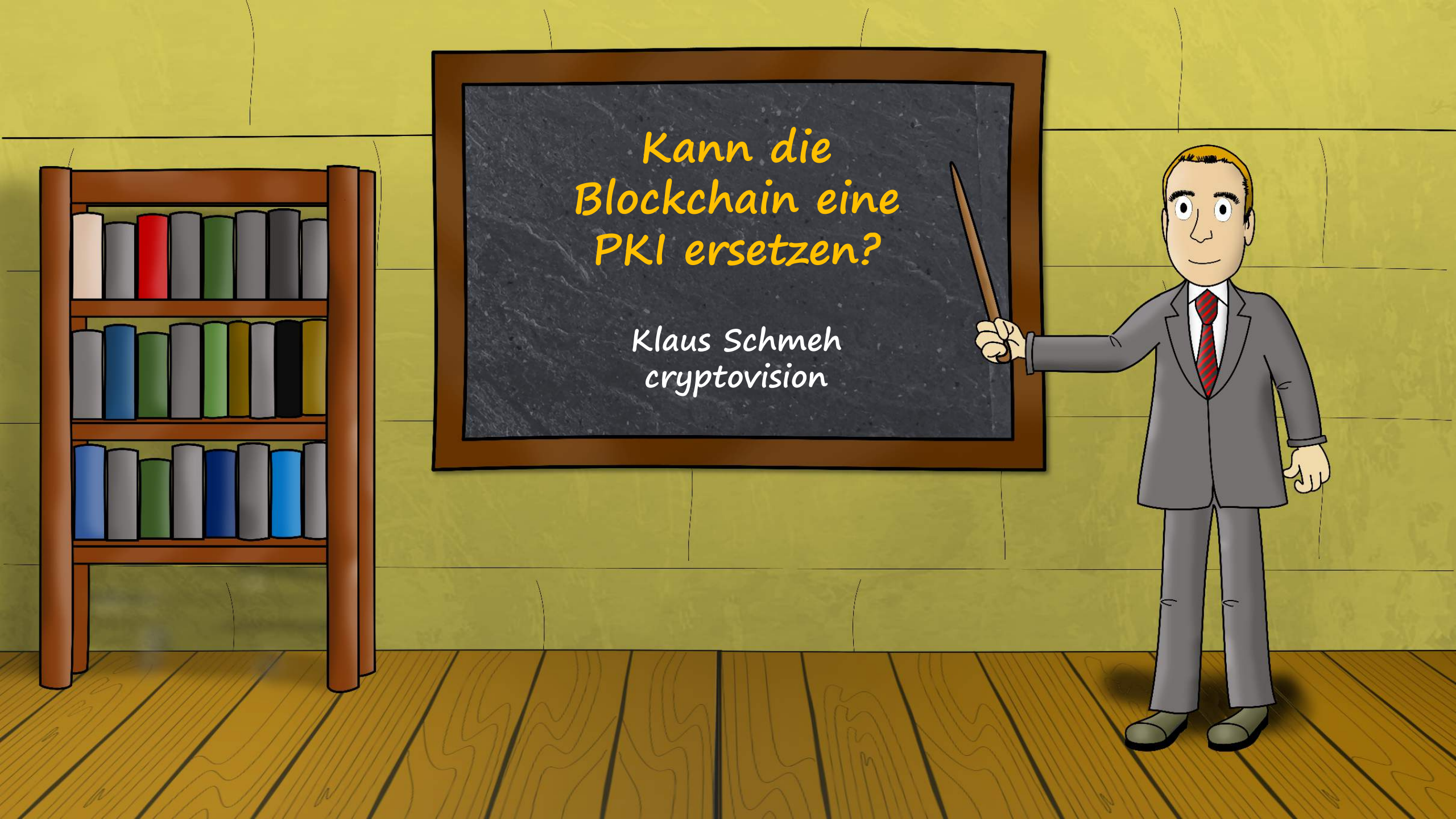
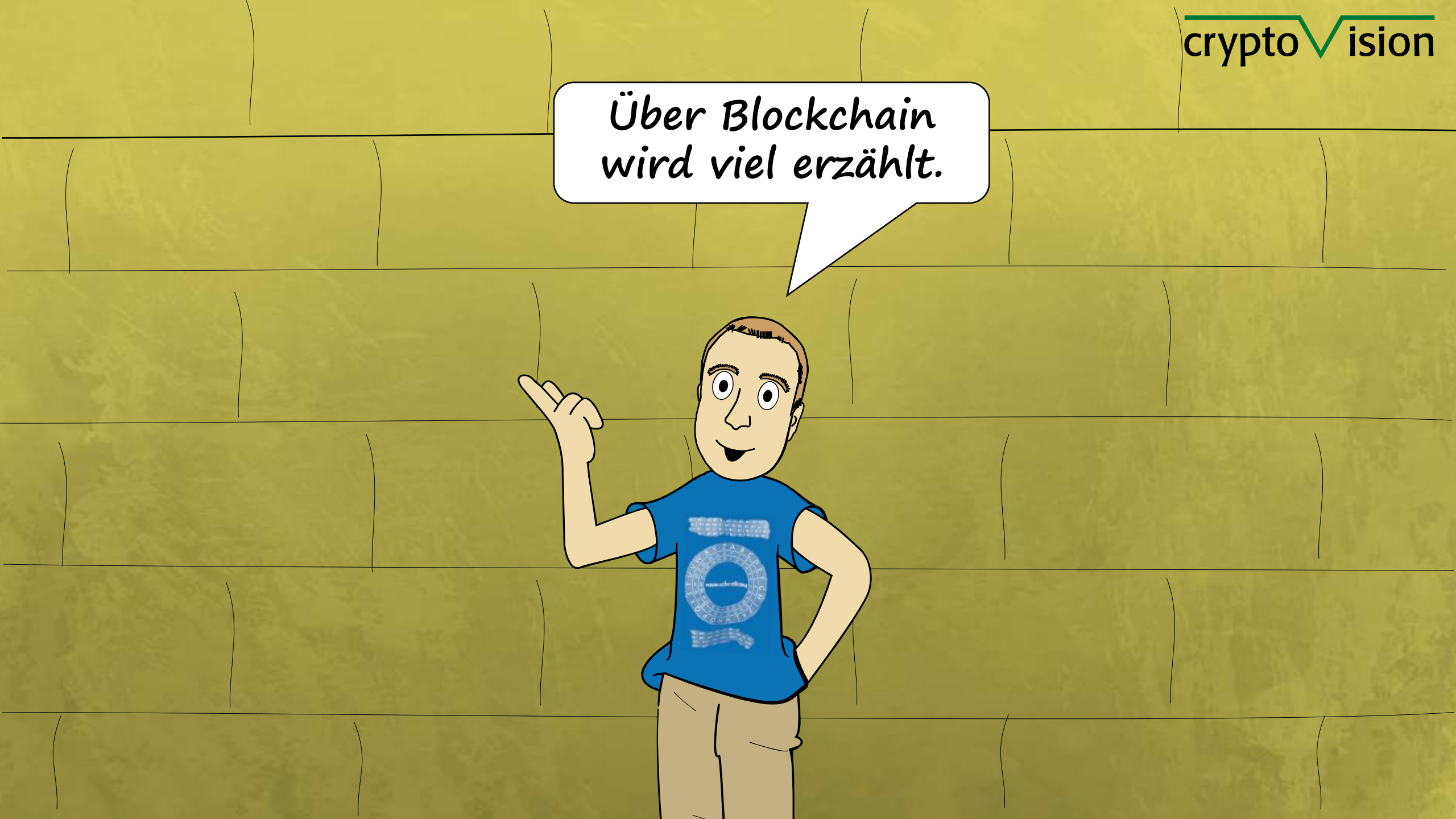
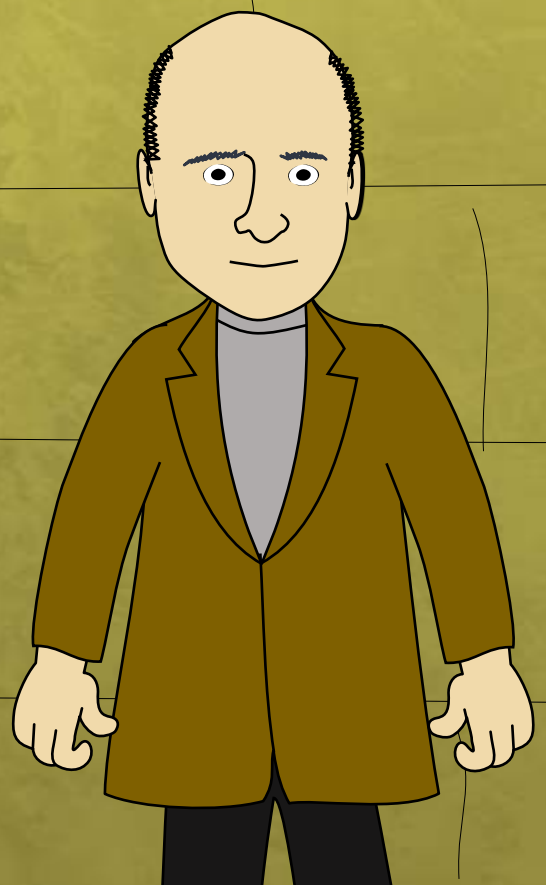
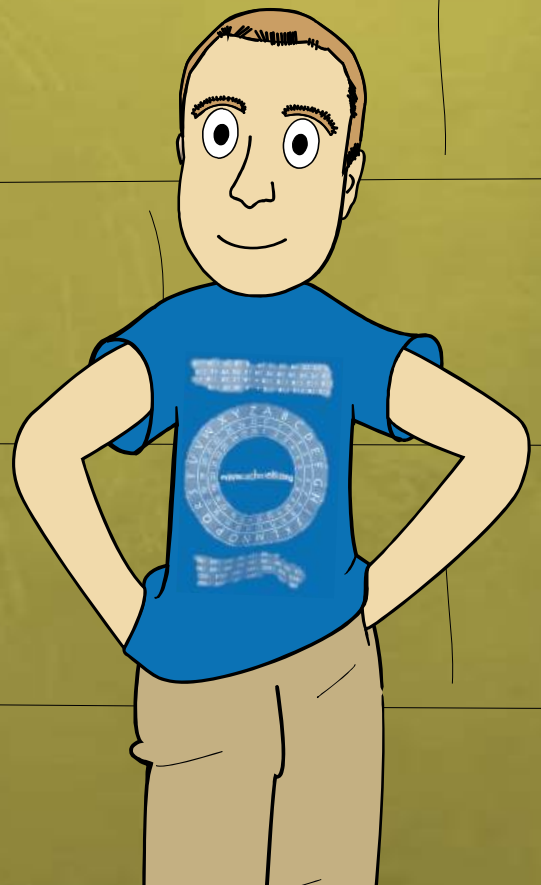

Kann die Blockchain eine PKI ersetzen?
Klaus Schmeh
cryptovision


Über Blockchain wird viel erzählt.


Die Blockchain ist nicht nur eine Revolution. Sie ist ein Tsunami-artiges Phänomen.
William Mougayar
Start-up-Experte
cryptovision

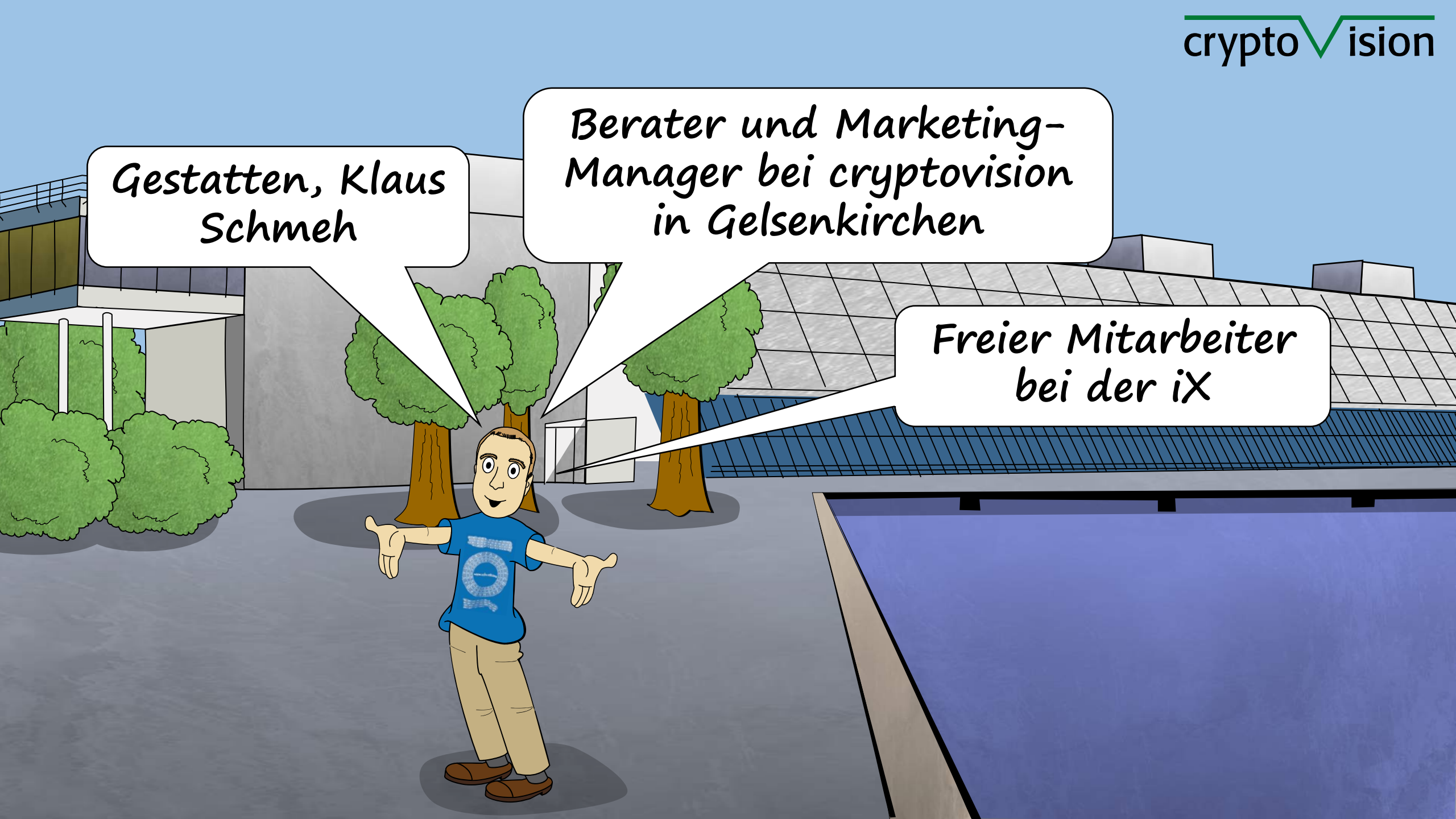
Es wird heute so viel über die Blockchain erzählt, dass es schwierig wird, die Realität vom Hype zu trennen.

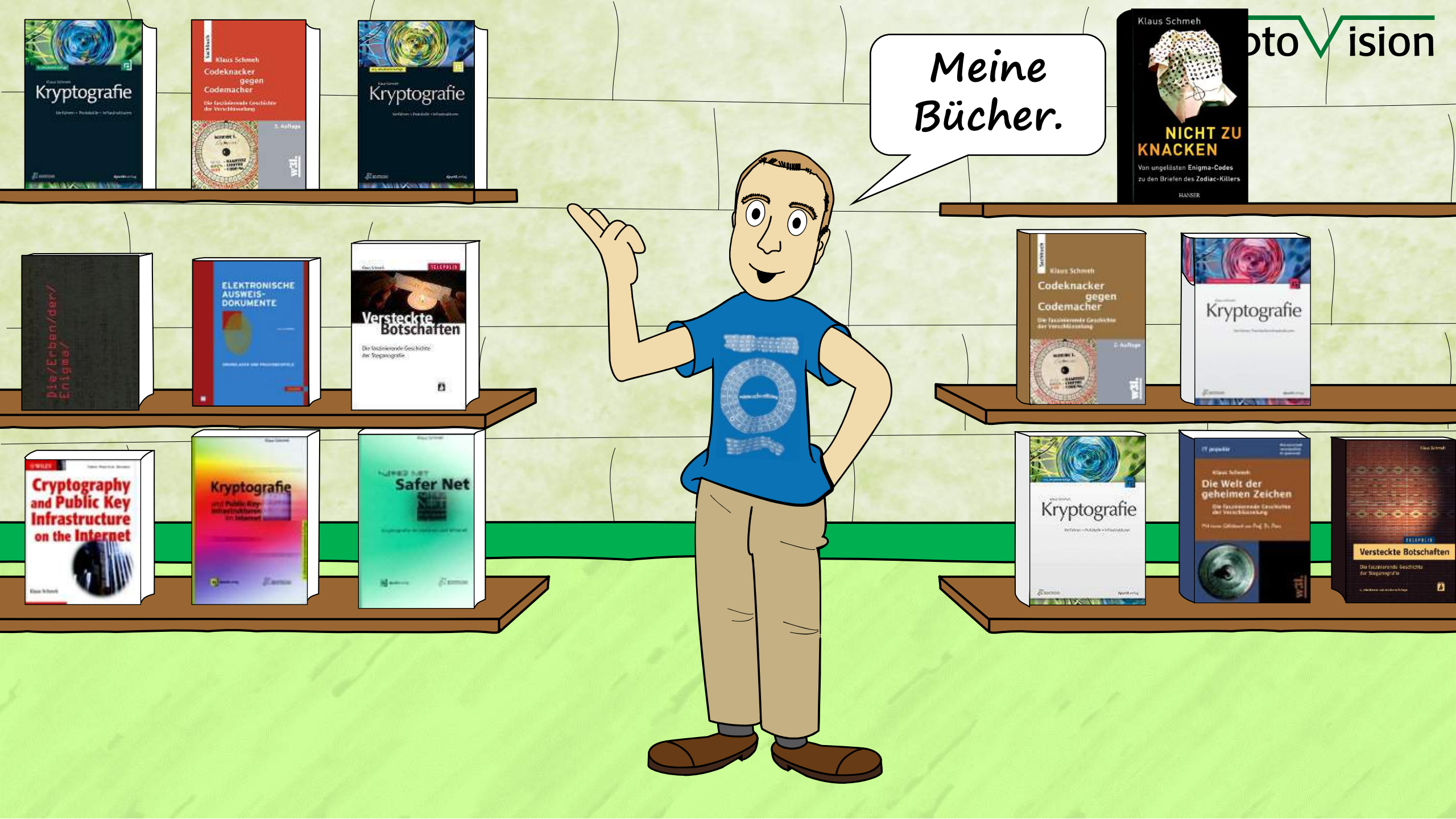




Ted Shorter
PKI-Experte

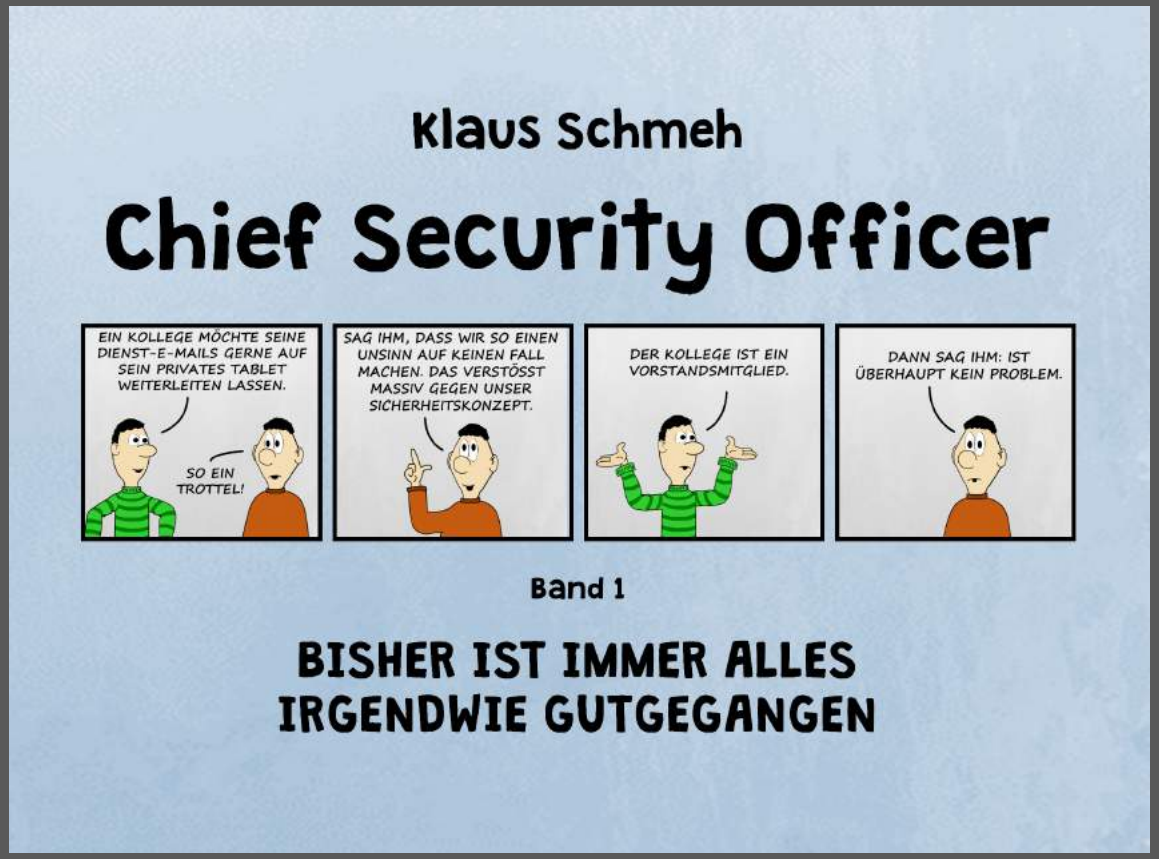

Tsunami oder Hype?
Wir werden sehen.
cryptoVision


cryptovision
Gestatten, Klaus Schmeh
Berater und Marketing-Manager bei cryptovision in Gelsenkirchen
Freier Mitarbeiter bei der iX


Meine Bücher.
Kryptografie
Klaus Schmeh
Codeknacker gegen Codemacher
Kryptografie
Klaus Schmeh
NICHT ZU KNACKEN
Von ungelösten Enigma-Codes zu den Briefen des Zodiac-Killers
HANSER
Die Erben der Enigma
ELEKTRONISCHE AUSWEISDOKUMENTE
Versteckte Botschaften
Codeknacker gegen Codemacher
Kryptografie
Cryptography and Public Key Infrastructure on the Internet
Kryptografie
Safer Net
Kryptografie
Die Welt der geheimen Zeichen
Versteckte Botschaften

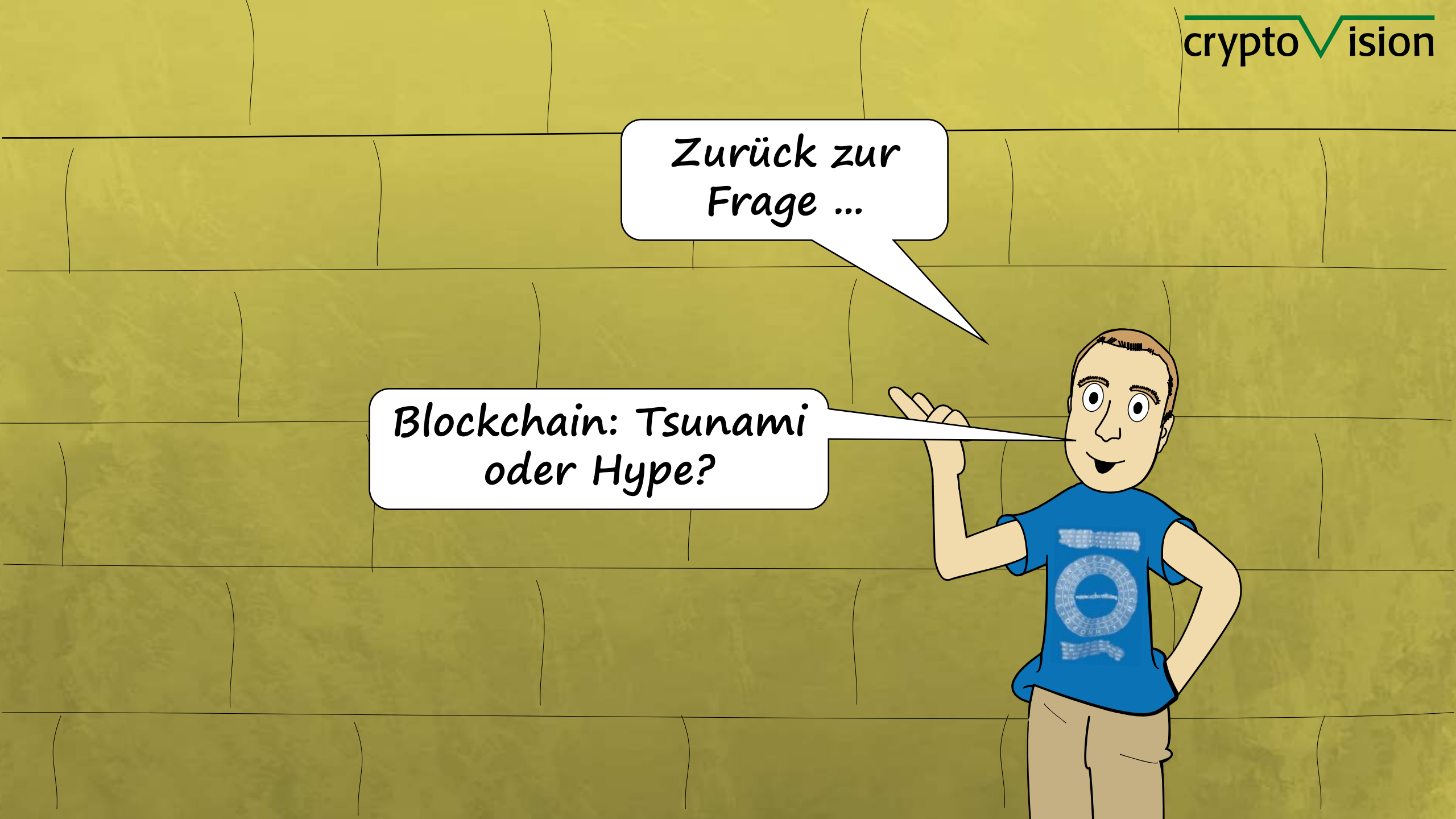
Comic-Buch

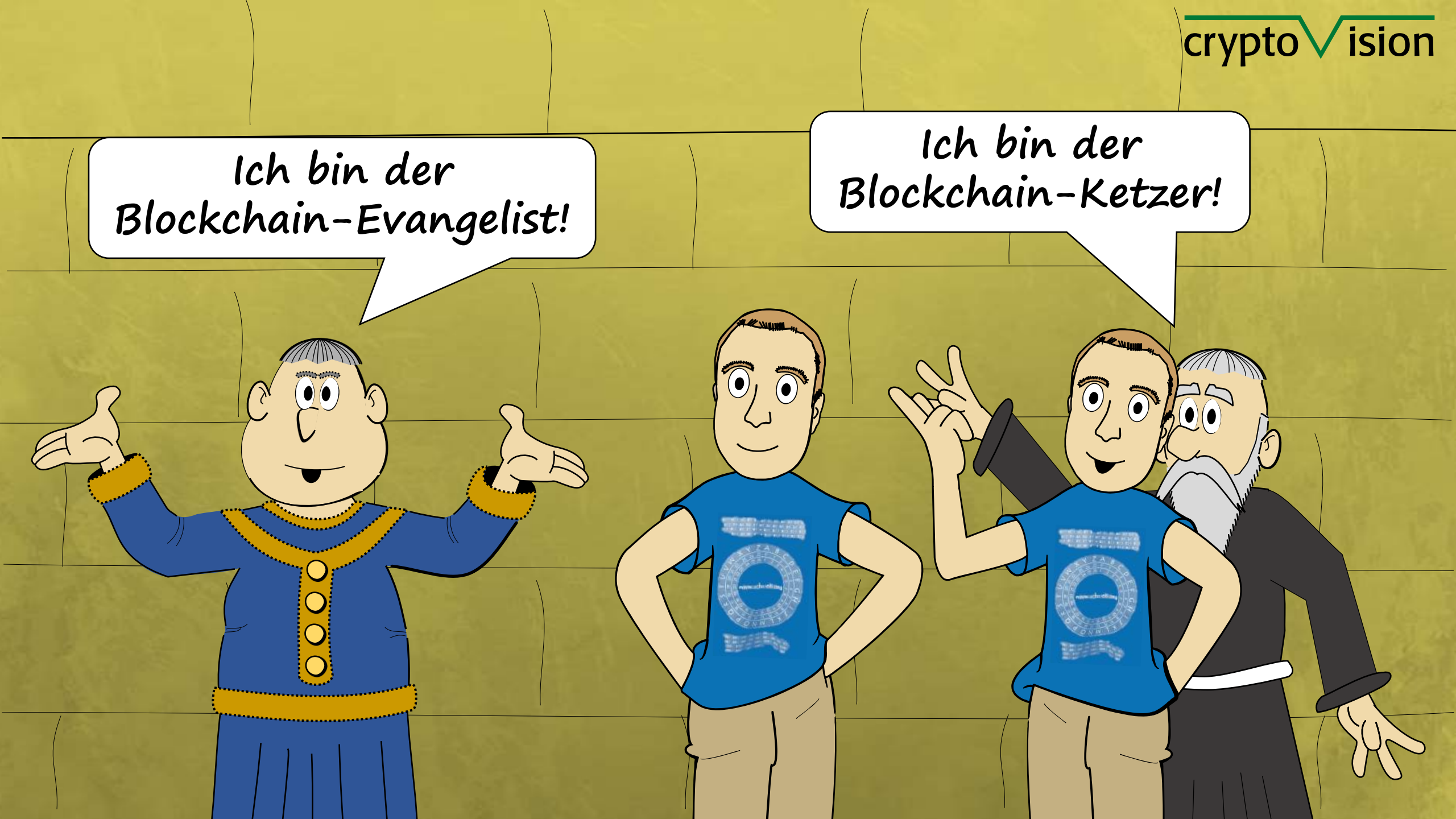

Chief Security Officer
by Klaus Schmeh
A US COMMITTEE HAS HIDDEN A MESSAGE IN A LETTER OF RESIGNATION TO DONALD TRUMP.
THE FIRST LETTERS OF EACH OF THE FIVE PARAGRAPHS COMBINE TO SPELL OUT "RESIST".
NICE STORY. BUT NOW, LET'S GET STARTED WITH OUR MEETING!
THANKS FOR PROVIDING THIS AGENDA!

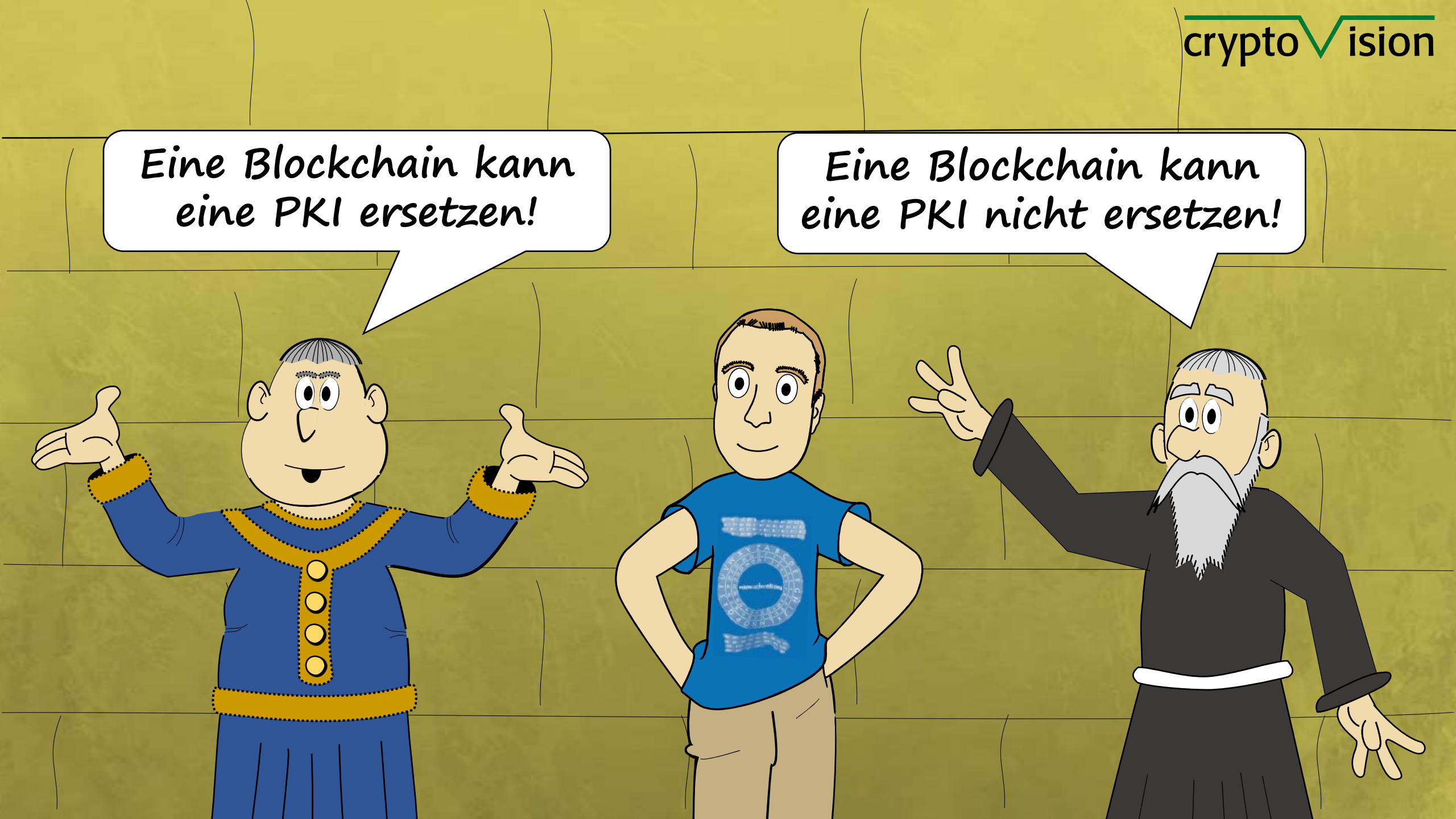

Klaus Schmeh
Chief Security Officer
EIN KOLLEGE MÖCHTE SEINE DIENST-E-MAILS GERNE AUF SEIN PRIVATES TABLET WEITERLEITEN LASSEN.
SO EIN TROTTEL!
SAG IHM, DASS WIR SO EINEN UNSINN AUF KEINEN FALL MACHEN. DAS VERSTÖSST MASSIV GEGEN UNSER SICHERHEITSKONZEPT.
DER KOLLEGE IST EIN VORSTANDSMITGLIED.
DANN SAG IHM: IST ÜBERHAUPT KEIN PROBLEM.
Band 1
BISHER IST IMMER ALLES IRGENDWIE GUTGEGANGEN


Chief Security Officer
by Klaus Schmeh
WHERE'S THE SHEET WITH THE MASTER PASSWORD?
IN THE SAFE.
AND WHERE'S THE COMBINATION FOR THE SAFE?
ON OUR ENCRYPTED DISK.
HOW CAN I DECRYPT OUR ENCRYPTED DISK?
WITH OUR MASTER PASSWORD.
THIS IS WHAT THEY CALL A CATCH-22.


cryptovision realisiert Public-Key-Infrastrukturen.
Wir werden oft nach der Blockchain gefragt.
Wirklich nutzen will sie aber bisher kaum jemand.


Zurück zur Frage ...
Blockchain: Tsunami oder Hype?

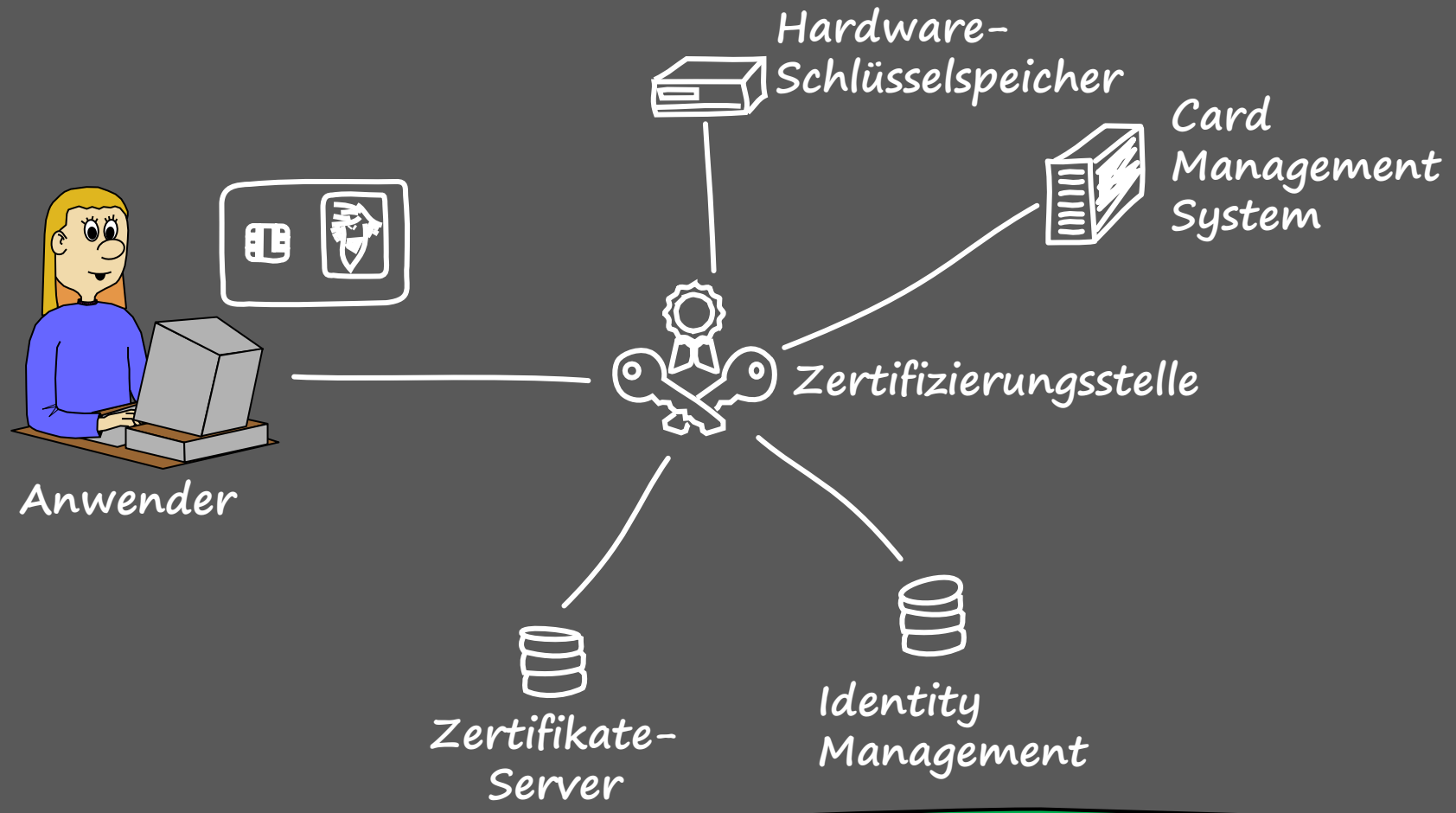

Ich bin der Blockchain-Evangelist!
Ich bin der Blockchain-Ketzer!

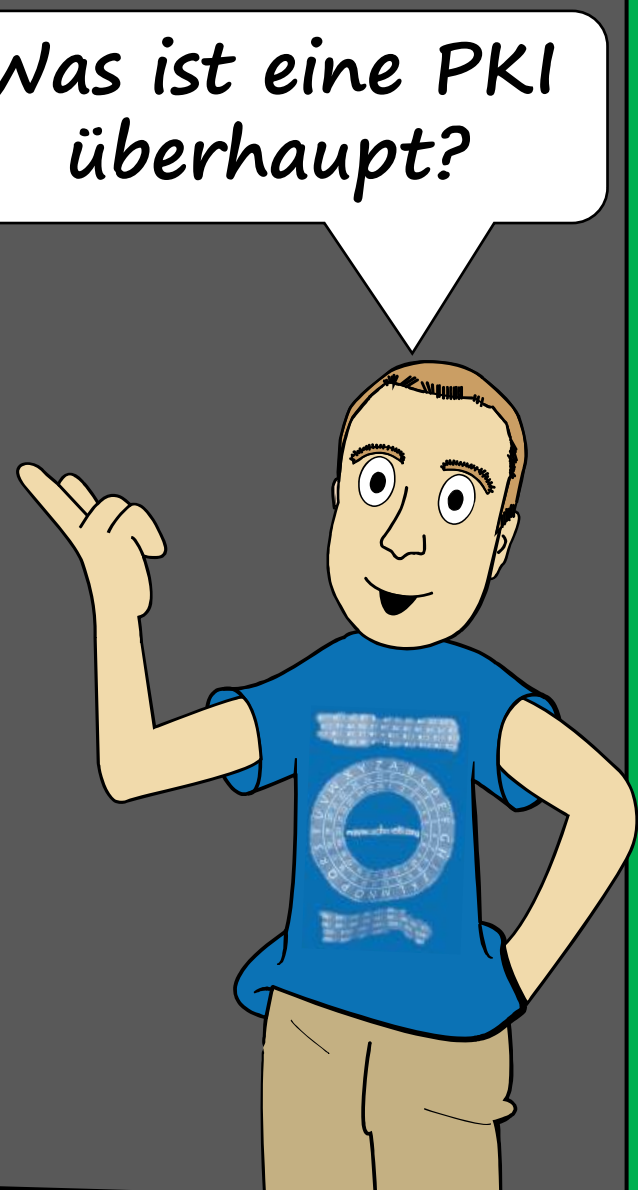

Eine Blockchain kann eine PKI ersetzen!
Eine Blockchain kann eine PKI nicht ersetzen!
cryptovision

Public-Key-Infrastruktur (PKI)

cryptovision

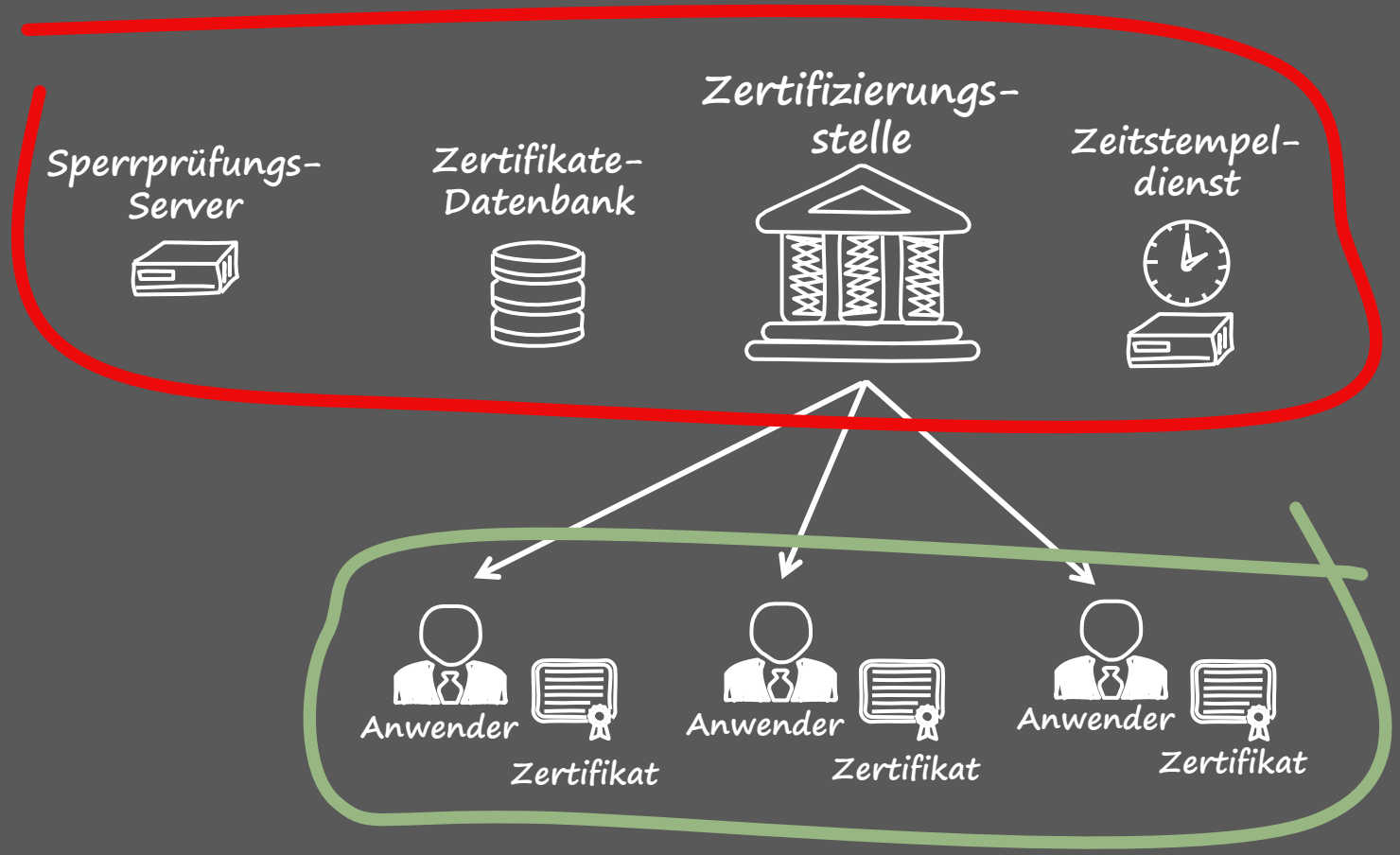
Infrastruktur für das Management digitaler Zertifikate

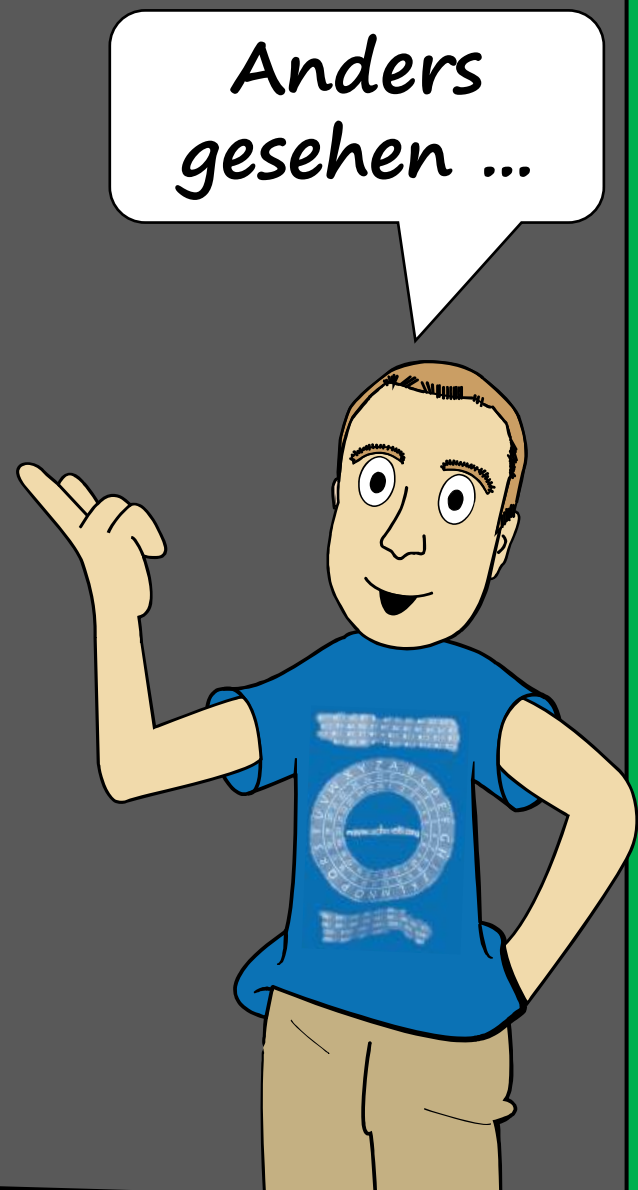




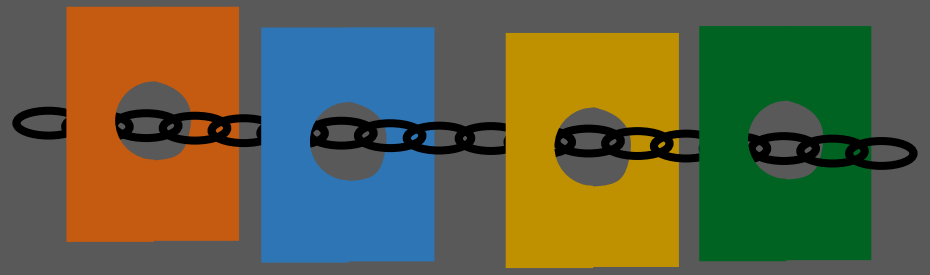
Public-Key-Infrastruktur (PKI)

Ansammlung von zentralen und dezentralen Komponenten



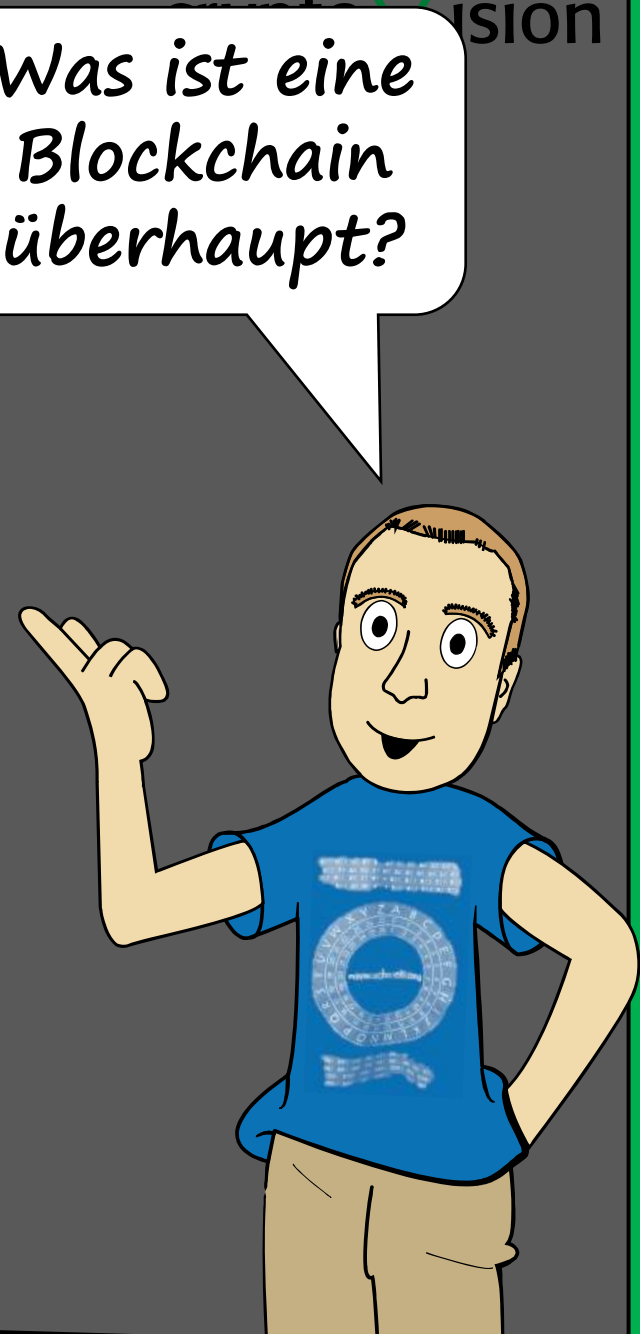


Blockchain



Einrichtung, die bestätigt, dass bestimmte Information zu bestimmtem Zeitpunkt vorlag

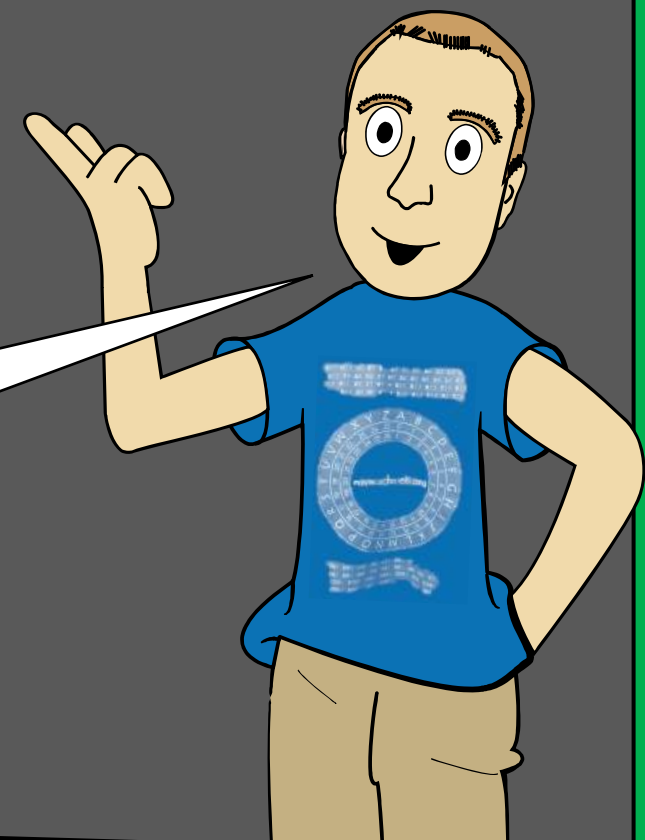
Kommt ohne zentrale Komponente aus!



Bitcoin: eine Blockchain-Anwendung

Information in der Blockchain: Geld-Transaktionen

Schauen wir uns eine Blockchain-Anwendung an.



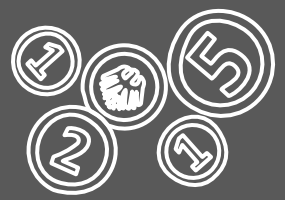
Verzicht auf zentrale Komponenten bedeutet: Niemand kann Geldmenge kontrollieren.

crypto Vision

Weitere Blockchain-Anwendungen

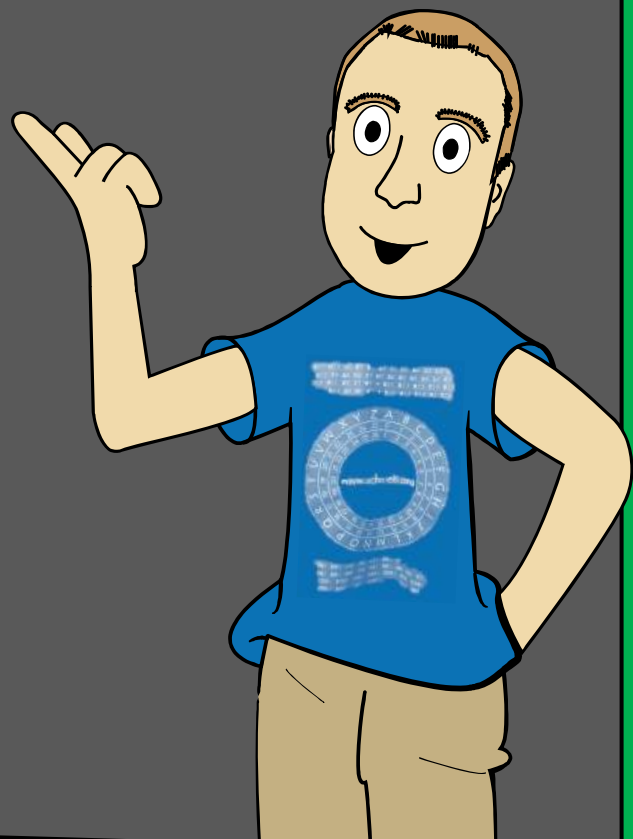
Blockchain ist mehr als BitCoin.

Payment



Smart Contracts

Identifizierung



ision

PKI

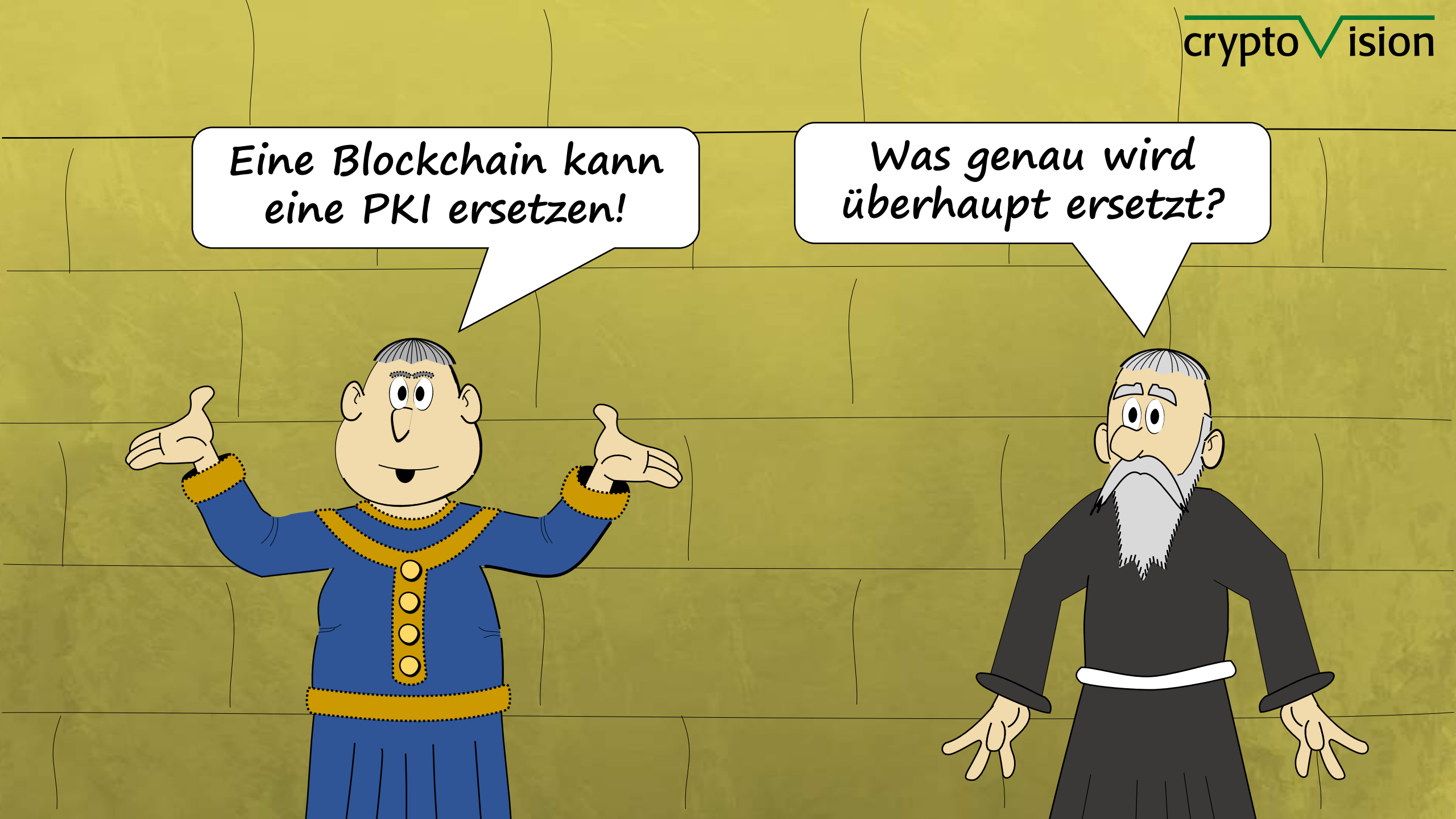
Hat mehrere zentrale Komponenten

Blockchain

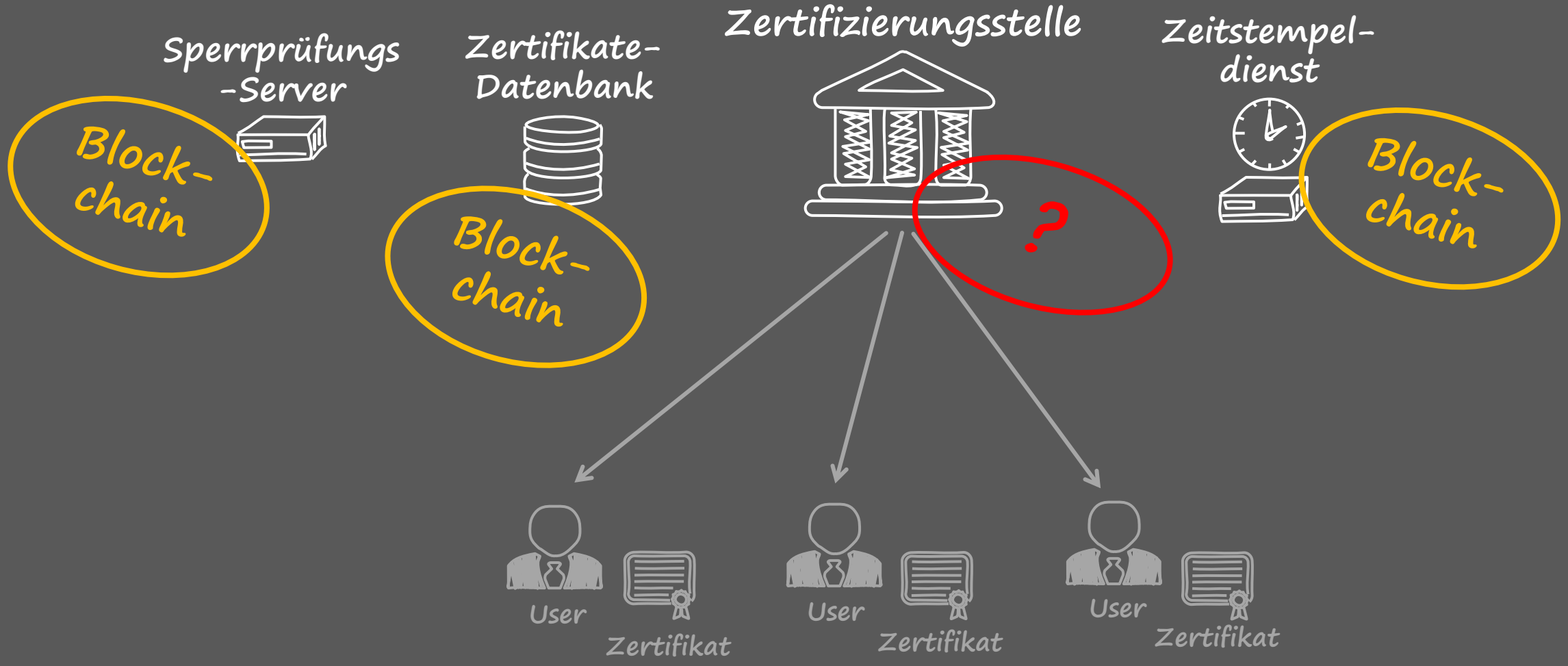
Kommt ohne zentrale Komponente aus

Eine PKI ohne zentrale Komponenten dank Blockchain?

Verzicht auf zentrale Komponenten bedeutet: Keine zentrale Kontrolle von Identitäten

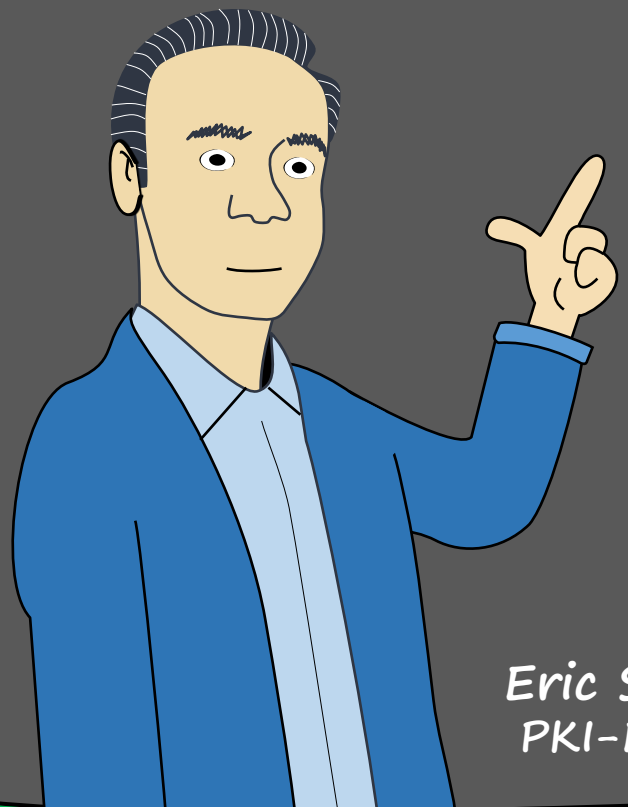

Eine Blockchain kann eine PKI ersetzen!
Was genau wird überhaupt ersetzt?
cryptoVision

Zentrale PKI-Komponenten



cryptovision

Blockchain wird PKI nicht ersetzen, sondern ergänzen!

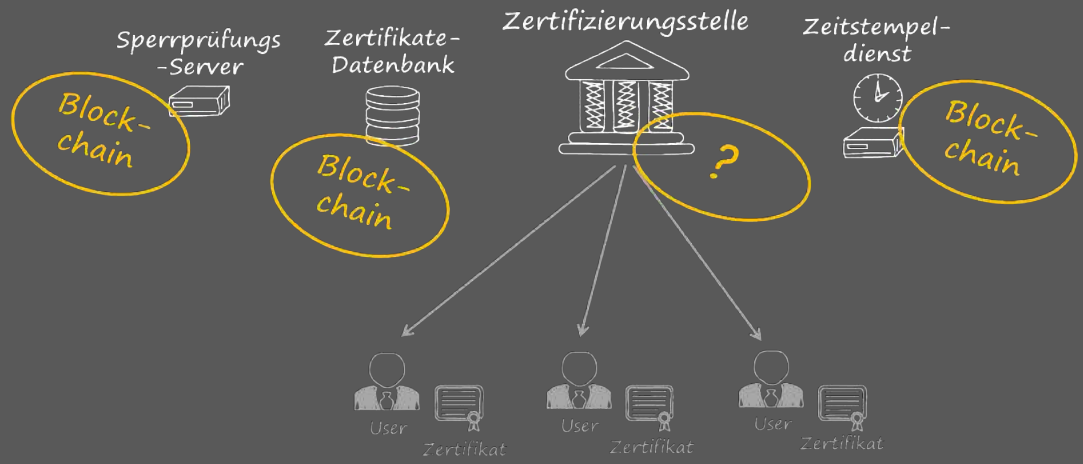


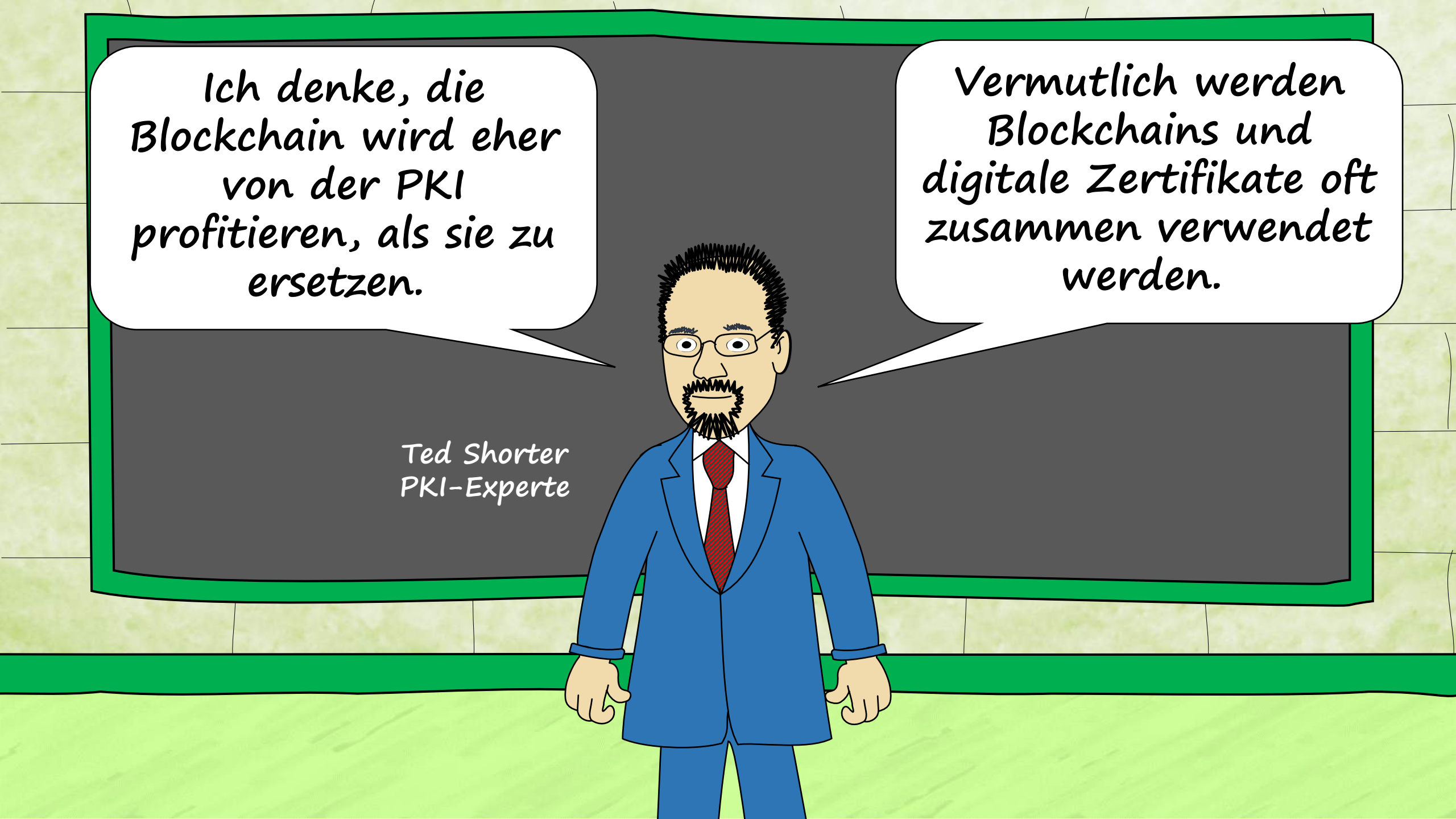
Eric Sharret
PKI-Experte

#1 Server-Zertifikate speichern

#2 Verteiltes Revocation Checking

#3 Zertifikate-Validierung



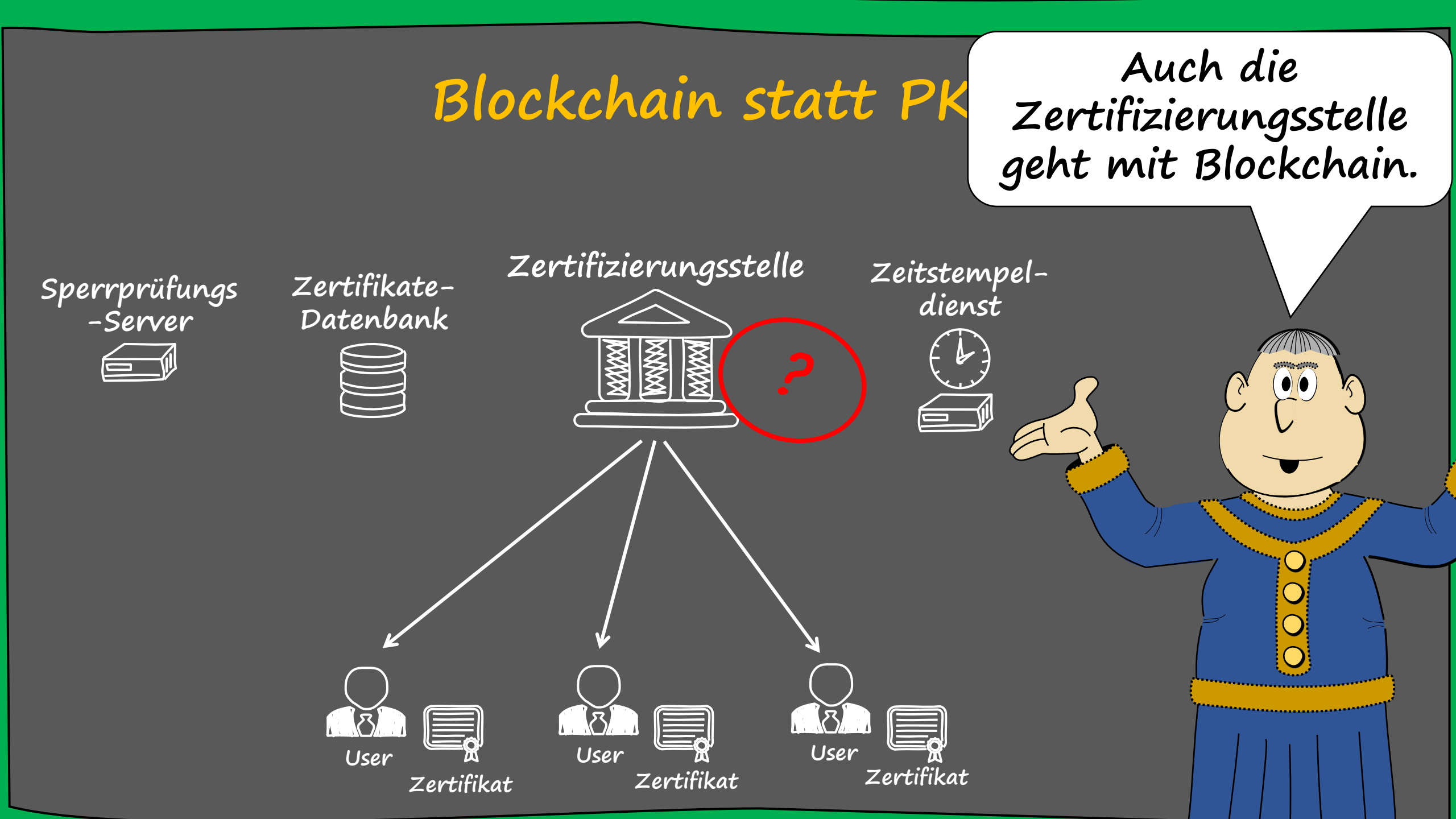

Ich denke, die Blockchain wird eher von der PKI profitieren, als sie zu ersetzen.
Vermutlich werden Blockchains und digitale Zertifikate oft zusammen verwendet werden.
Ted Shorter
PKI-Experte


Das sind vergiftete Komplimente.
Solange die Zertifizierungsstelle erhalten bleibt, ist eine PKI nicht wirklich Blockchain-basiert.

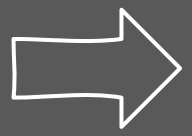

Stimmt, aber ...

Blockchain statt PKI

Auch die Zertifizierungsstelle geht mit Blockchain.

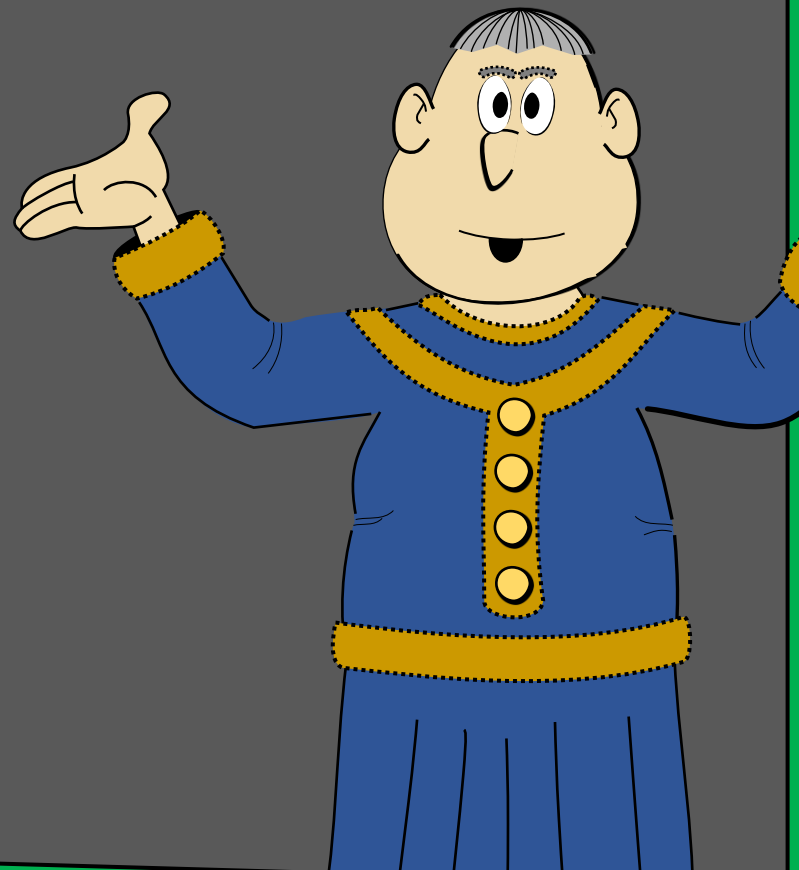


Zertifizierungsstelle



Zertifikat

Das, was ein Zertifizierungsstelle macht, kann die Blockchain auch.



Name

E-Mail-Addresse

Öffentlicher Schlüssel

Weitere Daten

Digitales Zertifikat
signiert durch Zertifizierungsstelle

Ein normales digitales Zertifikat!

Name

E-Mail-Addresse

Öffentlicher Schlüssel

Weitere Daten

In Blockchain geschrieben


cryptoVision
Und wer garantiert dafür, dass die Angaben im Zertifikat richtig sind?
Vermutlich keiner!
Das ist das Blockchain-Paradoxon.

Es gibt eben einen Unterschied zwischen Geld und PKI.

Blockchain-Paradoxon

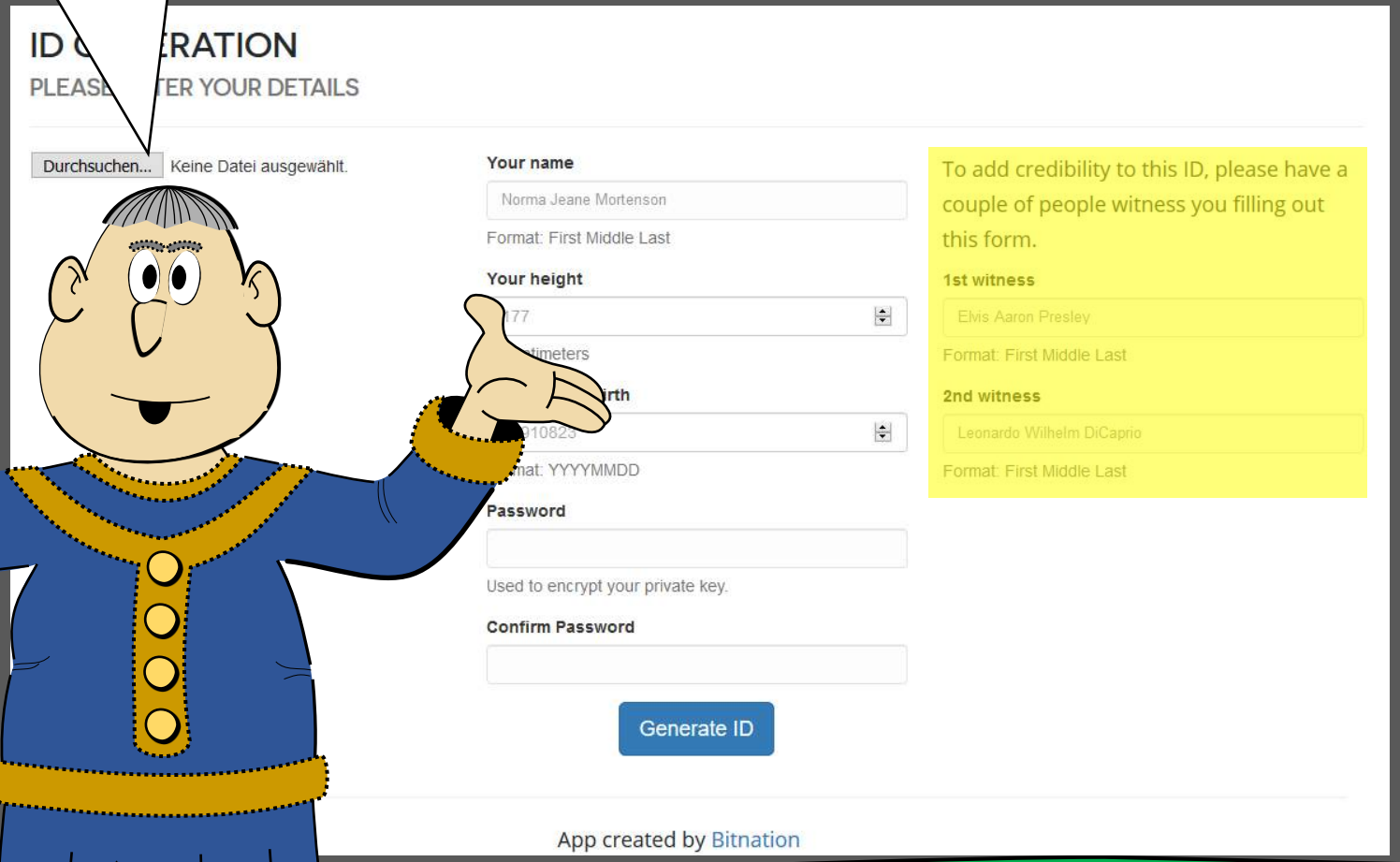
Jeder kann etwas in die Blockchain schreiben

=> zur Beglaubigung braucht man eine Zentralstelle

Eine Zentralstelle widerspricht der Idee einer Blockchain

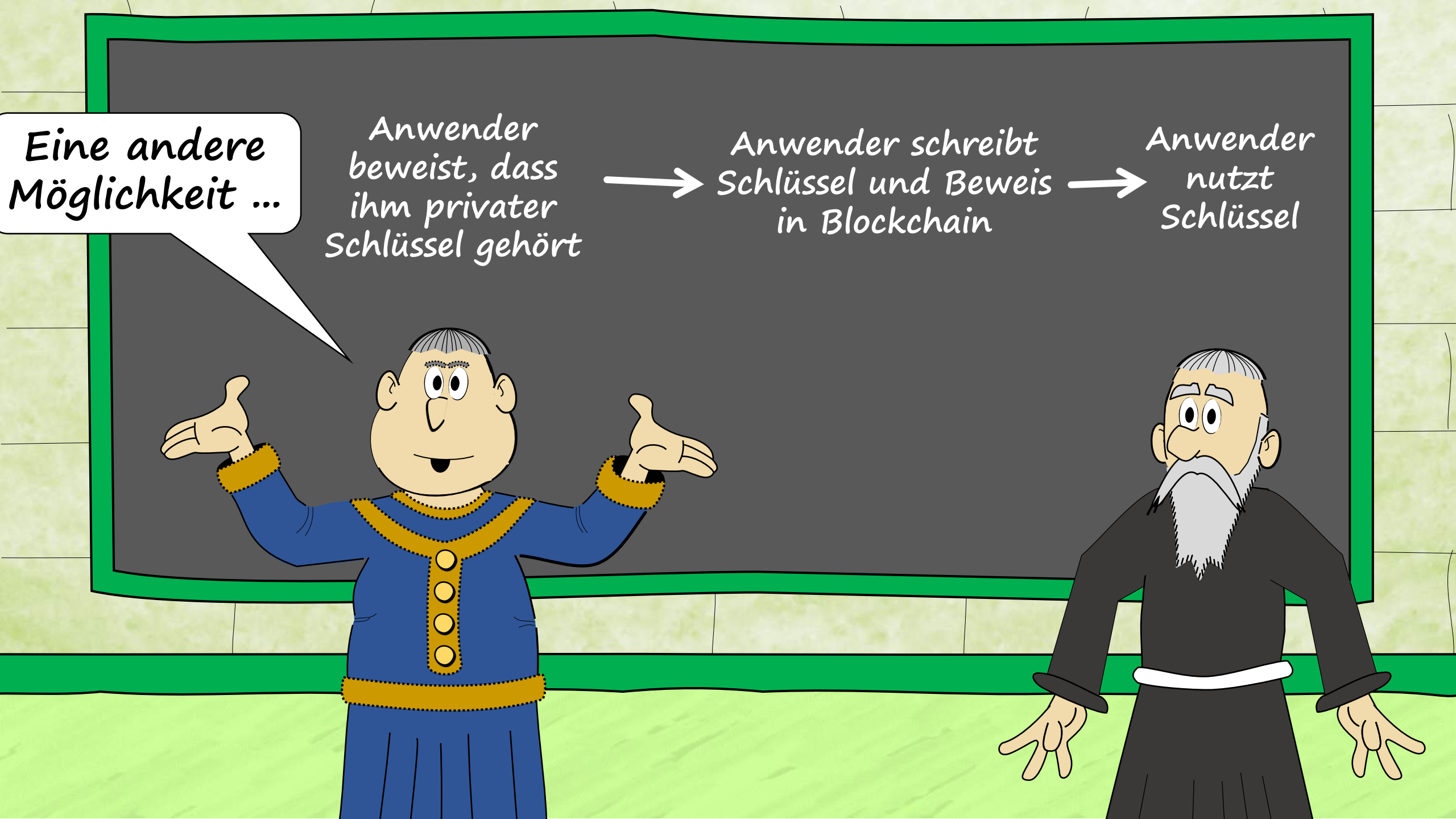

Blockchain-Paradoxon?
Dafür gibt es Lösungen.
cryptoVision

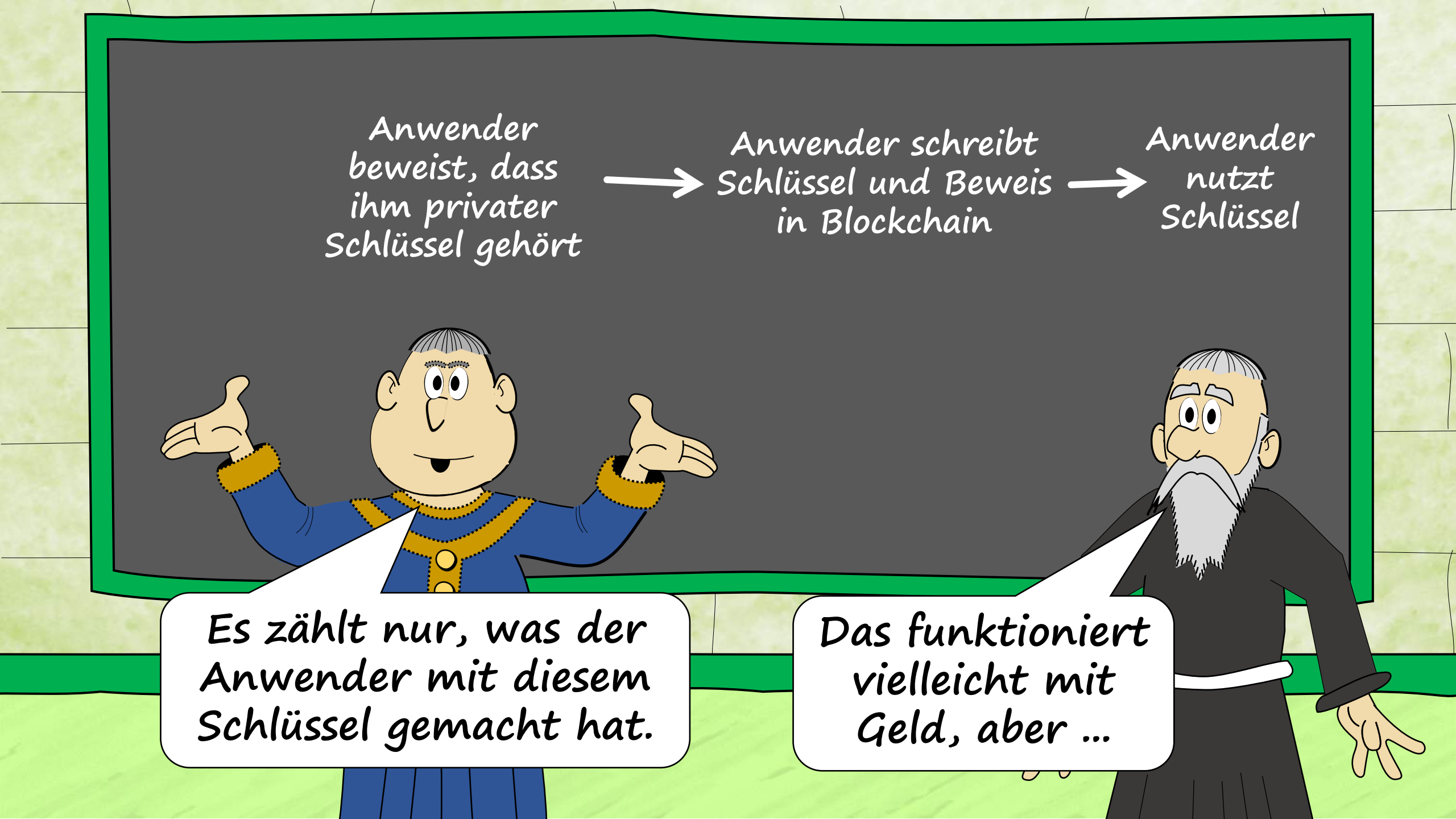
Zum Beispiel Bitnation.



Zwei Zeugen machen eine Identität?

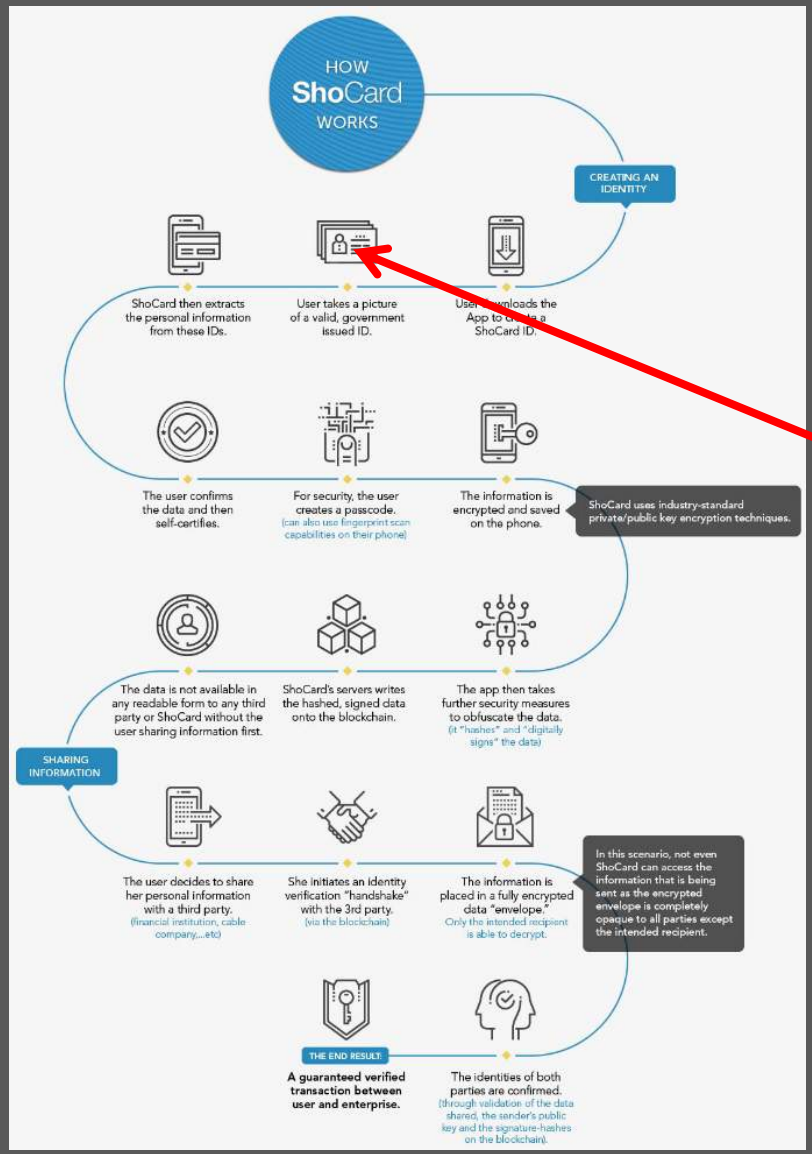
Juristisch ist das nicht wasserdicht.


Eine andere Möglichkeit ...
Anwender beweist, dass ihm privater Schlüssel gehört
Anwender schreibt Schlüssel und Beweis in Blockchain
Anwender nutzt Schlüssel

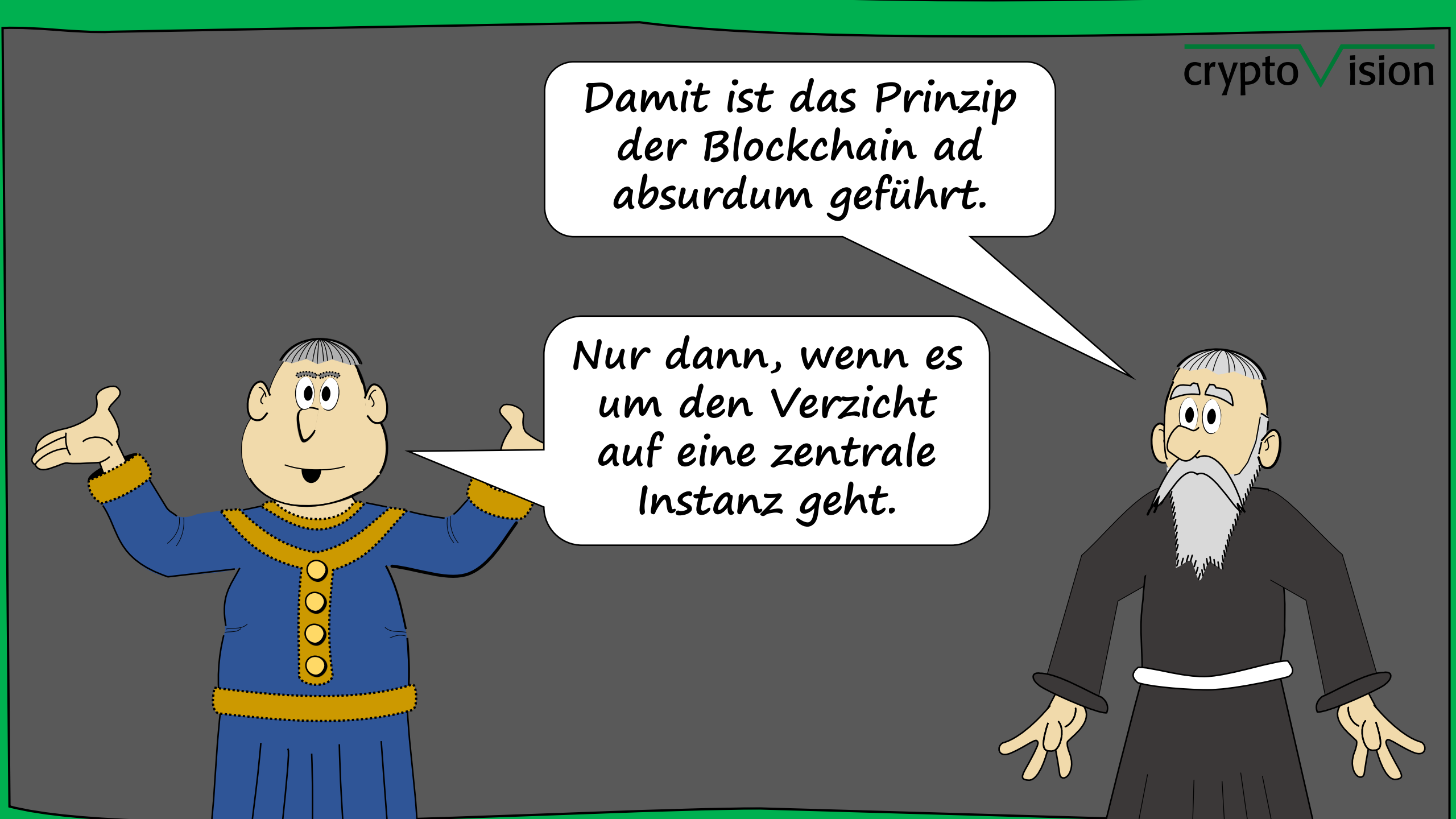

Anwender beweist, dass ihm privater Schlüssel gehört
Anwender schreibt Schlüssel und Beweis in Blockchain
Anwender nutzt Schlüssel
Es zählt nur, was der Anwender mit diesem Schlüssel gemacht hat.
Das funktioniert vielleicht mit Geld, aber ...

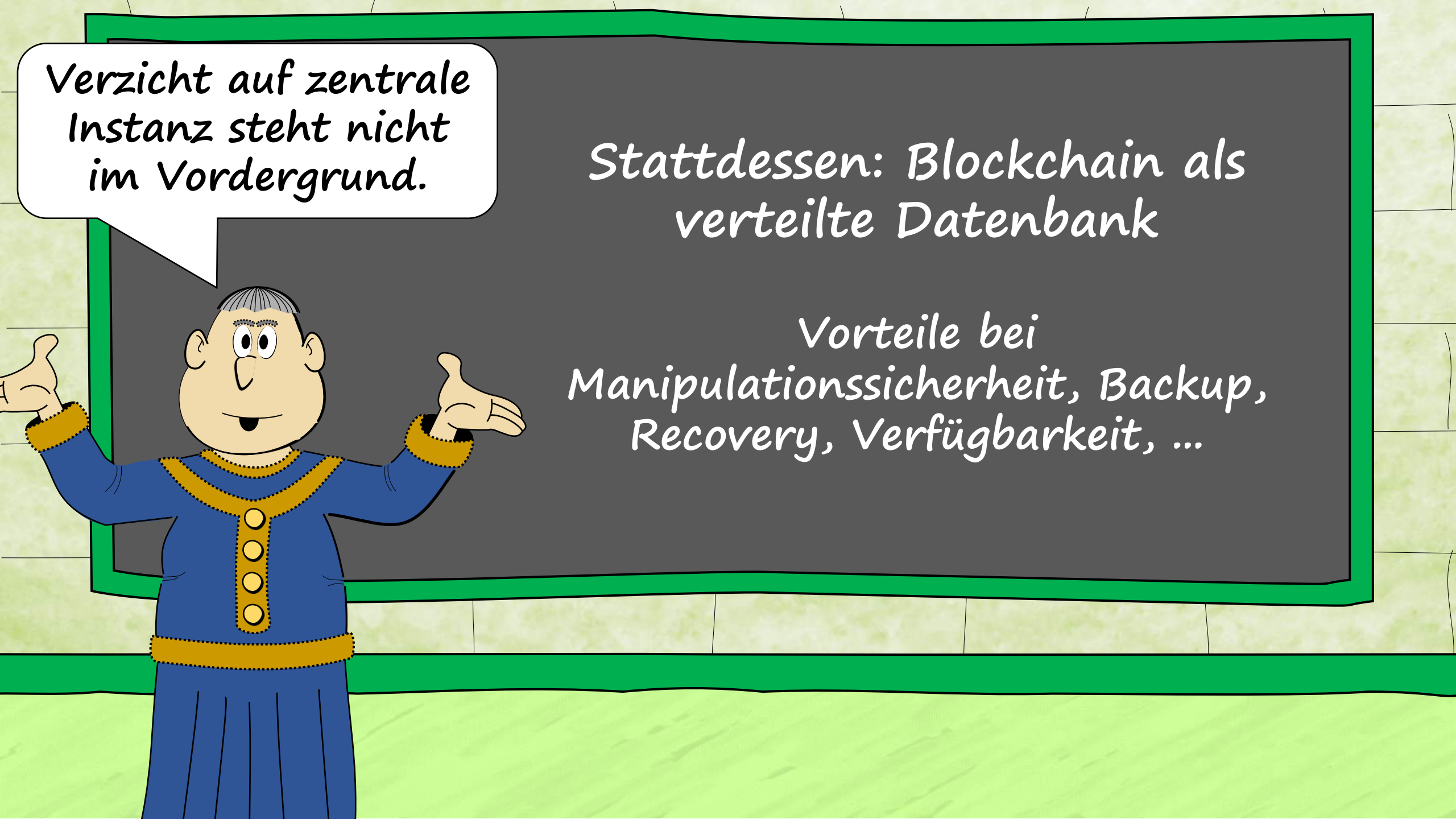

Wenn alle Stricke reißen, ...
... dann zieht man halt doch eine zentrale Instanz hinzu.

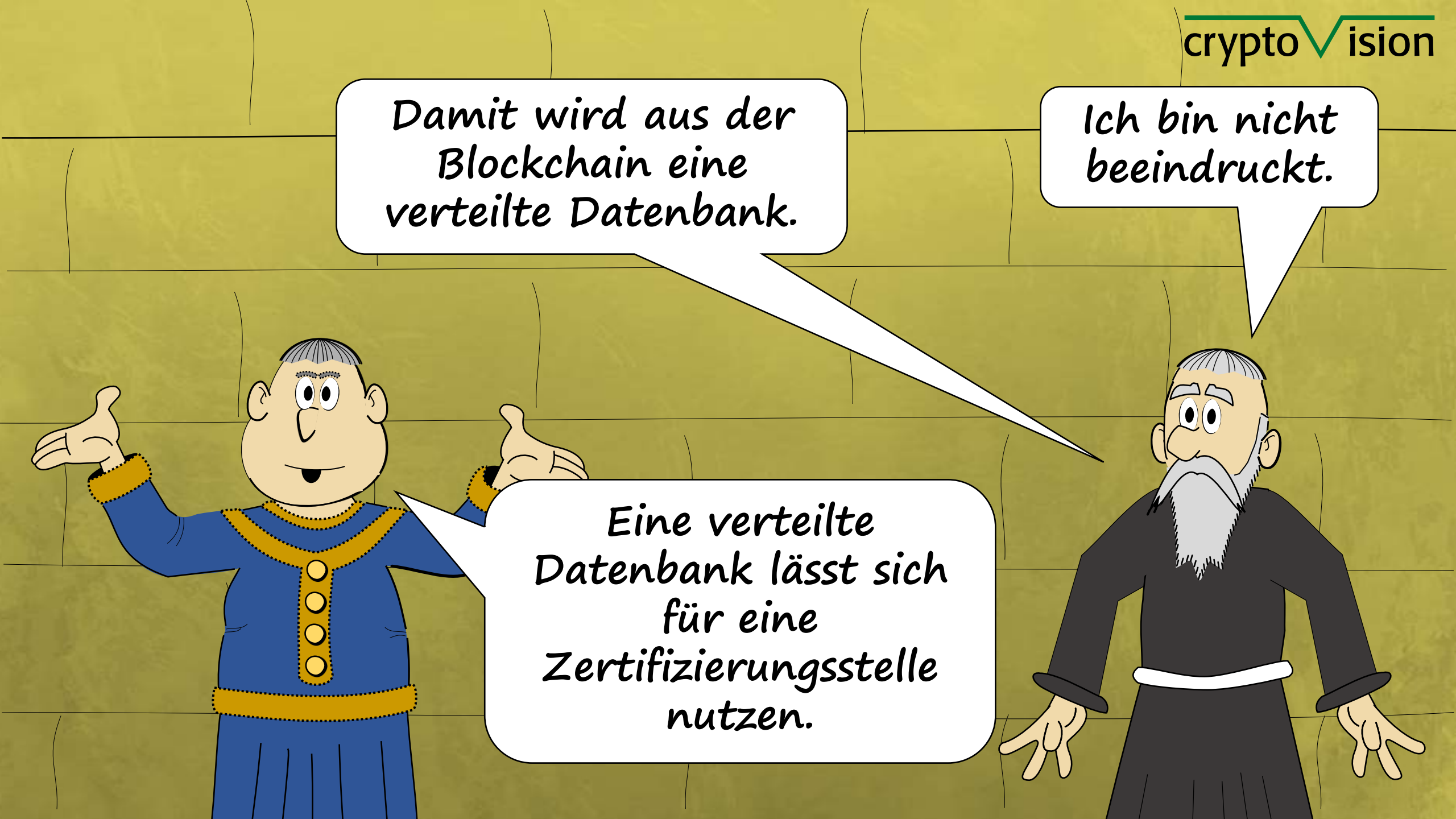
cryptovision

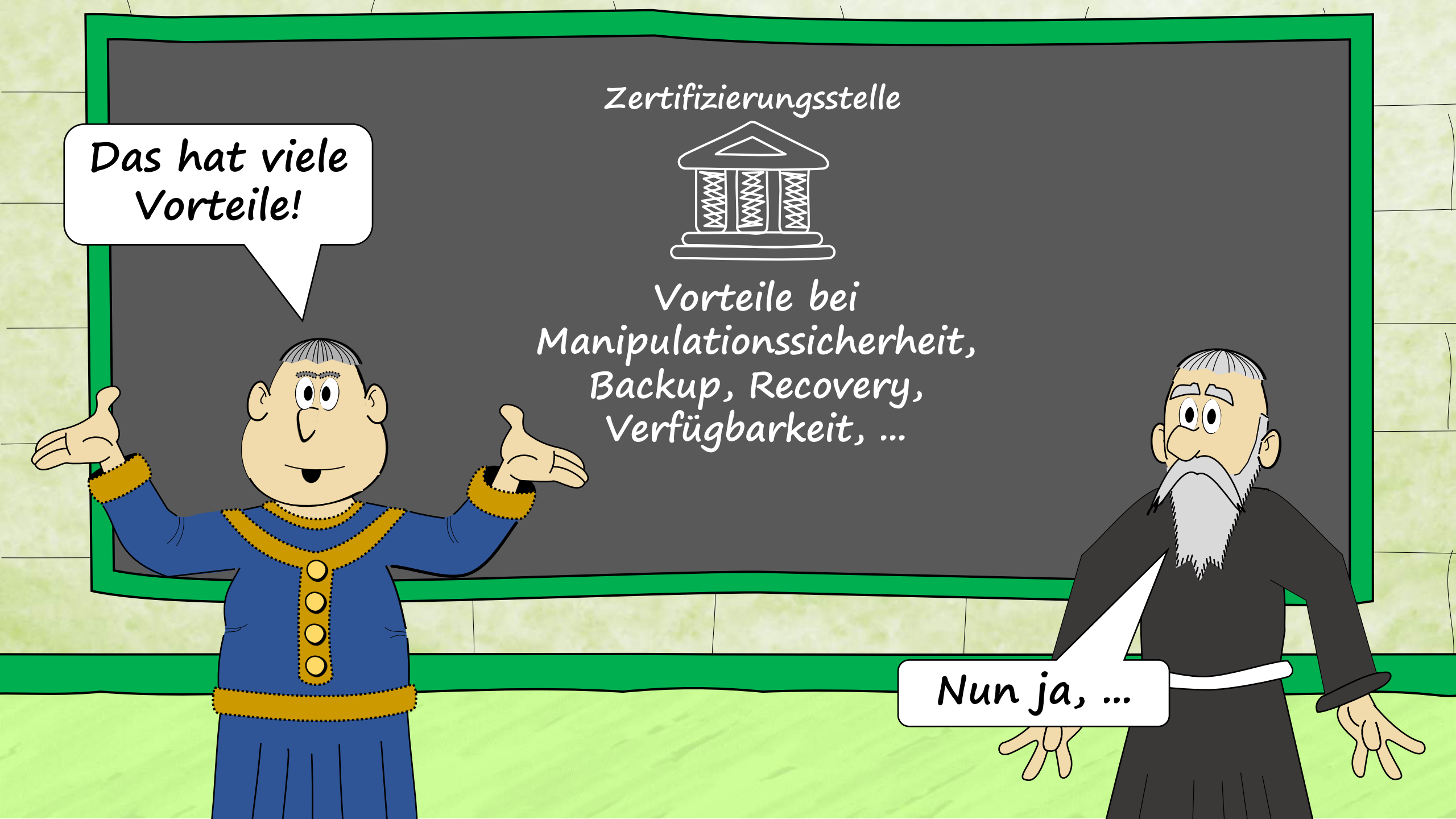


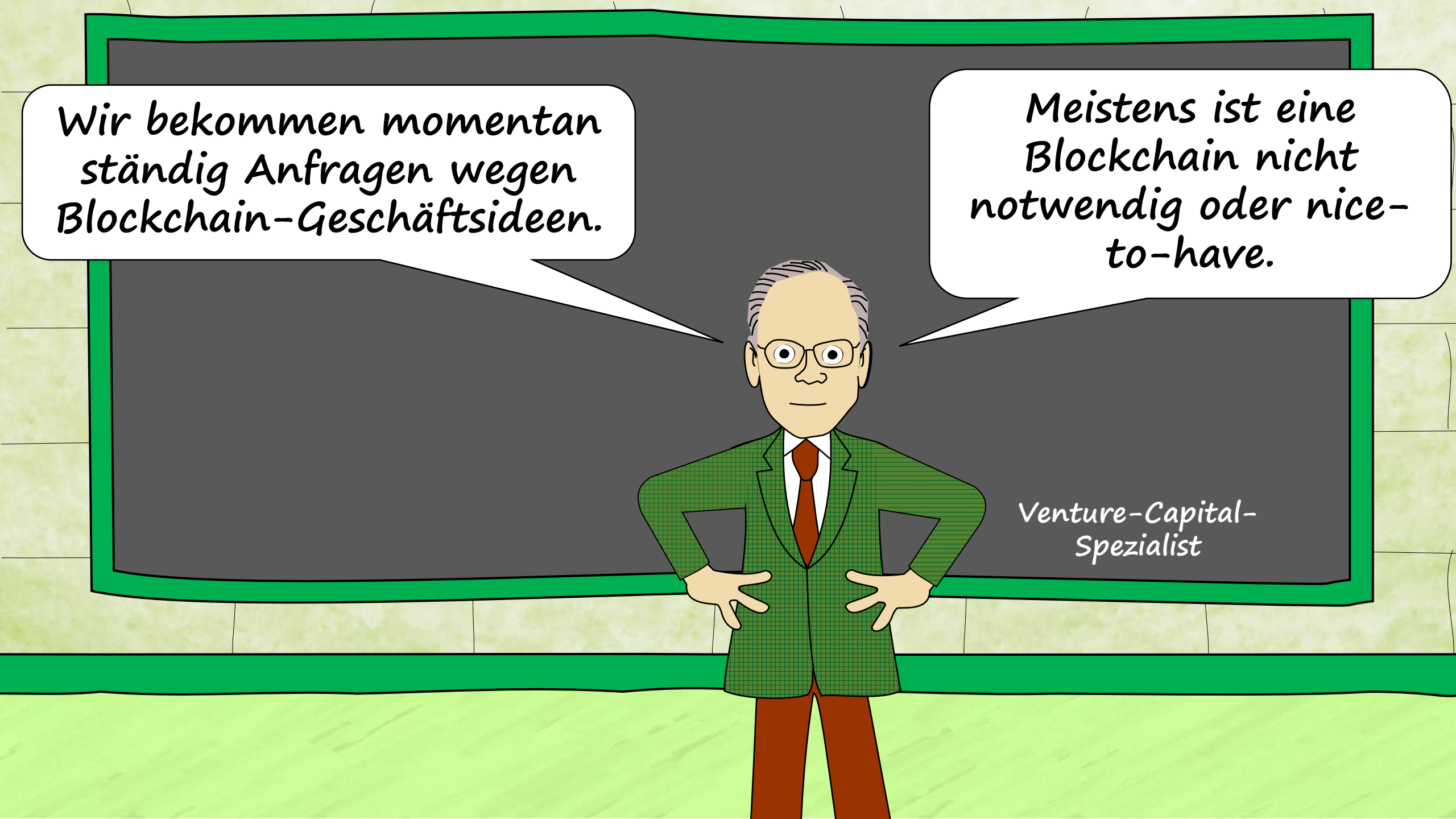
"valid government issued ID"

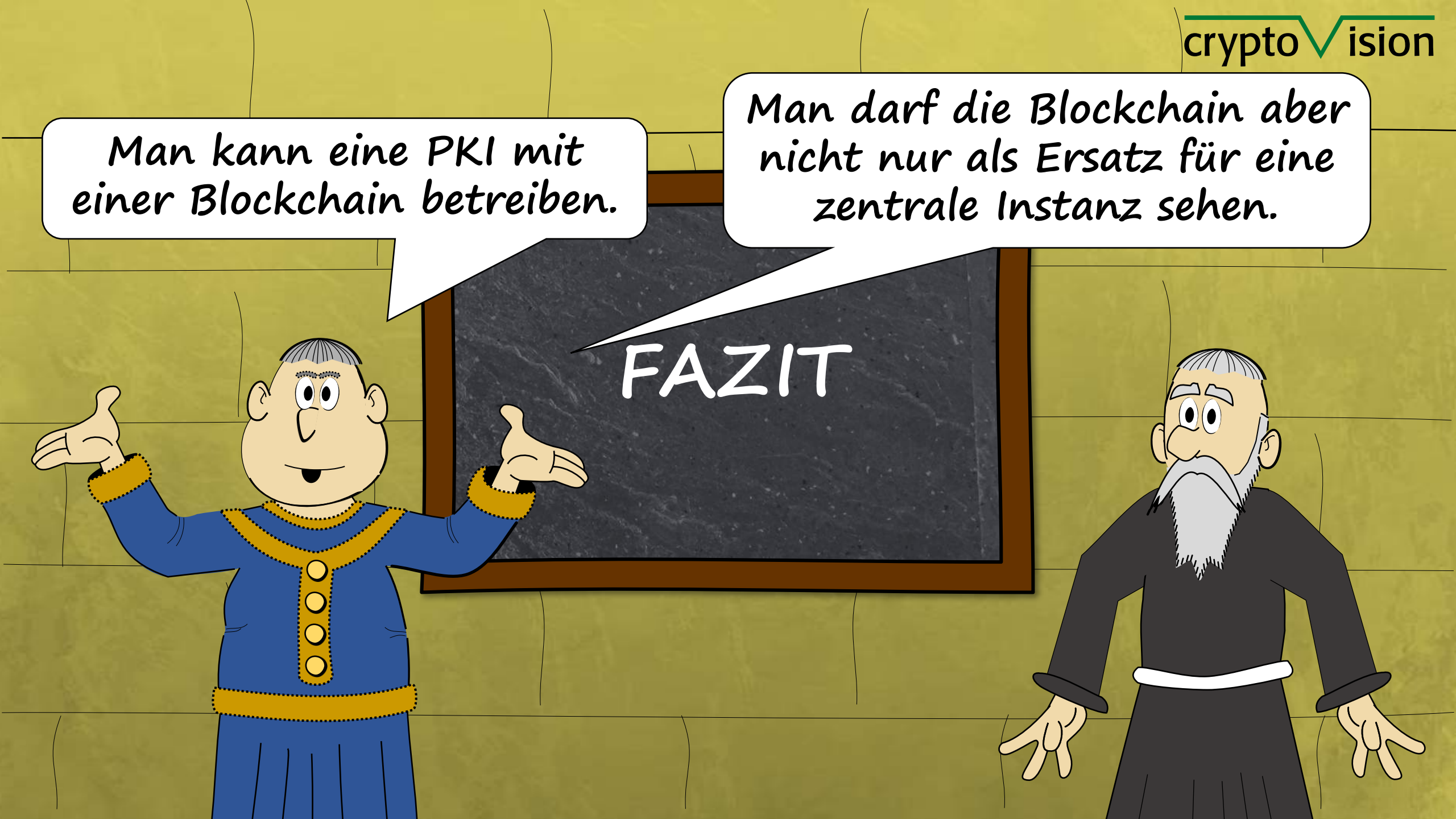

Damit ist das Prinzip der Blockchain ad absurdum geführt.
Nur dann, wenn es um den Verzicht auf eine zentrale Instanz geht.
cryptovision

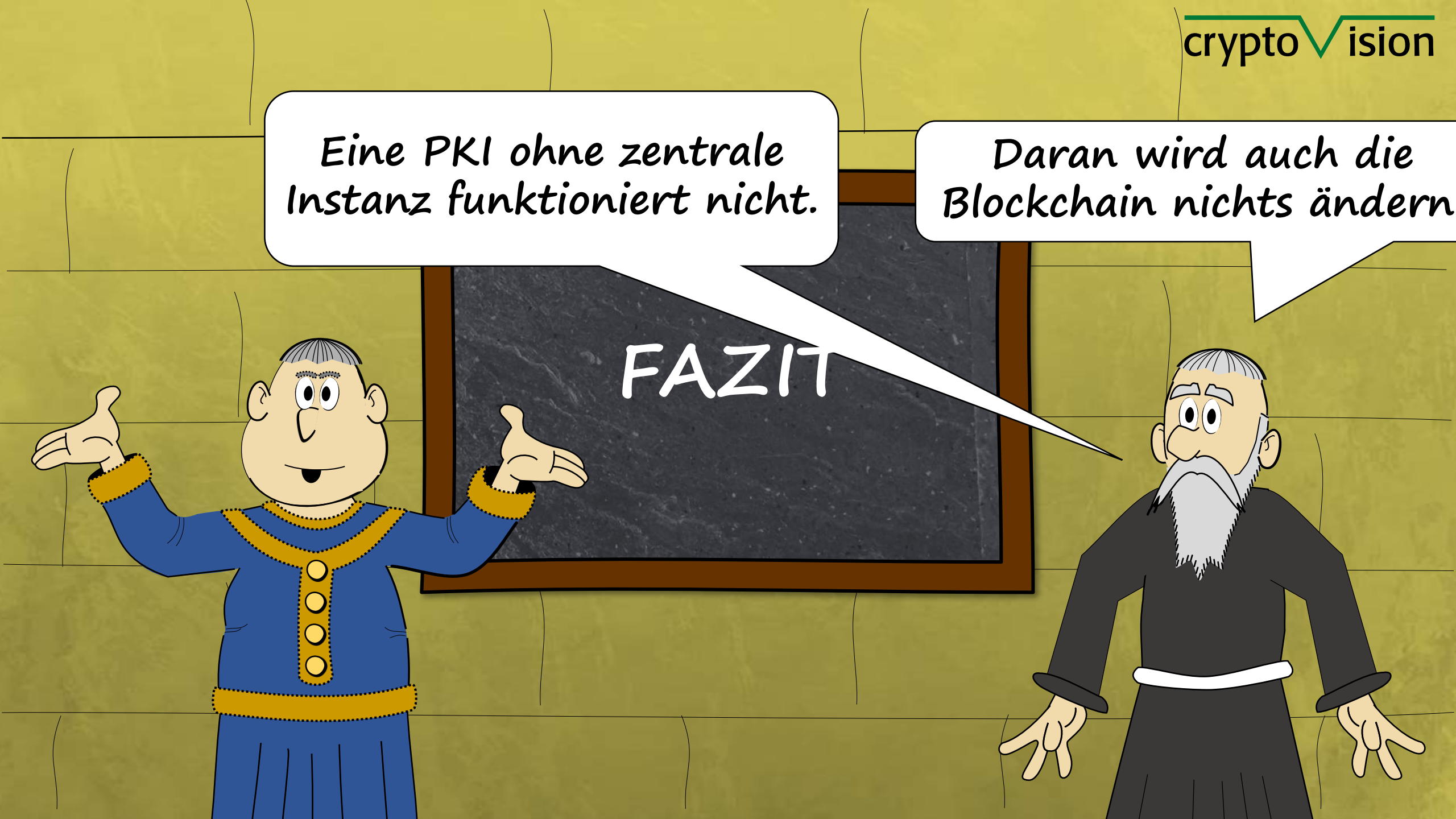

Verzicht auf zentrale Instanz steht nicht im Vordergrund.
Stattdessen: Blockchain als verteilte Datenbank
Vorteile bei Manipulationssicherheit, Backup, Recovery, Verfügbarkeit, ...


cryptoVision
Damit wird aus der Blockchain eine verteilte Datenbank.
Ich bin nicht beeindruckt.
Eine verteilte Datenbank lässt sich für eine Zertifizierungsstelle nutzen.


Zertifizierungsstelle
Vorteile bei Manipulationssicherheit, Backup, Recovery, Verfügbarkeit, ...
Das hat viele Vorteile!
Nun ja, ...

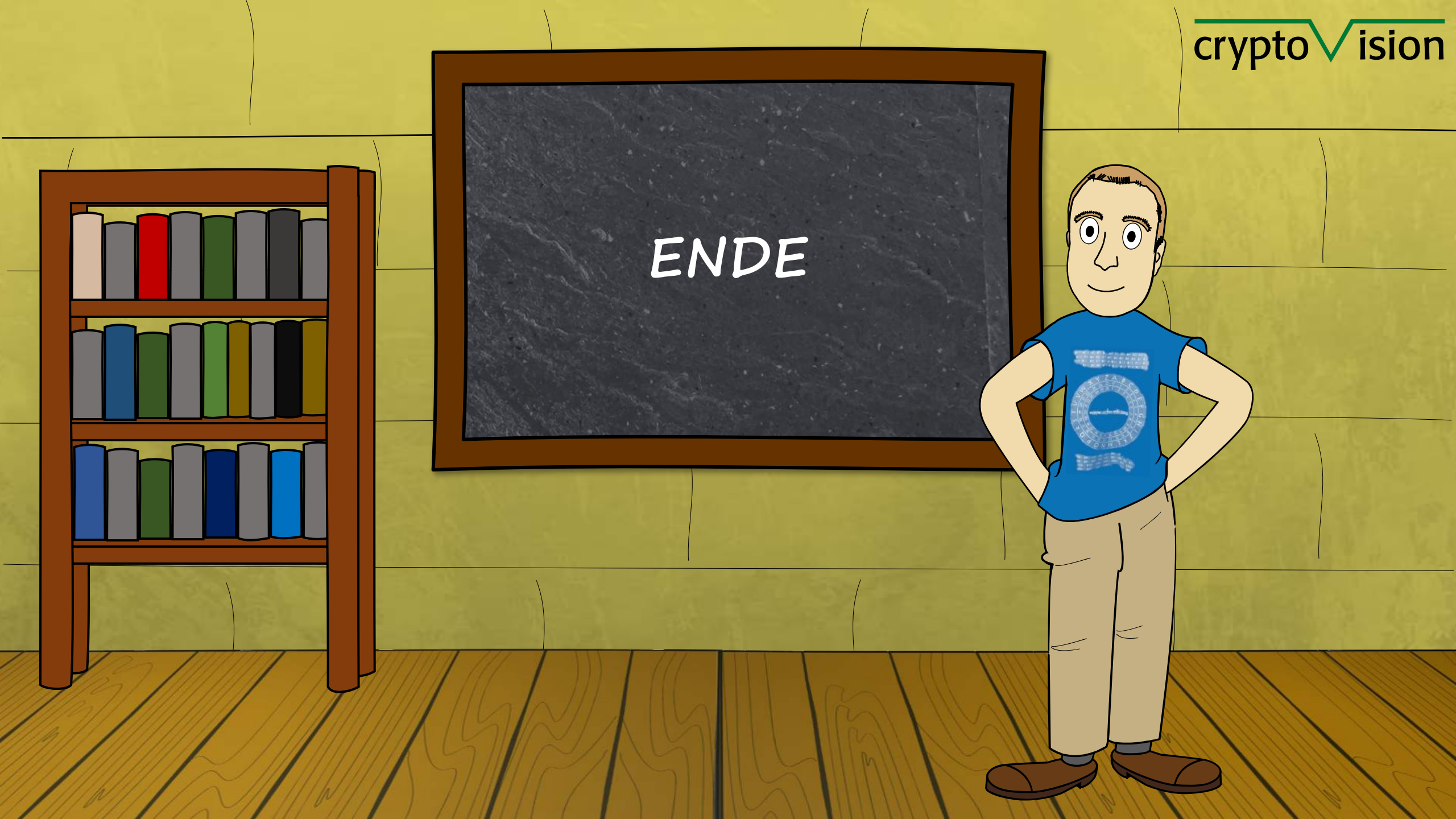

Wir bekommen momentan ständig Anfragen wegen Blockchain-Geschäftsideen.
Meistens ist eine Blockchain nicht notwendig oder nice-to-have.
Venture-Capital-Spezialist


cryptoVision
Man kann eine PKI mit einer Blockchain betreiben.
Man darf die Blockchain aber nicht nur als Ersatz für eine zentrale Instanz sehen.
FAZIT


cryptoVision
Eine PKI ohne zentrale Instanz funktioniert nicht.
Daran wird auch die Blockchain nichts ändern
FAZIT


Ich sehe die Blockchain nicht als vollständigen PKI-Ersatz.
Es gibt aber viele Einsatzmöglichkeiten für eine Blockchain in einer PKI.


Vielleicht ist die Frage falsch gestellt.
Sie müsste heißen: Kann man eine PKI mit einer Blockchain betreiben?
Antwort: Ja, aber man sollte keine Wunderdinge erwarten.
cryptovision


cryptovision
ENDE