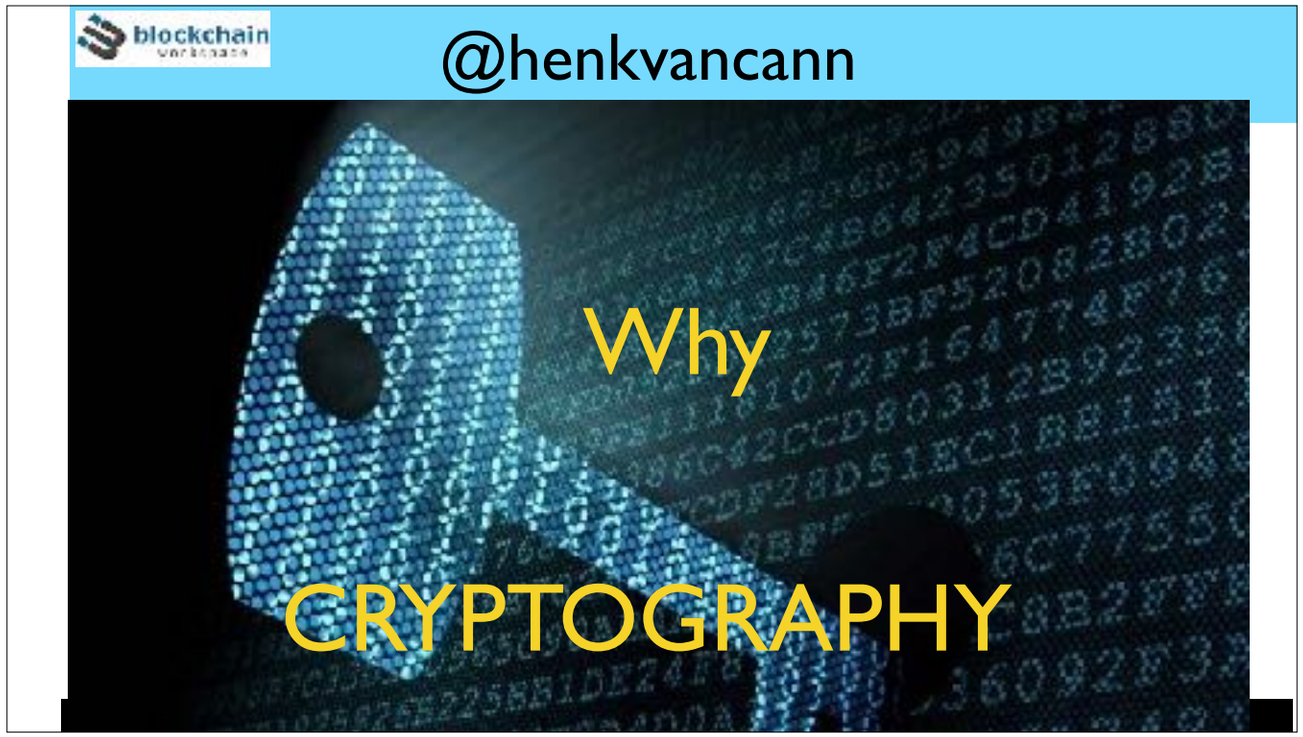
Safety is a feeling, security is U!

@henkvancann

Start learning: http://wiki.2value.nl/BCWS/meetup/study_more
<Who has any kind of crypto? >
<Who actually uses cold storage devices?>
<Who has inheritance protocols in place?>



The Crypto Anarchist Manifesto
Timothy C. May <tcmay@netcom.com>

“A specter is haunting the modern world, the specter of crypto anarchy.”

Previous Episodes

Never ever forget about…

- The beauty of hashes!

- Only pointers on the blockchain!

WHY is this preparatory knowledge important? -> Keys/signatures point to something too! (Moneybox example)

Previous Episode

Never ever forget about…

The beauty of hashes!

Blockchain - Verify proofs

Block 210000 July 2nd 2016 (1Megabyte)

000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e

NOW!

000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e

How we use Hashes

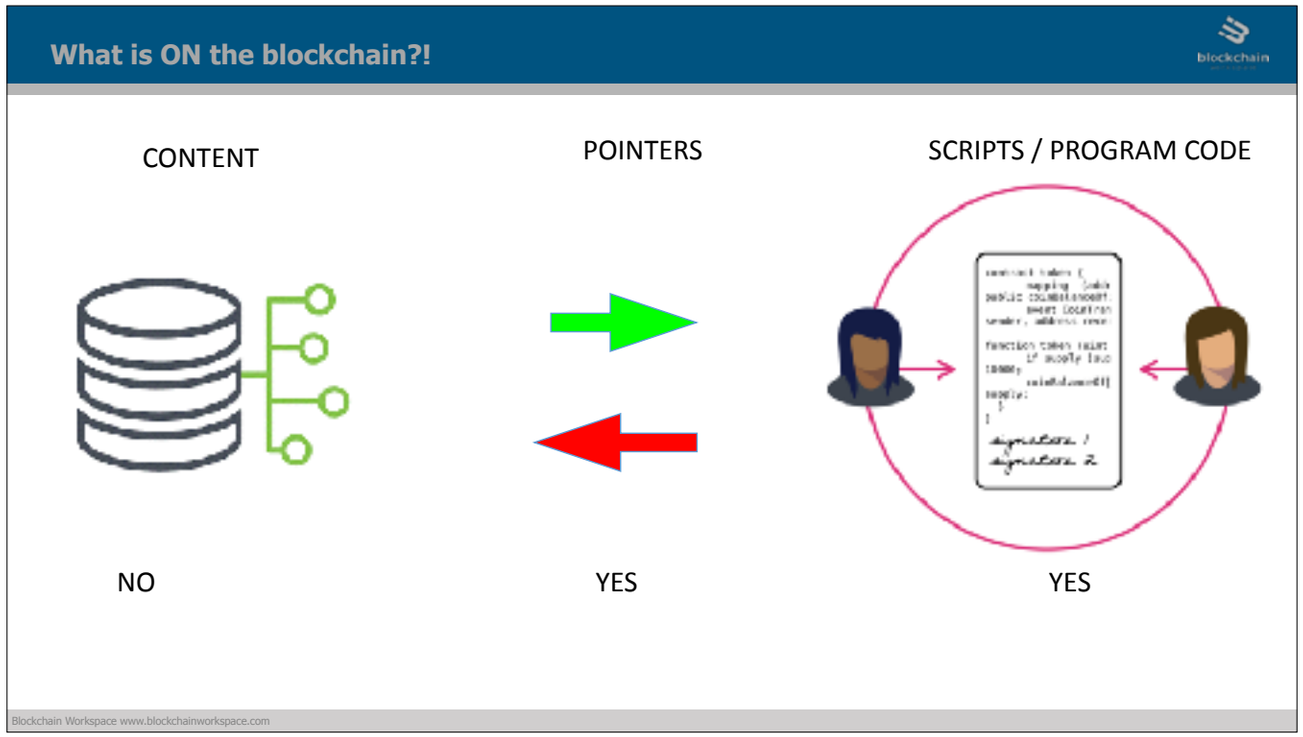
000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e Block 210000 July 2nd 2016 (starting with 13 zeros)

Question: Number of leading zeros increases! (2009 10, 2016 13, 2018 18), why is that?!
0000000000000000002f215bdc88c918a39f36002b2237a0f8fd57a9198fae7f Block 513158 (starting with 18 zeros)

Never ever forget…

Only pointers on the blockchain!

Previous Episode



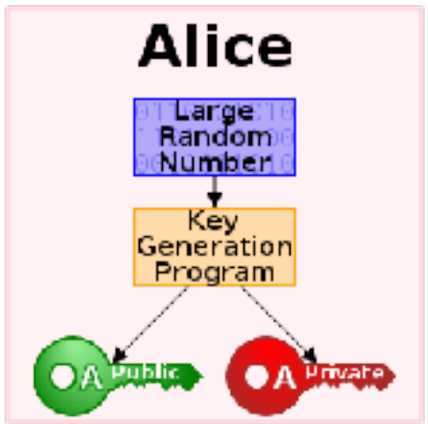
Picture of CODE: https://www.coindesk.com/information/ethereum-smart-contracts-work/
CODE spread out over many computers, transparent, open source, immutable, etc.
SCRIPTS as (optional) parts of the protocol

WHY is this preparatory knowledge important? -> Keys/signatures point to something too! (Moneybox example)

ECDSA = Elliptic Curve Digital Signature Algorithm
Economic Incentives versus Distributed / Decentralized consensus: it costs more than its return, the risk is too high to lose more than you might profit

but WE ACCEPT a certain technical chance that it happens, based on it's assessed likelihood and impact (what's at stake? and what's the probability)
WHY do I say this? To anticipate the Quantum Computing FUD storm
Is our feeling of vulnerability justified?! Are we really in danger while trying to cling to our crypto value? And if so, how can we better prepare, better assurance, and start developing an automatism in protecting ourselves?

Public Private Key-pairs



As boring as batshit!

Source: https://en.wikipedia.org/wiki/Public-key_cryptography

One way! Private to public
One way? Quantum computing…
DANGER FROM THE OUTSIDE?!

<Connect: Who has > <How can that be… we have {any crazy amount} of dollars of value represented in the room?>

<safety bar versus safety belt in a cart of the Python (a looping) in the Efteling adventure-park, my father desperately seeking the belt while the bar's already there; panicing, tormented face and automatism.>
<floorwork: quadrant IN/OUT - Real/Unreal Threads versus feeling Safe/in danger>
Suddenly 'we'…., why?
Inheritance, succession, organisations! -> DANGER FROM THE INSIDE

Fear, Uncertainty & Doubt (FUD)

JUSTIFIED?!

<ask for recent examples of FUD>
Is it justified to feel in danger to feel vulnerable? In most cases ‘no’
<analogy: game in the dark, one or more the opponents might have night vision glasses… >
What can you do? Study <learn to handle the night camera>, <protect yourself>
…and more over it might divert our attention….

Lots of FUD around crypto value

NIETZSCHE?:

“Man often suffers most
From the sufferings he fears
But never will occur.
So he will have more to bear
Than God gives to bear.”

THIS DOES NOT EXIST

ANTONOPOULOS:
There is no ‘mining’
There is no ‘bit’
There is no ‘coin’
There is no ‘address’ or ‘account’
There is no ‘**wallet**’
There is no ‘transaction’

These names serve as a bridge between old world new world. They enhance understanding, foothold and assurance: “Oooh, it’s a sort of gold coin, that ends in my wallet by a global transaction”…

Is this only positive? No, because it might introduce a dangerous feeling of security -> Wallet
Is our feeling of safety justified?!

What do most relevant crypto keys LOOK LIKE?

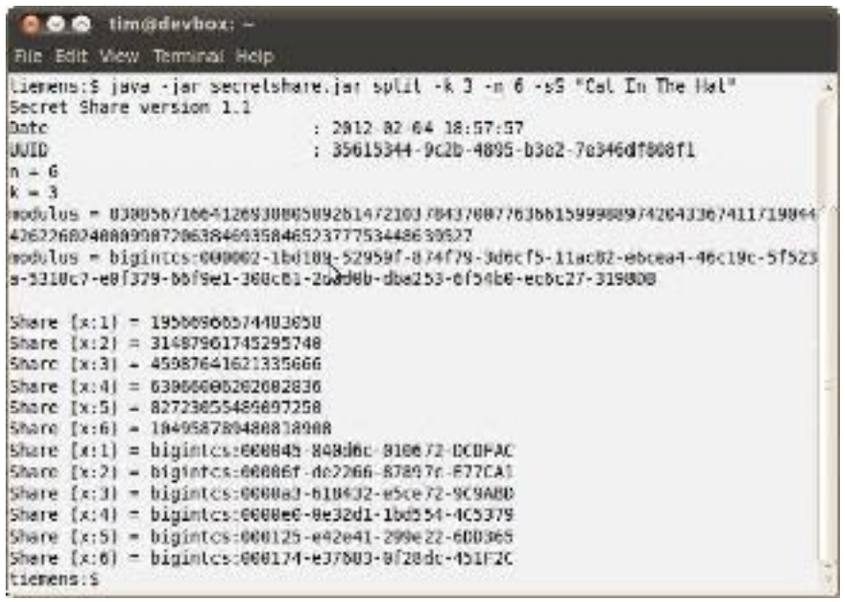
- Strong passwords: **2kWqP2AKQqVaiv]Pykk;**
- Seeds 12 words, 24 words, 25 words
- Hexadecimal strings
- QR codes

(we focus on control and private keys)
Strong passwords first : generated from and stored in a Password Manager.

What do most relevant crypto keys LOOK LIKE?

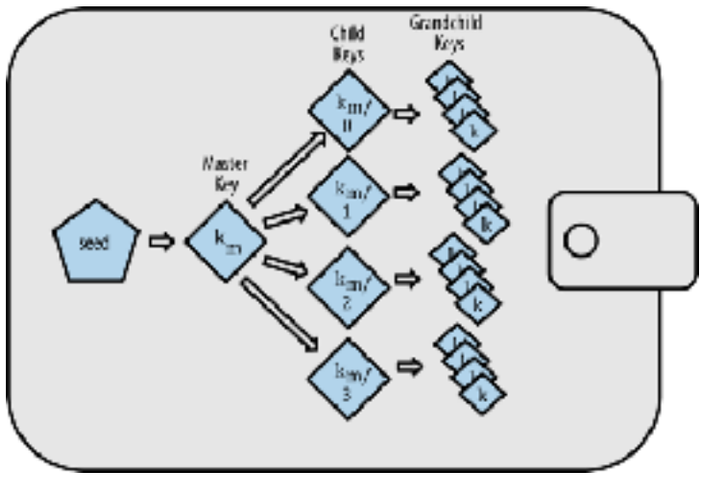
- **Shamirs**
- **Secret**
- **Sharing**
- **Scheme**

- K subkeys needed
- out of N subkeys



Inheritance > sort of ‘treasure map’ solution: 3 (remaining) people can form a group to find the private master key.

Hierarchical Deterministic Keychains



Source: http://nakamotoinstitute.org/bitcoin/#selection-229.4-232.0

<take out keychain>

A bitcoin address is in fact the hash of a ECDSA public key, BASE58 encoded

BIP0032
https://bitcoinmagazine.com/articles/deterministic-wallets-advantages-flaw-1385450276/

Should be unidirectional, point “backwards” only if you want and in a controlled way!

Vitalik Buterin 2013 (18 yrs old):
The problem is this: although you certainly can securely hand out child keys with no risk to the parent key, and you can hand out master public keys with no risk to the master private key, you cannot do both at the same time.

Solution : a. Don’t hand out master public key
b. making three hierarchical BIP32 wallets, with every address being a 2-of-3 multisignature address between the three wallets down some particular child key derivation path

“

Examples of protocols using asymmetric key algorithms

- S/MIME
- GPG, an implementation of OpenPGP
- Internet Key Exchange
- PGP
- ZRTP, a secure VoIP protocol
- Secure Socket Layer, now codified as the IETF standard Transport Layer Security (TLS)
- SILC
- SSH
- **Bitcoin**
- Off-the-Record Messaging

Source: https://en.wikipedia.org/wiki/Public-key_cryptography

Examples of protocols using asymmetric key algorithms

Examples of well-regarded asymmetric key techniques

- Diffie–Hellman key exchange protocol
- DSS (Digital Signature Standard), which incorporates the **Digital Signature Algorithm**
- ElGamal
- Various **elliptic curve** techniques
- Various password-authenticated key agreement techniques
- Paillier cryptosystem
- RSA encryption algorithm (PKCS#1)
- Cramer–Shoup cryptosystem
- YAK authenticated key agreement protocol

Source: https://en.wikipedia.org/wiki/Public-key_cryptography

In cryptography, the Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.

Key and signature-size comparison to DSA
As with elliptic-curve cryptography in general, the bit size of the public key believed to be needed for ECDSA is about twice the size of the security level, in bits. For example, at a security level of 80 bits (meaning an attacker requires a maximum of about operations to find the private key) the size of an ECDSA public key would be 160 bits, whereas the size of a DSA public key is at least 1024 bits. On the other hand, the signature size is the same for both DSA and ECDSA: approximately bits, where is the security level measured in bits, that is, about 320 bits for a security level of 80 bits.

Future:
https://en.wikipedia.org/wiki/Post-quantum_cryptography

Infringement of feeling safe or fraud

people are the decisive factor!
"If you control your keys, it's your bitcoin. If you don't control the keys, it's NOT your bitcoin."
Andreas Antonopoulos, 2015
<safety belt>

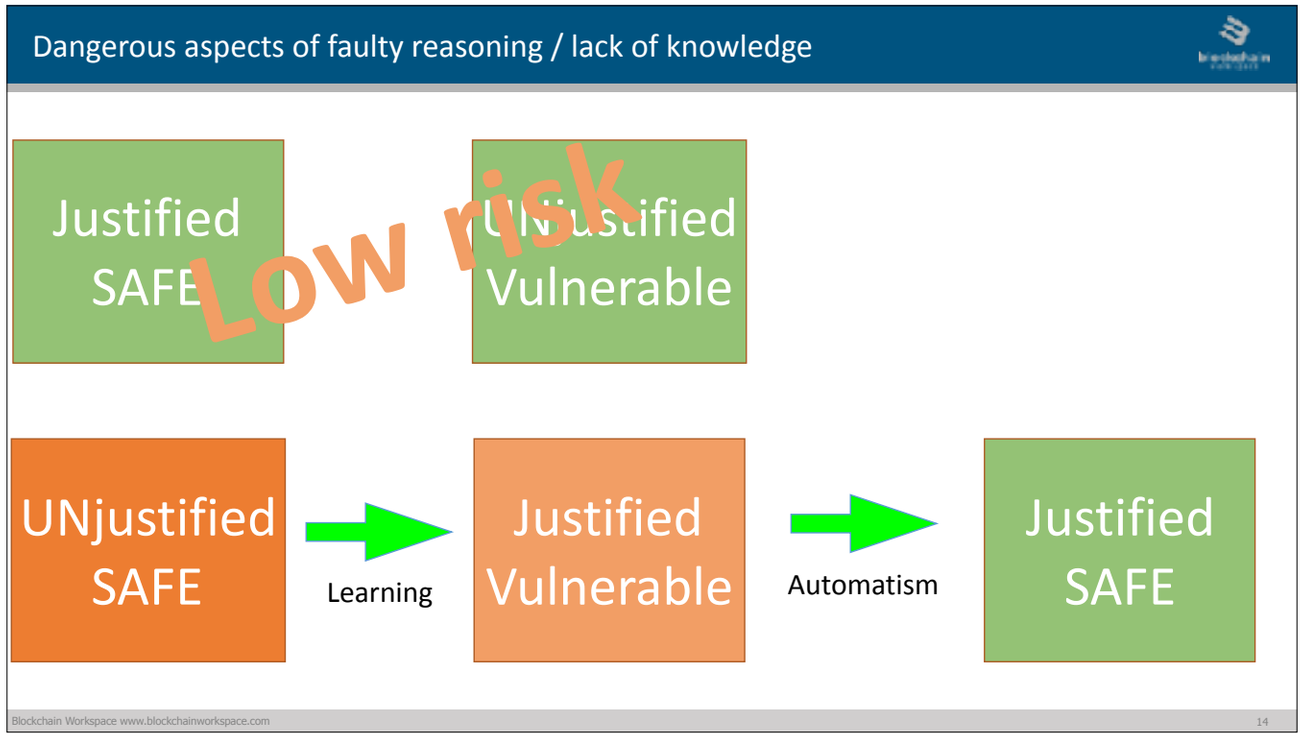
"If you control your keys, it's your bitcoin. If you don't control the keys, it's NOT your bitcoin."

Andreas Antonopoulos, 2015

"Why you have to carefully manage your keys. And why you won't"

Henk van Cann 2018 :)

It is not a one-off, instead it is a learning curve and psychological barriers to overcome.



It is not a one-off, instead it is a learning curve

The lack of Economic Incentives will save your ass in general;

but YOU might be the party pooper!

<You are in the house - how safe do you feel?>

How likely will it be that thieves get caught and your value returned?

What plays a role in our feeling of "safety"

- Complexity, difficult to enter
- Money & time, the costs higher than the benefits
- Discoverability, is a thief exposed?
- Maturity, how old is the technology?
- Recoverability, can I get my value back?

Economic incentives!

Security is always about "me":
The Technical network is solid and resilient! Faults, tampering, robbery, etc. by human beings!
Maturity : compare to how it used to be with electricity or aviation….

"Quantum Computers: Informatie die vandaag niet gevaarlijk is, kan in de nabije toekomst wel zijn."
Tanja Lange - @hyperelliptic

Informatie nu opgeslagen voor later

Het is verkeerd om te denken dat er nog geen probleem is, omdat het nog lang duurt voor wetenschappers 'klaar' zijn met de kwantumcomputer, zegt Tanja Lange, hoogleraar cryptologie aan de TU Eindhoven. Ze verwees naar de affaire rond Edward Snowden, de klokkenluider die grootschalige afluisterpraktijken van de Amerikaanse geheime dienst NSA naar buiten bracht. 'We weten dankzij Snowden dat geheime diensten alle communicatie opnemen en bewaren. Wat nu nog niet kan worden ontsleuteld, wordt alvast opgeslagen voor over twintig jaar, als de kwantumcomputer er is.'

Bron citaat: FD artikel

Speech op SURFnet - slides, CC by SA Tanja Lange.

Photo: Henk van Cann, SURFnet security & privacy 2018

Safety?! Ask yourself constantly: Did we secure the digital keys well enough?

Pamela Morgan quotes

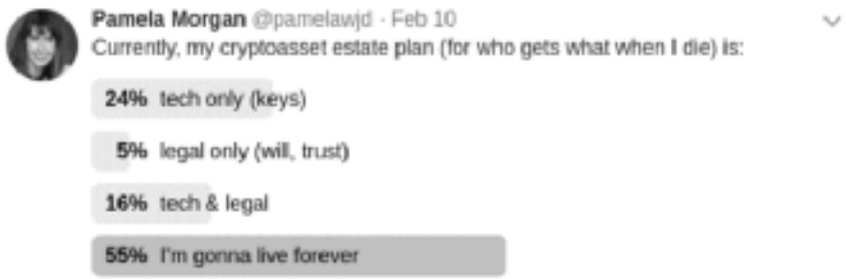
- ‘my failure to implement good security wasn’t totally my fault; it was a **combination of misunderstanding the risks, overestimating the effort it takes to implement’**
- ‘I had heard about people **getting hacked**. But it was **always other people’**
- **‘the risk wasn’t real enough for me to do anything about it’**
- **‘**Maybe you’re like I used to be: **simply unsure of what to do — so you do nothing’**

Where are you?

Stay inside the herd: Avoid risky behaviour - learn - stay fit with automatisms

Pamela Morgan quotes

- **‘Basic good security practices** are now part of my **routine** without even noticing. **Like putting on a seatbelt** after getting into a vehicle, it’s just something I do**.’**
- LINK TO ARTICLE



1. Mistaken Belief: I have to hire a lawyer.
2. Mistaken Belief: I have to trust a third party.
3. Mistaken Belief: Planning will make my assets easy to steal.
4. Mistaken Belief: The value of my cryptoassets is too low to plan.
5. Mistaken Belief: My heirs will figure it out.
6. Mistaken Belief: This can all be done with a simple smart contract.

NEXT Episode!

HOW to manage your crypto value /estate

DON'TS of crypto key management

As soon as some significant value is involved, use as little as possible…

- weak passwords
- hot wallets in any form
- brain wallets solo
- unmanaged passwords
- self invented seeds
- online computers to generate/print single paper wallets

Web, mobile, etc.
Solo -> without anybody knowing it

Not 100% sure but also do not:
- follow a step by step, created by yourself or an external source, because it introduces new vulnerabilities
- no mobile phone as a security factor

DO’s of crypto key management

Techniques, routines I recommend to test whether it works for you…

- managed strong passwords
- *Choose Wallet*: Create, backup, use hierarchical keys (from seeds)
- 2FA
- 3FA (Challenge Response Authentication)
- generated seeds
- spread over copies
- spread over media
- spread over geo-locations
- split over controlling people
- Paper wallets
- Cold stores
- Managed brain wallets

IAM Authentication: something you have, you are and you know
HOW??!! you ask someone else the details
Good question, because you obviously want to learn, but…
What if the expert is not trustworthy?

A managed brain wallet is something your loved ones can remember when you are not there anymore, a shared secret, indirectly put writing. Example: all family members remember that their lovely but long deceased dog jumped into a bassin back in 1994, the dog pulled out a puppet that looked like Elvis, that was funny. So you might write down: ‘Pepper swim 1994’ but only a subset of your beloved ones know the seed that is meant with that, which is ‘Dog jump bassin Elvis out’
Never mention the sentence itself ever again, repeat it to each other only once a year and always refer to ‘Pepper swim 1994’ when mentioning the passphrase. Just an example of course.

License

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 license

https://creativecommons.org/licenses/by-sa/4.0/

The lack of Economic Incentives will save your ass;

but YOU might be the party pooper!