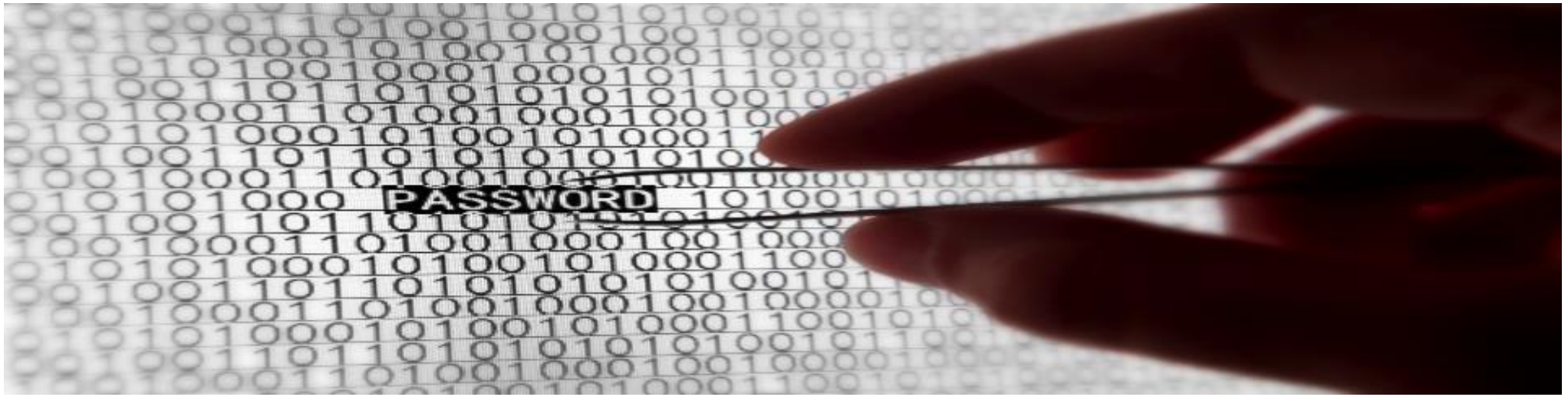
delacruz beranek

RECHTSANWÄLTE ▪ ATTORNEYS AT LAW



WSIS Workshop: Blockchain and the GDPR

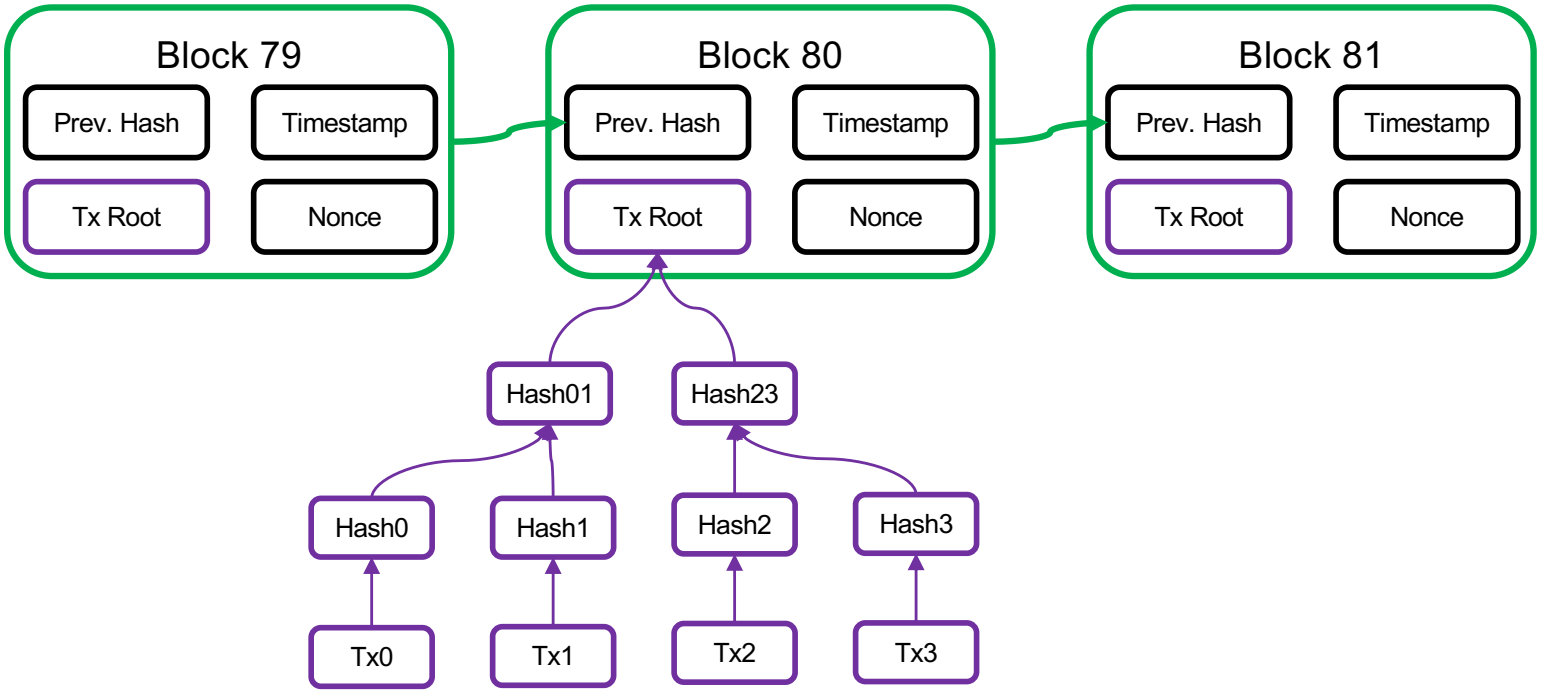
Encryption usually only renders personal data pseudonymous. Are there situations where encrypted data can be considered to be anonymous?

RA lic. iur Carmen De la Cruz

eidg. dipl. Wirtschaftsinformatikerin, Notarin


1

Blockchain basics – Chain of Blocks




2

GDPR – Data Subject Rights as main issue

Data Subjects rights of GDPR (art. 12 ssq GDPR):

- the right to be informed about the collection and the use of their personal data
- the right to access personal data and supplementary information
- the right to have inaccurate personal data rectified, or completed if it is incomplete
- **the right to erasure (to be forgotten)**
- the right to restrict processing in certain circumstances
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- the right to object to processing in certain circumstances
- **the right to withdraw consent at any time**

Personal data in a blockchain

- Problem: If the data on a blockchain is not completely anonymized it is subject to GDPR.

- **No encryption**:
  - Personal Data stored on a blockchain in **plain text** remains Personal Data for the purposes of the GDPR.

- **Encryption:**
  - **Encrypted** Personal Data which can be accessed with the correct keys is not irreversibly anonymized. E.g. encrypted data can be linked to the data subject when transactions are affected for off-chain goods or when cryptoassets are converted into fiat currency through an exchange that performs KYC and AML duties. After three transactions = pseudonymized.
  - Encryption is considered a **method of pseudonymization** under the EU data protection regime, given that the data subject can still be **indirectly identified**. As a consequence, it cannot, on its own, be considered an anonymization technique.

Personal data in a blockchain

Hashing process:

- Transactional data that has been subject to a hashing process also likely qualifies as personal data under the GDPR.
- Although a one-way hash function that cannot be reverse-engineered can offer stronger privacy guarantees than encryption, it will usually not allow data to evade the qualification as personal data for GDPR purposes.
- Article 29 Data Protection Working Party: hashing constitutes a technique of pseudonymization, not anonymization
- Statements that hashes should in some circumstances qualify as anonymous data -> no clear guidance as to whether, and if so under which circumstances that would be the case.

Conclusion:

- **Transactional data that is encrypted or has undergone a hashing process is likely personal data for the purposes of the GPDR.**

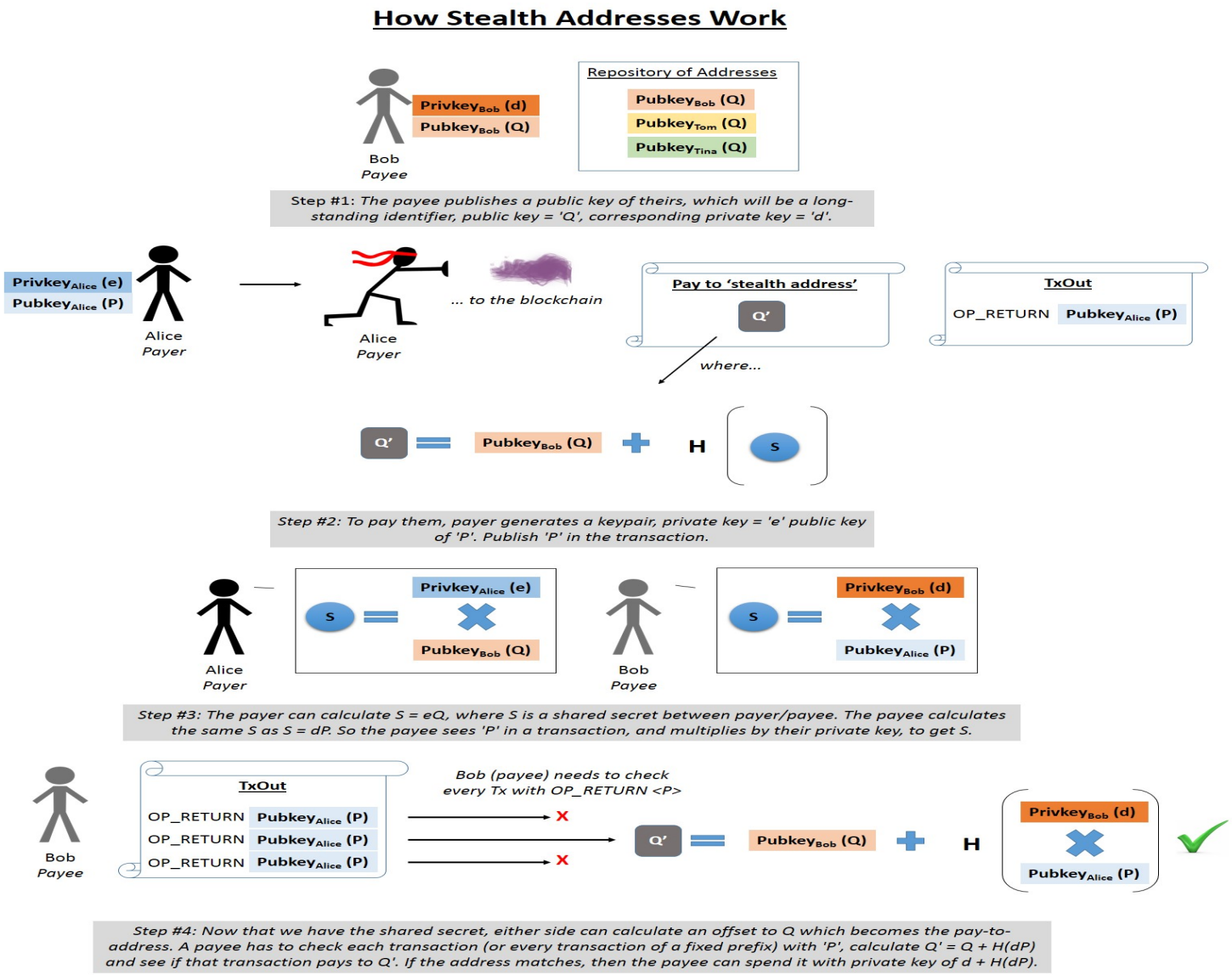
Personal data in a blockchain

- The conclusion that transactional data stored on a blockchain is subject to GDPR requirements may be avoided in some scenarios:
  - Complete anonymization:
    - Development of future cryptographic processes or a combination thereof will be declared capable of anonymizing personal data.
    - Cryptographically secure obfuscation as «holy grail» of privacy on blockchains, not available (yet).
    - Off-chain: Personal Data could be stored off-chain and merely linked to the blockchain through a hash pointer. However, on-chain data and likely also on-chain data hashes off-chain data would still qualify as Personal Data, yet it could be manipulated off-chain in line with GDPR requirements. In such scenario, Personal Data can be recorded in a referenced, encrypted and modifiable database and not on the blockchain.

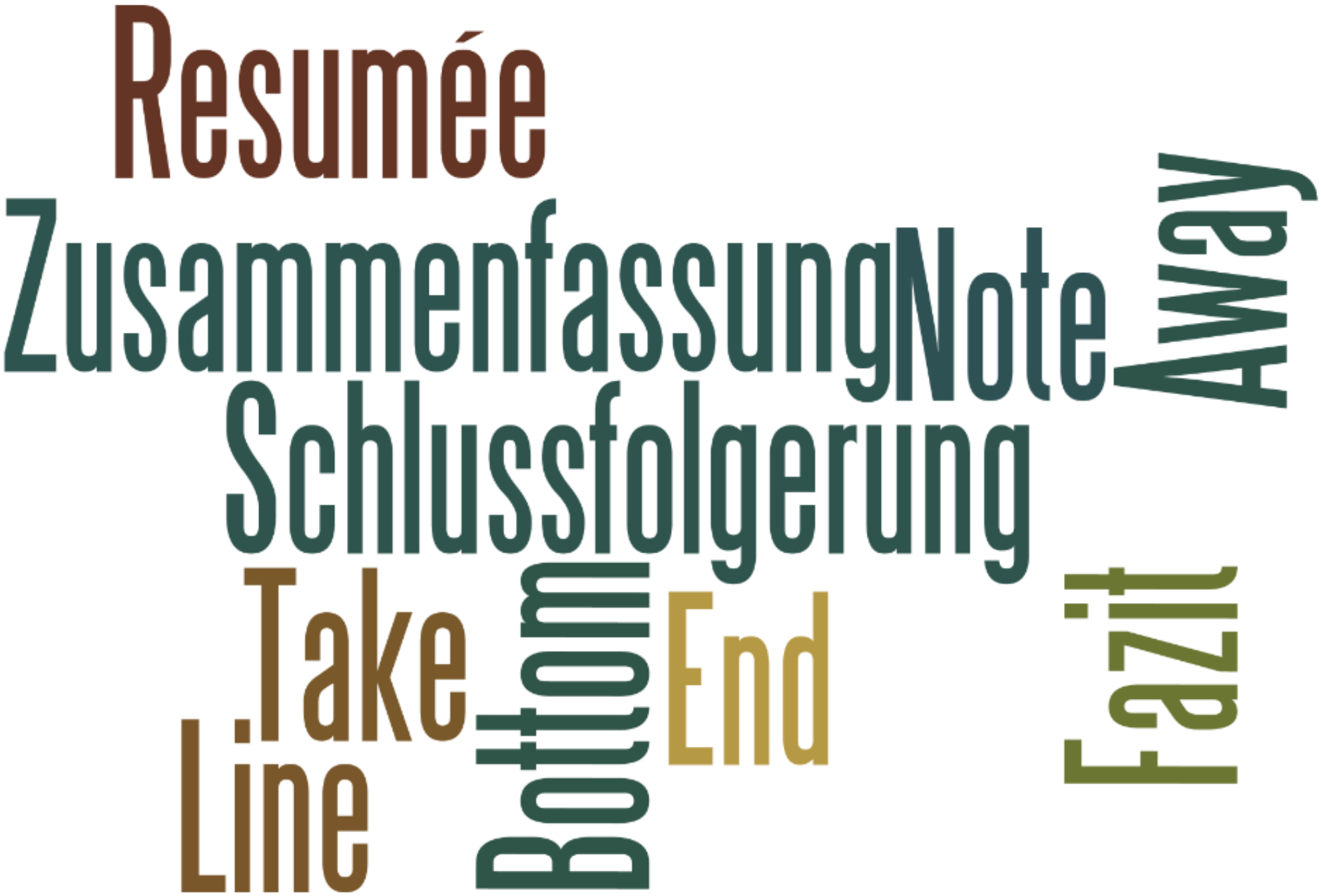
Usage of Encryption mechanism to be anonymous

- GDPR-compliant solutions:
  - **Use of stealth address** which uses a one-time transaction that relies on hashed one-time public and private keys (for example Monero)
  - **Adding noise to the data:** Several transactions are grouped together so that, from the outside, it is impossible to discern the identity of the respective senders and recipients of a transaction.
    - Art. 29 Working Party considers the addition of noise an acceptable anonymization technique provided that the necessary safeguards are complied with.
    - Difficult to predict whether any of these techniques is capable of anonymizing public keys for GDPR purposes.
  - Zero Knowledge Proofs
- As a consequence, public keys and transactional data stored on blockchains will often qualify as Personal Data.

GDPR – anonymization – stealth addresses



Source: http://i.imgur.com/rHhNKL6.jpg , visited 07.04.2019


Resumée
Zusammenfassung
Note
Away
Schlussfolgerung
Take
Bottom
End
Fazit
Line

delacruz beranek

RECHTSANWÄLTE ▪ ATTORNEYS AT LAW

Danke für Ihre Aufmerksamkeit

de la cruz beranek Rechtsanwälte AG
Industriestrasse 7
6300 Zug
Tel. 041 710 28 50
delacruz@delacruzberanek.com
www.delacruzberanek.com