CRYPTOGRAPHY:

A TECHNOLOGY USED IN BLOCKCHAIN

BLOCKCHAIN CRYPTOGRAPHY

Cryptography moves the burden of trust from central authorities to cryptographic algorithms allowing blockchain to be decentralized and distributed.

Cryptography Key Terms

Secret

The data which we are trying to protect

Key

A piece of data used for encrypting and decrypting the secret

Cipher

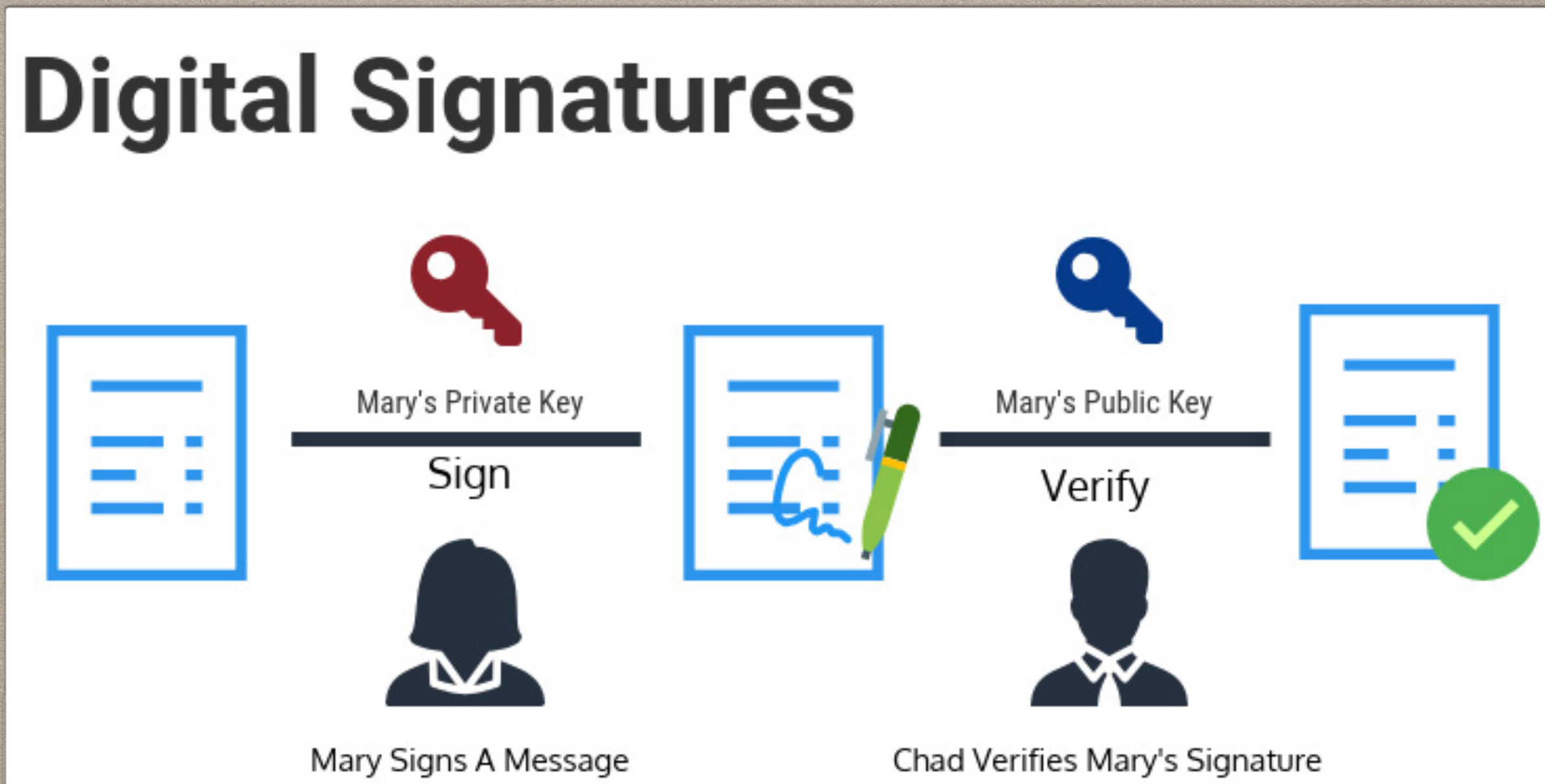
The encrypted secret data, output of the function

Function

BLOCKCHAIN:
TYPES OF CRYPTOGRAPHY

- Public Key Cryptography – Pair of public and private keys used for encryption and digital signatures.
- Zero-Knowledge Proof – Prove knowledge of a secret without revealing it.
- Hash Functions – One-way pseudo-random functions and Merkle trees.

PUBLIC-KEY CRYPTOGRAPHY



AUTHENTICATION, NON-REPUDIATION, INTEGRITY

ZERO-KNOWLEDGE PROOF

- zk-SNARKs – Zero Knowledge Succinct Non-interactive Arguments of Knowledge
- Cave door analogy

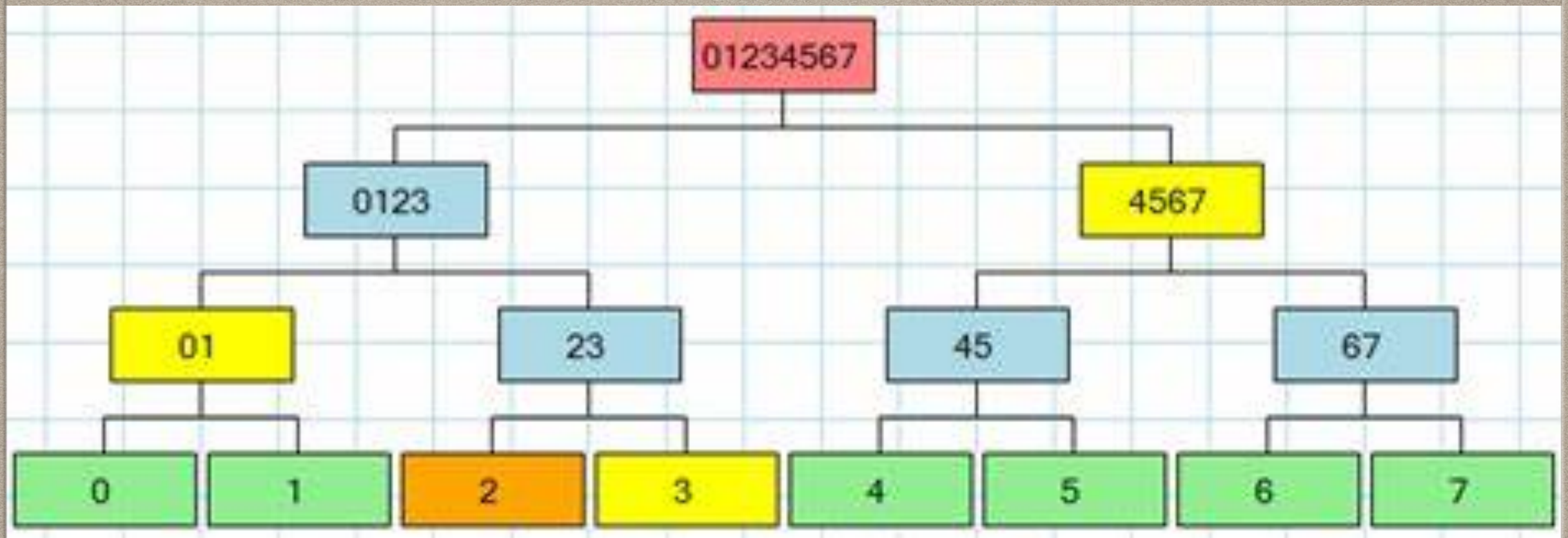
HASH FUNCTIONS:

MATHEMATICAL FUNCTIONS WITH 4 IMPORTANT PROPERTIES

- Hash functions take input of any size and produce output of fixed size.
- It’s easy to calculate a hash, but it’s difficult to determine hash input from the output.
- Inputs that differ by a single bit produce hashes that differ by about half their bits.
- It’s infeasible to find two inputs that produce the same output hash.

HASH EXAMPLE

Data	SHA-1 Hash
Merry Christmas	ebcefcf21408246493a4e626b771cd7120ec2f50
Merry Christmas!	767024003f02e580ec94a05dd1ba9af00b9ddc45



MERKLE TREE

ALLOWS VALIDATION OF DATA WITHOUT REQUIRING THE ENTIRE SET OF DATA

CONCLUSION

CRYPTOGRAPHY PROVIDES SECURITY FOR BLOCKCHAIN