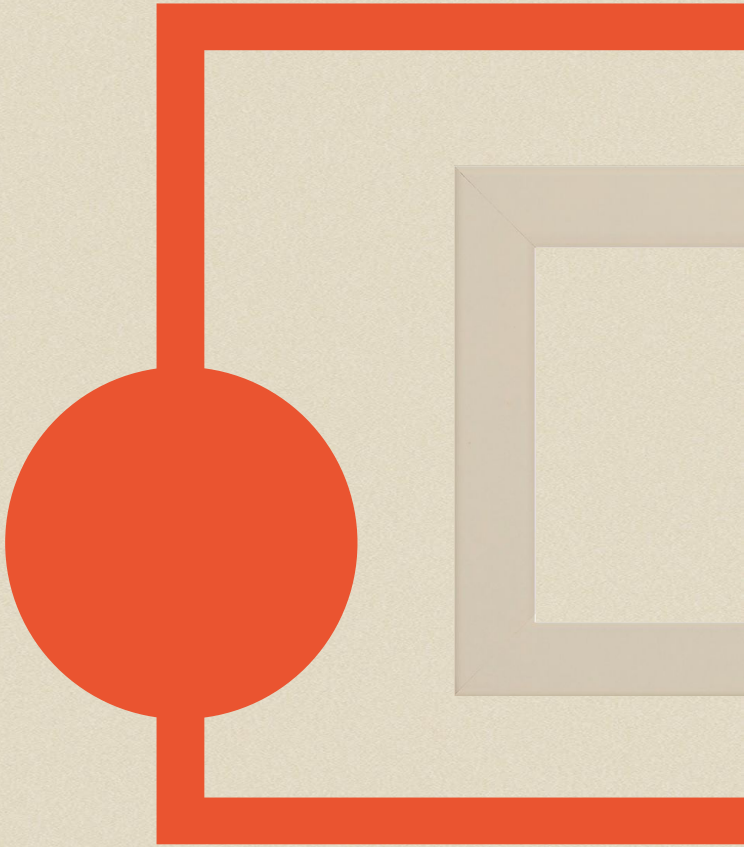
TRUST BUT VERIFY CHEAPLY:

Reducing Agency Costs Using Digital Signatures

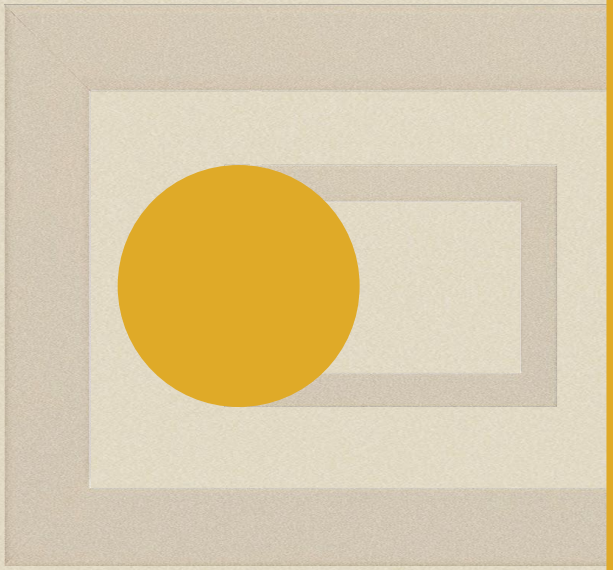
Kate Sills

APEE 2022



PRINCIPAL-AGENT PROBLEM

Agency relationship: a contract in which one person (the **principal**) engages another person (the **agent**) to perform some service on their behalf and delegates some decision-making authority to the agent.



Jensen, M.C., Meckling, W.H. (1979). Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure

AGENCY COSTS

= the monitoring expenditures by the principal
+ the bonding expenditures by the agent
+ the residual loss.

OPPORTUNISM

Opportunism: self-interest-seeking with guile

Opportunism can be **reduced** by supplying **cost-effective safeguards**.

This area of study requires more knowledge of the specific contractual devices and safeguards than is usual in economics.

Williamson, Oliver E. (1993). Calculativeness, Trust, and Economic Organization.
Williamson, Oliver E. (1983). Credible Commitments: Using Hostages to Support Exchange.

O.P.M. LEASING SERVICES

The New York Times

THURSDAY, MARCH 26, 1981

O.P.M. Bankruptcy: Questions Abound

Lessor Faces Fraud Charges

THE FRAUD

AGENT

PRINCIPAL

Leasing Client

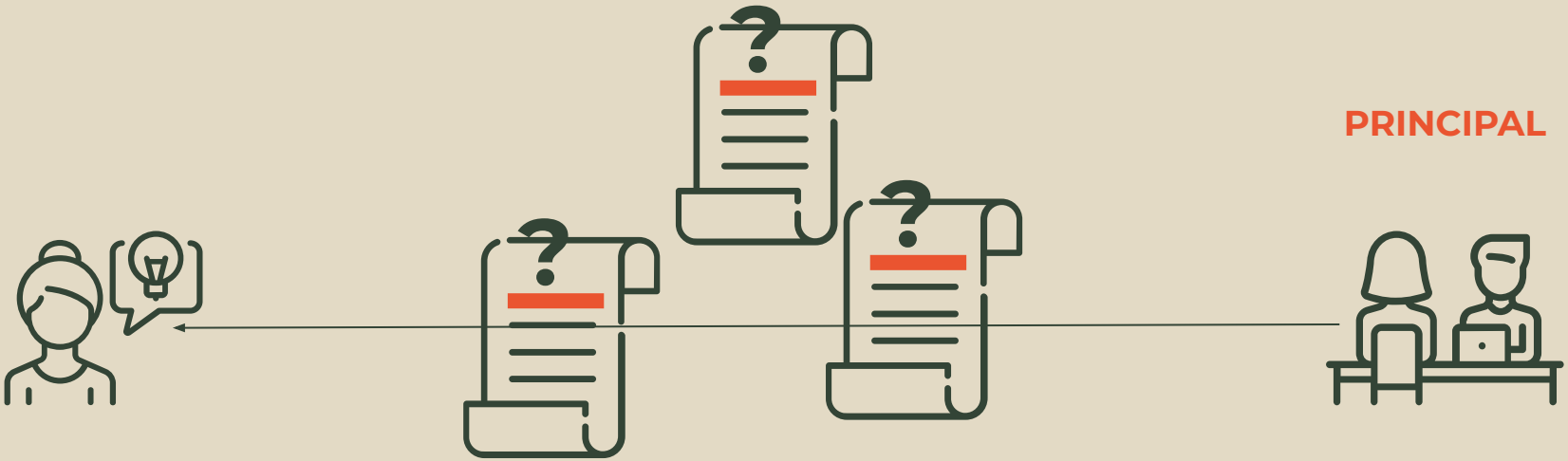
Original Contract

O.P.M.

Altered Contract

Investors

THE SAFEGUARD?



CRYPTOGRAPHY

The study of **secure communications**.

Only the sender and the recipient can read the message, even if the message falls into the wrong hands.

CRYPTOGRAPHY CAN DO MORE...

UNALTERABLE DOCUMENTS

Can easily detect even the smallest changes to a document

UNFORGEABLE SIGNATURES

Can easily verify that a document was signed by someone

TIMESTAMPED RECORDS

Can prove that a document existed in a certain point in time

DIGITAL SIGNATURES

Katelyn Sills

Digitally signed by Katelyn Sills
Date: 2022.04.02 18:23:38 -07'00'

3045022100e16236fc16c6a3cd5df8c47597f27a852f54b5c8f5cb4a1c18c215d48715a54002207868db852cf8c11c7c09086164fc0d8d754e46ddc50eb3fcf458c4cd6d9eda8d

DIGITAL SIGNATURES (1977)

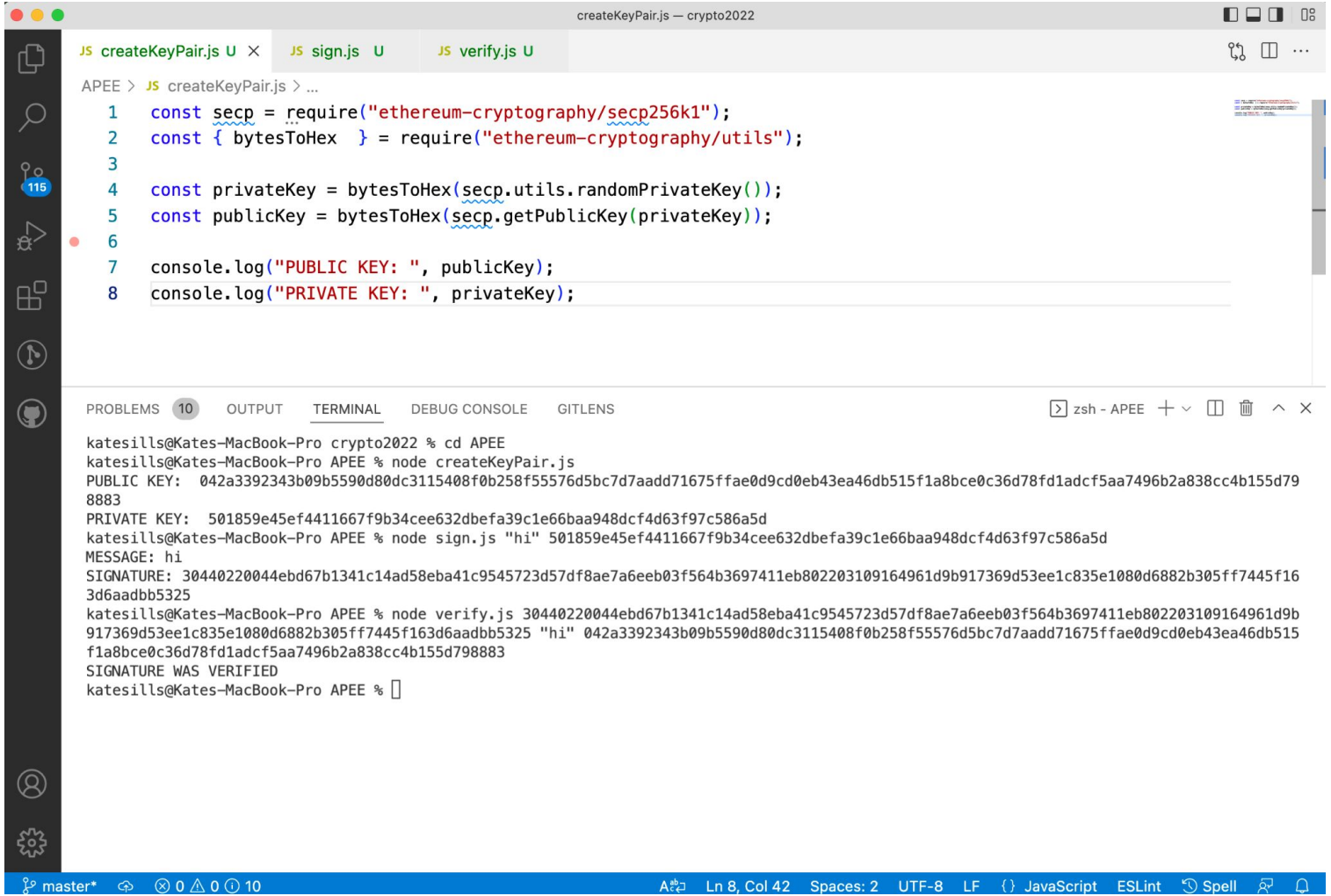
1 PRIVATE KEY

Only you* can make your signature.
No one can forge it!

* or whoever has your private key

PUBLIC KEY 2

Anyone who has your public key
can easily verify your signature


createKeyPair.js — crypto2022
createKeyPair.js U
sign.js U
verify.js U
APEE > createKeyPair.js > ...
1 const secp = require("ethereum-cryptography/secp256k1");
2 const { bytesToHex } = require("ethereum-cryptography/utils");
3
4 const privateKey = bytesToHex(secp.utils.randomPrivateKey());
5 const publicKey = bytesToHex(secp.getPublicKey(privateKey));
6
7 console.log("PUBLIC KEY: ", publicKey);
8 console.log("PRIVATE KEY: ", privateKey);
PROBLEMS 10
OUTPUT
TERMINAL
DEBUG CONSOLE
GITLENS
zsh - APEE
katesills@Kates-MacBook-Pro crypto2022 % cd APEE
katesills@Kates-MacBook-Pro APEE % node createKeyPair.js
PUBLIC KEY: 042a3392343b09b5590d80dc3115408f0b258f55576d5bc7d7aadd71675ffae0d9cd0eb43ea46db515f1a8bce0c36d78fd1adcf5aa7496b2a838cc4b155d798883
PRIVATE KEY: 501859e45ef4411667f9b34cee632dbefa39c1e66baa948dcf4d63f97c586a5d
katesills@Kates-MacBook-Pro APEE % node sign.js "hi" 501859e45ef4411667f9b34cee632dbefa39c1e66baa948dcf4d63f97c586a5d
MESSAGE: hi
SIGNATURE: 30440220044ebd67b1341c14ad58eba41c9545723d57df8ae7a6eeb03f564b3697411eb802203109164961d9b917369d53ee1c835e1080d6882b305ff7445f163d6aadbb5325
katesills@Kates-MacBook-Pro APEE % node verify.js 30440220044ebd67b1341c14ad58eba41c9545723d57df8ae7a6eeb03f564b3697411eb802203109164961d9b917369d53ee1c835e1080d6882b305ff7445f163d6aadbb5325 "hi" 042a3392343b09b5590d80dc3115408f0b258f55576d5bc7d7aadd71675ffae0d9cd0eb43ea46db515f1a8bce0c36d78fd1adcf5aa7496b2a838cc4b155d798883
SIGNATURE WAS VERIFIED
katesills@Kates-MacBook-Pro APEE %
master*
Ln 8, Col 42
Spaces: 2
UTF-8
LF
JavaScript
ESLint
Spell

USING DIGITAL SIGNATURES

The Signer:

1

PUBLISHES PUBLIC KEY

2

DIGITALLY SIGNS THE DOCUMENT

The Verifier:

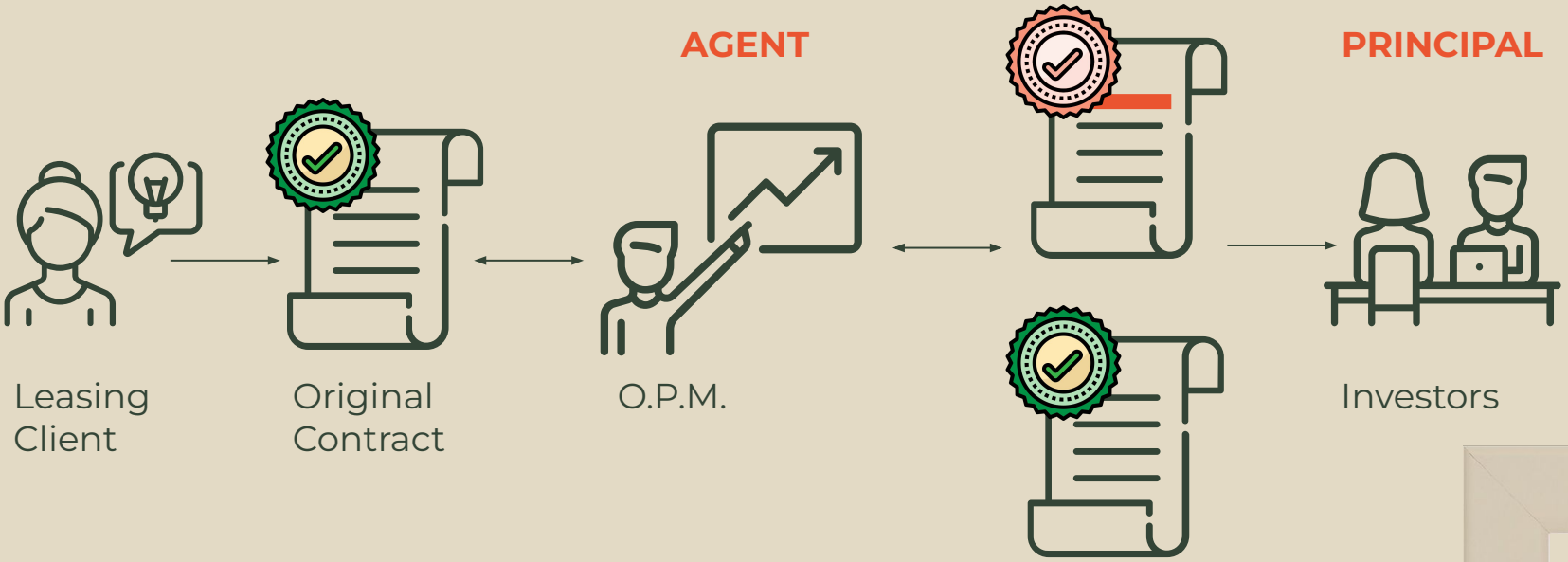
3

LOOKS UP PUBLIC KEY

4

VERIFIES THE SIGNATURE

WITH DIGITAL SIGNATURES




EESTI VABARIIK
Republic of Estonia
ISIKUTUNNISTUS
Identity Card
SPECIMEN
JÕEORG
JAAK-KRISTJAN
M/M
EST
08 01 1980
09 08 2023
38001085718
AS1234567
345678


EST
09 08 2018
SPECIMEN
IDESTAS12345671380010857l8<<<<
8001081M2001023EST<<<<<<<<<<<3
JOEORG<<JAAK<KRISTJAN<<<<<<<<<


CHASE
SAPPHIRE
PREFERRED


Ledger

MILLION DOLLAR NUT THEFT IN CA

A truck driver arrives at the orchard, the farm checks the paperwork, and everything looks good.

Then the truck driver leaves with the nuts, but they never arrive at their intended destination.

WHY ISN'T THIS IN USE ALREADY?

- Cryptography was a legal fight
- Disconnect between cryptographers (mathematicians) and the people that need the solutions (business)
- It's hard to create and teach new rules of interaction
- It's hard to write good software, but that has never stopped us before

BLOCKCHAINS ARE COSTLY

- blockchains were designed for securing fungible, digital cash
- transactions are sequential, not parallel, as in normal marketplace transactions.

CONCLUSION

Cryptography alone can transform society by lowering the monitoring costs in principal-agent relationships

THANKS!

katelynsills@gmail.com
@kate_sills
katelynsills.com

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, infographics & images by Freepik and illustrations by Storyset