東莞理工學院
DONGGUAN UNIVERSITY OF TECHNOLOGY

区块链技术与应用

v0.11.14

第八章：加密货币和智能合约

丁烨，网络空间安全学院 副教授
dingye@dgut.edu.cn

目录

加密货币概述

加密货币的起源

- Bitcoin: A Peer-to-Peer Electronic Cash System
- 2008 年 11 月 1 日
- 中本聪（Satoshi Nakamoto）
- 这封白皮书在当时并没有掀起轩然大波，因为它只是站在巨人肩膀上的另一次尝试

Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another

加密货币概述

加密货币的起源

- 分布式账本（Distributed Ledger）
- 又称共享账本（Shared Ledger）、分散式账本技术（Distributed ledger Technology，DLT）
- 是一个由多站点、多国家或多家机构所组成的在网络上进行电子数据复制、共享及同步的共识机制
- 通常不依赖也不存在中央管理员或集中的数据存储
- 对等网络与共识机制确保了跨节点间的数据能被正确复制
- 区块链系统是分布式账本的一种实现方法

加密货币概述

加密货币基础概念

Cryptocurrency

加密货币

分布式账本中记录的货币单位

加密货币概述

加密货币基础概念

Cryptocurrency

加密货币

分布式账本中记录的货币单位

加密货币概述

加密货币基础概念

Cryptocurrency

加密 = 共识

分布式账本中记录的货币单位

目录

加密货币的实现原理

加密货币技术需求

加密货币的实现原理

加密货币银行

- 银行（Bank）
- 办理结算等业务的金融机构，相当于区块链的分布式账本
- 银行通过账户（Account）来识别用户
- 类似银行，在加密货币中，账户采用先到先得的机制分配
- 用户需要提供一定的数据来证明自己拥有某个账户

加密货币的实现原理

数字签名

public

private

encrypted using
César's public key

decrypted using
César's private key

```
-----BEGIN PGP MESSAGE-----
Comment: GPGTools - https://gpgtools.org

hQIMA+IjWf8EQUhAAQ/+0AjcgHjZVAllxLQ8ua8an+bSNLbUW3bLkdhUpft/CZ0t
uHwlHkq95ZWaupVcO9sLDLVxANLskB8WdMQQZhaIGFIP2XsAr/GPuUnaWW+69PQ
jFRa4FS6Ezl0fdl6PgEQ3SI6FihztUwirP38CjxY5HeilCz/p/V6vIMVrnMUrPkn
gKSYcPSf7S69cvLZ/IITsdN4wjnrZXn5JAFoy5vJ2MuFBUg6v+ZX/FQaBisVy4bT
+5/qjmRLWrhxguNBYvs4tan9Gba7lY7yyMfV5HGF70k6lNohk1FTluEJn41YhQRV
YMS6ES3YnCXxa4nt6HeQLH4jbm+uoNUUnZ5SLWCpJ0XwXFKNHl1fGuLH+9FNjQWA
B6ooxGScvm0v2SxefuVz5u8KEqoIbOqwpk4cDhojBbw04ilrwRSDPLMCOY6JZ/1b
BpUPf34XYRLvQSywSTZDVYWwzV2LXln2pdgw/OjHa37b46TTdvZpbyhQFgp6gPPf
5QsYPsnV953eu+ByRSJQ/1g9MefChaTPaspMiAeCDeK7L4nuI1HkhX0oM4Jn1p04
HCjZ51gd8HexpsgcQ8bfVaArVZhqHqGpbrpVz8Tq1KYkZISWa/jwAgxpO6i/3nCG
49Gf23Eqql27Nwt9vwhXkp0psSS36fUZE52QkJ0JgvOHjagr9LHcvb+zmDSN4n7S
wW8B2I63TXYlAwunlUxF4h4ooGuZiMf3zomiuQQ7KBWjbLUNYxLmh6e07ulrS4Rn
BZE6zyB1LMztIQQ0xQaPmUVQSI2LiRBrpdsVyodo7bHPsZW0gaE3jQYJBpfbiEUt
d32NdOZtfiqo3+ha6ILLXqoYv1GYlp7Ucm+htWMjLZE1EysrdJzBtX39aUi2dpfx
tXoKK2HgNN7WTKvrsFB0IsP1BdUrHbxrAzL/yJlK41ZfFSCfXoeNg66Mz9nTFKbW
TXNv+6TBkY4r7BngepKs0CX3whkKsl9oMr9bqP5P787HxkAomPXodlqrDnhLV6xW
LHq/QR/0fGDbh0b9FDj3lDgt8b3IxpY3hA0KDAjxtWCDl+slvJOTfq4+t/sExU6F
nrPWl1f31c5n3pckwE2Y4FJSvKlczc7u57eBLDsS0mKJ4Wn46EsaVoaBrCvGc5G6
dqdkMgaLhAyPle52VOtBW4AxY4bu0tpJaonYEGvhX1sTC94xHGrWDYL+yvyAjv4C
5FyiAc31M5fwr8blMnIuWz/00X0gnc3NGTJFM9AZ+gCx
=/Ypa
-----END PGP MESSAGE-----
```

Meet me in the garden

加密货币的实现原理

数字签名

- 公开密钥密码学（Public-key Cryptography）
- 密码学的一种算法
- 也称非对称式密码学（Asymmetric Cryptography）
- 需要两个密钥：一个是公开密钥，另一个是私有密钥
- 公钥用作加密，私钥则用作解密
- 使用公钥把明文加密后所得的密文，只能用相对应的私钥才能解密并得到原本的明文，最初用来加密的公钥不能用作解密

加密货币的实现原理

数字签名

- 公开密钥密码学（Public-key Cryptography）
- 由于加密和解密需要两个不同的密钥，故被称为非对称加密
- 公钥可以公开，可任意向外发布
- 私钥不可以公开，必须由用户自行严格秘密保管，绝不透过任何途径向任何人提供，也不会透露给被信任的要通信的另一方

加密货币的实现原理

数字签名

- 公开密钥密码学（Public-key Cryptography）
- 基于公开密钥加密的特性，它还能提供数字签名的功能，使电子文件可以得到如同在纸本文件上亲笔签署的效果
- 公开密钥基础建设透过信任数字证书认证机构的根证书、及其使用公开密钥加密作数字签名核发的公开密钥认证，形成信任链架构

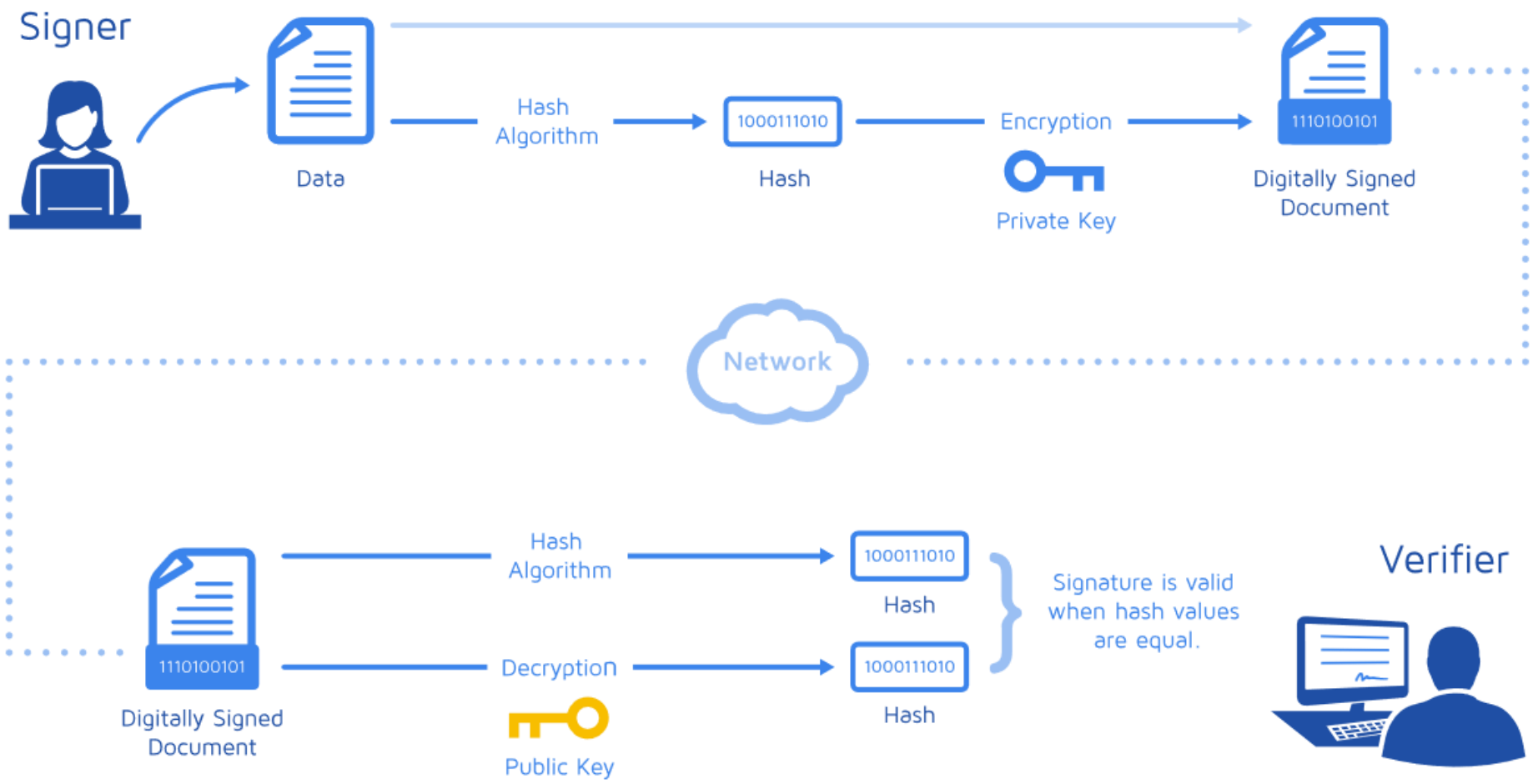
加密货币的实现原理

数字签名

- 数字签名（Digital Signature）
- 是一种功能类似写在纸上的普通签名、但是使用了公钥加密领域的技术，以用于鉴别数字信息的方法
- 数字签名了的文件的完整性是很容易验证的（不需要骑缝章、骑缝签名，也不需要笔迹鉴定）
- 而且数字签名具有不可否认性，不需要笔迹专家来验证

加密货币的实现原理

数字签名



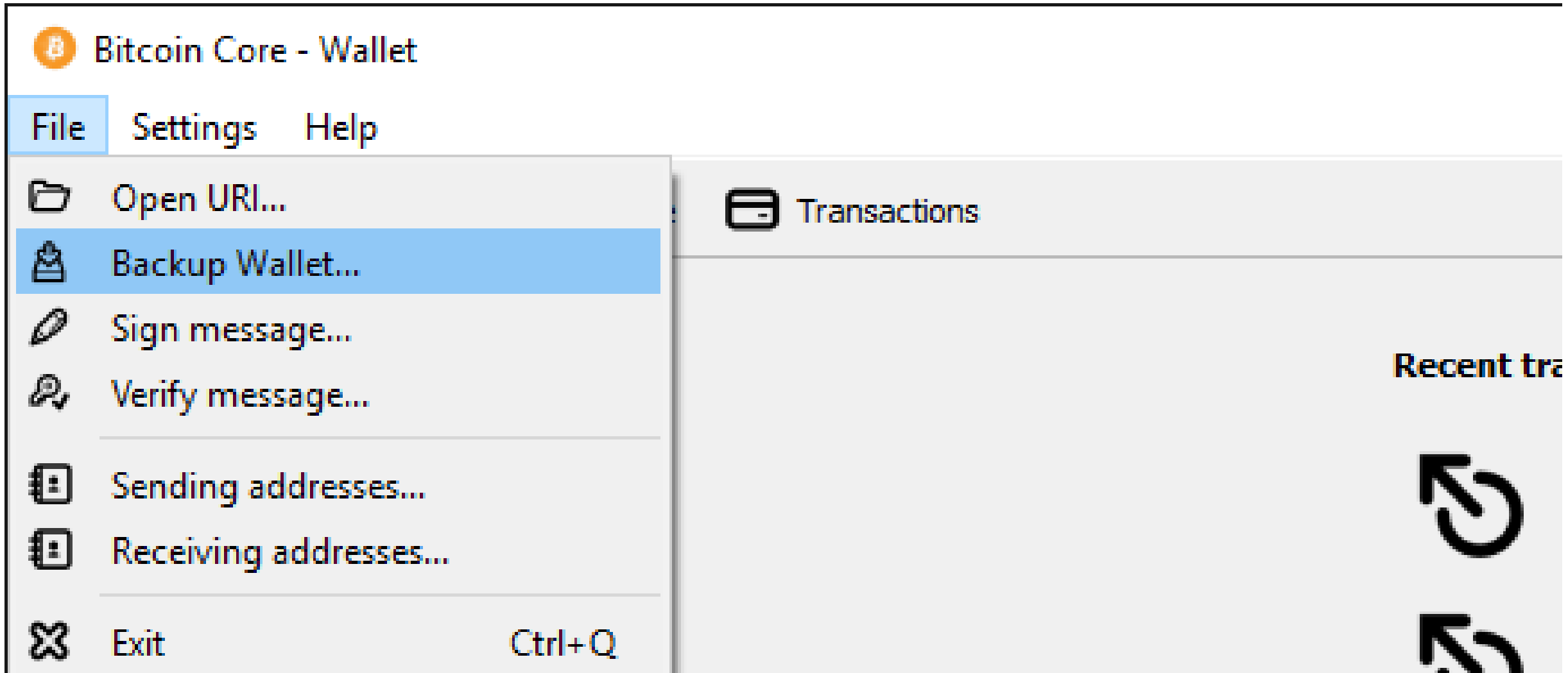
加密货币的实现原理

加密货币银行的工作流程

- 在加密货币银行中，用户可以首先自编账号（但要符合账号格式）
- 用户在本地自行生成一套公钥和私钥
- 使用选定的账号转一笔账，使用自己的私钥签名，并附上自己的公钥
- 第一个完成上述操作的用户即拥有该账号
- 以后每笔交易（Transaction）写入交易池（Pool）时，节点都会验证该笔交易的签名是否正确，且同账户的公钥是否和过往交易一致

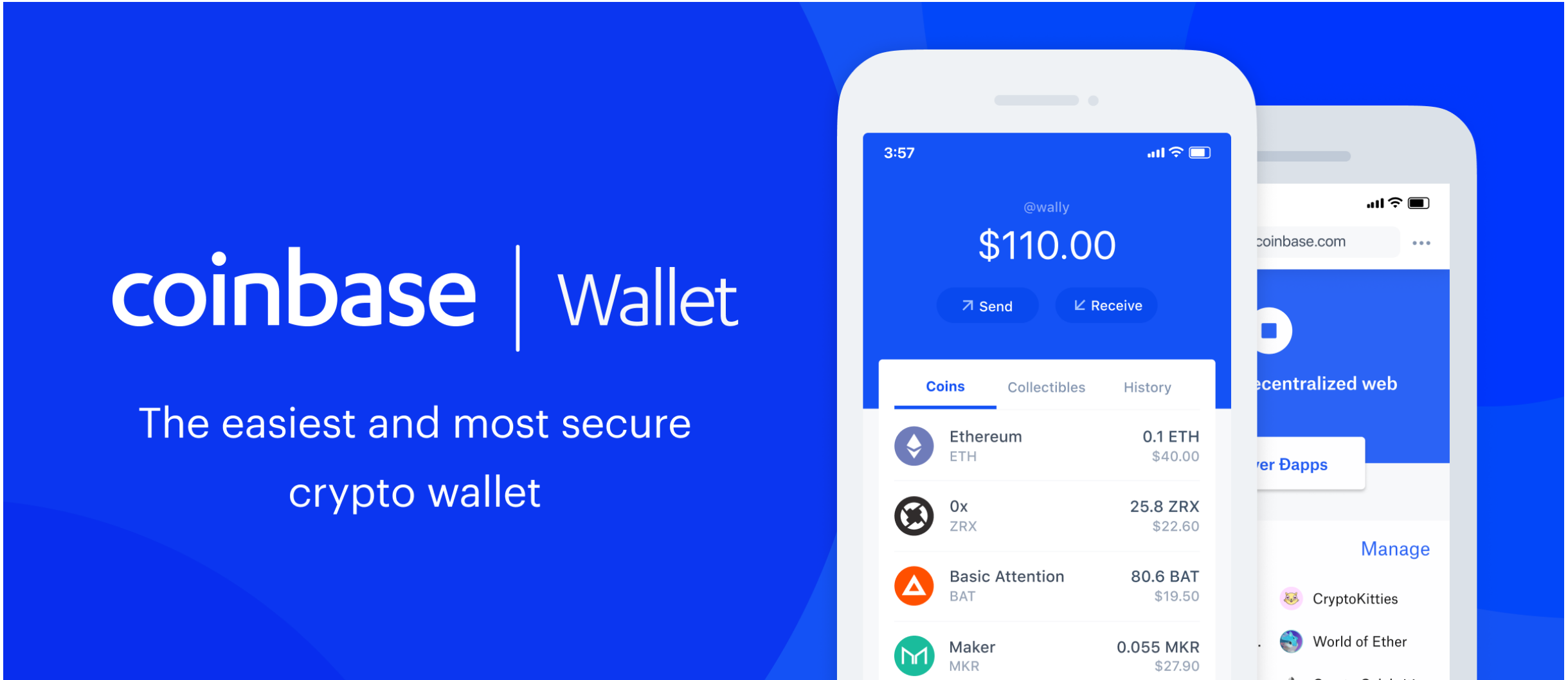
加密货币的实现原理

加密货币银行的应用



加密货币的实现原理

加密货币银行的应用



目录

加密货币生态

加密货币技术需求

加密货币生态

加密货币交易所

- 外汇市场（Foreign Exchange Market，简称 Forex 或 FX）
- 是一个分散于全球各地用于交易货币的金融市场
- 外汇市场决定不同货币之间的汇率
- 主要目的是允许企业通过转换不同的币种来促进国际间的贸易和投资
- 举例来说：它允许美国企业进口英国商品并以英镑支付其费用，尽管该企业的收支是以美元计算的
- 它也支持货币投机行为和套利交易

加密货币生态

加密货币交易所

- 加密货币交易所（Cryptocurrency Exchange）
- 加密货币交易所提供了法定货币（Fiat）和加密货币的交换服务
- 这种服务通常与区块链核心技术没有太大的关系
- 交易所可以接受用户通过传统银行系统转账法定货币
- 也可以接受用户通过区块链系统转账加密货币
- 加密货币交易所是外汇市场的一种特定形态

加密货币生态

加密货币交易的特点

- 7 x 24 不间断交易
- 极高的波动性（Volatility），适合量化交易
- 现代化、简单的交易终端
- 免费的高频交易（High-frequency Trading）接口
- 对冲交易的做市商（Market Maker）通常有挂单奖励
- 交易系统完善，包括品类多样的期货及其衍生品

加密货币生态

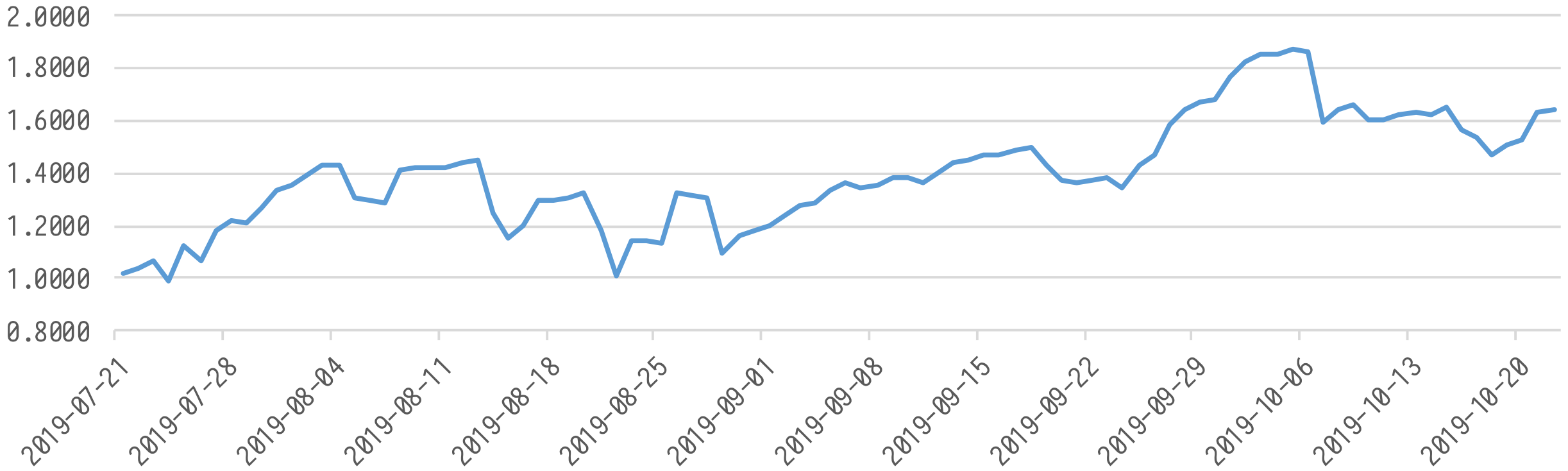
加密货币交易的特点

DR. QUANT

2019-07-21
2019-10-22

246.25%
Annual Return

-20%
Bitcoin Price



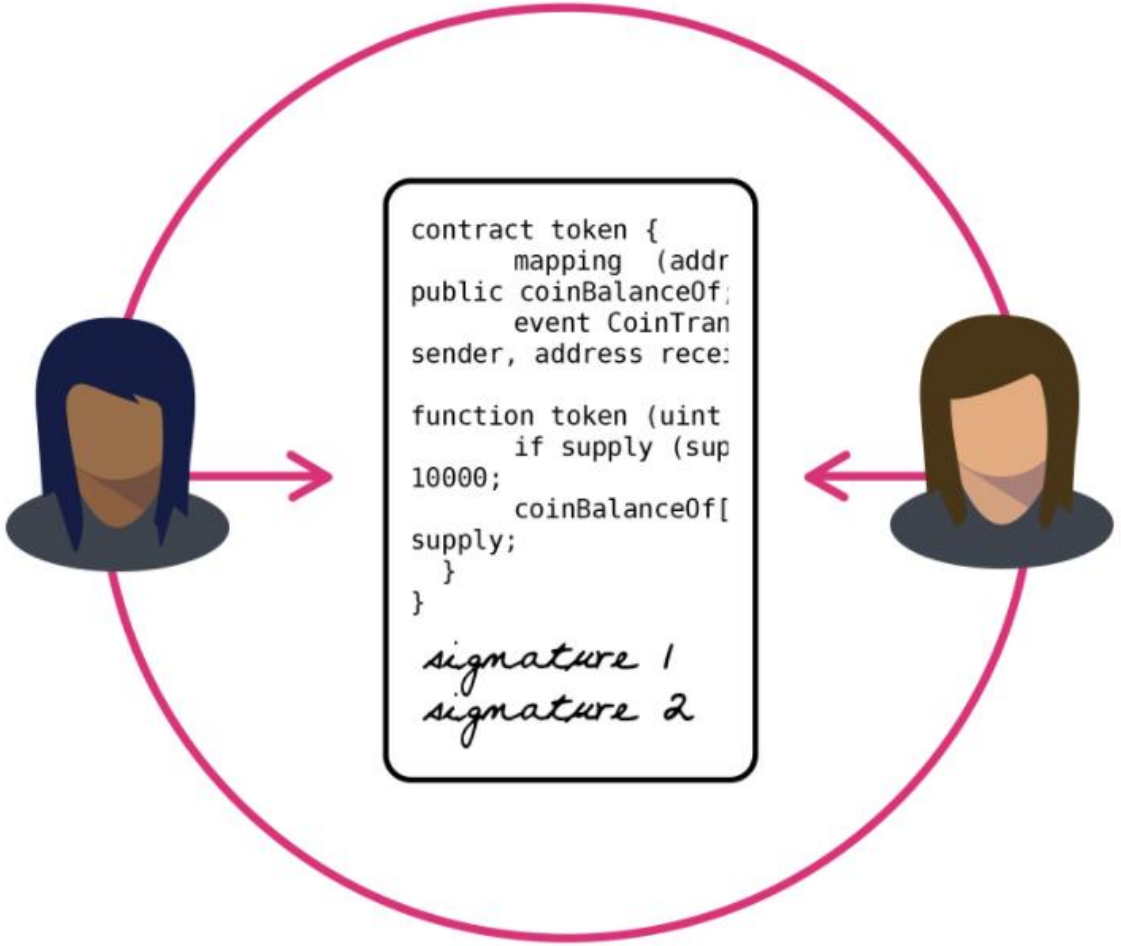
目录

智能合约概述

智能合约的基本概念

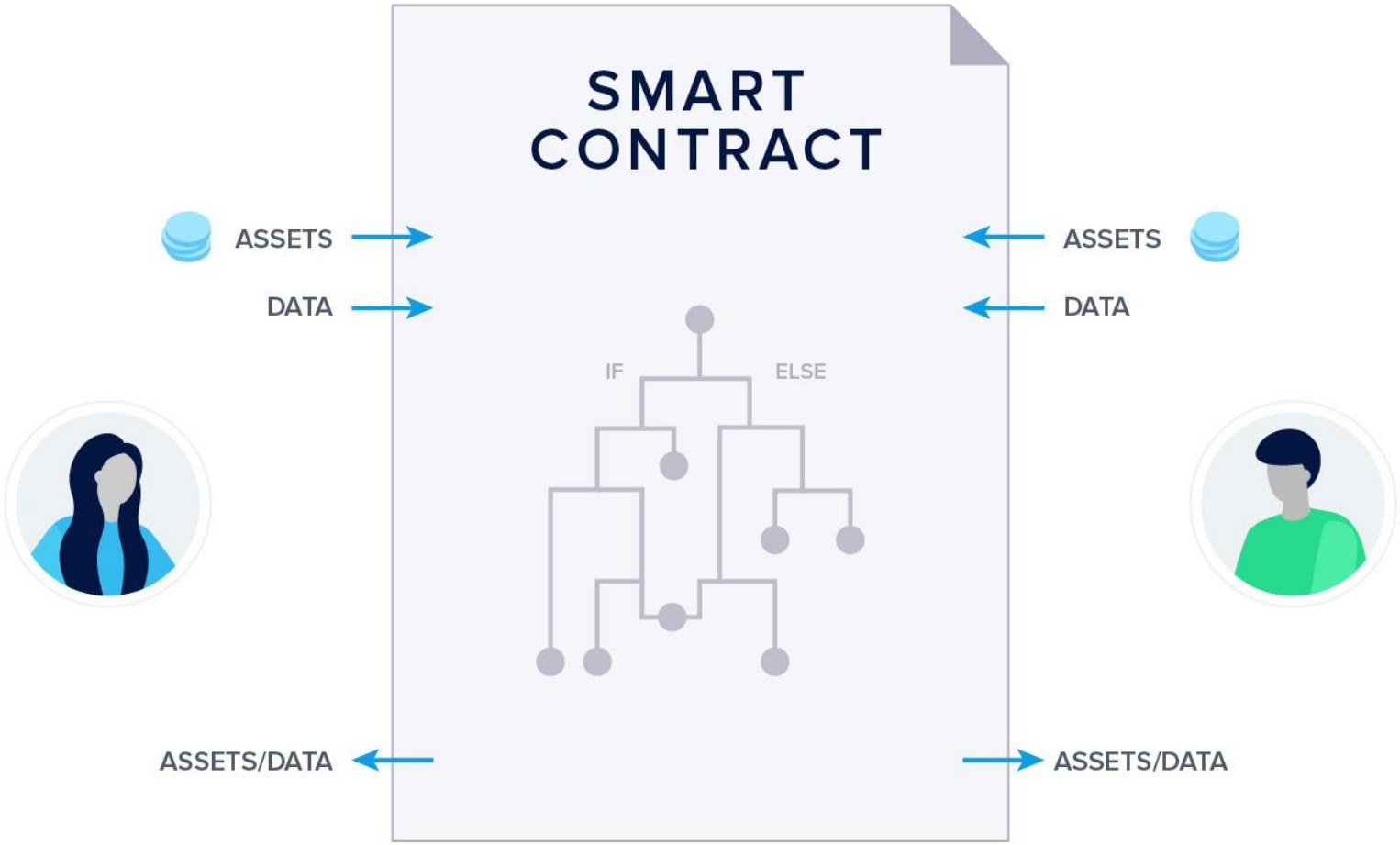
智能合约概述

智能合约的基本概念



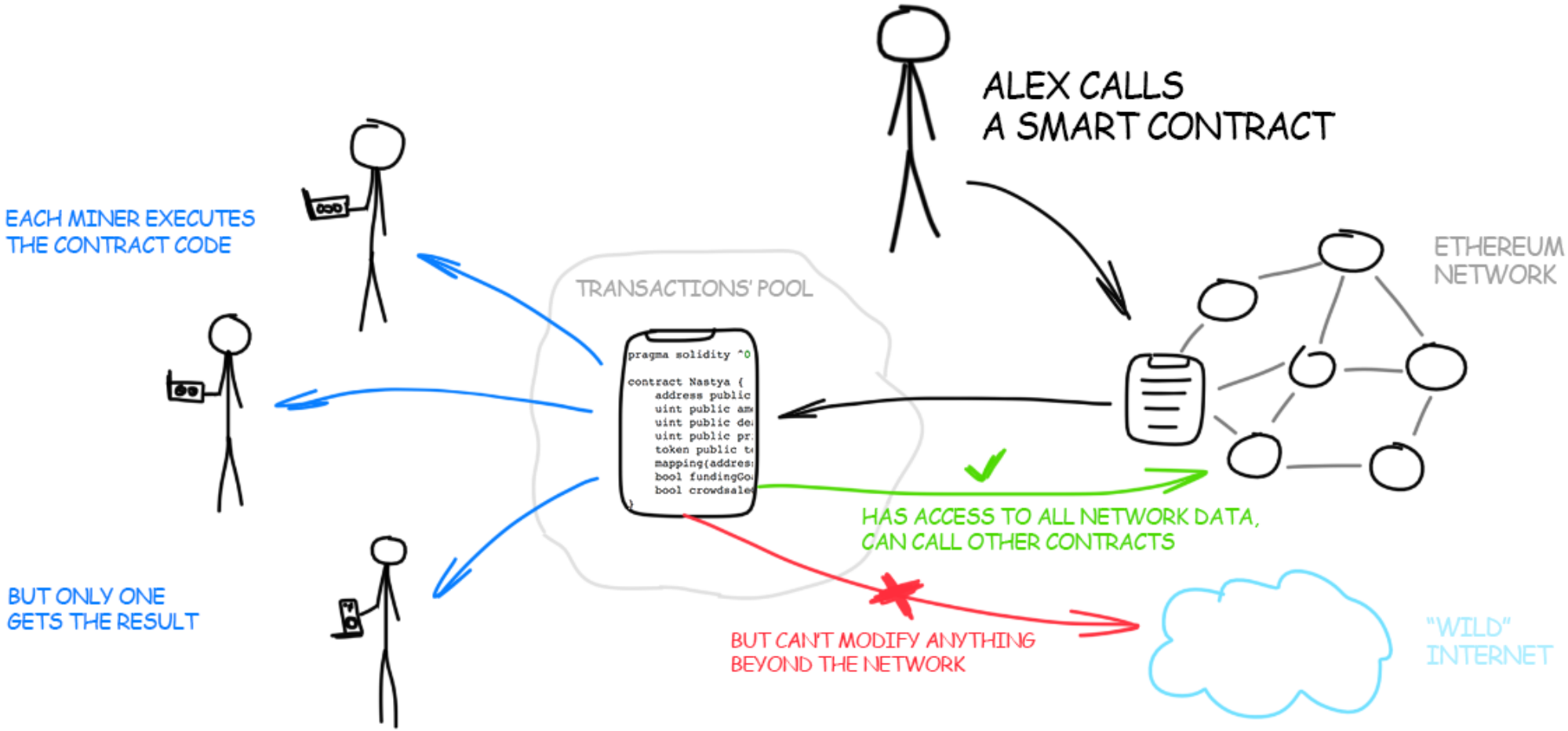
智能合约概述

智能合约的基本概念



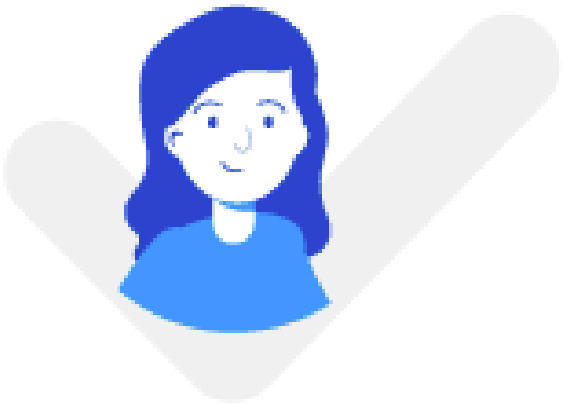
智能合约概述

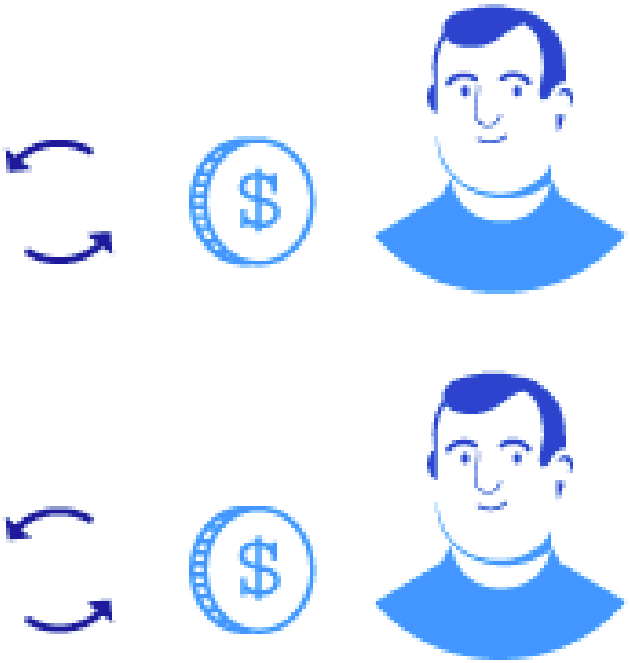
智能合约的基本概念



智能合约概述

智能合约的基本概念





智能合约概述

智能合约的基本概念

ethereum

目录

智能合约的实现原理

智能合约的工作原理

- 智能合约（Smart Contract）
- 一种在区块链体系内制定和执行合约时使用的特殊协议
- 协议中编写了代码函数（Function），函数可以执行基本的逻辑运算，亦能与其他合约进行交互、做决策、存储资料及发送代币（Token）等
- 为了执行协议，合约制定方（通常为交易记录的发起方）需要提供一定的加密货币给区块链节点作为代价
- 区块链节点将验证合约代码，并运行合约内所订立的条件

智能合约的实现原理

智能合约的工作原理

- 智能合约允许在没有第三方的情况下进行可信交易
- 这些交易可追踪且不可逆转
- 智能合约的主要目的是：
- 提供优于传统合约方法的安全性（例如法院）
- 减少与合约相关的其他附加成本（例如律师）

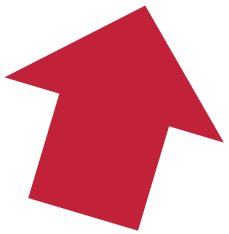
智能合约的实现原理

逻辑计算合约

```
from .sandbox import Sandbox


class Transaction(Base):
    def __init__(self, ···, contract: str = None):
        ···
        self.contract_code = contract
        self.contract_result = None
    ···

    def execute(self):
        self.contract_result = Sandbox.run(self.contract)
```



智能合约的实现原理

逻辑计算合约

```
class Builder:
    ...
    def run(self, ...):
        while True:
            pool = pickle.loads(self.db.get('pool'))
            ...

            for transaction in pool:
                ...

                transaction.execute()
                block.add(transaction)

        ...
```

智能合约的实现原理

逻辑计算合约

- AWS Lambda 函数计算
- https://aws.amazon.com/lambda/
- 函数计算是事件驱动的全托管计算服务
- 通过函数计算，用户无需管理服务器等基础设施，只需编写代码并上传
- 函数计算会准备好计算资源，以弹性、可靠的方式运行代码，并提供日志查询、性能监控、报警等功能

智能合约的实现原理

逻辑计算合约

- 分散式应用程序（Decentralized Application）
- 又名为去中心化应用程序
- 依靠区块链技术核心所开发出来的应用程序
- 简称 Dapp、dApp、Dapp 或 dapp
- 刚才展示的「掷骰子」的游戏就是一个典型的 Dapp

智能合约的实现原理

代币合约

- 代币（Token）
- 通过智能合约的方式记录自定义发行的数字货币
- 用户可以通过智能合约创建自己的发行规则
- 使用区块链技术创建属于自己的“侧链（Side-chain）”
- “使用 C++ 撰写 C++ 的编译器”

智能合约的实现原理

代币合约

- ERC-20 合约规范
- https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
- 一个通常被用于建立同质化代币（Fungible Tokens，简称“代币”）交易记录的共识规范
- 主要由 ETH 创立，其他的主链也有遵守或模仿

智能合约的实现原理

代币合约

- ERC-721 合约规范
- http://erc721.org/
- 一个通常用于建立非同质化代币（Non-fungible Tokens 或 Unique Tokens）交易记录的共识规范
- 主要由 ETH 创立，其他的主链也有遵守或模仿

智能合约的实现原理

智能合约的优点

- 智能合约在不同节点上的运行结果保持一致
- 合约一旦执行，不可逆转
- 合约内容完全开源，任何用户都可验证合约及节点的可靠性
- 合约的运行结果无需额外的质检和验证流程

智能合约的实现原理

智能合约的缺点

- 通常难以衡量合约的工作量，因此定价并不完全合理
- 合约运行结果非实时，这对实时类应用造成了很大的影响
- 如果安全性要求较高，则由于重复运算而浪费了大量的算力
- 在节点数量较少时无法确认运行结果

目录


tether


BNB


UNISWAP

MAKER

大作业

答辩安排

- 第九章：期末大作业点评
- 2021-12-03
- 10:25-12:00
- 6C-402

大作业

答辩安排

- 答辩顺序将按照分组顺序执行
- 每个小组 15 分钟
- 答辩过程需要包括 PPT 展示、项目展示（可录视频）、Q&A 三部分
- PPT 只需要一个人来讲，但全部小组成员必须到场

大作业

答辩安排

- 在答辩开始之前：
- 将全部源代码打包（建议 7z 或 tar.gz 格式）
- 准备好 PPT 和大作业报告
- 将以上三份文件提交到作业系统的“期末大作业”中

总结

- 袁煜明《区块链技术进阶指南》，机械工业出版社
- http://product.dangdang.com/28538836.html

- 安德烈亚斯·安东诺普洛斯《精通区块链编程：加密货币原理、方法和应用开发》第二版，机械工业出版社
- http://product.dangdang.com/27877333.html

总结

- Bitcoin 比特币
- https://bitcoin.org

- Ethereum 以太坊
- https://ethereum.org

東莞理工學院
DONGGUAN UNIVERSITY OF TECHNOLOGY

Thank You!

丁烨，网络空间安全学院 副教授
dingye@dgut.edu.cn