Cryptocurrencies, Blockchains, and Applications

Nicolas Christin
Associate Research Professor
Carnegie Mellon University
School of Computer Science and Department of Engineering & Public Policy
nicolasc@cmu.edu

Agenda

1. Fundamentals: Bitcoin as a case study
2. Production and incentives
3. Beyond currencies: smart contracts and ICOs
4. Beyond currencies: How to select the right (if any) blockchain and case studies

1. Fundamentals

Bitcoin primer (1/2)

- A peer-to-peer digital payment system
- Completely decentralized digital currency
  - **No central mint** to produce currency
  - **No central bank** to verify transactions
    - Verification needed for digital currencies, are duplication of coins simply means "copying bits"
      - Without verification double-spending is possible
      - Physical currencies avoid this by using physical security features
  - Once confirmed, transactions are **irreversible**
  - Predictable, capped, currency supply
- Key innovation in Bitcoin: coin production and verification is done by **network consensus**

Bitcoin primer (2/2)

- **There is actually no notion of a "coin"**
  - Although Casascius provides neat physical artifacts
    - Those are technically one-time use wallets

- Bitcoins are exchanged from "wallet" to "wallet"
- **Transactions** are at the heart of the protocol
- Wallets are represented by **addresses** (e.g., *1VayNert*…)
  - (An address is essentially the public key of the wallet)

Bitcoin transactions

- Alice wants to send 1 BTC to Bob
  - She picks a transaction (or a group of transactions) that she has previously been the recipient of and that cumulatively contain at least 1 BTC
  - She then appends Bob's wallet address to the transaction and digitally signs it
- When Bob subsequently wants to spend the 1 BTC, all he has to do is to repeat the operation

Title search: Cryptocurrencies, Blockchains and Applications

Also available as part of the eCourse
2019 Nonprofit Organizations eConference

First appeared as part of the conference materials for the
36th Annual Nonprofit Organizations Institute session
"Demystifying Blockchain, Bitcoin, and Cryptocurrencies"