Blockchain technology and its' use-cases in computer networks

Sabidur Rahman

Networks Lab

UC Davis

Oct. 19, 2018

krahman@ucdavis.edu http://www.linkedin.com/in/kmsabidurrahman/

Cash

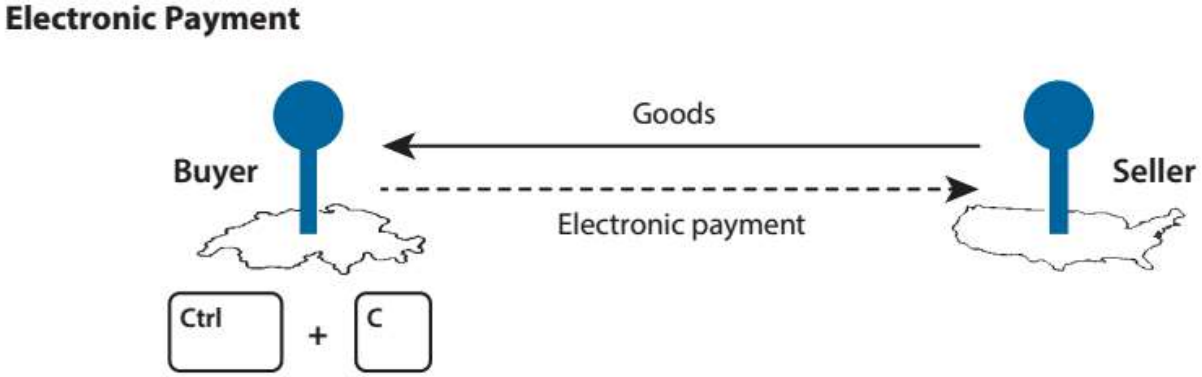
- Cash is represented by a physical object, usually a coin or a note
- When Cash is handed to another individual, its unit of value is also transferred, without the need for a third party to be involved

Aleksander Berentsen and Fabian Schär, "A Short Introduction to the World of Cryptocurrencies ", *Federal Reserve Bank of St. Louis Review*, vol. 100, no. 1, pp. 1-16, 2018.

UCDAVIS

Digital cash - electronic payments

- An ideal payment system would be one in which monetary value could be transferred electronically via cash data files
- But, electronic files can be copied and used again. This problem is termed the "**double spending problem**"

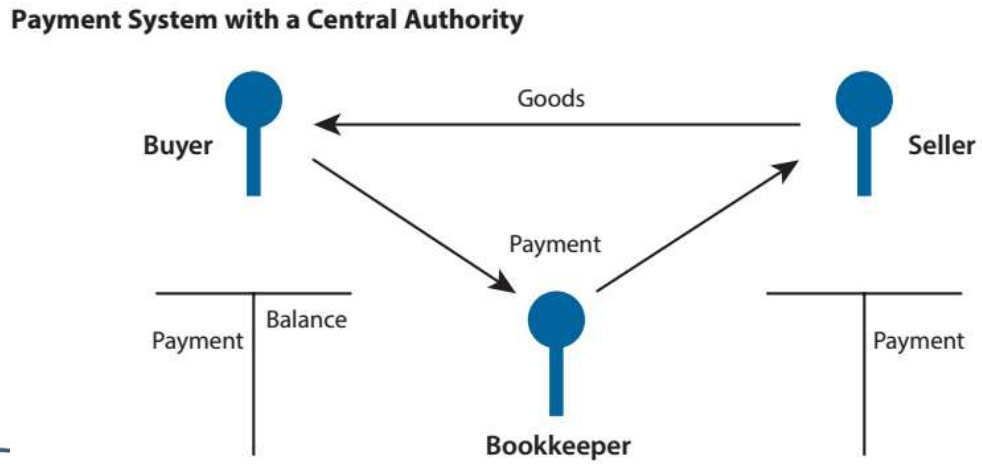


Aleksander Berentsen and Fabian Schär, "A Short Introduction to the World of Cryptocurrencies ", *Federal Reserve Bank of St. Louis Review*, vol. 100, no. 1, pp. 1-16, 2018.

UCDAVIS

Digital cash - electronic payments

- Classical electronic payment systems are based on a central authority that verifies the legitimacy of the payments and keeps track of the current state of ownership. In such systems, a central authority (usually a bank) manages the accounts of buyers and sellers



Aleksander Berentsen and Fabian Schär, "A Short Introduction to the World of Cryptocurrencies ", *Federal Reserve Bank of St. Louis Review*, vol. 100, no. 1, pp. 1-16, 2018.

Stone Money of Yap Island

- Protection against inflation: stones were quarried almost 280 miles away on the island of Palau and brought to Yap by small boats, costly laborious process
- Virtual ownership transfer, avoiding costly physical transfer of the stone money
- Publicly shared ownership: It was sufficient that all the inhabitants knew who the owner of every stone was

https://www.amusingplanet.com

William H. Furness, "*The Island of Stone Money: Uap of the Carolines,*" J. B. Lippincott, Philadelphia, 1910.

UCDAVIS

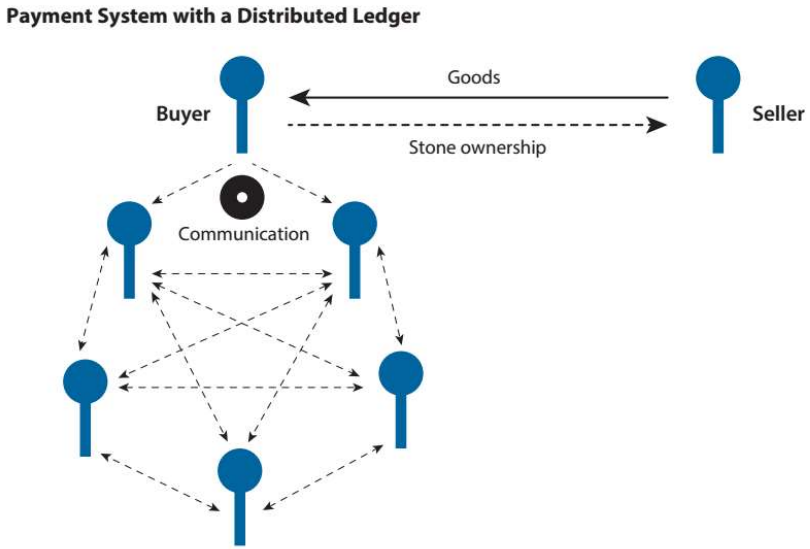
Bitcoin and blockchain

- Bitcoin (and its' public transaction ledger technology "blockchain") was originated with the white paper that was published in 2008 under the pseudonym "Satoshi Nakamoto" (still anonymous). It was published via a mailing list for cryptography and has a similar appearance to an academic paper
- The creators' original motivation behind Bitcoin was to develop a cash-like payment system that permitted electronic transactions but that also included many of the advantageous characteristics of physical cash
- The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server

Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008; https://bitcoin.org/bitcoin.pdf.

Bitcoin and blockchain

- Key feature of the Bitcoin system is the absence of a centrally managed ledger. There is no central authority with an exclusive right to keep accounts
- "It was sufficient that all the inhabitants knew who the owner of every stone was"



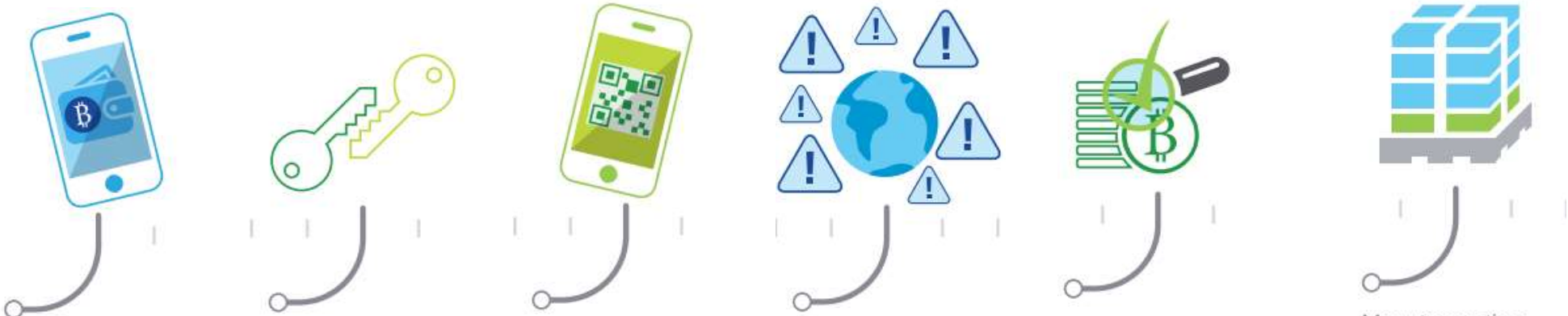
What is in a blockchain?

- Despite its apparent complexity, a blockchain is just another type of database for recording transactions – one that is copied to all of the computers in a participating network
- A blockchain is thus sometimes referred to as a 'distributed ledger'
- Data in a blockchain is stored in fixed structures called 'blocks'
- The important parts of a block are:
  - Header, which includes metadata, such as a unique block reference number, the time the block was created and a link back to the previous block
  - Content, usually a validated list of digital assets and instruction statements, such as transactions made, their amounts and the addresses of the parties to those transactions
- Given the latest block, it is possible to access all previous blocks linked together in the chain, so a blockchain database retains the complete history of all assets and instructions executed since the very first one – making its data verifiable and independently auditable. As the number of participants grows, it becomes harder for malicious actors to overcome the verification activities of the majority. Therefore the network becomes increasingly robust and secure

Bitcoin and Blockchain

- Satoshi Nakamoto defined an **electronic coin** – the Bitcoin – as *"a chain of digital signatures"* known as the 'blockchain'
- The **blockchain** enables each coin owner to transfer an amount of currency directly to any other party connected to the same network without the need for a financial institution to mediate the exchange
- Bitcoin, like other implementation of blockchains, uses cryptography to validate transactions, which is why digital currencies are often referred to as '**cryptocurrencies**'
- Bitcoin users gain access to their balance through a password known as a private key
- Transactions are validated by a network of users called '**miners**', who donate their computer power in exchange for the chance to gain additional bitcoins using a shared database and distributed processing

How does blockchain based cryptocurrency work?



Bob owes Alice money for lunch. He installs an app on his smartphone to create a new Bitcoin wallet. A wallet app is like a mobile banking app and a wallet is like a bank account.

To pay her, he needs two pieces of information: his private key and her public key.

Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.*

The app alerts Bitcoin 'miners' around the world of the impending transaction. 'Miners' provide transaction verification services.

The miners verify that Bob has enough bitcoins to make the payment.

Many transactions occur in the network at any time. All the pending transactions in a given timeframe are grouped (in a block) for verification. Each block has a unique identifying number, creation time and reference to the previous block.

"Blockchain Enigma. Paradox. Opportunity" by Deloitte LLP, 2017.

Blockchain breakdown

The new block is put in the network so that miners can verify if its transactions are legitimate. Verification is accomplished by completing complex cryptographic computations.

When a miner solves the cryptographic problem, the discovery is announced to the rest of the network.

The algorithm rewards the winning miner with 25 bitcoins, and the new block is added to the front of the blockchain. Each block joins the prior block so a chain is made – the blockchain.

Within ten minutes of Bob initiating the transaction, he and Alice each receive the first confirmation that the bitcoin was signed over to her.

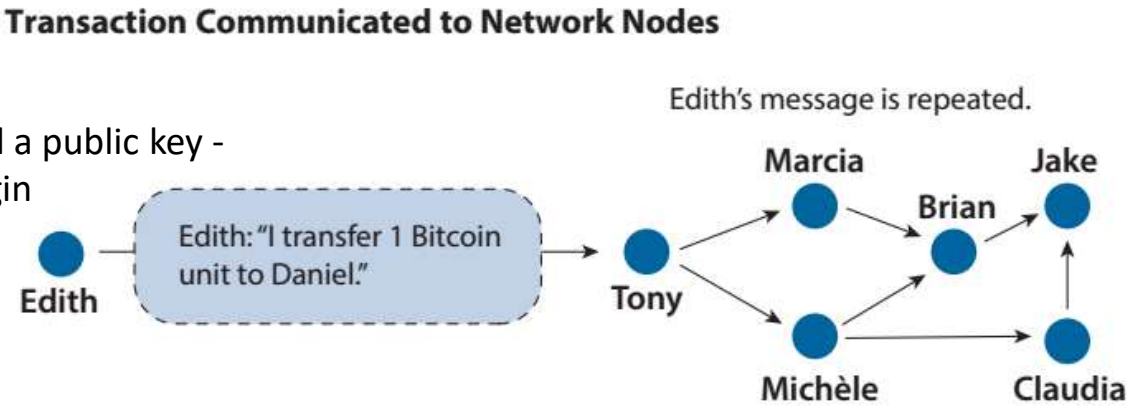
All the transactions in the block are now fulfilled and Alice gets paid.

Security aspects - authenticity

proof-of-work consensus protocol: a game theoretical perspective

- How do the nodes know that the initiator of the transaction is the rightful owner and that he or she is thereby entitled to transfer the Bitcoin units?

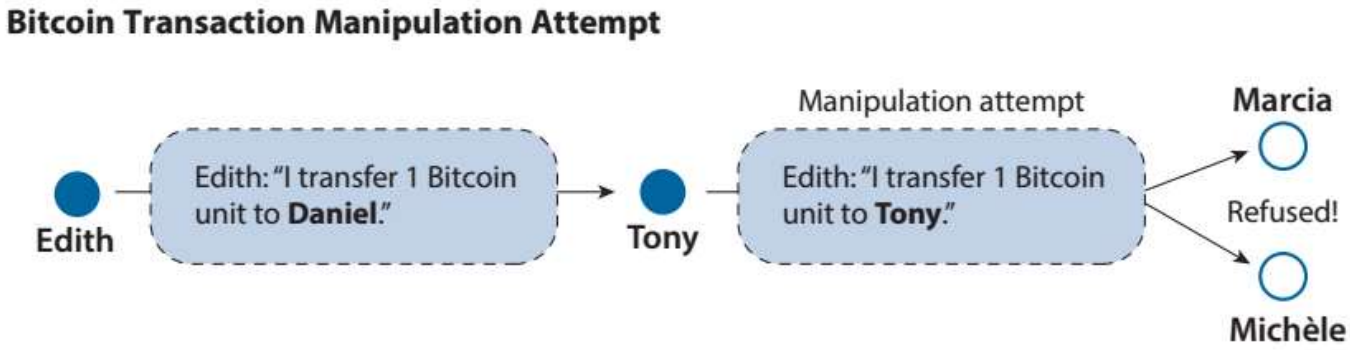
Signature: using a private and a public key - validate the transaction's origin



Security aspects - integrity

- How can one ensure that the transaction message will not be tampered with before it is passed from one node to the next?

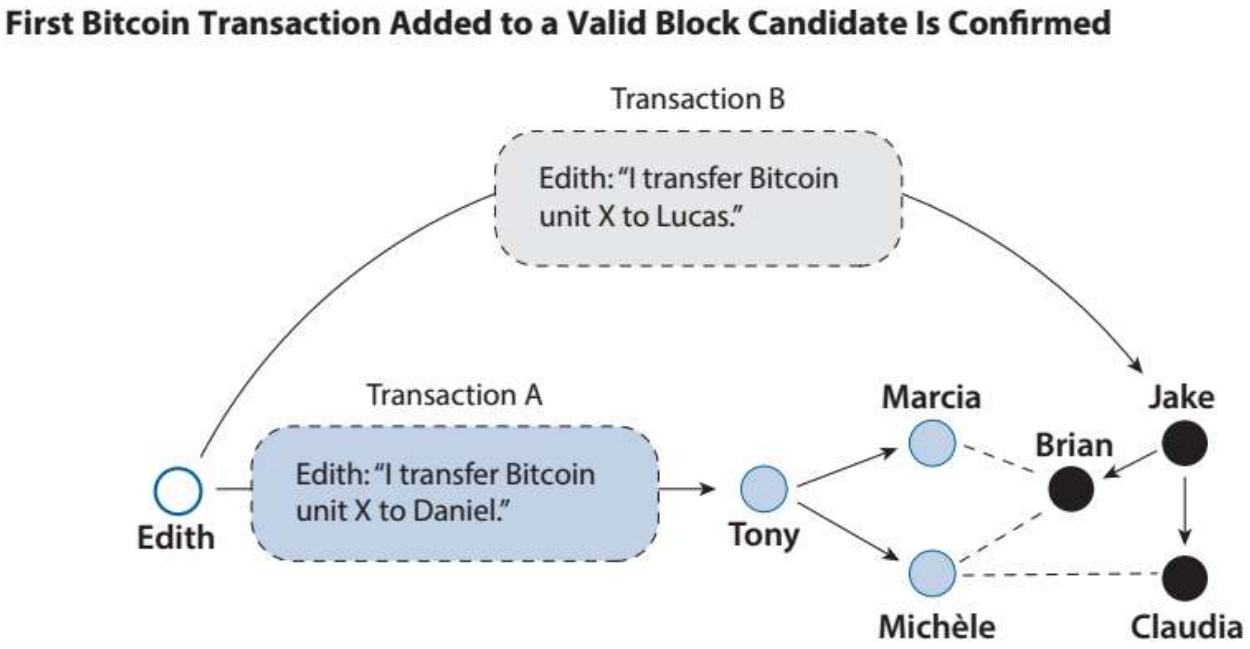
Signature: using a private and a public key - validate the transaction's origin



Security aspects - double spending problem

- If two transactions both referencing to the same Bitcoin units are issued. Both transactions could be propagated simultaneously over the network (transaction capability), and both would display a valid origin (transaction legitimacy).
- Because of differences in the propagation of these two messages in the Bitcoin network, some of the nodes would first receive a message for transaction A while others would first receive a message for transaction B
- Transaction that is first added to a valid block candidate, and therefore added to the Blockchain, is considered confirmed. System ceases to process the other one. Miners will stop adding the conflicting transaction to their block candidates
- It is not possible for a miner to add conflicting transactions to the same block candidate. Such a block would be illegitimate and thus be rejected by all the other network participants

Security aspects - double spending problem



What's next?

- Blockchain in internet of things – Smart City
  - The proposed architecture is hierarchical, and consists of smart homes, an overlay network and cloud storages coordinating data transactions with BC to provide privacy and security
- Blockchain in Vehicular Network
  - A Distributed Blockchain Based Vehicular Network Architecture in Smart City
  - Block-VN is a reliable and secure architecture that operates in a distributed way to build the new distributed transport management system

Blockchain solutions are being planned to protect data from the UK's nuclear power stations, flood-defence mechanisms, and other critical infrastructure

P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart City", Journal of Information Processing Systems, vol. 13, no. 1 pp. 84, Mar. 2017.

A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," In IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618-623, Mar. 2017

B. Leiding, P. Memarmoshrefi, D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," In Proceedings of ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 137-140, Sep. 2017.

Thanks!

krahman@ucdavis.edu

http://www.linkedin.com/in/kmsabidurrahman/