



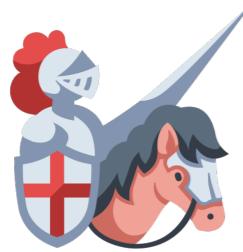
Blockchain Background

Byzantine Generals' Problem

Byzantine Generals' Problem



Byzantine Generals' Problem



Attack?



Byzantine Generals' Problem



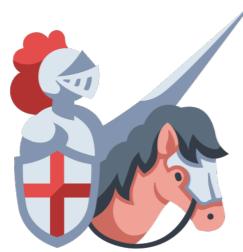
Attack?



Retreat?



Byzantine Generals' Problem



Attack?



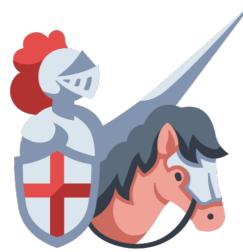
Retreat?



Attack?



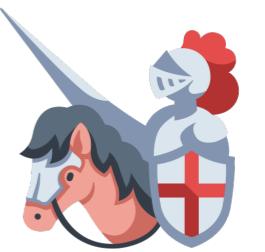
Byzantine Generals' Problem



Attack?



Retreat?



Attack?



Surrender?

Byzantine Generals' Problem

- Everyone has to know X
- Everyone knows that everyone knows X
- Everyone knows that everyone knows that everyone knows X



Attack?



Retreat?

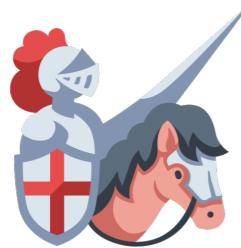


Attack?



Surrender?

Byzantine Generals' Problem



Who does this
coin belong to?



Who does this
coin belong to?



Who does this
coin belong to?



Who does this
coin belong to?

Byzantine Generals' Problem



Who does this
coin belong to?



Who does this
coin belong to?



Who does this
coin belong to?



Who does this
coin belong to?

Byzantine Generals' Problem

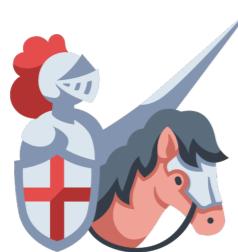


Who does this
coin belong to?

Far away



Who does this
coin belong to?



Who does this
coin belong to?

How to agree, before
taking an action?



Who does this
coin belong to?

(Centralised) Digital Payment Systems



Alice



The coin belongs to Alice.



Bob



- Examples
 - Pepper Micropayments [Rivest]
 - ECash [David Chaum] (privacy preserving)

(Decentralised) Digital Payment Systems



The coin belongs
to Alice.



The coin belongs
to Alice.

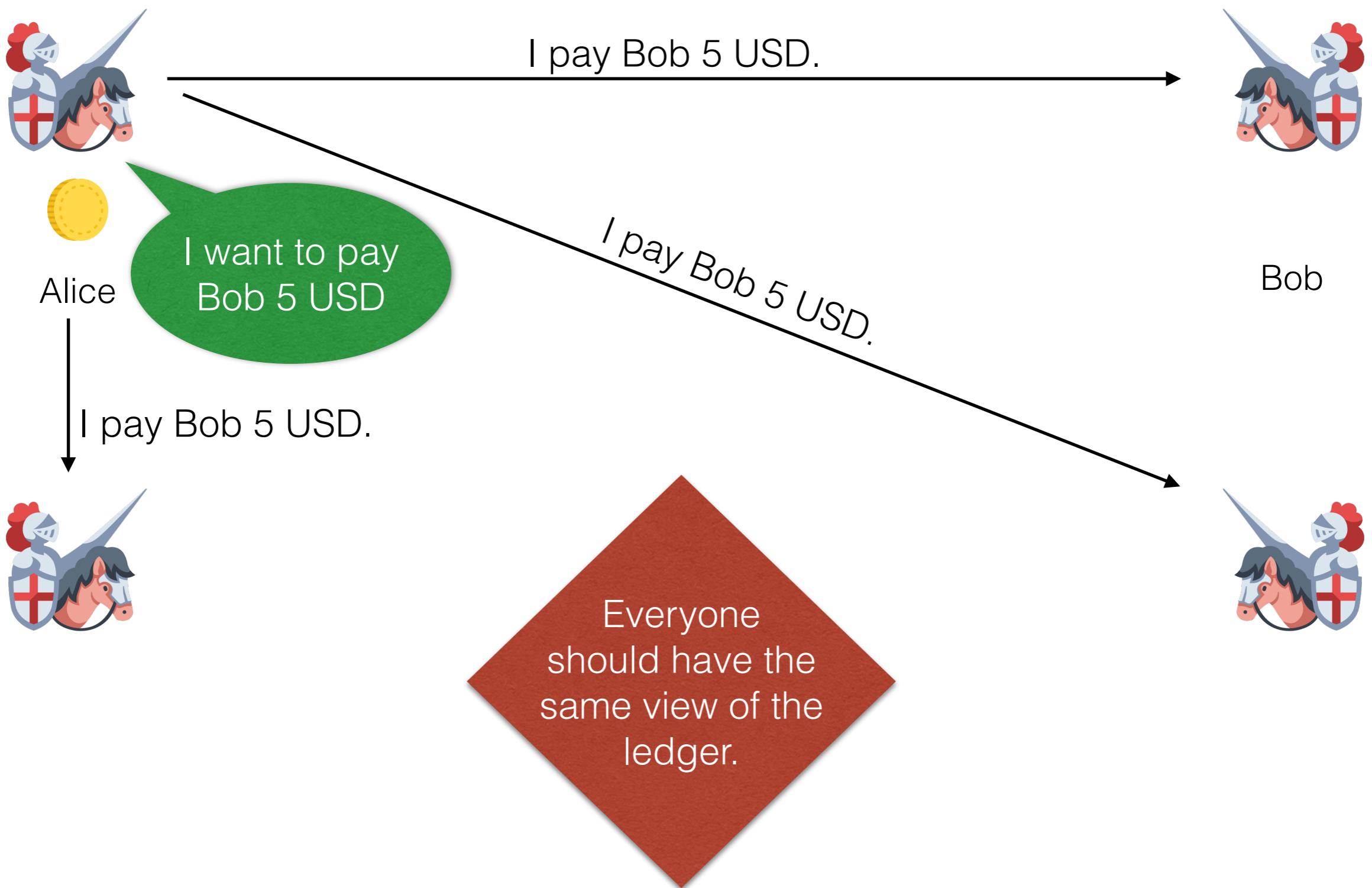


The coin belongs
to Alice.



The coin belongs
to Bob.

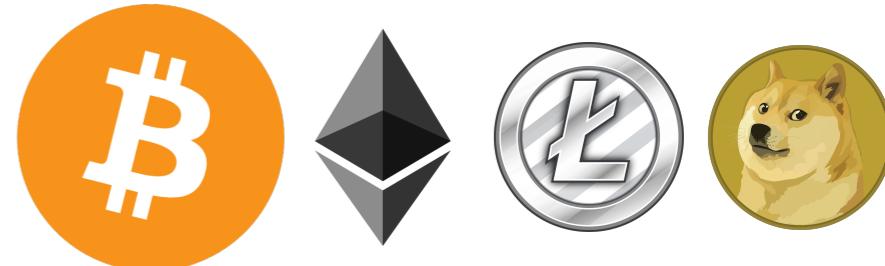
(Decentralised) Digital Payment Systems



Blockchain != Blockchain

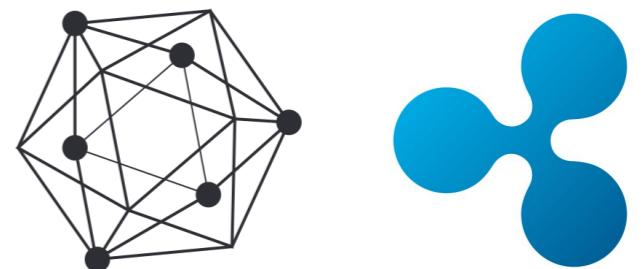
Open and Decentralised Blockchains

- Ethereum
- Bitcoin



Permission-based Blockchains

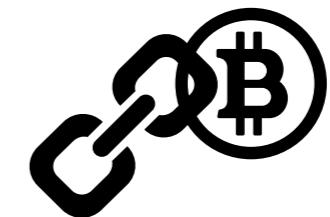
- Hyperledger
- Ripple
- Stellar



Bitcoin



- First introduced in 2009
 - Pseudonym Satoshi Nakamoto
- Peer-to-peer decentralised currency
- No trusted third parties (???)
- Blockchain: distributed DB
 - ▶ Transactions
 - ▶ Blocks



Bitcoin

- First introduced in 2009
- Pseudonymous
- Peer-to-peer
- No trusted third party
- Blockchain
- ▶ Transactions
- ▶ Blocks

The screenshot shows a PDF document titled "Is Bitcoin a Decentralized Currency?" by Arthur Gervais, Ghassan O. Karamé, Srdjan Capkun, and Vedran Capkun. The document is from an IACR eprint, specifically https://eprint.iacr.org/2013/829.pdf. The abstract discusses the decentralized nature of Bitcoin, noting that while it promises decentralization, recent incidents and observations reveal significant centralization. It highlights that a limited set of entities control vital operations like mining and incident resolution. The keywords listed are Bitcoin and Decentralized decision process.

Is Bitcoin a Decentralized Currency?

Arthur Gervais* Ghassan O. Karamé** Srdjan Capkun*
Vedran Capkun***
*ETH Zurich, 8092 Zuerich, Switzerland.
**NEC Laboratories Europe, 69115 Heidelberg, Germany.
***HEC Paris, France.

Abstract

Bitcoin has achieved large-scale acceptance and popularity by promising its users a fully decentralized and low-cost virtual currency system. However, recent incidents and observations are revealing the true limits of decentralization in the Bitcoin system. In this article, we show that the vital operations and decisions that Bitcoin is currently undertaking are not decentralized. More specifically, we show that a limited set of entities currently control the services, decision making, mining, and the incident resolution processes in Bitcoin. We also show that third-party entities can unilaterally decide to “devalue” any specific set of Bitcoin addresses pertaining to any entity participating in the system. Finally, we explore possible avenues to enhance the decentralization in the Bitcoin system.

Keywords: Bitcoin, Decentralized decision process

1 Introduction

Bitcoin has witnessed a wider adoption and attention than any other digital currency proposed to date. One reason for such a broad adoption of Bitcoin has been a promise of a low-cost and decentralized currency that is inherently independent of governments and of any centralized authority [1]. In this work, we analyze the (de-)centralized nature of Bitcoin and show that—contrary to widespread belief—Bitcoin is not a truly decentralized system as it is deployed and implemented today.

Namely, in Bitcoin, the users “vote” with their computing power to prevent double-spending (i.e., by *power-voting*) which effectively limits the power of individual users and makes Sybil attacks difficult. Given the huge computing power harnessed in the Bitcoin system (currently around 30,000 Tera hashes per second), users believe that it is unlikely for any entity to acquire such power alone. However, even a quick look at the distribution of computing power in Bitcoin reveals that the power of dedicated “miners” far exceeds the power that individual users dedicate to mining, allowing few parties to effectively control the currency; currently the top-three (centrally managed) mining pools control more than 50% of the computing power in Bitcoin. Indeed, while mining and block generation in Bitcoin was originally designed to be decentralized, these processes are currently largely centralized.

On the other hand, other Bitcoin operations, like protocol updates and incident resolution are not designed to be decentralized, and are controlled by a small number of administrators whose

