Summary of Ethereum

Xiaojie Zhu

February 27, 2018

1 Introduction

Ethereum is proposed to make up the weakness of the Bitcoin. Specifically, It address the problem of lack of turing-completeness, value-blindness, lack of state and blockchain-blindness.

Since Bitcoin does not support loop, it is space in-efficient. For example, repeated code has to be included for implementing a loop. However, due to this setting, Bitcoin does not have infinite loop issue. In Ethereum, the loop is supported. For solving the infinite loop, it adopts the maximum operation and gas limit mechanism. For each contract, the maximum number of operations is set and each operation is supported by the gas cost. If the gas is spent out before the contract is executed completely, the gas is assigned to miner and the contract is reverted. In Bitcoin, the UTXO only has two states. spent or unspent, which is limited in applications. For example, multi-stage contracts or scripts are not supported. Since the UTXO only supports the binary states, it is hard to record the *internal* state, which results in lack of supporting applications referring to internal states, e.g., withdrawal. In Ethereum, the state is maintained in the contract. Although it needs extra storage and operations, it brings more application support. Value blindness and blockchain blindness results from the lack of state. As no state is maintained, it is impossible to trace back to evaluate the value. Due to that, the applications referring to modifying the multi-stage data is not supported.

2 Applications

Generally, all the applications based on the ethereum can be classified into three categories, financial applications, semi-financial applications, and non-finantial applications.

The financial applications provides users a powerful way to entering into the smart contracts by using money. For example, users can buy the system currency in ethereum. For the semi-financial application, the token system is a representative. Based on the token issued in the ethereum, many applications is executed by adopting the token as a metric. In

addition to financial applications, it also can be applied to other scenario, e.g., file storage, identity management, and reputation system.