Mimblewimble and Grin（メモ）

じょんた

2017 年 6 月 28 日

1 Introduction

- Grin は Mimblewimble を実装するためのプロジェクトの名前
- デフォルトで匿名性を保とうぜ
- トランザクションの数ではなく、ユーザーの数でスケールする。したがって従来のブロックチェーンと比べて容量を節約できる
- 楕円曲線暗号を使う
- asic-resistent というマイニングアルゴリズムが decentralization を encourage するらしい

2 Tongue Tying for Everyone

2.1 ECC について簡単に

楕円曲線上の点の集合について考える。ある点 H について、和と積が定義されていて、それらは交換法則と結合法則を満たす。ある数 k を点 H に掛けた答え $k * H$ もまた、楕円曲線上の点の集合に属する。また、実数 k, j と点 H の計算には分配法則も成り立つ。

$$(k + j) * H = k * H + j * H \tag{1}$$

楕円曲線暗号において考えると、十分に大きい数 k を秘密鍵とすると、それに H を掛けた $k * H$ は公開鍵に対応するものだと考えられる。暗号をとこうとして $k * H$ の値から k の値を計算することは不可能に近いので（EC 上での「割り算」はとてもむずかしい)、秘密鍵が悪意のある第三者に知られることはない。

式 (1) が示すのは、２つの秘密鍵の和から計算された公開鍵は、それぞれの秘密鍵から計算された公開鍵の和に等しいということ。Bitcoin の HD ウォレット（階層決定ウォレット？）や Mimblewimble の実装は、この原理が出発点らしい。（Mimblewimble のは点を合計するとゼロってやつだと思われる）

2.2 Mimblewimble での Transaction

Mimblewimble でのトランザクションの承認は以下の２つの原理によって行われる

1. input-output の値がゼロに等しいこと。これだけを確認すればいいので実際の input と output の量は不必要

2. 秘密鍵を所有していることの証明：これは他のブロックチェーンと違うのは、直接トランザクションに署名をするわけではない

2.3 残高

トランザクションの値とは何か。

v がトランザクション input または output だとすると、v の代わりに $v * H$ をトランザクションに組み込める。また、それらの値の和についても

$$v_1 + v_2 = v_3 => v_1 * H + v_2 * H = v_3 * H \tag{2}$$

ということが分かる。

$$\text{commitment} = \text{SHA256}(\ (\text{blinding factor}) \text{ or } (\text{data})\ )$$