Birthday attack:
اگر ۲ مجموعه هر کدام دارای حداقل $k=N^{0.5}$ عنصر از یک مجموعه‌ی N عضوی باشند، احتمال وجود حداقل یک عنصر مشترک بین آن‌ها بیشتر از ۰.۵ است.
با n بیت می‌توان ۲^{n} پیام تولید کرد. پس برای ایجاد حمله نیاز است که $۲^{n/۲}$ پیام تولید کنیم و هر کدام را هش کنیم، یکبار برای مجموعه‌ی اول و یکبار برای مجموعه‌ی دوم. پس در مجموع $۲^{n/2+۱}$ پیام نیاز است.
نکته: اگر در زمان hash کردن، هش تکراری مشاهده شد، در همان لحظه collision یافته‌ایم.

تنها چیزی که در بلاکچین ذخیره می‌شود، مرکل روت است. خود تراکنش‌ها که شامل هش و امضا هستند به صورت جداگانه ذخیره می‌شوند. آخرین وضعیت موجودی‌ها نیز در utxo ذخیره می‌شود.
به عبارتی دیگر، تراکنش‌ها شامل امضا هستند. این تراکنش‌ها را هش کرده و در قالب درخت مرکل در می‌آوریم و سپس ریشه را در بلاک ذخیره می‌کنیم.

عدد بزرگ به راحتی فاکتور می‌شود. در نتیجه، p و q به دست می‌آید سپس $p-1$ و $q-1$ به دست می‌آید و می‌توان کلید خصوصی را به دست آورد.

با کوچک شدن p و q، فضای جستجو کوچک می‌شود و حمله‌ی brute force راحتتر می‌شود.

Message Authentication using HMAC provides integrity and authenticity.
Hash functions doesn’t provide confidentiality and availability.

مانند بیتکوین در تولید آدرس، تولید digest تراکنش و ساخت زنجیره با اشاره به بلاک قبلی استفاده می‌شود. همچنین کاربردهای زیر را دارد:

- تولید آدرس قراردادهای هوشمند
- تولید اعداد تصادفی
- تشخیص داده‌های تکراری (مقاله‌ی hyperloglog)