

displaced paper currencies in millions of transactions per year. Improvements in the verification and recordation of such electronic transactions will continue to increase the features and options available to operators engaging in electronic transactions.

SUMMARY

[003a] According to a first aspect of the present invention, there is provided a cryptologic system comprising: memory; a blockchain stored in the memory, the blockchain comprising a block with original data, the blockchain secured by a first integrity output for a first integrity code, the first integrity code is configured to yield the first integrity output when applied to the original data; and rewrite circuitry in data communication with the memory, the rewrite circuitry configured to: access the blockchain; access a key secret for the first integrity code, the key secret facilitating identification of collision data, the collision data different from the original data, the first integrity code is configured to yield the first integrity output when applied to the collision data; receive a command to rewrite the original data in the block with altered data that is different than the original data, the first integrity code does not yield the first integrity output when applied to the altered data; generate additional data responsive to the key secret and the altered data; generate the collision data based on the altered data and the additional data; and rewrite the block with the collision data.

[003b] According to a second aspect of the present invention, there is provided a method comprising: in a cryptologic hardware security system: accessing, using processing circuitry, a key secret for a blockchain; determining, with the processing circuitry, to rewrite original data in a selected block of the blockchain with altered data that is different than the original data previously stored in the selected block; and determining, with the processing circuitry and using the key secret, collision data including the altered data, the collision data coding-consistent with a previously determined integrity output stored within a specific block of the blockchain that follows the selected block, the previously determined integrity output generated responsive to and coding-consistent with the original data.

BRIEF DESCRIPTION OF THE DRAWINGS

- [004]** Figure 1 shows two example views of a blockchain.
- [005]** Figure 2 shows two example rewrites to the example blockchain of Figure 1.
- [006]** Figure 3 shows an example blockchain processing system.
- [007]** Figure 4 shows an example blockchain rewriting system.
- [008]** Figure 5 shows example rewrite management logic.
- [009]** Figure 6 shows example rewrite logic.
- [010]** Figure 7A shows two example collision searches.
- [011]** Figure 7B shows an example rewrite to a blockchain using a collision.
- [012]** Figure 8 shows an example blockchain portion paired with an example updated blockchain portion.
- [013]** Figure 9 shows an example dual-link blockchain portion.
- [014]** Figure 10 shows an example hybrid blockchain.
- [015]** Figure 11 shows an example rewritable blockchain scenario.
- [016]** Figure 12 shows an example distributed key secret blockchain rewrite scenario.
- [017]** Figure 13 shows an example blockchain record maintenance scenario.
- [018]** Figure 14 shows an example internet of things rewriteable blockchain scenario.
- [019]** Figure 15 shows example blockchain loops.

DETAILED DESCRIPTION

[020] A blockchain may include a series of data blocks, the blocks including a code, such as a cryptographic hash or checksum, which may be coding-consistent with the content of previous blocks in the series. In some cases, determining multiple different sets of blocks that produce the same integrity code may be insoluble, prohibitively computationally complex, or otherwise effort intensive enough to frustrate attempts to tamper with the contents of the blockchain while maintaining the self-consistence of the integrity codes. However, in some implementations a trusted party may have access to a key secret, or portion of a key secret, such that the party, acting alone or with those in