Addressing the Conflict Between Blockchain and GDPR Article 17

By Jeff Stollman, Principal Consultant, Rocky Mountain Technical Marketing, inc. (RMTM)

One of the principal goals of blockchain technology is to create an immutable source of truth that can be trusted by all parties to provide a durable, immutable, and accurate log of transactions committed to the blockchain.

One of the goals of the European Union's General Data Protection Regulation (GDPR) is to afford individual actors the "right to erasure", i.e., to allow them to remove their personal information from shared data bases. Specifically, GDPR Article 17 states,

> 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
>
>   1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
>   2. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
>   3. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
>
>   4. the personal data have been unlawfully processed;
>
>   5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
>
>   6. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

These two goals give the immediate appearance of being in conflict with one another. The authors of the GDPR had the foresight to recognize that there may be technical or economic challenges to addressing this requirement. Article 17 goes on in Section 2 to acknowledge that:

> 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

In Section 3, Article 17 also provides a list of exceptions to the regulation including:

5. for the establishment, exercise or defence of legal claims.

Arguably, the above exception may apply to most blockchains that may be implemented to track a wide array of personal and public health information tracked on blockchains. But wouldn't it be better to be able to comply with Article 17 to satisfy the "data subject" desiring to have his/her record removed from the blockchain and still be able to address the exercise or defense of legal claims?

We looked into this problem because it has applicability well beyond the healthcare industry. As a result of our investigation, we devised a simple technical solution that

1. satisfies the needs of a data subject to have its personal information removed from the blockchain
2. retains the immutable history of the blockchain record
3. provides the necessary support for legal claims that may be evidenced by the blockchain record.

1. RMTM's solution

Our solution is relatively simple; we create sequenced versions of the blockchain. For those old enough to remember, printed encyclopedias provide an example of our solution. To keep their expensive publications from going out of date, Encyclopedia publishers sold customers a large set of volume that covered the world up to the point of publication. But such volumes would rapidly be out of date shortly after publication because historical events and new technologies continued to introduce new information. Customers did not want to pay for an entirely new volume each year. So the publishers issued year books that summarized the new information that would be added to the next version of the encyclopedia. Existing customers could then purchase the yearbook for a significant discount over buying the entire set again.

We propose a similar model for blockchains. The original blockchain will include all records from Transaction 1 to Transaction "n" at a certain point in time. It is the original encyclopedia.

We create the first "yearbook" supplement in four steps.

1. Transactions in the original blockchain are halted at an agreed upon period of time. We then create a "net state" of the initial blockchain. That is, we determine the ending balance for each account on the initial blockchain at the time transactions are halted. For example, if we are tracking the supply chain of widgets, we see that Alice find that Alice started with 20 widgets. She transferred 5 to Bob. If we temporarily halt the blockchain at that point, Alice's "net state" would be 15, Bob's would be 5, and Carol's would be zero..

   We illustrate the "net state" in Figure 1. In the figure, at time t_0 Alice has 20 widgets. No one else has any. This provides a "net state" for Carol of 20 and for Bob and Carol of 0 each.

Partipant	t_0	Net State t_0
Alice	20	20
Bob		0
Carol		0
TOTAL		20

Figure 1: At time t_0, Alice is the only one with widgets. She has a "net state" of 20. Bob and Carol have "net state"s of 0.

Carol then transfers 5 widgets to Bob as shown in Figure 2. At time t_1, Alice's "net state" is reduced from 20 to 15. Bob's "net state" becomes 5. Carol's "net state" remains at 0.

Partipant	t_0	Net State t_0	t_1	Net State t_1
Alice	20	20	-5	15
Bob		0	5	5
Carol		0		0
TOTAL		20		20

Figure 2: At time t_1, Alice has a "net stae" of 15, Bob has a "net state" of 5, and Carol has a "net state" of 0.

Bob then transfers his 5 widgets to Carol as shown in Figure 3. At time t_2, Alice's "net state" remains at 15, Bob's "net state" drops to zero. And Carol's "net state" is now 5.

Partipant	t_0	Net State t_0	t_1	Net State t_1	t_2	Net State t_2
Alice	20	20	-5	15		15
Bob		0	5	5	-5	0
Carol		0		0	5	5
TOTAL		20		20		20

Figure 3: At time t_2, Alice's "net state" remains at 15. Bob's drops to 0. Carol's "net state" is now 5.

A new yearbook version can be created at any point in time. If it is created at t_2, then only the "net state" at time t_2 is carried forward into the new supplement. No prior information is carried forward into the supplement. But all transactions remain in the version that has been halted.

2. We will then create a seed block for the first "yearbook" supplement at t_2.showing the "net state" transactions of each account at t_2. The yearbook will not show the transaction history that brought Alice from 20 to 15, or Carol from 0 to 5. And it will show nothing for Bob, because his "net state" is 0. The individual transactions will remain only in the initial version of the blockchain. We then follow this process for every item tracked on the blockchain for each account owner as illustrated in Figure 4.

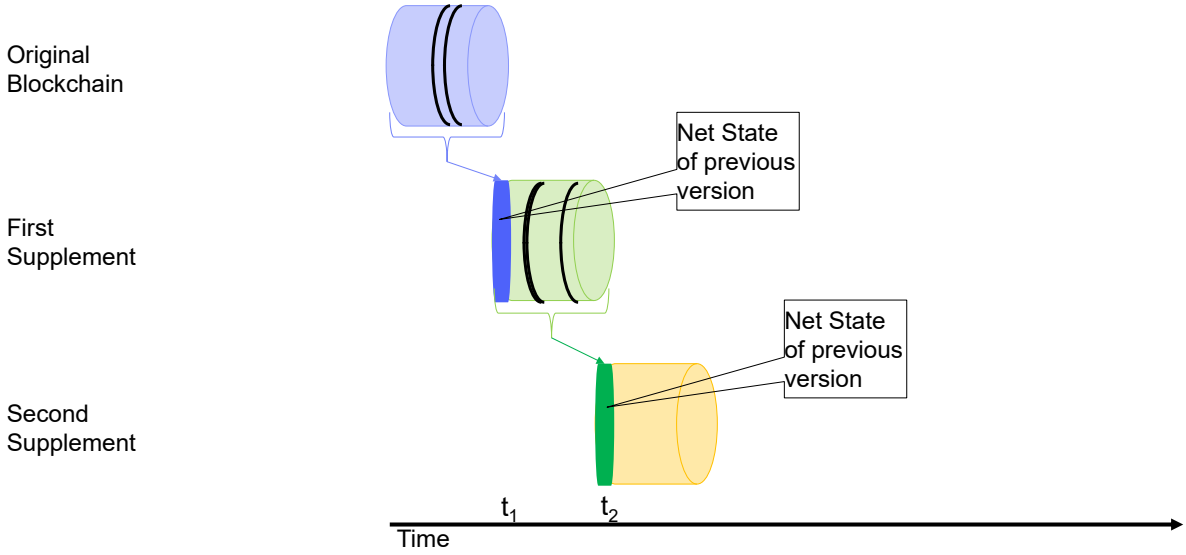

Figure 4: The original blockchain is summarized into new blocks that carry only the "net state" closing balance of the original which serve as the "seed" blocks of the first supplement. Similarly, the first supplement is summarized by creating its "net state" which serves as the starting balance for the second supplement. The black transactions represent those that are not carried forward into the "net state" opening balance of each new supplement. But they remain as part of the archived version of the supplement in which they were created.

We do not add to the yearbook records which the data subject has requested removal. These are represented by the black transactions in Figure 4. These transactions are not carried forward into the next supplement. But they remain in the version in which they were created to maintain the immutability of the blockchain.

Depending on the rules for that blockchain, there may be additional requirements imposed for removing "net states" from the next supplement. For example, in tracking a pharmaceutical inventory, data subjects may only be able to request removal of records for which there is a zero balance. In such a case, only Bob would be allowed to request removal. As can be seen in Figure 3, if Bob is removed from the supplement, the total of the beginning and ending "net state" balances show that the total of all 20 widgets are still accounted for.

In such a case, if Alice or Carol wanted their records to be removed from the supplement, they would be obligated to transfer their widgets before the current version is halted.

3. All new transactions are routed to the current supplement after the "net state" balance has been added as a "seed" block (or blocks).
4. The original blockchain is then taken offline. It can be stored as required by the rules and the blockchain in accordance with any applicable regulatory requirements for either data retention or destruction. (We do not address the potential for conflicting regulations that may arise for blockchains that may be subject to the laws of multiple jurisdictions.)

2. Solution Variations

In some cases, removing the "net state" closing balance for some accounts may be problematic. For example, if a blockchain's rules do not require a zero balance as a condition for removal, the removal of Alice's record from the next supplement will make the total of the closing balances add up to only 5, leaving 15 widgets unaccounted for in the blockchain tracking system.

There are several ways to address this. First, a new identifier could be created to account for all such non-zero transactions. This generic identifier would then be used to add the "net state" of all such transactions to the seed block(s) of the new supplement of the blockchain. To avoid deanonymization of this new identifier, the same identifier might be used for all accounts that have records removed. Depending on the type of information being tracked on the blockchain, this may cause Alice to forfeit her widgets. For example, if the blockchain was tracking cryptocurrency, Alice might lose the value of her currency once her record is removed from the supplement. But if the value is negligible, she might prefer to forgo it to gain the privacy she desired in having her identifier removed from future supplements.

Another way to address this is to bypass the "net state" calculation for each supplement and recreate the entire blockchain, substituting the "generic" identifier for Alice and/or all other removed account owners. This method would require recalculation of all new hashes and nonces for every block in the blockchain (i.e., re-mining) to accommodate the changes to the new supplement. Depending on the block-validation protocol being used by the blockchain, this could be both time consuming and expensive.

For more information on RMTM's blockchain privacy solution, please go to RMTMinc.com and fill-out a contact request.