CouncilFS[A Working Title]

Blockchains and Cryptocurrencies 601.441/641

Gabrielle Beck
Department of Computer Science
Johns Hopkins University
Baltimore, MD
becgabri@jhu.edu

Tushar Jois
Department of Computer Science
Johns Hopkins University
Baltimore, MD
tushar.jois@jhu.edu

April 8, 2019

1 Introduction

2 Related Work

2.1 Alternative Proofs of Work

Our work exists at the cross-section of many different active fields of research. Before this paper, there have been many proposals for Proof-of-Work schemes that serve some useful function or purpose like PrimeCoin. In a previous paper, there has also been a proposal to utilize a POR as a proof of work for the purpose of storing archival information that would be known by all miners so that validation of the files could be assured $\mathcal{F}$. The authors also assume that this file would not be updated and introduce a new stateful signature scheme that should be relatively efficient while also ensuring that a miner cannot "outsource" their computation. This differs from our scheme as we allow for the existence of other files carried by clients that are given directly to trusted nodes, called *Alderman*, and are not verifiable by every single node on the network.

Other alternative proofs of work that are similar to PORs include Proofs of Space, Proofs of Data Possession and Proofs of Erasure. Proofs of Space, for example, guarantee that a miner is holding some space it could be doing computation open and then answer challenges to ensure this is in fact the case. The way this scheme is commonly implemented is to use a form of pebbling and pebble the spaces and prove something about the graph to a verifier. One popular Proof of Space is spacemint which is unique in that it implements two different blockchains and utilizes a punishment mechanism to disincentivize miners from deviating from the protocol in ways that are unlikely to happen if Proof of Work algorithms (for example, nothing at stake problems and block/challenge grinding). In our future work, we propose a similar kind of punishment mechanism. However, we use this tool to demote misbehaving *Alderman* and to provide recompense for grief-stricken clients. We do not propose two different blockchains/ledgers for history either.

2.2 Censorship Resistant File Storage

There has also been work done previously in the creation of file storage resistant to the takedown of particular governments and agencies. Publius, for example, was proposed as a method of resistance in which n servers host the encrypted content but in order to get the key a client must obtain k-out-of-n secret shares that are also controlled by these servers. While there is plausible deniability on the part of the servers, as they are hosting encrypted material, there is no mechanism or recompense in place for servers electing to delete their shares and no way to communicate this information to all of the other servers readily on the network. What this paper attempts to do is fundamentally different as we not only want to provide a mechanism by which servers can help dissidents/clients but we want to provide them an incentive to do so as well. Namely, in the form of currency.

2.3 Headings: second level

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

$$\xi_{ij}(t) = P(x_t = i, x_{t+1} = j | y, v, w; \theta) = \frac{\alpha_i(t) a_{ij}^{w_t} \beta_j(t+1) b_j^{v_{t+1}}(y_{t+1})}{\sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i(t) a_{ij}^{w_t} \beta_j(t+1) b_j^{v_{t+1}}(y_{t+1})} \tag{1}$$

2.3.1 Headings: third level

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Paragraph Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

3 Examples of citations, figures, tables, references

[5]

The documentation for `natbib` may be found at

```
http://mirrors.ctan.org/macros/latex/contrib/natbib/natnotes.pdf
```

Of note is the command `\citet`, which produces citations appropriate for use in inline text. For example,

```
\citet{hasselmo} investigated\dots
```

produces

> Hasselmo, et al. (1995) investigated…

```
https://www.ctan.org/pkg/booktabs
```

3.1 Figures

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi. See Figure 1. Here is how you add footnotes. [1] Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

[1] Sample of the first footnote.

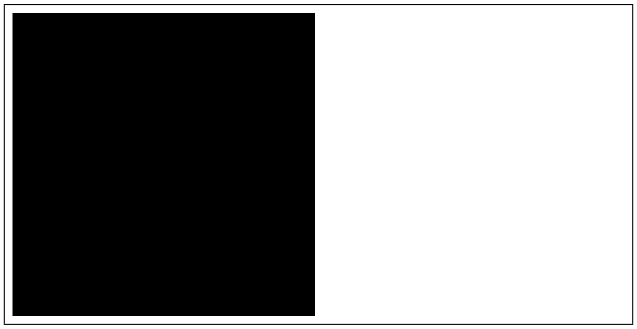

Figure 1: Sample figure caption.

Table 1: Sample table title

Part		
Name	Description	Size (μm)
Dendrite	Input terminal	$\sim$100
Axon	Output terminal	$\sim$10
Soma	Cell body	up to 10^6

3.2 Tables

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo. See awesome Table 1.

3.3 Lists

- Lorem ipsum dolor sit amet
- consectetur adipiscing elit.
- Aliquam dignissim blandit est, in dictum tortor gravida eget. In ac rutrum magna.

References

[1] Sunoo Park, Albert Kwon, Georg Fuchsbauer, Peter Gai, Jol Alwen, and Krzysztof Pietrzak. Spacemint: A cryptocurrency based on proofs of space. Cryptology ePrint Archive, Report 2015/528, 2015. `https://eprint.iacr.org/2015/528`.

[2] George Kour and Raid Saabne. Real-time segmentation of on-line handwritten arabic script. In *Frontiers in Handwriting Recognition (ICFHR), 2014 14th International Conference on*, pages 417–422. IEEE, 2014.

[3] George Kour and Raid Saabne. Fast classification of handwritten on-line arabic characters. In *Soft Computing and Pattern Recognition (SoCPaR), 2014 6th International Conference of*, pages 312–318. IEEE, 2014.

[4] Guy Hadash, Einat Kermany, Boaz Carmeli, Ofer Lavi, George Kour, and Alon Jacovi. Estimate and replace: A novel approach to integrating deep neural networks with existing applications. *arXiv preprint arXiv:1804.09028*, 2018.

[5] Andrew Miller, Ari Juels, Elaine Shi, , and Jonathan Katz. Permacoin: Repurposing bitcoin work for data preservation. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, May 2014.