A Literature Survey of Energy Efficiency Within Blockchain Networks

Sharan Duggirala and Siddharth Kulkarni[1]

***Abstract*— Blockchain is a decentralized transaction and data management technology developed primarily for the Bitcoin cryptocurrency. Applying blockchain to the cloud efficiently, which will allow on-demand, secure and low cost access to computing infrastructures, may not be possible currently. This is due to the limited computing capacities, to run distributed applications, and the inefficient power consumption models pertaining to Blocchain technologies. We review four methods of improving energy efficiency within the blockchain. The first paper looks at the fundamentals of how power of efficiency works with blockchain, and why energy efficiency equates to optimizing Bitcoin mining. The second paper deals with the facilitating the generation of Bitcoins at a fixed rate hence developing a new scheme of energy-efficient Bitcoin. The penultimate paper proposes a novel method of performing PoW(Proof of Work) with a combination of GPUs and CPUs. In the final paper we look at CoinTerras dedicated hardware for mining bitcoins. We conclude with the discovery that CoinTerras system is, indeed, the most efficient among the four papers being reviewed here.**

I. Table of Contents

II. List of Acronyms

1) **BTC** - Bitcoin
2) **HPC** - High Performance Computing
3) **PoW** - Proof of Work
4) **P2P** - Peer to Peer
5) **CPU** - Central Processing Unit
6) **GPU** - Graphical Processing Unit
7) **ASIC** - Application-Specific Integrated Circuit
8) **SPI** - Serial Peripheral Interface Bus
9) **USD** - United States Dollar
10) **FIFO** - First in First out
11) **PCR** - Pipe Control Register
12) **SHA** - Secure Hash Algorithm
13) **RAM** - Random access memory
14) **J/GH** - Joules per GigaHash
15) **PH/s** - Peta Hashes per second
16) **EVM** - Ethereal Virtual Machines

[1]S. Duggirala & Siddharth Kulkarni are with the Department of Computer Science, San Jose State University, 1 Washington Square, San Jose, CA, USA

III. Introduction

Blockchain is a **decentralized** transaction and data management technology developed first primarily for the cryptocurrency Bitcoin. The interest in Blockchain technology has been steadily increasing, since the idea was coined in 2008[2]. It essentially is a continuously growing list of records, called **blocks**, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a **timestamp** and **transaction data** (see *Fig 2* for more details). By design, blockchains are inherently resistant to modification of the data.

A blockchain can serve as "an open, **distributed ledger** that can record transactions between two parties efficiently and in a verifiable and permanent way[2]. For use as a distributed ledger, a blockchain is typically managed by a **peer-to-peer** network, collectively adhering to a protocol, for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which needs a collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high **Byzantine fault tolerance**[3]. Due to the nature of a decentralized consensus, blockchains are potentially suitable for the recording of events, medical records, and other record management activities. The information about every transaction, completed in Blockchain, is shared and available to all nodes. This attribute makes the system more transparent, than a system which employs centralized transactions involving a third party. In addition, the nodes in Blockchain are all anonymous, which makes it more secure for other nodes to confirm the transactions. Bitcoin was the first application that introduced Blockchain technology. Bitcoin created a decentralized environment for cryptocurrency, where the participants can buy and exchange goods with digital money.

A popular question, *Is Blockchain needed for building a Distributed Cloud?* needs to be addressed. There is a growing demand for computing power from scientific communities and industries to run large applications and process huge volumes of data. The computing power to run **Big Data** application is most often provided by **HPC** and Cloud infrastructures. A Blockchain- based Distributed Cloud will allow on-demand, secure and low-cost access to the most competitive computing infrastructures.

However, some research needs to be conducted within the blockchain environment to ameliorate the disadvantages that are hampering its widespread usage. The fact that blockchains offer very limited computing capacities, to run

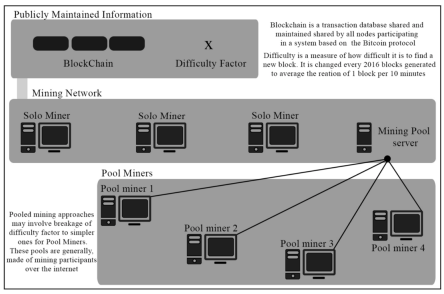

Fig. 1: Pool Mining

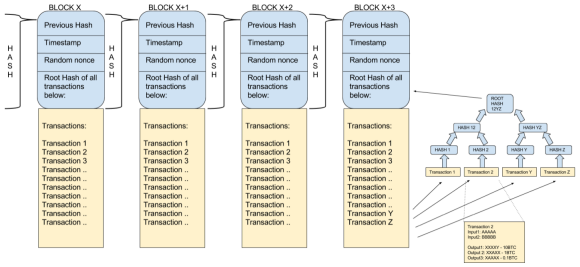

Fig. 2: A Diagram Detailing the Inner Contents of a Blockchain

distributed applications: a few *kb* of storage, very inefficient virtual machines and a very high latency protocol, are its major disadvantages. Eventually blockchain technologies will evolve to overcome some of these issues. We plan to research and tackle one of the primary issues with **Blockchain** and **Proof of Work**, which is its inefficient energy consumption.

IV. Literature Survey

A. Exploring Miner Evolution in Bitcoin Network

In order to better understand how to optimize the Blockchain, the most popular usage of blockchain and relevant parameters, need to be examined. As of now, blockchain is primarily used in the **Bitcoin** Network which was conceived to support the popular Bitcoin currency[1]. Through Wang, Liu[5] we understand that a user of the Bitcoin network can create bitcoins by packing and verifying new transactions in the network using their own computational power. Thus users have consequently been investing in specialized hardware for this process, called '*Bitcoin Mining*'. These particular set of users, may also pool their resources, to conduct **pool mining**. The aforementioned paper focuses on understanding how the bitcoin price, motivated by economic, political and legal facts, affects a miners' mining behaviour. A diagramatic explanation of pool mining has been presented in Figure 1[12].

The Bitcoin protocol is driven by the fact, that, there exists only a finite amount of Bitcoins. It is designed in such a way, that, Bitcoins are mined at a steady rate until all available bitcoins are mined. The steady growth of the price of Bitcoins has now motivated miners to adapt and invest their computational resources, to gain the advantage of faster mining. Therefore, it has become increasingly difficult to mine Bitcoins, as there has been a massive growth in both the number of miners and the computational power of their hardware. We can now proceed to examine the different governing facets of the Bitcoin Network:

a) Account and Transaction: The Bitcoin network is a **P2P** network without a central authority. An account within the network is a pair of public/private keys. A transaction within the network involves a set of senders, a set of receivers and the amount being sent. All senders sign the transaction with their private key and any users, that receive the transaction, will first verify whether the senders have the amount of BTCs indicated in the transaction. Instead of a central database to maintain the bitcoin balance of each account, the network stores and verifies these transaction using a blockchain. Thus any user can verify any transaction or balance by backtracking through the blockchain.

b) Block and Blockchain: The Blockchain contains a chain of chronologically ordered blocks, which each contain transactions within a time window of ten minutes and a transaction indicating which account packed this particular block. Each user downloads and synchronizes the a copy of this blockchain to verify incoming transactions. Once this is done, the transaction will be packed into a new block and then broadcasted to the entire network. Whenever a user receives a block, they will validate the transactions using the current blockchain and thus discard invalid transactions will appending valid transactions. An example of a blockchain is shown below in Figure 1 [6].

c) Bitcoin Mining: Multiple users can volunteer to verify and pack new transactions to the block. While a lot of users are performing and packing simultaneously, only the user, who created the newest valid block, will be awarded a varying amount of BTC (which is the **Proof or Work mechanism**). This can be described as the process where, when packing new transactions to the block, a miner first generates a special transaction, indicating that the network send them the mining reward. Along with all other transactions the miner will repeatedly generate a **random number** and run a **hash function**. If the hash value is below the **target value**, the user claims that the block has been created by this particular miner and then proceeds to broadcast the updated block and the random number (the **nonce**). Using this random number, the other users can verify the block.

d) Bitcoin Protocol: According to Nakamoto[7], There are 21 million *BTC* to be mined and the last *BTC* is the Block #6,929,999, estimated to be mined near 2140. A new block is created approximately ever ten minutes independent of the computational power within the network. To control the new block creation speed, a **difficulty value** is introduced. The target value for the block hash calculation is inversely promotional to the difficult value. At a given difficulty value D, for a miner with computation power of H hashes per second, the expected time for the miner to generate a valid

block is given below [5]:

$$E[T] = \frac{D \times 2^{32}}{H} seconds$$

During the advent of *BTC*, miners mined blocks individually in an approach called **solo mining**. One of the main advantages to this approach, is the fact that the single miner gets all the reward for creating a block. However, due to the increase of computational power, as mentioned before, the difficulty value of *BTC* has been steadily increasing. Thus **pool mining** has been introduced for miners to pool their resources to solve hash problems. The pool operator is responsible for distributing the reward to the pool miners. With pool mining, the expected payout is pretty much the same as solo mining, but the variance of the payout over time is largely reduced.

With a given difficulty value of D, if N blocks are mined in a day, the aggregate hash rate per day of the entire network is given in below[5]:

$$H_{\text{total}} = \frac{N \times D \times 2^{32}}{86,400}$$

Since the technique in which pools distribute payouts varies according to the pool, there isnt a unified idea where we can calculate much *BTC* each pool miner earns each day, using pool payout transactions.

Wang, Liu proceed to propose economic models for miners. The **Capital Cost** is defined as the purchase of the CPUs, GPUs and/or ASICs that compose the computational power of a user. The **Operational Cost** on the other hand is the cost of electricity, air conditioning, housing and maintenance of the computational resources. If the hardware of hash rate H, based on equation detailing the expected time for a miner to generate a valid block, works twenty four hours a day, the expected amount of *BTC* mined daily is given below:

$$N(t,h) = \frac{H \times 86,400}{D(t) \times 2^{32}} R$$

Where $D(t)$ is the difficulty value in day t and R is the number of bitcoins being awarded for each block. If the hardware power consumption is PKW, and the price is (t) per KWh, the daily electricity bill is $24P$. If we only consider the electricity operational cost, the profit rate $r(t)$, can be represented as below:

$$r(t,H,P) = N(t,H)\rho(t) - 24P(t)$$

To maintain a profit the miners need for the *computation-over-power* efficiency to satisfy:

$$\frac{H}{P} > K\frac{(t)D(t)}{R\rho(t)}$$

Where K is a constant in above[5]. Wang and Liu also describe how the miners are paying a zero-sum computation race game. Since miners are constantly motivated to increase their computational power, and, the bitcoin price is kept flat, as to keep a steady number of coins that can be mined each day. This race will end when no existing machine can satisfy the computation-over-power efficiency equation above, thus concluding our findings from this particular paper.

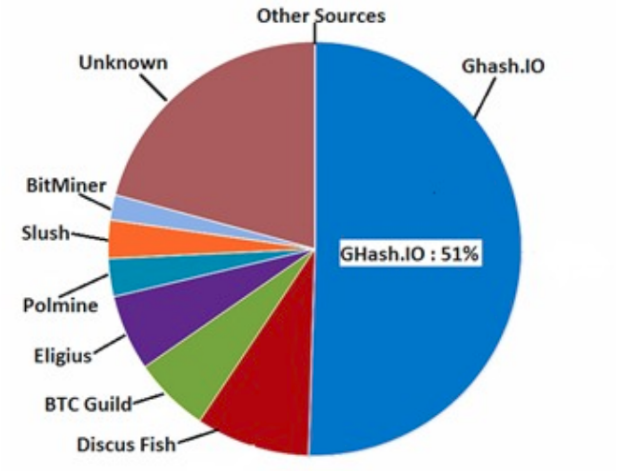

Fig. 3: Ghash.io 51% attack

B. Towards a More Democratic Mining in Bitcoins

Bitcoin has enjoyed superiority compared to other cryptocurrencies, but, has also attracted attackers to take advantage of possible operational insecurities that plague its system.

51% attack[8] is the the situation where a single entity or a group contributes to the majority of the networks mining hashrate. The attackers therefore have full control of the network and can change the current blocks and the future blocks of the blockchain at will. They can generate majority of the blocks and include the transactions at will, due to the nature of the verification of blockchain. They can also prevent people from sending bitcoins between different addresses. Lastly they can prevent other miners from finding any blocks for a given period of time.

On 14th June 2014, a particular mining pool was able to take control of 51% of Bitcoins processing power , thus extracting the maximum amount of profit for their work. **Ghash.IO** secured 51% of the mining rights (as seen in Figure 3), creating a 51% attack possibility[9].

The authors have cited various techniques to solve this issue. The first being the paper titled *Preventing Selfish Mining*[10]. **Block races** consists of mining pools pursuing selfish mining to prevent the blocks of other users from being added into the blockchain. This can lead to 51% attack. The authors suggest a fair mining process and thus remove the chances of block races and selfish mining. The second technique is the titled *Guaranteed Fixed Generation Rate*[11]. The bitcoins are generated at a highly variable output at an average of 10 minutes. This variation can lead to problems like transaction malleability, which in turn can lead to frauds.

The authors propose to modify the target achieving proof-of-work protocol through **minimum hash generation** by miner nodes across the Bitcoin network. The user with the

minimum hash after a given amount of time (ten minutes was primarily decided upon on this paper) gets the mining rights. This process has been divided into three phases[9] described below.

a) Hash Generation Phase:

- Call $Initialize()$ with H_{min} for each node N_{i}
- Update the M_{min} to the message containing H_{min}
- Update $STATE$ to $ACTIVE$
- Start the Hash Broadcasting phase

Listing 1: The Hash Generation Algorithm

```
Procedure Initialize(Hash Message M):
for all Nodes in the network do
   Ni.Mmin = M, where Mmin is the minimum
       hash message at each node;
   Ni.STATE = ACTIVE;
end for
```

b) Hash Broadcasting Phase:

- Each leaf node starts this phase by broadcasting it M_{min} to its parents and changes its state to $PROCESSING$ (calls $LeafSending()$)
- Each internal node that has received the message, goes through this process:
  1) Calls the $Receiving\_Active(M)$ function on receiving a message M from its neighbors.
  2) Processes the message by calling Process $Message(M)$.
  3) If it has received a message from all neighbors except one, then it forwards the M_{min} to the one neighbor, which in turn, becomes its parent and changes its state to $PROCESSING$.

Listing 2: Hash Broadcasting Algorithm

```
Procedure LeafSending():
   for all Active Leaf Nodes do
      parent <= Neighbors;
      send Ni.STATE = PROCESSING;
   end for
Procedure Receiving_Active(M)
   for all Active Internal Nodes do
      Ni.Mmin = Process Message(M);
      Neighbors:= Neighbor - sender;
      if number of Neighbors = 1 then
         parent <= Neighbors;
         send Ni.Mmin to parent;
         Ni.STATE = PROCESSING;
      end if
   end for
Procedure Process_Message(M)
   for all Nodes in the network do
      if Ni.Mmin.H < M.H then
         return Ni.Mmin;
      else
         return M;
      end if
   end for
```

Name	Byte Size	Description
Version (V)	4	Block Version Number.
Previous Hash (P_h)	32	This is the hash of the previous block header.
Merkle Root (H_t)	32	The hash based on all the transactions present in the current block.
Time (T)	4	Current Timestamp in seconds (unix format).
Target	4	Target value in compact form.
Nonce (R)	4	User adjusted value starting from 0.

Present Block Header Format

Name	Byte Size	Description
Version (V)	4	Block Version Number.
Previous Hash (P_h)	32	This is the hash of the previous block header.
Merkle Root (H_t)	32	The hash based on all the transactions present in the current block.
Time (T)	4	Current Timestamp in seconds (unix format).
Bitcoin Address (U_a)	20	Hash of the Public key of the receiving address.
Nonce (R)	4	User adjusted value starting from 0.

Proposed Block Header Format

Fig. 4: Modifications made to Block Header Format

c) Hash Verification Phase:

- Finds the true minimum hash of the system
- The hash message chosen by the two saturated nodes, is verified by the peers.
- Any node having lower hash message can claim its hash if any one of these conditions is true:
  1) Its message is verified.
  2) The broadcasted hash message is discarded.
  3) The owner of the message generates the next block .
- The hash broadcast and verification stage continues for eight minutes.

Listing 3: Hash Verification Algorithm

```
Procedure Verify_Hash(M):
for all Nodes in the network do:
   if Ni.Mmin.H < M.H then
      return Ni.Mmin;
   else
      return M;
   end if
end for
```

The changes introduced, are modifications to the present *BTC* header. The target field has been replaced by the *BTC* address of the miner. The advantages of democratic mining are *BTC* generation at a **fixed rate**, which can be adjusted. Decentralization of the *BTC* mining process leads to a reduced power consumption (**20%** of the original power consumption).

To conclude, the authors of this paper address the problem of 51% attack and introduce a new defense against this problem. Modification of the present block header by introducing some extra bytes and utilizing the timestamp more effectively in the hash generation, suggests an alternative to the existing Proof-of-Work scheme. The proposed approach not only relies on finding a hash values lower than the target, but awards the miner involved in generating the minimum hash value across the entire distributed network. Fraudulent

$$Ch(X,Y,Z) = (X \wedge Y) \oplus (\overline{X} \wedge Z)$$
$$Maj(X,Y,Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$$
$$\Sigma_0(X) = RotR(X,2) \oplus RotR(X,13) \oplus RotR(X,22)$$
$$\Sigma_1(X) = RotR(X,6) \oplus RotR(X,11) \oplus RotR(X,25)$$
$$\sigma_0(X) = RotR(X,7) \oplus RotR(X,18) \oplus ShR(X,3)$$
$$\sigma_1(X) = RotR(X,17) \oplus RotR(X,19) \oplus ShR(X,10)$$

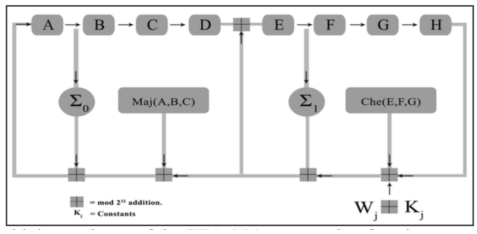

Fig. 5: The SHA-256 j^{th} step

activities are easier to determine due to effective use of the Timestamp. The new scheme thus introduces fair competition among the miners. Moreover, it facilitates the generation of *BTC* at a fixed rate hence developing a new scheme of an energy-efficient *BTC* network.

C. Bitcoin Mining Acceleration & Performance Quantification

We can learn more about the mining through Jega Anish Devs paper[12]. The paper categorizes mining into two different methods, legal and illegal. Mining by legal means involves the mining rig consisting of hardware powerful enough to solving a block in practical amounts of time and probability, when in consideration of the investment and costs. Pooled mining is most commonly done by publicly pooled bitcoin mining with users having machine setups that use multiple GPUs with software that encompasses *CUDA* for *Nvidia* GPUs, *STREAM* for *ATI* GPUs or *OpenCL* for common access, if supported. Although CPU usage is usually discouraged due to low hash rates, some users still run CPU miners.

The work expended in generating a **Proof-of-Work** can be considered as the computation cycles involved in the repeated *SHA-256* computation needed to discovering the required hash seed. The process for any random jth step, in terms of both GPU and CPU mining is shown in Figure 5.

In order to understand more about the SHA-256 process please refer to *Gilbert, H. and Handschuh, Security analysis of SHA-256 and sisters* [17]. Dev proposes a novel technique where the computational prowess of both the CPU and the GPU are used in the mining process. In order to achieve this, separate algorithms were described for each hardware.

The following steps were performed on an *Nvidia* graphics card that uses the *CUDA* library:

1) **Allocation** of resources on the device, such as a single instance of the structure holding block header details that is used in hashing and a copy of the best nonce for each thread being executed in the device. In this particular paper, the nonce was created by the calculating the product of the number of blocks in use and the number of threads running in each block.
2) **Initialization** of the variables in the kernel function for concurrent SHA256 operations.
3) **Execute** the SHA256 computation on the trial block structure which is filled with static data that was received during the usage of the BTC protocol and with an incremented trial.
4) **Test** if the hash obtained from *step 2* is smaller than the target hash given by the difficulty. An efficient technique for this is described within the paper, where a certain number of required zeros being present in the beginning of the target hash, followed by the remainder of the hash being smaller than the remainder of the target is tested.
5) If success, **report** the winning nonce. Otherwise increment the nonce and perform *step 2*.

The following algorithm was described for the mining process on a CPU:

- **Allocation** of the resources as described before, but on the RAM.
- **Initialization** of the variables to concurrently provide an id for starting values of the nonce to each parallel instance of the SHA256 operation.
- **Execute** SHA256 operation in the same manner as described in GPU mining.
- **Test** hash and on success, report winning nonce. Otherwise, increment the nonce and perform *step 2*.

Two different machines were used for testing, dubbed **C1** and **C2**. **C1** had an *Intel i7* CPU and an *Nvidia GTX* 550 TI GPU. **C2** had an *Intel i5* CPU, and a similar GPU. The results of this technique were quite positive, and are given below in Table 1 in terms of the hash rate from [12]:

TABLE I: Table showing the improvements of using both a GPU and a CPU

Machine	GPU	CPU	CPU + GPU	Boost %
C1	20.4	1.9	22.3	9.3
C2	46.1	18.3	64.4	39.69
C1 + C2	66.5	20.2	153	30.37

The approach discussed in Devs paper is not expected to be comparable with custom hardware based mining, but provide a relevant boost to hash rates for non custom equipment users. In fact, these users contribute significant fractions of the total number of mining units in operation on the *BTC* network, and therefore are a very important subset of the miners that need to be examined within any given research on the Bitcoin Network.

D. CoinTerras First-Generation Cryptocurrency Mining Processor for Bitcoin

This paper describes the architecture and implementation of **CoinTerras** first generation *BTC* mining processor, **GoldStrike-1** and how it was used to design a complete *BTC* mining machine called **TerraMiner-IV**. Because of high power density in the *BTC* mining processor, delivering power

and cooling to the die posed enormous challenges. This paper describes some of the solutions adopted to overcome these challenges.

As the difficulty of *BTC* mining continued to increase, it had spawned a new design orientated industry that develops powerful custom computing hardware for *BTC* mining applications. From the design and production of specialized integrated circuits for *BTC* mining processors, this new industry provides a complete solution by integrating these processors into custom *BTC* mining appliances that can easily be used by individual consumers as well as large datacenters. A defining attribute of *BTC* mining hardware, is that, it requires to be operated at peak performance consistently at all times of the day. In contrast, a general-purpose computing processor or a graphics processor uses only a small fraction of the computing resources at peak level at any given instant of time. This particular usage model for *BTC* mining hardware results in extremely high and sustained power consumption, creating new design challenges. A couple of design challenges to overcome includes, maximizing the energy efficiency of the application-specific integrated circuit (ASIC) processor and achieving efficient and stable power transmission and thermal solutions, while keeping the cost structure viable for *BTC* mining operations. This article describes the architecture and implementation of CoinTerras first-generation *BTC* mining processor, GoldStrike 1, and how these processors are integrated into a complete *BTC* mining appliance called Terra-miner IV.

a) GoldStrike 1 Architecture: Like any other chip design project, there can be many **tradeoffs** when building the architecture of a semi-conductor for a Bitcoin mining application. Many methods have been proposed for efficient implementation of the SHA-256 algorithm, such as various **loop unrolling** and **signal timing schemes** [14]. The basic tradeoffs are resolved into dollar per giga-hash per second ($\$/GH/s$) of a complete miner appliance. The authors considered many factors such as silicon yield, die size, clock frequency, and cooling cost etc. to finally arrive at a multi-die package design containing four dies per package, with each package delivering 0.5 TH/s. This set the design target of 125 GH/s per die.

The Architecture in particular contains:

- A **Motorola** compatible 4-pin SPI Port
- A **PLL** with simple bit-bang interface
- **120 Hash Engines** arranged into 16 super-pipes
- 128 deep input work **FIFO**
- 384-bit **Pipe Control Register** (PCR) to enable/disable individual hash engine.

We shall look at each component of the architecture in detail from this point on:

b) Hash Engine: The hash engine consists of two SHA-256 function blocks in series. The iterative loop within each SHA-256 block is unrolled into a 64-stage pipeline. Some of the defining attributes of this engine are:

1) Two rounds of SHA-256 processing (Each round consists of 64 iterations).

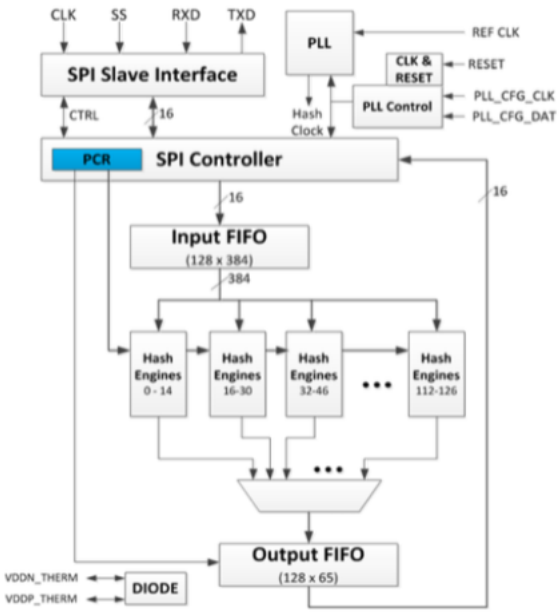

Fig. 6: GoldStrike 1 Architecture

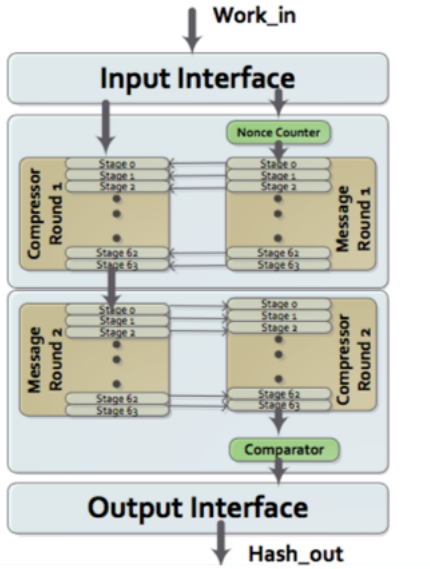

Fig. 7: Hash Engine Architecture

2) Searches for a result in 232 nonce range.
3) Two parallel but connected pipelines - **message** & **compressor**.

This engine only generates a result, if target criteria has been met.

c) Compressor Stage of SHA-256 Pipeline: Each stage computes new values for words A and E and stores the new values in output registers A and E. The remaining output registers are simply staging registers for previous stage values.

The authors of this paper detail some future trends, such as, moving the Bitcoin mining operations to data centers

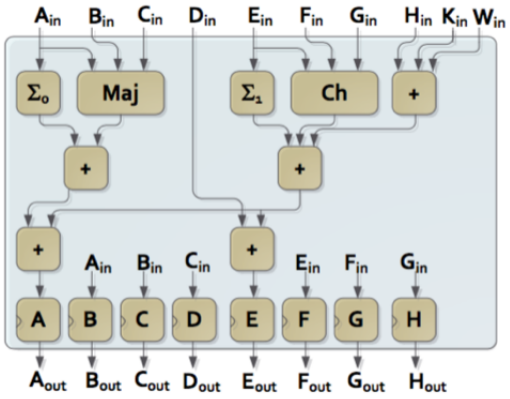

Fig. 8: Compressor Stage of SHA-256 Pipeline

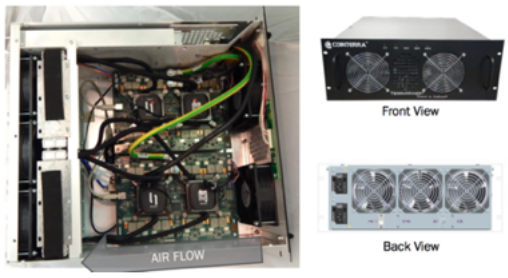

Fig. 9: Front and Back View

locations with the lowest electricity and cooling cast costs. There has also been a lot of focus on increasing the ASICs energy efficiency, by employing more advanced process nodes, lower supply voltages, and a highly configurable ASIC back-end design. To increase the energy efficiency, the switching capacitance along with the supply voltage must be minimized. Current trends point towards older process technologies for lower power and lower hash rate chip design on a cheaper process node, and deploy a massive amount of these chips to get a higher total hash rate.

Based on the exchange rate and the operational costs, at the time of the conception of the paper, Cointerra is able to perform with an efficiency of $0.8J/GH$(Joules/GigaHash) at full clock, with a Hashrate of $179.7PH/s$(PetaHashes/second).

In conclusion this paper discusses the architecture and implementation of CoinTerras first generation bitcoin mining processor. It also explains various techniques to reduce power consumption and still have efficient operational capacity.

V. Existing Industry Technology

a) VISA: Visa is an American multinational financial serves corporation headquartered in Foster City, California, United States. It facilitates electronic funds transfers throughout the world, most commonly through VISA branded credit cards and debit cards. In Oct, 2016, VISA announced their partnership with blockchain enterprise company Chain in which the two firms decided to develop a simple, fast and secure way to process B2B payments globally. The Visa B2B Connect platforms pilot is expected to launch in 2017, thus indicating a connection between the USPTO digital asset network patent and the new B2B solution. [15]

b) Ethereum: Although commonly associated with Bitcoin, blockchain technology has many other applications that go way beyond digital currencies. In reality, Bitcoin is only one of several hundred applications that use blockchain technology today.

Until recently, building an application that uses the blockchain technology has required a complex background in coding, cryptography, mathematics as well as significant resources. Ethereum is an open distributed public blockchain network that facilitates easier development of these applications. While blockchain in the context of Bitcoin is used to track ownership of digital currency(*BTC*), Ethereum focuses on running the programming code of any decentralized application[16].

In the Ethereum, instead of mining for bitcoin, miners work to earn Ether, a type of crypto token that fuels the network. Beyond a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network.

Before the creation of Ethereum, blockchain application were designed to do a very limited set of operations. With the invention of the **Ethereal Virtual Machine**(EVM), a Turing complete software that runs on the Ethereum network, anyone can run a program, regardless of programming language, on Ethereum. Instead of having to build an entirely original blockchain for each new application, Ethereum enables the development of countless applications on the same environment. For example, Dapp provides its users with a P2P electronic cash system that enables online Bitcoin payments. Due to the nature of Ethereum, a particular centralized service can be adapted to be more decentralized.

VI. Conclusion

We have learnt how to calculate the computation-over-power efficiency from the first paper. Using this parameter we can judge other algorithms and/or systems that have been proposed in the other papers. From the second paper, we understand that due to hash generation there is decentralization of bitcoin mining from the hands of mining pools and introduction of a luck factor in mining. This alternate scheme reduces power consumption by 80% the original PoW protocol. We proceed to examine the combination of CPUs and GPUs to optimize the performance of miners by approximately 40%. The final paper discusses various techniques to reduce power consumption, yet maintain efficient operation. The Cointerra is able to perform with an efficiency of $0.8J/GH$(Joules/GigaHash) at full clock with a Hashrate of $179.7PH/s$(PetaHashes/second).

We present three scenarios and relevant optimal solutions:

1) A business with multiple servers in the office should buy a platform of CoinTerras.

2) A home user with high capital should use should buy a single/multiple CoinTerras (depending on capital).
3) A home user with low capital should use should use the combined computational power of both a CPU and a GPU through democratic mining.

In conclusion, a combination of all three solutions presented in this survey is probably the best solution for the energy efficiency problems we are facing within blockchain.

REFERENCES

[1] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K., 2016. Where Is Current Research on Blockchain Technology?A Systematic Review.PloS one,11(10), p.e0163477. [2] https://hbr.org/2017/01/the-truth-about-blockchain. (2017). [Blog].

[2] https://hbr.org/2017/01/the-truth-about-blockchain. (2017). [Blog].

[3] Large Purse Shop. (2017).What are Blockchains (Block Chains)?. [online] Available at: https://largepurseshop.com/blogs/the-residual-income-solution/what-are-blockchains-block-chains [Accessed 25 Oct. 2017].

[4] Blockgeeks. (2017).What is Blockchain Technology? A Step-by-Step Guide For Beginners. [online] Available at: https://blockgeeks.com/guides/what-is-blockchain-technology/ [Accessed 25 Oct. 2017].

[5] Wang, L. and Liu, Y., 2015, March. Exploring miner evolution in bitcoin network. InInternational Conference on Passive and Active Network Measurement(pp. 290-302). Springer, Cham.

[6] esotera. (2017).Thin Clients and Blockchain Explorers - esotera. [online] Available at: https://esotera.eu/clients-explorers/ [Accessed 25 Oct. 2017].

[7] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

[8] Floyd, D. (2017).51% Attack. [online] Investopedia. Available at: http://www.investopedia.com/terms/1/51-attack.asp [Accessed 25 Oct. 2017].

[9] Paul, G., Sarkar, P. and Mukherjee, S., 2014, December. Towards a more democratic mining in bitcoins. InInternational Conference on Information Systems Security(pp. 185-203). Springer, Cham

[10] Woodward, A. (2017).Preventing Selfish Mining In The Blockchain. [online] Profwoodward.org. Available at: https://www.profwoodward.org/2016/05/preventing-selfish-mining-in-blockchain.html [Accessed 25 Oct. 2017].

[11] En.bitcoin.it. (2017).Controlled supply - Bitcoin Wiki. [online] Available at: https://en.bitcoin.it/wiki/Controlled_supply [Accessed 25 Oct. 2017].

[12] Dev JA. Bitcoin mining acceleration and performance quantification. InElectrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on 2014 May 4 (pp. 1-6). IEEE.

[13] Lexology.com. (2017).The Fueling Of MLM through Bitcoins — Lexology. [online] Available at: https://www.lexology.com/library/detail.aspx?g=1babaa6e-b19c-4498-9012-5846beb31152 [Accessed 25 Oct. 2017].

[14] Barkatullah, J. and Hanke, T., 2015. Goldstrike 1: Cointerra's first-generation cryptocurrency mining processor for bitcoin.IEEE micro,35(2), pp.68-76.

[15] itarisWriter, B., Vitaris, B. and Vitaris, B. (2017).Visa Files Patent for Blockchain-Based Digital Asset Network. [online] Bitcoin Magazine. Available at: https://bitcoinmagazine.com/articles/visa-files-patent-blockchain-based-digital-asset-network/ [Accessed 25 Oct. 2017].

[16] Blockgeeks. (2017).What is Ethereum? A Step-by-Step Beginners Guide [Ultimate Guide]. [online] Available at: https://blockgeeks.com/guides/what-is-ethereum/ [Accessed 25 Oct. 2017].

[17] Gilbert, H. and Handschuh, H., 2003, August. Security analysis of SHA-256 and sisters. In International workshop on selected areas in cryptography (pp. 175-193). Springer, Berlin, Heidelberg. Vancouver