David Husband, M.Sc in IT, *Baremetal Engineer Extraordinaire*

What you see detailed on my CV are "merely" the things I have done to earn money...
In reality, my abilities, knowledge and capabilities range far beyond my CV..

In http://baremetal.engineer/baremetal.software.engineer.pdf I showed my proven abilities, including researching, analysing, extracting and applying freshly acquired knowledge from within the TCP/IP subject domain.

In http://baremetal.engineer/baremetal.hardware.engineer.pdf I showed how electronic hardware has not changed in essence over the last 60 years or so, due to being based upon the principles of physics established hundreds of years ago. I showed how, counter-intuitively, electronics hardware was actually ***easier now*** due to ever increasing integration and increasing functionality...

In this document, I will discuss the subject of another emerging technology, ***Blockchain***[1] which is the underlying data structure used by ***Bitcoin***[2], a cryptocurrency[3]

Blockchain Fundamentals

BEWARE: It is very important to understand the fundamental distinction between ***Blockchain*** and ***Bitcoin*** !! They are not at all the same things! Many don't appreciate this, and use the terms interchangeably, even those who should know the difference![4]

Blockchain is really about distributed, secure TRACEABILITY & TRANSPARENCY !

As part of my own learning efforts on the subject, I have some videos from ***YouTube*** below in the order of my own suggestion for a watching order...

---

http://baremetal.engineer/Blockchain/[1] Blockchain Expert Explains One Concept in 5 Levels of Difficulty WIRED.mp4

This is my #1 choice for the first video to watch because Bettina Warburg clearly has a very deep understanding of Bitcoin and its underlying principles, ***BUT she TALKS ABOUT BLOCKCHAIN*** when ***she is really talking entirely about the Bitcoin cryptocurrency***! In my opinion that is a major boo-boo, but it does not detract from her sound understanding!

She starts to redeem herself around point 5:20, but she still talks about Blockchain in terms of "assets" and "trading" and Blockchain is far wider in scope and application than that... See "***Blockchain, IoT & Embedded systems***" later...

---

http://baremetal.engineer/Blockchain/[2] 19 Industries The Blockchain Will Disrupt.mp4

This video attempts to expand the scope of Blockchain by illustrating various areas that Blockchain is already being used in... Like a long sales video!

#10 Voting Talks about using Blockchain as part of the voting process

http://baremetal.engineer/Blockchain/Blockchain voting.mp4 from another source, discusses Blockchain Voting in more detail...

---

http://baremetal.engineer/Blockchain/[3] Can Blockchain Help Law Enforcement Blockchain of Evidence - Jeff Neithercutt.mp4

I so love this video!! It encapsulates ALL the things Blockchain can do when properly engineered. Jeff Neithercutt clearly knows what he is talking about and is the driving force here to applying Blockchain to the management of the *Criminal Evidence Chain of Custody*

---

[1] ***https://en.wikipedia.org/wiki/Blockchain*** *"A blockchain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a* **Merkle Tree***)"*

https://en.wikipedia.org/wiki/Merkle_tree *"In cryptography and computer science, a hash tree or Merkle tree is a tree in which every leaf node is labelled with the cryptographic hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains"*

[2] ***https://en.wikipedia.org/wiki/Bitcoin*** *"Bitcoin is a cryptocurrency invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto and started in 2009 when its implementation was released as open-source software"*

https://en.wikipedia.org/wiki/Satoshi_Nakamoto *"Satoshi Nakamoto is the name used by the presumed pseudonymous person or persons who developed bitcoin, authored the bitcoin white paper, and created and deployed bitcoin's original reference implementation. As part of the implementation, Nakamoto also devised the first blockchain database. In the process, Nakamoto was the first to solve the double-spending problem for digital currency using a peer-to-peer network. Nakamoto was active in the development of bitcoin up until December 2010. Many people have claimed, or have been claimed, to be Satoshi Nakamoto"*

[3] ***https://en.wikipedia.org/wiki/Cryptocurrency*** *"A cryptocurrency is a digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a ledger existing in a form of computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership. It typically does not exist in physical form (like paper money) and is typically not issued by a central authority"*

[4] From watching a few YouTube videos, there seem to be many around who actually seem to have very little in-depth knowledge of Blockchain or Bitcoin... !!

The blockchain-based system he is developing is hosted on the ***Hyperledger***[5] ***platform*** and is known as the "***Blockchain of Evidence***" and his system illustrates a number of key Blockchain concepts:

- A Private, "*Permissioned*" Blockchain
- The public has limited & controlled Read Access
- Users uploading ("writing") data are controlled & authenticated
- "*Chain of Custody*"[6] traceability

Jeff has other videos: http://baremetal.engineer/Blockchain/What is Blockchain anyway.mp4

At point 0:49 while talking about the Blockchain ledger generally, he shows an image of the iconic "golden Bitcoin"[7]

And: http://baremetal.engineer/Blockchain/Blockchain of Evidence.mp4

---

http://baremetal.engineer/Blockchain/[4] Real world examples of blockchain projects.mp4

This is an IBM video that shows a number of useful Blockchain applications -- virtually all about "*traceability*". The example of Walmart is covered in more detail in the next video

---

http://baremetal.engineer/Blockchain/[5] Genius of Things Blockchain and Food Safety with IBM and Walmart.mp4

John Cohn of IBM talks about the Hyperledger platform that IBM participate in. (See footnote#5)
Frank Yiannas, the V.P. of Food Safety at Walmart talks about Walmart's involvement with Blockchain
Very insightfully, Frank draws an important distinction between "***traceability***"[8] and "***transparency***"[9]...
I think this video is very insightful !! Traceability issues again !!

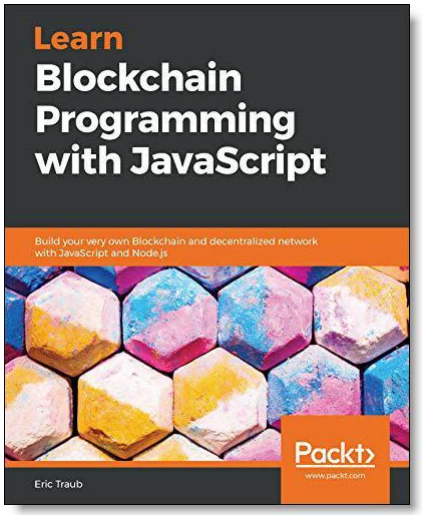
---

http://baremetal.engineer/Blockchain/[6] The Blockchain and Us (2017).mp4

This is an insightful "film" from Manuel Stagers. I recommend watching it

So how is Blockchain relevant to me as a "Baremetal Engineer" ?

I have had an ongoing "watch" on Blockchain (and Bitcoin to a lesser degree) for quite a while now because Blockchain has some properties that fit in with my interest in the ***linked-list***[10] ***data structure*** within the context of some research I am doing working towards creating an opportunity to do a self-financing Ph.d



What changed everything was coming across this book !!
At last somebody with a real low-level understanding of the basic structure of Blockchain as a complex linked-list of data and able to explain the "how", "what", "why" and "when" of all that complexity - all with working, example code

Ok, so his favourite language was ***JavaScript*** with a ***Node.js*** interpreter, but that has turned out to be a bonus for me as *JavaScript* within *Node.js* seems to be worth learning (even for a baremetal engineer!)

The only issue I have with this book is with Chapter 1, where in my opinion the setting-up description is very weak. I struggled with understanding what was being used, where it was downloaded from and what purpose it would perform. In addition he discussed and illustrated a number of utility applications being used, without making it clear they were running on an Apple Mac system...

---

[5] ***https://en.wikipedia.org/wiki/Hyperledger*** *"Hyperledger (or the Hyperledger project) is an umbrella project of open source blockchains and related tools, started in December 2015 by the Linux Foundation, and has received contributions from IBM, Intel and SAP Ariba, to support the collaborative development of blockchain-based distributed ledgers"*

[6] ***https://en.wikipedia.org/wiki/Chain_of_custody*** *"Chain of custody (CoC), in legal contexts, is the chronological documentation .... that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Of particular importance in criminal cases, the concept is also applied in civil litigation and more broadly in drug testing of athletes and in supply chain management, e.g. to improve the traceability ..."*

[7] Aaaahhhh!!, why do people keep doing this ??!!

[8] ***https://en.wikipedia.org/wiki/Traceability*** *"Traceability is the capability to trace something. In some cases, it is interpreted as the ability to verify the history, location, or application of an item by means of documented recorded identification. Other common definitions include the capability (and implementation) of keeping track of a given set or type of information to a given degree, or the ability to chronologically interrelate uniquely identifiable entities in a way that is verifiable"*

[9] ***https://en.wikipedia.org/wiki/Transparency_(behavior)*** *"Transparency, as used in science, engineering, business, the humanities and in other social contexts, is operating in such a way that it is easy for others to see what actions are performed. Transparency implies openness, communication, and accountability"*

[10] ***https://en.wikipedia.org/wiki/Linked_list*** *"In computer science, a linked list is a linear collection of data elements whose order is not given by their physical placement in memory. Instead, each element points to the next. It is a data structure consisting of a collection of nodes which together represent a sequence. In its most basic form, each node contains: data, and a reference (in other words, a link) to the next node in the sequence"*

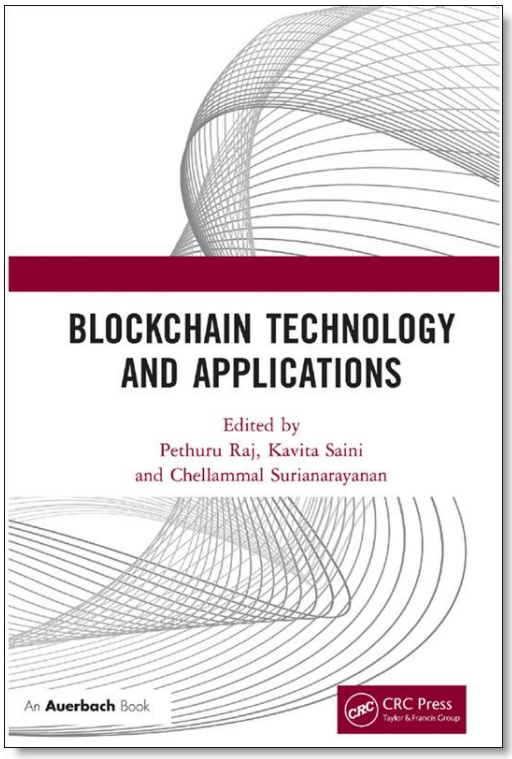
This just illustrates a classic dilemma for all us experts when we come to describe and discuss subjects that we are very familiar with, with the intention of introducing our work to those who know very little about the topic...

Using the examples in this book, I am intending to learn a lot more about ***JavaScript***[11] and ***Node.js***[12] but in the meantime I used my understanding from the book to implement the ***SHA-256 Hash routine***[13] in assembler within a Forth environment on my nascent eZ80 Development Platform[14]

I will discuss my SHA-256 implementation later in this document...

So how is Blockchain relevant to the "Internet of Things"[15] *?*

I had been asking myself that question for a while, when I came across this fabulous book:



Published in September 2020, and like all books seeking to explain Blockchain, this book is fairly generic in content but with much more insight than normal!

In particular, Chapter 3, "Blockchain and IoT Security" says: "*We can define IoT as the things which are capable of sending and receiving data in the world of the Internet for controlling the device or analyzing and manipulating the data shared. IoT begins with home appliances such as lights, fans, refrigerators, televisions, etc., and broadens to any electronic device in the network. IoT works with a combination of sensors as the input medium, software to control it and the network for passing data between any objects in the network*"

"*Smart homes, using the Internet of Things, which produces data from different sensors, video cameras and any other connected smart home appliances, can be coupled with blockchain technology for the utmost security of data and processes*"

However the Blockchain needs to be "optimised" for IoT use in a number of fundamental aspects...

These include: Proof-of-Work, Mining, Consensus, Deciding upon the "staleness" of data, Archiving "Stale" Data, The Roles of Various Nodes, including if a Node Role of "Central Co-ordinator" is required. These issues would all be defined and resolved when the architecture of a particular embedded IoT system is devised...

Blockchain, IoT & Embedded systems

Embedded IoT Blockchain Nodes might be defined as:

- ***Light Client***: Where the system only possesses a "*shallow-copy*" of the *System Blockchain*
- ***Full Node***: Where the system possesses a "*full-copy*" of the *System Blockchain*
- ***Mining Node***: Where the system verifies the transactions
- ***Archiving Node***: Where the system decides what & when data is "*stale*" and saves it to an archive
- ***Co-Ordinator*** A Node that makes sure the other Nodes are working properly?

A node can perform more than one role

---

[11] ***https://en.wikipedia.org/wiki/JavaScript*** *"JavaScript often abbreviated as JS, is a programming language that conforms to the ECMAScript specification. JavaScript is high-level, often just-in-time compiled, and multi-paradigm. It has curly-bracket syntax, dynamic typing, prototype-based object-orientation, and first-class functions. As a multi-paradigm language, JavaScript supports event-driven, functional, and imperative programming styles. It has application programming interfaces (APIs) for working with text, dates, regular expressions & standard data structures. JavaScript engines were originally used only in web browsers, but they are now embedded in some servers, usually via Node.js*"

[12] ***https://en.wikipedia.org/wiki/Node.js*** *"Node.js is an open-source, cross-platform, back-end, JavaScript runtime environment that executes JavaScript code outside a web browser. Node.js lets developers use JavaScript to write command line tools and for server-side scripting—running scripts server-side to produce dynamic web page content before the page is sent to the user's web browser. Consequently, Node.js represents a "JavaScript everywhere" paradigm*"

[13] ***https://en.wikipedia.org/wiki/SHA-2*** *"SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001. They are built using the Merkle–Damgård structure, from a one-way compression function itself built using the Davies–Meyer structure from a specialized block cipher. SHA-2 includes significant changes from its predecessor, SHA-1.* ***SHA-256*** *is a novel hash function computed with a 32-bit word*"

[14] The eZ80 development platform as described in ***http://baremetal.engineer/baremetal.software.engineer.pdf*** (Image#14 on Page 10)

[15] ***https://en.wikipedia.org/wiki/Internet_of_things*** *"The Internet of Things ("IoT") describes the network of physical objects - "things" - that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. The definition of the Internet of Things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of Things*"

So, I have now discovered sufficient information to enable me to continue "baremetal" developing, implementing & testing embedded IoT Blockchain functionality on my eZ80 Development Platform[16]

I have already implemented & tested assembler code within a Forth environment to perform ***SHA-256 hash*** functions, and over time I will implement a Merkle Tree and other Blockchain functionality...

Summary

Watch this space !!

 Created: 22/11/2020 Updated: 26/11/2020

[16] The eZ80 development platform as described in ***http://baremetal.engineer/baremetal.software.engineer.pdf*** (Image#14 on Page 10)