An attempt to give the most abstract possible definition of a blockchain.

1 BlockChain

Given a set S, let $\textsc{List}(S)$ and $\textsc{Set}(S)$ be the sets of all finite lists and all finite sets of elements of S, respectively. Given $L \in \textsc{List}(S)$, we use notation $|L|$ to refer to the number of elements in L, and notation $L[i]$ to refer to the i-th element in L, where $i \in \{1, \ldots, |L|\}$. From now on, assume that Σ is a finite alphabet, and that $\mathbf{B} \subseteq \Sigma^*$ is the set of all possible blocks.

Definition 1. *A validation rule is a function* $V : \textsc{List}(\mathbf{B}) \to \textsc{Set}(\mathbf{B})$

Intuitively V is a function taking a list L of block as input, and returning the set of blocks that could be added to L to produce a valid blockchain.

Definition 2. *Let* $G \in \textsc{List}(\mathbf{B})$ *be non-empty, and* V *be a validation rule. Then a function* $f : \{1, \ldots, n\} \to \mathbf{B}$ *with* $n \in \mathbb{N}$ *is a validated chain with respect to* (G, V) *if:*

1. $|G| \leq n$ *and* $f(i) = G[i]$*, for every* $i \in \{1, \ldots, n\}$.
2. $f(1) \in V([\,])$ *and* $f(i+1) \in V([f(1), \ldots, f(i)])$*, for every* $i \in \{1, \ldots, i-1\}$.

Function f in this definition is a valid chain according to the validation rule V and the lists G of genesis blocks (whose role is to provide the blocks to startup the system). Let $\textsc{Log}(G, V)$ be the set of validated chains with respect to (G, V).

Definition 3. *Let* $G \in \textsc{List}(\mathbf{B})$ *be non-empty, and* V *be a validation rule. Then* $\textsc{Log}(G, V)$ *is safe if for every* $f \in \textsc{Log}(G, V)$ *such that* $f : \{1, \ldots, n\} \to \mathbf{B}$*, and every* $b_1, b_2 \in \mathbf{B}$ *such that* $b_1 \neq b_2$*:*

$$V([f(1), \ldots, f(n), b_1]) \cap V([f(1), \ldots, f(n), b_2]) \quad = \quad \emptyset$$

Intuitively, in order to be secured V should depend on the last block b that is included in the blockchain.

Notation. *For all* $f : \{1, \ldots, n\} \to \mathbf{B}$ *with* $n \in \mathbb{N} \in LOG_{G,V}$ *we denote*

$$f^L = [f(1), \ldots, f(n)]$$

Definition 4. *Let* P *be a set of players and* K_T *a function :*

$$K_T : P \times [\![0; T]\!] \times \mathbb{N} \to \textsc{Set}(\mathbf{B} \times [0; 1])$$

Then (P, K_T) *is a valid knowledge representation if :*

$$\begin{gathered}
\forall p \in P, \forall t \in [\![0; T]\!], (b, \alpha) \in K_T(t, 0, p) \implies \alpha = 1 \vee \alpha = 0 \\
\forall p \in P, \forall t, t' \in [\![0; T]\!], t' \geq t, \forall b \in \mathbf{B}, (b, 1) \in K_T(t, 0, p) \implies (b, 1) \in K(t', 0, p) \\
\forall p \in P, \forall t \in [\![0; T]\!], \forall \delta \in \mathbb{N}, \forall b \in \mathbf{B}, (b, 1) \in K_T(t, 0, p) \implies (b, 1) \in K(t, \delta, p) \\
\forall p \in P, \forall t \in [\![0; T]\!], \forall \delta, \delta' \in \mathbb{N}, \delta' \geq \delta \implies \forall (b, \alpha) \in K_T(p, t, \delta), \exists (b, \alpha') \in K_T(p, t, \delta'), \alpha' \geq \alpha
\end{gathered}$$

Notation. $\forall p \in P, \forall t \in [\![0; T]\!]$ *we denote*

$$K_T(p, t) = \{b | (b, 1) \in K_T(p, t, 0)\}$$

Definition 5. *Let* $T, T' \in \mathbb{N}$ *such that* $T > T'$ *we say that* $K'_{T'}$ *extend* K_T *if*

$$\forall p, K_T(p, T) = K'_{T'}(p, T)$$

Definition 6. *A block chain protocol is a function noted $P_{G,V}$:*

$$P_{G,V} : \textsc{Set}(LOG_{G,V}) \times [\![0,T]\!] \to \textsc{Set}(LOG_{G,V})$$

such that :

$$\forall S, \forall t \in [\![0,T]\!], P_{G,V}(S,t) \subseteq S$$

Remark. *$P_{G,V}$ can be seen as the rule in case of fork and new block.*

Definition 7. *Considering $LOG_{G,V}$ the set of validated chains with respect to (G,V), (P,K_T) a valid knowledge representation and $P_{G,V}$ a block chain protocol. We denote $S_{t,p}$ where $t \in [\![0,T]\!]$ and $p \in P$ the set:*

$$S_{t,p} = \{f | f \in LOG_{G,V} \wedge \forall i \in \{1,\ldots,|f^L|\}, f(i) \in K_T(p,t)\}$$

We call a BlockChain at time $t \in [\![0,T]\!]$ for user $p \in P$ noted $BC_{t,p}$ a tuple:

$$BC_{t,p} \in P_{G,V}(S_{t,p},t)$$

Remark. *Intuitively the blockchain for a user p at a time t is one of the best chain he fully knows regarding the protocol function and the validity at time t (time-stamping).*

Definition 8. *Considering $LOG_{G,V}$ the set of validated chains with respect to (G,V), (P,K_T) a valid knowledge representation. We denote α^* the function*

$$\mathbb{N} \times LOG_{G,V} \times P \to [0,1]$$

such that :

$$\alpha^*(\delta, f, p) = max\{\alpha | \exists b \in \mathbf{B}; (b,\alpha) \in K_T(p,T,\delta) \cap V(f^L)\}$$

We said that $LOG_{G,V}$ is alive regarding (P,K_T) if:

$$\exists p, \exists f, \forall \in K_T(p,T) \wedge V(log_{G,V}(N)^-) \cap K_T(p,T) = \emptyset \wedge lim_{\delta\to\infty}\alpha^*(\delta, log_{G,V}, N, p) = 1$$

2 Draft

Definition 9. *We call an alive set of validated chain a tuple $(LOG_{G,V}, P, K_P)$ where $LOG_{G,V}$ is an set of infinite validated chain and P, K_P an alive set of player.*

Proposition. *Let $(LOG_{G,V}, P, K_P)$ an alive set of validated chain then:*

$$\forall log_{G,V} \in LOG_{G,V}, \forall i \in \mathbb{N}, \exists p \in P, \exists t \in T, V(log_{G,V}(i)^-) \cap K_P(p,t) \neq \emptyset$$

Remark. *To be honest i am not sure as we are dealing with infinite number. I may have to trick things here. I want to ensure the fact that the chain will eventually move forward.*