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 $i \in \{1, \dots, |L|\}$. 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* $f : \{1, \dots, n\} \to \mathbf{B}$ *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* $i \in \{1, \dots, n\}$.
2. $f(1) \in V([\,])$ *and* $f(i+1) \in V([f(1), \dots, f(i)])$, *for every* $i \in \{1, \dots, i-1\}$.

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* $f : \{1, \dots, n\} \to \mathbf{B}$, *and every* $b_1, b_2 \in \mathbf{B}$ *such that* $b_1 \neq b_2$:

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

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

Definition 4. *We call player's knowledge a tuple* (P, K_T) *where* P *is a set of player and* K_T *a function:*

$$K_T : P \times [0; T] \times \mathbb{R}^+ \to \mathscr{P}(\Sigma^* \times]0; 1])$$

such that:

$$\begin{aligned}
&\forall p \in P, \forall t \in [0; T], (b, \alpha) \in K_T(t, 0, p) \implies \alpha = 1 \\
&\forall p \in P, \forall t, t' \in [0; T], t' \geq t \implies K_T(t', 0, p) \subseteq K(t, 0, p) \\
&\forall p \in P, \forall t \in [0; T], \forall \delta \in \mathbb{R}^+, K_T(t, 0, p) \subseteq K_T(t, \delta, p) \\
&\forall p \in P, \forall t \in [0; T], \forall \delta, \delta' \in \mathbb{R}^+, \delta' \geq \delta \implies \forall (b, \alpha) \in K_T(p, t, \delta), \exists (b, \alpha') \in K_T(p, t, \delta'), \alpha' \geq \alpha
\end{aligned}$$

Notation. $\forall p \in P, \forall t \in [0; T]$ *we denote* $\{b | (b, 1) \in K_T(p, t, 0)\} : K_T(p, t)$

Definition 5. *Let* $T, T' \in \mathbb{R}^+$ *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* $P_{G,V}$:

$$P_{G,V} : (LOG_{G,V} \times \mathbb{N}) \times (LOG_{G,V} \times \mathbb{N}) \times T \to (LOG_{G,V} \times \mathbb{N})$$

such that :

$$\forall log_{G,V}, log'_{G,V} \in LOG_{G,V}, \forall n, n' \in \mathbb{N}, \forall t \in T; P_{G,V}(log_{G,V}, n, log'_{G,V}, n', t) = (log_{G,V}, n) \vee (log_{G,V}, n')$$

Remark. *$P_{G,V}$ can be seen as the rule in case of fork and new block. Have to be improve to impose that there is no cycle (an order ?)*

Definition 7. *Considering an validated chain $LOG_{G,V}$, a player's knowledge (P, K_T) and a block chain protocol $P_{G,V}$. We denote $S_{t,p}$ where $t \in [0,T]$ and $p \in P$ the set of tuple :*

$$S_{t,p} = \{log_{G,V}(N)^- | log_{G,V} \in LOG_{G,V} \wedge log_{G,V}(N)^- \subseteq K_T(p,t)\}$$

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

$$\begin{aligned}
&BC_{t,p} \in S_{t,p} \\
&\forall log \in S_{t,p}, P_{G,V}((log, |log|), (BC_{t,p}, |BC_{t,p}|), t) = (BC_{t,p}, |BC_{t,p}|)
\end{aligned}$$

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

Definition 8. *We denote α^* the function*

$$\mathbb{R}^+ \times LOG_{G,V} \times N \times P \rightarrow [0,1]$$

such that :

$$\alpha^*(\delta, log_{G,V}, N, p) = max\{\alpha | \exists b; (b, \alpha) \in K_T(p, T, \delta) \cap V(log_{G,V}(N)^-)\}$$

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

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

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.*